Vincenzo Morabito

Business Innovation Through Blockchain

The B^3 Perspective

Springer

Business Innovation Through Blockchain

Vincenzo Morabito

Business Innovation Through Blockchain

The B^3 Perspective

Springer

Vincenzo Morabito
Department of Management
and Technology
Bocconi University
Milan
Italy

ISBN 978-3-319-48477-8 ISBN 978-3-319-48478-5 (eBook)
DOI 10.1007/978-3-319-48478-5

Library of Congress Control Number: 2016961332

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

The word "blockchain" is one of the most hyped IT buzzwords to have emerged in the last couple of years. Blockchain has found its way into major media headlines on a near-daily basis, but a year and a half ago, it was a word used by a relatively small number of people to describe the peer-to-peer distributed ledger technology that underpins bitcoin. What is so special about blockchain, and is it deserving of all the hype?

I was happy to discover that Bocconi University Prof. Vincenzo Morabito, whom I recently had the good pleasure to meet, was writing this book about blockchain technology and its impact on business. Dr. Morabito's aim in this book is to take readers thorough the current state of the art on blockchain technology, as well as its future economic and practical implications. Readers who are new to the topic of blockchain will be surprised by the extensive and very diverse range of applications it enables, while those who are more familiar with the subject will gain from Dr. Morabito's perspective and insights.

The challenge of innovation in an increasingly digitized business world requires a clear understanding about the role of information technologies like blockchain and how they can be fastened to shape new business models. Addressing the impact of blockchain is likely to require significant change on the part of both organizations and individuals, and significant change is something that many (if not most) of us often find hard to do.

The function and impact of complex technologies such as blockchain can often be difficult to grasp, and I hope Prof. Morabito's book will positively effect blockchain literacy among not just business people but also policymakers, who will play a key role in shaping blockchain's future.

Dr. Garrick Hileman
Cambridge Centre for Alternative Finance
University of Cambridge Judge Business School
Cambridge, UK

Preface

In this book, we aim to discuss and present the main challenges and trends related to blockchain for digital business innovation to a composite audience of practitioners and scholars. Blockchain became a hype topic, thanks to bitcoin diffusion at a global level. However, this cryptocurrency is often considered the main application of blockchain, and today, we are assisting to the implementation of blockchain also in other domains; property transfer and digital identity are among the most common examples. Industries that will be soon involved in this phenomenon are telco, data storage, registration services, insurance, and so on. Furthermore, notwithstanding the interest that surrounds blockchain as a key trend, especially with regard to the financial technology (*fintech*) industry, the phenomenon has been not yet fully investigated from a strategic and organizational perspective by both academic and practitioners. Actually, apart from the volume by Tapscott and Tapscott [1], most of the published monographic contributions concern technical, computational, and engineering facets of blockchain.

Taking these issues into account, this volume aims to provide a unified survey of current academic and practitioners' work on blockchain and related phenomena such as bitcoin, considering different perspectives, from information systems as well as technology management and innovation research to computer science and engineering, among others. Consequently, the main goal of this book is to connect research and industry practices suitable to be used by practitioners in their day-to-day activities as well as an update on what academia may offer with regard to the industry proposals. Yet, this book follows the same mission of the former volumes published by the author, thus aiming to identify the challenges, ideas, and trends that may represent "food for thoughts" to practitioners. Accordingly, as in previous books, each topic considered will be analyzed in its technical and managerial aspects, also through the use of case studies and examples.

Finally, please note that in this book, two topics are being used across all chapters: bitcoin and the distributed autonomous organization (DAO). The reasons behind using these two concepts at different points in this book are twofold: First, bitcoin and DAO have been the cornerstone for the advent of blockchain, and therefore, these will naturally emerge when we look at the blockchain from the different viewpoints adopted in each chapter. Second, the chapters of this book are meant to be part of a coherent whole, but also are meant to be read individually

without the need to read all other chapters, so the readers can select those chapters and themes that are more relevant to their personal interests. Therefore, it is needed to introduce and repeat some concepts of bitcoin and DAO to contextualize them within the chapter's theme.

Outline of this Book

This book argument is developed along three main axes. We consider first (*Part I*) *Blockchain Technology and Management* issues that are the structure and characteristics of the blockchain *paradigm change* (Chap. 1), its *value system* (Chap. 2), *governance* (Chap. 3), and *security layers*, by focusing on the challenges, advantages, and limitations of blockchain from a security point of view, likewise (Chap. 4). Subsequently, *Part II* (*Bitcoin Phenomenon and Trends*) will focus on *digital currencies* (Chap. 5), *smart contracts*, and *licensing* (Chap. 6), particularly discussing how organizations can leverage the smart contract technology and the blockchain for the purpose of overseeing agreements and licensing. An analysis of how blockchain can fit into the world of *enterprise systems* (ES) conclude this part of this book, by comparing the value system of existing enterprise systems to that of the blockchain technology (Chap. 7). Finally (*Part III*), this book will present and review cases of *business innovation* related to blockchain at a global level in a section called *Blockchain practices* (Chap. 8) and will end by presenting the B^3 *perspective* we propose for blockchain business innovation (Chap. 9).

As in my previous volumes [2–5], this book adopts both a scientific approach and a concrete stance to introduce blockchain characteristics, challenges, and opportunity from the viewpoints of managers, thus adopting a clear and easy-to-understand language.

Milan, Italy Vincenzo Morabito

References

1. Tapscott D, Tapscott A (2016) Blockchain revolution: how the technology behind bitcoin is changing money. Business, and the World. Portfolio
2. Morabito V (2013) Business technology organization—Managing digital information technology for value creation—The SIGMA approach. Springer, Berlin/Heidelberg
3. Morabito V (2014) Trends and challenges in digital business innovation. doi:10.1007/978-3-319-04307-4
4. Morabito V (2015) Big data and analytics. Springer International Publishing, Heidelberg, New York, Dordrecht, London
5. Morabito V (2016) The future of digital business innovation. doi:10.1007/978-3-319-26874-3

Acknowledgements

This book is the result of the last two years of research, where several people are worth to be acknowledged for their support, useful comments, and cooperation. A special mention is to Prof. Vincenzo Perrone at Bocconi University, Prof. Vallabh Sambamurthy, Eli Broad Professor at Michigan State University, and Prof. Franco Fontana at LUISS University as main inspiration and mentors.

Moreover, I acknowledge Prof. Giuseppe Soda, Head of the Department of Management and Technology at Bocconi University, and all the other colleagues at the department, in particular Prof. Arnaldo Camuffo, Prof. Anna Grandori, Prof. Severino Salvemini, and Prof. Giuseppe Airoldi, all formerly at the Institute of Organization and Information Systems at Bocconi University, who have created a rich and rigorous research environment where I am proud to work.

I acknowledge also some colleagues from other universities with whom I have had the pleasure to work, whose conversations, comments, and presentations provided precious insights for this book: among others, Anindya Ghose, Professor of Information, Operations, and Management Sciences at New York Stern School of Business, Vijay Gurbaxani, Professor of Business and Computer Science at the University of California, Irvine, Saby Mitra, Associate Director of Risk for the Institute for Information Security and Privacy at the Georgia Institute of Technology, Ravi Bapna, Board of Overseers Professor in the Information and Decision Sciences at the University of Minnesota's Carlson School of Management, Stephanie Woerner, Research Scientist at the MIT Center for Information Systems Research, Sam Ransbotham, Associate Professor of Information Systems at Boston College, Tobias Kretschmer, Head of the Institute for Strategy, Technology and Organization of Ludwig Maximilians University, Jan Mendling, Professor at the Institute for Information Business at Wirtschaftsuniversität Wien, Christopher L. Tucci, Dean of the College of Management and Professor of Management of Technology at the Ecole Polytechnique Fédérale de Lausanne, Garrick Hileman, Economic Historian at the University of Cambridge and London School of Economics, Marinos Themistocleous, Associate Professor of Digital Systems at the University of Piraeus, Federico Pigni and Vincent Mangematin from Grenoble Ecole de Management, Antonio de Amescua and Román López-Cortijo, Professors of Computer Science at the Universidad Carlos III de Madrid, Paolo Aversa, Strategy Lecturer at the Cass Business School, Stefano Zanero, Associate Professor

of Computer Engineering at Politecnico di Milano, Angela Sasse from the University College London, and Ferdinando Ametrano, "bitcoin and blockchain technologies" Lecturer at Politecnico di Milano and Bicocca University.

Furthermore, I want to gratefully acknowledge all the companies that have participated in the research interviews, case studies, and surveys.

In particular, for the financial institutions: Agos Ducato, Banca Carige, Banca Euromobiliare, Banca Fideuram, Banca d'Italia, Banca Mediolanum, Banca Passadore, Banco Popolare, Banca Popolare dell'Emilia Romagna, Banca Popolare di Milano, Banca Popolare di Sondrio, Banca Popolare di Vicenza, Banca Popolare di Bari, Banca Sistema, Barclays, BCC Roma, BNL-BNP Paribas, Borsa Italiana, Cariparma Credit Agricole, CACEIS Bank Luxemburg, Carta Si, Cassa Depositi e Prestiti, Cassa di Risparmio di Firenze, Cedacri, Che Banca!, Compass, Corner Bank, Credito Emiliano, Deutsche Bank, Dexia, FCA Bank, HypoVereinsbank, Istituto Centrale delle Banche Popolari Italiane, ING Direct, Intesa SanPaolo, Intesa SanPaolo Servitia, Istituto per le Opere Religiose, Luxemburg Stock Exchange, JP Morgan Chase, Key Client, Mediobanca, Monte Titoli, Banca Monte dei Paschi, Profamily, Poste Italiane, SEC Servizi, Société Européene de Banque, Standard Chartered, Royal Bank of Scotland, UBI Banca, Unicredit, Unicredit Leasing, Veneto Banca, Widiba, WeBank, Aldermore Bank, UBS, and Raiffeisen Bank.

For the insurance sector: Allianz, Assimoco, Aspe Re, Aviva, Cardif, Coface, Cattolica Assicurazioni, Ergo Previdenza, Europe Assistance, Eurovita Assicurazioni, Assicurazioni Generali, Groupama, Munich RE, Poste Vita, Reale Mutua, Novae, Sara Assicurazioni, UnipolSai, Uniqa Assicurazioni, Vittoria Assicurazioni, and Zurich.

For the industrial sector: A2A, ABB, Accenture, Acea, Aci, Aci Informatica, Acqua Minerale S. Benedetto, Adidas, Alitalia, Alpitour, Alliance Boots, Amadori, Amazon, Amplifon, Anas, Angelini, ArcelorMittal, Armani, Astaldi, ATAC, ATM, AstraZeneca, Arval, Auchan, Audi, Augusta Westland, Autogrill, Autostrade per l'Italia, Avio, Baglioni Hotels, Bayer Pharmaceuticals, BMW, BASF, Barilla, BasicNet, Be Consulting, Benetton, Between, Bottega Veneta, Business Integration Partners, Brembo, Bravo Fly, Brunello Cucinelli, BskyB, BSH, BOSH, Boeing Defence, Calzedonia, Cementir, Centrica Energy, Cerved, Chiesi Farmaceutici, CNH Industrial, Coca Cola HBC, Coop Italia, Costa Crociere, Comau, D'Amico, Dainese, Danone, Daimler, De Agostini, Diesel, Dimar, Dolce & Gabbana, General Electric, Ducati, Elettronica, Elica, Edipower, Edison, Engie, Eni, Enel, ENRC, ERG, Fastweb, FCA, Fendi, Ferservizi, Ferrero, Ferrari, Ferretti, Ferrovie dello Stato, Fincantieri, GlaxoSmithKline, GE Capital, GFT, Gruppo API, Technologies, Grandi Navi Veloci, G4S, Glencore, Gruppo Hera, Gruppo Coin, Gruppo De Agostini, Gucci, H3G, Hupac, IGT, Infineon, Interoll, Il Sole24Ore, IREN, Istituto Europeo Oncologico, Istituto Poligrafico e Zecca dello Stato, ITV, ItalGas, Kuwait Petroleum, La Perla, Labelux Group, Lamborghini, Lavazza, Linde, LBBW, Leonardo-Finmeccanica Levi's, L'Oreal, Loro Piana, Lottomatica, Luxottica, Jaguar Land Rover, Lucite International, MAN, Magneti Marelli, Mail Boxes Etc, Mapei, Marcegaglia, Mediaset, Menarini, Messaggerie Libri, Metaenergia, Miroglio, Mondelez International, Mossi & Ghisolfi, Natuzzi, NH Hotel, Novartis,

Oerlikon Graziano, Olivetti, OSRAM, Piaggio, Perfetti, Pernod Ricard, Philips, Pirelli, Porsche, Postel, ProSiebenSat1, Premier Oil, Procter&Gamble, Prysmian, RAI, Rexam, Rolex, Roche, Retonkil Initial, RWE, Saipem, Sandoz, Sanofi Aventis, Sisal, SEA, Seat PG, Selex, Sigma-Tau, Snam, Sorgenia, Sky Italia, Schindler Electroca, Suzuki, Pinko, Pfizer, RFI, TIM, Tenaris, Terna, Tods, Trenitalia, Tyco, Trussardi, TuevSued, Telefonica, Uber, Unilever, Unicoop Firenze, Valentino, Virgin Atlantic, Volkswagen, Vodafone, and Whirlpooland Wind.

For the ICT sector: Almaviva, Engineering, Ericsson, and Cabel Holding.

For the public sector: Agenzia per l'Italia Digitale, Comune di Milano, Regione Lombardia, and Consip.

I would especially like to acknowledge all the people that have supported me during these years with insights and suggestions. I learned so much from them, and their ideas and competences have inspired my work: Silvio Fraternali, Paolo Cederle, Massimo Milanta, Massimo Schiattarella, Diego Donisi, Marco Sesana, Gianluca Pancaccini, Mario Di Mauro, Giovanni Damiani, Gianluigi Castelli, Salvatore Poloni, Milo Gusmeroli, Pierangelo Rigamoti, Danilo Augugliaro, Ranieri De Marchis, Francesco Giordano, Gianluigi Castelli, Nazzareno Gregori, Edoardo Romeo, Elvio Sonnino, Pierangelo Mortara, Massimo Messina, Mario Collari, Giuseppe Capponcelli, Massimo Castagnini, Pier Luigi Curcuruto, Giovanni Sordello, Maurizio Montagnese, Massimo Tessitore, Alberto Sferch, Enrico Bagnasco, Carlo Brezigia, Massimo Malagoli, Riccardo Sfondrini, Fabio Ugoste, Giuseppe Virano, Domenico Fileppo, Giovanni Mori, Roberto Di Fonzo, Umberto Angelucci, Giuseppe Dallona, Davide Tesoro Tess, Gilberto Ceresa, Rene Keller, Jesus Marin Rodriguez, Fabio Momola, Rafael Lopez Rueda, Eike Wahl, Marco Cecchella, Maria-Louise Arscott, Antonella Ambriola, Andrea Rigoni, Giovanni Rando Mazzarino, Paolo Martella, Alfredo Altavilla, Silvio Sperzani, Samuele Sorato, Alessandro Preda, Andrea Cardamone, Alberto Ripepi, Alfredo Montalbano, Cristina Porzio, Gloria Gazzano, Massimo Basso Ricci, Giuseppe De Iaco, Isabella Fumagalli, Riccardo Amidei, Davide Ferina, Massimo Ferriani, Roberto Burlo, Cristina Bianchini, Dario Scagliotti, Ettore Corsi, Luciano Bartoli, Marco Ternelli, Stewart Alexander, Luca Ghirardi, Francesca Gandini, Francesco Del Pizzo, Vincenzo Tortis, Agostino Ragosa, Sandro Tucci, Vittorio Mondo, Giangaddo Prati, Andrea Agosti, Roberto Fonso, Federico Gentili, Nino Lo Banco, Fabio Troiani, Federico Niero, Sebastiano Marulli, Gianluca Zanutto, Mario Bocca, Marco Zaccanti, Anna Pia Sassano, Fabrizio Lugli, Alessandro Garofalo, Marco Bertazzoni, Vittorio Boero, Carlo Achermann, David Cis, Stefano Achermann, Jean-Claude Krieger, Mario Martinelli, Reinhold Grassl, François de Brabant, Maria Cristina Spagnoli, Pietro Amorusi, Alessandra Testa, Mario, Martinelli, Anna Miseferi, Matteo Attrovio, Giorgio Mosca, Roberto Saracino, Nikos Angelopoulos, Igor Bailo, Stefano Levi, Luciano Romeo, Alfio Puglisi, Gennaro Della Valle, Massimo Paltrinieri, Luca Vanetti, Pierantonio Azzalini, Carlo Garuccio, Enzo Contento, Marco Fedi, Fiore Della Rosa, Dario Tizzanini, Francesca Durì, Gabriele Scarponi, Carlo Capalbo, Bruce Hodges, Simone Battiferri, Pietro Maranzana, Vittorio Giusti, Piera Fasoli, Carlo di Lello, Gian Enrico Paglia, George Sifnios, Francesco Varchetta, Gianfranco Casati, Fabio Benasso, Angela Gemma, Olaf

Foschi, Alessandro Marin, Gianluca Guidotti, Fabrizio Virtuani, Luca Verducci, Marco Valioni, Luca Falco, Francesco Pedrielli, Riccardo Riccobene, Roberto Scolastici, Paola Formenti, Andrea Mazzucato, Stefano Malvicini, Nicoletta Rocca, Emanuele Balisteri, Mario Breuer, Fabio Caressa, Simonetta Consiglio, Luca Gasparini, Mario Costantini, Matteo Colombo, Marco Lanza, Marco Poggi, Gianfranco Ardissono, Alex Eugenio Sala, Daniele Bianchi, Giambattista Piacentini, Daniele Savarè, Fabio Cesaretti, Marcello Ronco, Tommaso Pellizzari, Filipe Teixeira, Andrea Giovanni Mugnai, Roberto Riccardi, Graziano Tosi, Barbara Monfredini, Luigi Zanardi, Valerio Momoni, Daniele Panigati, Christian Ciceri, Maurizio Pescarini, Ermes Franchini, Francesco Mastrandrea, Vincenzo Cervino, Federico Boni, Vincenzo Pensa, Roberto D'Attili, Ernesto Ciorra, Fabio Veronese Mauro Minenna, Giampiero Astuti, Massimo Romagnoli, Vasco Tomaselli, Nicola Grassi, Alessandro Capitani, Mauro Frassetto, Bruno Cocchi, Marco Tempra, Martin Brannigan, Alessandro Guidotti, Monica Colleoni, Gianni Leone, Stefano Signani, Domenico Casalino, Fabrizio Lugoboni, Giorgio Piotti, Roberto Ghislanzoni, Giuliano Capizzi, Fabrizio Rocchio, Mauro Bernareggi, Claudio Sorano, Marcus Heidmann, Paolo Crovetti, Antonio Perrotti, Alberto Ricchiari, Alessandro Musumeci, Luana Barba, Pierluigi Berlucchi, Matthias Schlapp, Ugo Salvi, Giovanni Paolo Bruno, Elisabetta Torri, Daniela Manuello, Danilo Gismondi, Elisabetta Nobile, Patrick Vandenberghe, Daniele BalboClaudio Colombatto, Frediano Lorenzin, Alfredo Folla, Giuseppe Rudi, Paolo Trincianti, Massimiliano Ciferri, Danilo Ughetto, Tiberio Strati, Massimo Nichetti, Fabio Maini, Stefano Firenze, Remo Nadali, Vahe Ter Nikogosyan, Giorgio Voltolini, Franco Caraffi, Andrea Maraventano, Martin Giersich, Michela Scovazzo, Massimo Bertolotti, Guido Oppizzi, Alessandro Bruni, Marco Franzi, Stefano Gentili, Guido Albertini, Massimiliano De Gregorio, Chiara Pellistri, Vincenzo Russi, Franco Collautti, Massimo Dall'Ora, Fabio De Ferrari, Giuseppe Alibrandi, Marco Moretti, Mauro Ferrari, Domenico Solano, Pier Paolo Tamma, Susanna Nardi, Massimo Amato, Alberto Grigoletto, Nunzio Calì, Arturo Baldo, Fabio De Santis, Gianfilippo Pandolfini, Guido Rindi, Cristiano Cannarsa, Fabio Degli Esposti, Riccardo Scattaretico, Claudio Basso, Mauro Pianezzola, Piergiorgio Grossi, Marco Zanussi, Alberto Fenzi, Davide Carteri, Giulio Tonin, Simonetta Iarlori, Marco Prampolini, Luca Terzaghi, Christian Altomare, Paolo Gasparato, Pasquale Tedesco, Fabio Boschiero, Franco Colzani, Elisabetta Castro, Maria Dentamaro, Roberta Crispino, Carlo Castiglioni, Nicoletta Carlomagno, Francesco Modesti, Isabel Castillo, Aldo Borrione, Paolo Beatini, Maurizio Pellicano, Ottavio Rigodanza, Gianni Fasciotti, Lorenzo Pizzuti, Angelo D'Alessandro, Marcello Guerrini, Stefano Torcello, Francesco Germini, Michela Quitadamo, Massimo Severin, Salvatore Rocco, Chiara Galli, Dario Castello, Giorgio Degli Abbati, Giuseppe Bramante, Marco Casati, Stefano Boscolo, Fabio Boschiero, Silvia Zanni, Pierluigi De Marinis, Fabio Cestola, Roberto Mondonico, Alberto Alberini, Pierluca Ferrari, Umberto Stefani, Elvira Fabrizio, Salvatore Impallomeni, Dario Pagani, Eric Peyer, Jean-Luc Martino, Marino Vignati, Giuseppe Rossini, Paolo Calvi, Francesco Genovese, Alfio Puglisi, Renzo Di Antonio, Maurizio Galli, Filippo Vadda, Roberto Casula, Marco De Paoli, Paolo Cesa, Armando Gervasi, Riccardo Delleani, Luigi Di Tria, Marco

Gallibariggio, David Alfieri, Graziano Cavallo, Mirco Carriglio, Pier Francesco Gavagni, Maurizio Castelletti, Gaetano Scebba, Roberto Andreoli, Barbara Monfrini, Vincenzo Campana, Marco Ravasi, Antonella Cirina, Fabio Grassi, Mauro Viacava, Giacomo Carelli, Flavio Glorio, Alessio Pomasan, Salvatore Stefanelli, Roberto Scaramuzza, Marco Zaffaroni, Giuseppe Langer, Francesco Bardelli, Davide Barbavara, Daniele Rizzo, Silvia De Fina, Gabriele Raineri, Paulo Morais, Massimiliano Gerli, Andrea Facchini, Massimo Zara, Luca Paleari, Alessandra Ardrizzoia, Andrea Dupplicato, Alberto Maldino, Carlo Bozzoli, Luigi Borrelli, Marco Iacomussi, Enrico Senatore, Marco Tendas, Mario Dio, Giulio Mattietti, Alessandro Poerio, Fabrizio Frustaci, Roberto Zaccaro, Maurizio Quattrociocchi, Gianluca Giovannetti, Francesco Frau, Massimo Alberti, Pierangelo Colacicco, Paolo Lissoni, Alessandro Seghezzi, Silvio Sassatelli, Filippo Passerini, Mario Rech, Claudio Sordi, Tomas Blazquez De La Cruz, Luca Spagnoli, Fabio Oggioni, Dante Buccelloni, Luca Severini, Roberto Conte, Federica Dall'Ora, Alessandro Tintori, Giovanni Ferretti, Alberta Gammicchia, Patrizia Tedesco, Antonio Rainò, Claudio Beveroni, Chiara Manzini, Simone Macelloni, Francesco Del Greco, Luca Sacchi, Alessandro Sala, Miriam Imperato, Lorenzo Tanganelli, Ivano Bosisio, Alessandro Campanini, Pietro Donati, Matteo Ortenzi, Giovanni Pietrobelli, Pietro Pacini, Vittorio Padovani, Luciano Dalla Riva, Grazia Campanile, Jarvis Macchi, Gabriele Lunati, Lucinda Spera, Paolo Pecchiari, Francesco Donatelli, Massimo Palmieri, Rossana Barzizza, Giovanni Rossi, Matteo Bonfanti, Alessandro Cucchi, Riccardo Pagnanelli, Raffaella Mastrofilippo, Roberto Coretti, Alessandra Grendele, Ruggero Platolino, Stefano Smareglia, Roberto Corradini, Luca Del Din, Marianna Pepe, Massimo Rigobon, Antonina Tornabene, Matteo Dell'Orto, Sonia Aidani, Gabriele De Villa, Myrtille Clement Fromentel, Matteo Nube, Daniele Galleani, Andrea Arrigoni, Davide Casagrande, Lucia Gerini, Filippo Cecchi, Silvia Spadaccini, Massimilano Spadini, Gianlorenzo Magnani, Antonio Chiappara, Roberto Privitera, Fabio De Maron, Alberto Peralta, Stefano Sala, Massimo Pernigotti, Massimo Rama, Francisco Souto, Oscar Grignolio, Gianni Rumi, Mario Mella, Massimo Rosso, Mauro Restelli, Filippo Onorato, Stefan Caballo, Ennio Bernardi, Gianluigi Zarantonello, Matteo Formenti, Aldo Croci, Giuseppe Genovesi, Gianrico Sirocchi, Maurizio Romanese, Daniele Pagani, Derek Barwise, Luca Ingrao, Guido Vetere, Christophe Pierron, Pietro Giardina, Guenter Lutgen, Lorenzo Marietti, Domenico Porto, Alessandro Di Fonzo, Carlo Romagnoli, Claudio Luongo, Riccardo Angeli, Giovanni Bagnoli, Andreas Weinberger, Luca Martis, Stefano Levi, Paola Benatti, Massimiliano Baga, Matteo Baido, Marco Campi, Laura Wegher, Sebastiano Cannella, Diego Pogliani, GianpieroPepino, Rosy Bellan, Simona Tonella, José González Osma, Sandeep Sen, Thomas Steinich, Barbara Karuth-Zelle, Ralf Schneider, Rüdiger Schmidt, Wolfgang Gärtner, Alfred Spill, Cristina Boschesi, Lissimahos Hatzidimoulas, Marco Damiano Bosco, Mauro Di Pietro Paolo, Paolo Brusegan, Arnold Aschbauer, Robert Wittgen, Peter Kempf, Michael Gorriz, Wilfried Reimann, Abel Archundia Pineda, Jürgen Sturm, Stefan Gaus, Andreas Pfisterer, Peter Rampling, Elke Knobloch, Andrea Weierich, Andreas Luber, Heinz Laber, Michael Hesse, Markus Lohmann, Andreas König, Herby Marchetti, Rainer Janssen, Frank Rüdiger Poppe, Marcell Assan, Klaus

Straub, Robert Blackburn, Wiebe Van der Horst, Martin Stahljans, Mattias Ulbrich, Matthias Schlapp, Jan Brecht, Enzo Contento, Michael Pretz, Gerd Friedrich, Florian Forst, Robert Leindl, Wolfgang Keichel, Stephan Fingerling, Sven Lorenz, Martin Hofmann, Nicolas Burdkhardt, Armin Pfoh, Kian Mossanen, Anthony Roberts, John Knowles, Lisa Gibbard, John Hiskett, Richard Wainwright, David Madigan, Adam Ewell, James Freeborough, Matt Hopkins, Gill Lungley, Simon Jobson, Glyn Hughes, John Herd, Mark Smith, Jeremy Vincent, Guy Lammert, Steve Blackledge, Mark Lichfield, Jacky Lamb, Simon McNamara, Kevin Hanley, Anthony Meadows, Rod Hefford, Stephen Miller, Giovanni Leone, David Edwards, Dean Eaves, Paul Johnson, Martin Beaver, Diana Medeiros-Placido, Parker Humbert, Rob Lankey, Chris Michael, Willem Eelman, Alessandro Ventura, David Bulman, Neil Brown, Alistair Hadfield, Rod Carr, and Neil Dyke.

I would especially like to gratefully acknowledge Gianluigi Viscusi at the College of Management of Technology (CDM)-École polytechnique fédérale de Lausanne (EPFL) and Alan Serrano-Rico at Brunel University who provided me valuable suggestions and precious support in the coordination of the production process of this book.

Furthermore, I acknowledge the support of Business Technology Foundation (Fondazione Business Technology) and all the bright researchers at Business Technology Outlook (BTO) Research Program who have supported me in carrying out interviews, surveys, and data analysis: Florenzo Marra, Giovanni Roberto, Massimo Bellini, Fabrizio Conte, Fabrizio Manzo, Luca Parravicini, Lorena Marturana, Valeria Lorenzi, Martino Scanziani, Alessia Bonanno, Miguel Miranda, Piercarlo D'Ambrosio, Francesco Papa, Andrada Comanac, Marco Castelli, Andrea Zinzi, Giacomo Giorgianni, Felice Pescatore, Gianluca Del Mastro, Francesca Oberti, Alessio Campi, Giuseppe Vaccaro, Antonio De Falco, Antonio Attinà, Matteo Pistoletti, Tommaso Cenci, Marco Favia, Daniele Durante, and Cesare Mauri e Lorenzo Capodicasa.

A special acknowledgement goes to the memory of Prof. Antonino Intrieri who provided precious comments and suggestions throughout the years.

Finally, I acknowledge my family whose constant support and patience made this book happen.

Vincenzo Morabito

Contents

Acronyms

API	Application Programming Interface
CEO	Chief Executive Officer
CIO	Chief Information Officer
CMO	Chief Marketing Officer
COO	Chief Operating Officer
CRM	Customer Relationship Management
CTO	Chief Technology Officer
DAO	Decentralized Autonomous Organizations
DLT	Distributed ledger technology
DNS	Domain Name System
ERP	Enterprise Resource Planning
EU	European Union
HTTP	Hyper Text Transfer Protocol
ICTs	Information and Communication Technologies
ID	Identification; Identity
IO	Input/Output device
IP	Internet Protocol address
IS	Information Systems
IT	Information technology
KSI	Keyless Signature Infrastructure
KYC	Know Your Customer
KYCC	Know Your Customer's Customer
LOC	Letter of Credit
MBA	Master of Business Administration
PLM	Product Life Cycle Management
PoS	Proof of stake
PoW	Proof of work
RFID	Radio-frequency identification
ROI	Return on investment
SCM	Supply Chain Management
SHA	Secure Hash Algorithm
SME	Small to medium-sized enterprise
SRM	Supplier Relationship Management

SSH	Secure Shell
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCP	Transmission Control Protocol
UK	United Kingdom
URL	Uniform Resource Locator
US	The United States
USD	United States dollar(s)

Part I
Blockchain Technology and Management

The Blockchain Paradigm Change Structure

1

Abstract

Technological advancements and innovation is constantly evolving and growing at such a fast rate that everyone is required to stay abreast of these advancements and innovations. The paradigm change of Blockchain is not left out from this evolution. The technological concept behind the Blockchain is interestingly closely identical to that of a database. However, it is clearly one of the key concepts that needs to be understood for the future. There are five key concepts that not only need to be understood but also explored in a manner that examines how they interrelate one to another: smart contracts, decentralized consensus, the Blockchain, trusted computing and proof of work/state. This exciting computing paradigm is critically important because it will be instrumental to the creation of decentralized applications. This chapter will explore 4 main key concepts of Blockchain Technology—Blockchain, Decentralized databases application consensus, Proof of work/stake and Smart contracts—while appreciating the Blockchain paradigm change structure.

1.1 Introduction

Following the over two decades of scientific examinations in order to seek principles, techniques advances and theories, there have been immense acceleration in the areas of decentralized (peer-to-peer) computer networking as well as communication security (cryptography). As a result of this, a new technology referred to as 'Blockchain' emerged.

It is to no surprise that Blockchain technology being a buzzword of the day has attracted the attention of entrepreneurs, Governments, banks and plenty more. They all seem to be allocating portions of investments and resources to quickly gain a more vivid understanding of the Blockchain paradigm while attempting to jump

V. Morabito, *Business Innovation Through Blockchain*,
DOI 10.1007/978-3-319-48478-5_1

ahead of what seems to be a key technology of the future. Blockchain can be easily be seen as next level from distributed computing architectural constructs, to a universally global database of interfaces and data which will integrate loads of machines also plugin various sources of data.

Blockchain refers to a distributed, encrypted database, which is a public depository of information that cannot be reversed and is incorruptible [1]. In other words, a Blockchain can be defined as a distributed public ledger or database of records of every transaction that has been carried out and shared among those participating in the network [2]. Every transaction or digital event in the public ledger has to be authenticated via the agreement of more than half of those participating in the network [2]. This implies that no participant or user as an individual can modify any data within a Blockchain without the consent of other users (participants). It could be observed clearly, that the technological concept behind the Blockchain is interestingly closely identical to that of a database.

The Blockchain makes it possible for first time participants to reach an agreement on how a specific transaction or digital event can occur without requiring any controlling authority. This technology (Blockchain technology) is unique in the sense that it reduces the function of the middleman. This allows a distinctive piece of data to be transferred to participants in a secure and safe manner.

Moreover, the Blockchain technology can produce 'smart contracts'. These smart contracts are defined as digital currencies that are independent of any governmental institution as they are termed 'self-enforcing digital contracts'. They do not require any form of regulation or human involvement.

It is to no surprise that Blockchain technology being a buzzword of the day has attracted the attention of entrepreneurs, governments, banks and many more people across the globe see the advent of the Blockchain technology to 'the Internet'. Also, they foresee the shift of power balance from centralized bodies in the communications and business sectors [1].

The technology of Blockchain is not contentious as it has in a long time functioned impeccably and is being applied to financial and non-financial sectors applications successfully [2]. This exciting computing paradigm is critically important because it will be instrumental to the creation of decentralized applications.

1.2 The Blockchain Phenomena

In the past couple of years, a key technological innovation referred to as the 'Blockchain' appeared to be a possible disturbing technological innovation. The fundamental of this technology is built around the theory of 'distributed ledger' in which the ledger is stored and maintained on a distributed computer network [3].

Moreover, the ledger brings about the possibility of the network as a whole to cooperatively produce, develop and record past transactions as well as consecutive digital events. In recent times, cryptocurrency has been the foremost application of

Blockchain technology. This cryptocurrency is referred to as Bitcoin. Given the popularity and importance of Bitcoin, it will be used throughout this book highlighting different aspects of this digital asset.

Bitcoin used a ledger referred to as 'Blockchain', which was where the name (Blockchain technology) was derived from [3]. However, Bitcoin is the first of the numerous possible lists of Blockchain technological applications.

Furthermore, when numerous users are required to be dependent on the same data historically, Blockchain technology then comes to play.

Blockchain technology is a data store that is characterized by the following:

- It subsists within a decentralized peer-to-peer network
- Specific users can write it
- It employs the use of digital signatures and communication security(cryptography) to authenticate, verify user identity and implement access rights in a read or write format
- Its scheme brings about a huge difficulty in altering historical records
- Its scheme brings about a great level of ease in the awareness of users in cases of any attempt to alter historical records
- Financial transactions are typically a part of the constituent of Blockchain technology
- Specific users as well as an extensive audience can read it
- In virtually real-time, it is reproduced throughout a couple of systems on the network.

Figures 1.1 and 1.2 show the centralized database and the decentralized database. In the centralized database, there is the need for intermediaries (third parties) whereas in the decentralized database, the need for intermediaries (third parties) has been eliminated [4].

The four key concepts of Blockchain Technology—*Blockchain*, *Decentralized Databases*, *Proof of Work/Stake* and *Smart Contracts* will be looked into.

1.2.1 Blockchain

The Blockchain was brought to life as a result of Bitcoin and this Blockchain is otherwise called Bitcoin Blockchain. Before we discuss the Bitcoin Blockchain, it will be ideal to have an overview of Bitcoin.

Bitcoin is one of the most widely used digital currency that was launched in 2009 and has not looked back ever since. It is an innovative technology that deals with payment systems. It is an example of virtual currency, which is built on a log of transaction and is circulated across participating users within the network. It makes use of the 'Distributed Ledger' scheme.

Furthermore, the reason behind the design of Bitcoin was for it to perform three main purposes of traditional money. These three main purposes are:

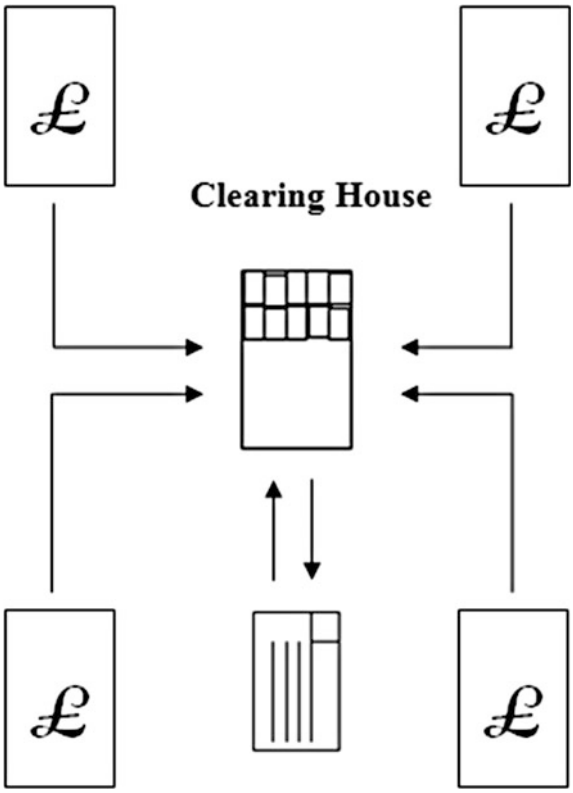


Fig. 1.1 Centralized Database. Adapted from Lewis et al. [4]

- To simplify exchange commercially
- To store value by users for future purpose
- To act as the basic unit for measuring the values of market goods and services rendered [5].

Before the invention of Bitcoin and its Blockchain, digital currencies were perceived not to be practicable as a result of the comparative effortlessness in the manner digital currencies could be replicated. This was referred to as '*double-spend*' problem in which every transaction bears a risk [3]. This risk involves the sending of a copy of the digital transaction to the merchant by the holder whereas the holder keeps the original copy of the digital transaction. This risk was conventionally guarded against by deploying a trusted centralized intermediary to keep up to date with every transaction carried out.

However, with Bitcoin Blockchain in which the history of transactions and authentication of such transactions by participants within the network system, the obligation of keeping up to date with every transaction has been transferred to the entire network system. A well-structured and detailed diagram explaining the Blockchain value system can be seen in Chap. 2. It can be seen that there are nodes

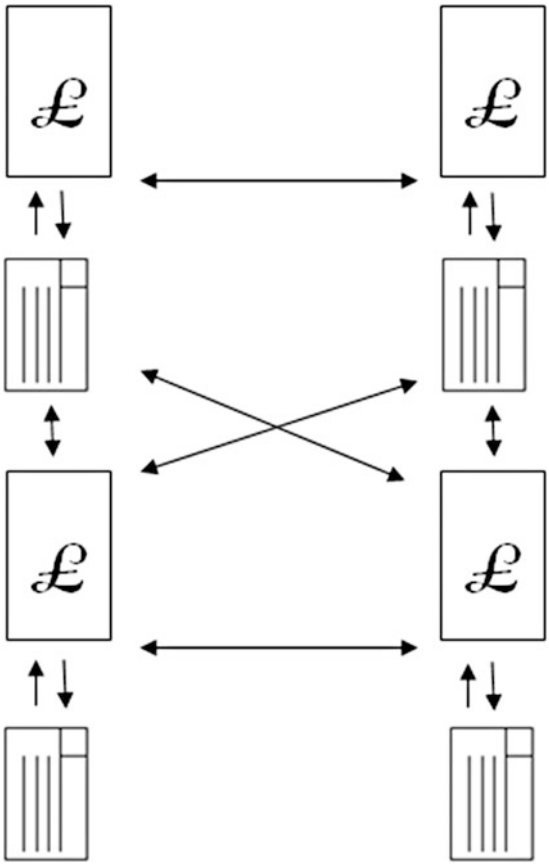


Fig. 1.2 Decentralized Database. Adapted from Lewis et al. [4]

(users of the network) and these nodes hold a Blockchain made up of all the historical transactions carried out on the network. The system of the Bitcoin Blockchain is really a multifaceted system as it has the following aims.

- The ability of anyone to write to the Blockchain and
- Centralized control should be eliminated
- The system of Bitcoin Blockchain performs in a way similar to a network or system of computer-generated databases with each consisting of historical transactions of Bitcoin.

The approach of Bitcoin to various decisions can be grouped into seven different categories. These are; data storage, data distribution, mechanism of agreement, mechanism upgrade, criteria for participation, defense mechanism and incentivization scheme. Table 1.1 highlights the categories, questions and approaches of Bitcoin [6]. It is of utmost importance that people would want to ask some

Table 1.1 The categories, questions and approaches of Bitcoin

Category	Question	Approach of Bitcoin
Data storage	How should data be stored?	Data should be stored via the blockchain technology
Data distribution	How should the distribution of new data be?	The distribution of new data should be in a peer-to-peer format
Mechanism of agreement	How should conflicts be resolved?	Conflicts should be resolved via the longest chain rule
Mechanism upgrade	How do the rules change?	The rules change via; BIPs (for writing the rules) Vote by hashing power (for the implementation of the rules)
Criteria for participation	Who can submit transactions?	Transaction submission is anonymous and open
Criteria for participation	Who can read data?	Data reading is anonymous and open
Criteria for participation	Who can authenticate transactions?	Transaction authentication is anonymous and open
Defense Mechanism	How is bad behaviour prevented?	Bad behaviour is prevent through the use of proof-of-work
Incentivisation scheme	How are block-makers incentivised?	Block-makers are incentivised through block reward and is to be replaced by transaction fees
Incentivisation scheme	How are transaction validators incentivised?	How transaction validators are incentivised is not considered

Adapted from Lewis [6]

questions with regards to the outlined categories. However, the approach of Bitcoin with regards to each category provides suitable answers to some of these questions as shown in Table 1.1.

1.2.2 Public Blockchains and Private Blockchains

A highpoint of public Blockchains is the high capability of this innovation to uphold transactional agreement in the network, which gives room for blocks of transactions to be written to the Blockchains (*distributed ledgers*) by anyone, the creation of transactions and the ability to send such transactions. Moreover, all these do not require the approval of any third party or intermediary (middleman).

On the other hand, the limitations of users in the private Blockchains involve the use of firewalls within the private network. The systemized pattern of the private Blockchains can be done in such a way that only known participants (users) can include data to the Blockchain. Moreover, the private Blockchains do not give neither read nor write access to unknown participants (Table 1.2).

Table 1.2 The differences between Public Blockchains and Private Blockchains

Public Blockchains	Private Blockchains
Participants are not necessarily known	Participants are known and trusted
Participants are not necessarily trusted	Participants are trusted
Anyone without permission granted by another authority can read data	Only permitted participants can read data
Anyone without permission granted by another authority can write data	Only permitted participants can write data

Adapted from Lewis [6]

Examples of public Blockchains and private Blockchains include; *Ripple* (which could be placed between both public Blockchains and private Blockchains) [4] and *Ethereum* (which employs the use of public Blockchains) [4]. We will now take a look at *Decentralized Database*, which is another key concept of Blockchain technology.

1.2.3 Decentralized Database

Blockchains have been having an immense influence on the manner in which communication as well as data sharing online is concerned. This impact is as a result of the fact that Blockchains employ the use of decentralized database.

Moreover, with the advent of decentralized database, the necessity of routing communications or sharing of files (photos and videos) via a centralized network or electronic platforms such as Google Drive, Yahoo, Gmail and so on has been less essential. With the use of a decentralized and encrypted communication protocols, messages can be transferred, stored and retrieved at anytime without any form of intervention from the government [7].

Decentralized Database also allows both decentralized and secure manner of data exchange. If required, information can be published and distributed across a huge number of computers in an encrypted manner thereby eliminating the ability of a single entity to censor [1]. An example of the Decentralized Database is the *Anonymous Decentralized Cloud Storage System*, which employ the use of Blockchain technology in collaboration with other peer-to-peer technology to make it possible for people to use surplus space on hard disks [1]. This looks like the centralized cloud computing platforms to users, but form the technological view, the mode of operation of such platforms is not similar [1].

As a result of the advent of Blockchain technology, organizations are now looking for a way to use the features of Decentralized Database, which Blockchain technology offers to make it possible for unrelated people to vote over the internet or using their mobile devices securely [1]. This is due to the ability of Decentralized Database to function as distributed irreversible and encrypted public paper, which can be effortlessly audited as every voter would be able to validate that their votes

were counted [1]. By reason of the encryption of any voting system that is based on Blockchain technology, such voting system is not vulnerable to hacking.

Decentralized Database systems are perceived to be a technical replacement for the Domain Name System (DNS) that support the whole Internet [1].

1.2.4 Proof of Work

A decentralized ledger is the fundamental structure of the database used for digital currencies transactions including Bitcoin transactions as it serves as storage for all historical transactions [8]. It is of utmost importance to note that the operation of digital currency schemes should include a means of security against attacks on the Blockchain. If an attacker decides to spend a particular amount of money and then tries to reverse that particular transaction, the attacker could broadcast his own version of the Blockchain in which that particular transaction is not included, then the participants would not have any form of awareness as to the valid version of the ledger prior to the attack.

The Bitcoin network security is dependent on a network security protocol called '*proof of work*' *(PoW)*. In 1993, Cynthia Dwork and Moni Naor initially proposed this network security protocol (proof of work). This network security protocol is a piece of data that is expensive to create in order to meet particular prerequisites and its verification is inconsequential. This implies that in order to perform a specific role, this protocol inserts an extra cost. This concept will be revised in Chap. 4, when we look at the security aspects of blockchain.

Putting Bitcoin into consideration, it should be noted that within a specific period of time, every transaction carried out is recorded and stored into the Bitcoin block. The block is then broadcasted to all the participating nodes within the Bitcoin network [9]. The *Hashcash* proof of work scheme is used in this case. This Hashcash proof of work scheme was introduced in 1997 by Adam Back (see [9]). Under this Hashcash proof of work scheme, each participant adds a piece of data referred to as 'nonce' to the block to form a 'block + nonce'. This 'block + nonce' is then taken and placed in an algorithm referred to as 'hash algorithm'.

This hash algorithm consists of a hash that matches up to some particular prerequisites. The hash algorithm then comes up with a complex mathematical computation in which each participating node tries to provide a solution to using the SHA (Secure Hash Algorithm)-256 hash function. As soon as a solution is provided to the mathematical computation by a node, the particular prerequisites by the proof of work scheme is then thought to be met and this now becomes 'block + nonce + hash'. As soon as this occurs, the 'block + nonce + hash' is then included with the Bitcoin Blockchain and broadcasted to every of the participating nodes within the network.

Furthermore, the Bitcoin protocol (proof of work protocol) operates in a manner that physically scarce resources assist the network. These physically scarce resources are:

- the hardware required to run the mathematical computations and
- the electric power required to run the hardware [8].

This implies that the use of Bitcoin protocol (proof of work protocol) is highly demanding on resources. As a result of this, many similar systems not based on costly computations have been built for which 'proof of stake' is one.

Proof of work protocol as used in emails have as well been recommended as a form of measure for visiting websites, guarding against denial-of-service attacks, rate limiting TCP connections and the provision of motivation to peer-to-peer systems [10].

1.2.5 Proof of Stake

Proof of stake (PoS) scheme serves as an alternative to the proof of work scheme. Proof of stake is a scheme built on less-costly computations. This implies that the proof of stake scheme is not based on costly computations as compared to the proof of wok scheme. Rather than depending on the scarce resources (costly computations), the proof of stake scheme is dependent on the entities that hold stake within the network (this implies a proof of stake holding). In other words, we can say that the resource that the network security is dependent on is the ownership of the coin itself, which implies *proof-of-ownership* that is also scarce. For the authentication and reception of a transaction to occur (whether fees of transaction or new coins), some of the coin must be owned by a miner [9]. The probability that a miner is successful in the creation of a new block is dependent on the amount of coin owned by the miner and not dependent on the computational power whenever the proof of stake scheme is used [9]. Therefore, the energy cost in this transaction is every minute. In order to dent the reliability of the system, one would have ownership of over 50% of the coin presently being staked, which would be very costly [9].

Proof of stake scheme has more advantages over the proof of work scheme. One advantage PoS has over PoW is the low latency ability of PoS, however, it is not free from challenges. Also, it has proven not to be efficient in guarding against the risks encountered by cryptocurrencies.

One of the challenges encountered by the proof of stake scheme is the issue of centralization as the stakeholders with large stake holdings could attempt to display a level of domination over the network.

A hybrid of both proof of work and proof of stake schemes was later created. We will now discuss the Hybrid proof of work and proof of stake scheme.

1.2.6 Hybrid Proof of Work and Proof of Stake

The hybrid proof of work and proof of stake scheme was first recommended and applied by Scott Nadal and Sunny King in their whitepaper "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake". The hybrid proof of work and proof of

Table 1.3 The major characteristics of the proof of work, proof of stake and hybrid proof of work and proof of stake schemes

Scheme	Low latency	Long-run low energy cost
Proof of Work (PoW)	No	No
Proof of Stake (PoS)	Yes	Yes
Hybrid Proof of Work and Proof of Stake (PoW/PoS)	Yes	Yes

Adapted from Farell [9]

stake scheme employs the use of the proof of work scheme for the mining and distribution at the initial stage and this implies that it makes it possible for the distribution of new coins to miners via the network [9]. The proof of stake scheme provides the cryptocurrency with good energy effectiveness.

Furthermore, the generation of block in this hybrid scheme is dependent on a model referred to as 'coinage', which is the multiplication of the total amount of coin a miner owns and the span of ownership the present coin owner has. Hence, the block generation goes to the block with the highest coinage [9]. The low consumption of energy by this scheme is one of the standout features of this scheme.

Table 1.3 highlights the major characteristics of the proof of work, proof of stake and Hybrid proof of work and proof of stake schemes. It can be seen from Table 1.3 that the proof of work scheme has high latency the energy cost on the long-run for proof of work is high while the proof of stake scheme as well as the hybrid proof of work and proof of stake scheme have low latency and their energy cost based on the long-run is low.

1.3 Benefits of Blockchain Technology

There are immense benefits the Blockchain technology provides. Some of these benefits include; *Trust*, *Openness*, *Independence*, *Speed*, *Robustness*, *Global Nature* and *Effectiveness*.

Before any data is added to an explicitly defined Blockchain, it is expected that a greater number of users of the system reach an agreement. This pattern is quite distinct from the centralized pattern in which there is a central authority. A more trustworthy system is created when majority of the users have a say over the writing, creation and alteration of such data [4]. This high level of trust has been the case of the innovation brought about by Blockchain technology.

Also, through the use of smart contracts that reconciles in real-time, the level of openness has drastically improved with the advent of Blockchain technology. Also, since trade data is published to a common platform, trades can be viewed by participants in real-time [4]. This helps to forestall any form of manipulations or alterations.

The design of Blockchain technology was done in such a manner that this technology is not dependent on any financial institution such as banks or government. This makes it more attractive and less prone to regulations. Furthermore, the technology of Blockchain has enhanced the level of speed of transactions. Since Blockchains can automate messages by the addition of code snippets called 'smart contracts' that does not involve the involvement of any human in any way, the speed of payment is enhanced. This implies that there will be a lower transaction completion time as third parties have been eliminated. The robustness of the Blockchain technology makes it possible for data to be stored across a large number of nodes [4]. The higher the number of nodes, the more resilient the data [4].

Also, the ability for Blockchain technology to serve both locally and globally makes it more attractive. Moreover, the technology of Blockchain has enhanced the level of effectiveness that exists when reconciliation is brought to play in the financial sector. Taking banks for example, banks usually delegate a system to serve as the trade data for a specific security and this will result into deficiencies in reconciliation. Since Blockchain technology exists, reconciliation is carried out in real-time.

1.4 Future of Blockchain

Blockchain technology has a great future if well harnessed and implemented on various platforms. Blockchain technology could govern the future of finance as it will result into huge reduction of cost for all participants in the market thereby changing global banking [11].

Just of recent, the governor of the Bank of Japan (Haruhiko Kuroda) highlighted that with the development of Blockchain technology, there could be an evolution in the manner in which financial services are designed [12]. He pointed out that artificial intelligence and Blockchain technology could bring about an immense impact on financial services and he also highlighted that ledgers (the basic information infrastructure) have significantly supported the development of financial services [12]. Furthermore, in May 2016, the deputy governor of Bank of Japan (Hiroshi Nakato) stated that a close monitoring of the development of Blockchain technology and digital currencies should be done by the central banks [12]. Actually, Blockchain technology can be applied in areas which include; trade finance, the capital market, payments and a host of other areas [13]. We will now discuss these three key areas that Blockchain technology can be applied to.

1.4.1 Trade Finance

This area is one of the key areas that Blockchain technology can be applied. It has great potential. If some banks make a decision to position the financial supply chain by putting the letters of credit on the Blockchain, this will be immense as these

letters have highly complicated and sophisticated flow of information, even if a Blockchain solution is used mainly by a small number of participants [13].

Recently, HSBC and Bank of America Merrill Lynch venture and financial technology firm R3 separately reported that they have been able to generate ways by which Blockchain technology can be used to simplify trade finance processes [14]. Furthermore, the two banks highlighted that they had partnered with the Infocomm Development Authority of Singapore to emulate a transaction of Letter of Credit (LOC). These letters of credit are one of the predominantly used means for risk reduction between importers and exporters [14]. Thus, Blockchain technology is important for use in the area of trade finance as it offers solutions which include the ability to trace as Blockchain provides genuineness of products in the supply chain and the ability to be transparent as Blockchain guards against fraud and saves transaction reconciliation cost [14].

The two key areas of trade finance that Blockchain technology could be of immense benefits include; the transfer of the information of trade and financing [15]. We will now highlight these two key areas.

1.4.2 Financing

When Blockchain technology is used in data exchange during trade, it serves to provide irreversible and simple matching of data. Also, it serves to increase the effectiveness and speed of reconciliation (as this is done in real-time) and helps to increase the level of security of transactions between parties involved in buying and selling and their banks.

It is to be noted that a consensus should be reached with regards to the financing terms and the issues of compliance and this should not be done within the distributed ledger. However, the use of common distributed ledgers can serve to activate necessary actions within financing agreement [15].

With the ability to make the events along a supply chain visible in real-time and the ability of non-bank participants such as the shipping companies to keep ledgers up-to-date as soon as transactions are completed, the release of funds can be carried out faster, thus helping banks to save time as well as resource as the banks do away with the manual processing and data matching that is in existence today. This also helps the banks to divert the time and resources saved to other profitable propositions that are key to local and global trade [15].

1.4.3 The Capital Market

As earlier highlighted, some of the benefits the Blockchain technology include: Trust, Openness, Independence, Speed, Robustness, Global Nature and Effectiveness among other benefits. These benefits of Blockchain technology can as well

have an immense impact on the future of the capital market. The capital market has four key areas and these areas are; pre-trade, trade, post-trade and custody and securities servicing [16]. In the area of Pre-Trade in the capital market, the benefits of Blockchain technology are in the authentication of holdings as well as the openness of such holdings, static data mutualisation, reduction in the exposure of credit, easier means to Know Your Customer (KYC) and easier means to Know Your Customer's Customer (KYCC) via look through to holdings [16]. Moreover, higher level of openness in the supervision of market authorities, automatic reporting, secure and real-time matching of transactions, the ability for settlements to be immediately irreversible and improved standard of anti-money laundering are some of the benefits of Blockchain technology in the area of Trade in the capital market [16]. Also, the reduction in the requirements for collateral, higher effectiveness of post-trade processing, the auto-execution of Smart Contracts and the elimination of a central clearing for real-time cash transactions are some of the benefits of Blockchain technology in the area of Post-Trade in the capital market [16].

Direct Primary issuance onto a Blockchain, the ability to have richer datasets, automation of de-duplication of servicing processes and the ability to possess common reference data are some of the benefits of Blockchain technology in the area of Custody and Securities Servicing in the capital market [16].

In order to shape the future of the capital market with regards to the benefits that Blockchain technology provides, the industry is required to take a collective view of and embrace these benefits while also preserving the strengths of the existing ecosystem [16].

1.5 Smart Contracts

Smart Contracts will be thoroughly analyzed in detail in Chap. 6—Smart Contracts and Licensing. In this section, we will take a look at the general overview of Smart Contracts.

Blockchains can automate messages by the addition of code snippets. These code snippets are referred to as 'smart contracts'. These smart contracts employ the use of the 'if-this-then-that' logic. The execution of smart contracts does not involve the use of any human in any way. This signifies that Smart contracts are decentralized and they tend to operate without any middleman or third party regulation. Furthermore, they employ the use of a distributed database so that participants can verify that there is an occurrence of a digital event without requiring any middleman or third party. Moreover, smart contracts are not written in legal languages but are written as computer programs and these computer programs have the ability to define strict rules [17].

In addition, smart contracts can be coded in order to reflect a business logic driven by data. This business logic driven by data could include:

- prioritizing a repayment structured note
- loan collateralization and
- voting for a post in a forum [17].

Figure 1.3 shows the flowchart for the application of business logic with smart contracts. Figure 1.3 is further explained by the use of Table 1.4, which highlights the flowchart number, flowchart event and the respective description of the

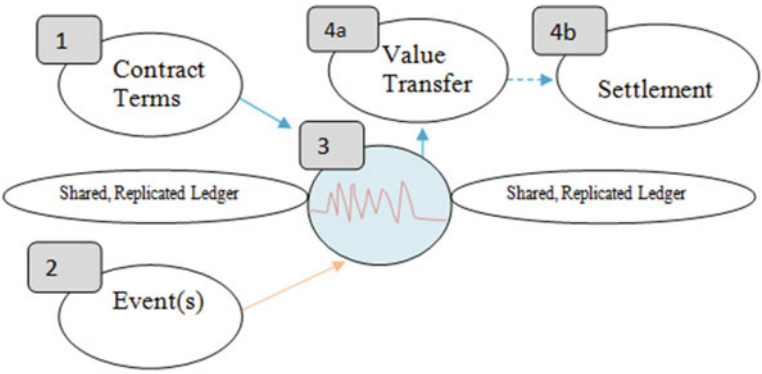


Fig. 1.3 Flowchart for the application of business logic with smart contracts. Adapted from Skinner [14]

Table 1.4 The flowchart number, flowchart event and the respective description of the flowchart

Flowchart number	Flowchart event	Description of flowchart
1	Contract terms	Counterparties establish obligations and settlement instructions Assets put under custody of smart contract Conditions for execution ("If… then…")
2	Event(s)	Event triggers contract execution Event can refer to transaction initiated or information received
3	Business logic	Business logic (Terms of contract) dictate movement of value based on conditions met
4a	Value transferred	Value transferred to intended recipient as dictated by contract terms For digital assets on the chain (Bitcoin) accounts are settled automatically
4b	Settlement	For assets represented off the chain (e.g. securities)accounts off-chain match settlement instructions Changes to accounts will be reflected on ledger

Adapted from Skinner [14]

flowchart. In flowchart number 1 which has a flowchart event called *Contract* Terms, counterparties establish obligations and settle instructions, the assets are put under the custody of the Smart Contract and the conditions for execution are stated. In flowchart number 2, which has a flowchart event, called *Event(s)*, the events can refer to transactions initiated or information received and contract executions are triggered.

In flowchart number 3, which has a flowchart event, called *Business Logic*, the movement of value is dictated by the terms of contract. In flowchart number 4a which has a flowchart event called *Value Transferred*, the value is transferred to the intended recipient as dictated by the contract terms while in flowchart number 4b which has a flowchart event called *Settlement*, the assets represented off the chain (e.g. securities) accounts off-chain match settlement instructions.

The areas of relevance of smart contracts to the financial sector are; in the areas of loans, the capital market, booking of trade and wallet control of cryptocurrency among others. In addition, the growth of smart contracts has been so speedy and up till now, the creation of smart contracts has mainly been to routinely carry out swaps and derivatives. A couple of open source projects, which include Counterparty [18] and Ethereum [19] have advanced technologically to produce programming languages that give rise to the production of state-of-the-art smart contracts.

Point of Attention However, there are some issues related to smart contracts. Some of these issues include; *Flexibility* (as smart contracts believe everything that pertains to negotiations at the commencement of negotiations can be decided by participants and this is sometimes inaccurate), *Liability* (as a result of the lack of intermediaries, regulators could be faced with some level of difficulties) and *Enforcement* (it will be quite difficult if not impossible at present to structure all transactional terms by total reliance on smart contracts) [17].

One of the first market which is expected that smart contracts will be functional is syndicated loans as this market, which is worth about $4 trillion runs on faxes, emails and excel spreadsheets [20]. Smart property requires controlling the ownership of a property (physical property for example a laptop, a house and so on) and non-physical properties such as a company's shares [2].

1.6 Case Studies

In this Section, we shall focus on a digital asset exchange company called *Coinbase* and *Blockstream*, which is a company that develops Bitcoin applications and other applications.

Coinbase was founded by Brian Armstrong and Fred Ehrsam on June 20, 2012 [21]. It has its headquarters in San Francisco, California. The company is known to provide a platform for the creation of a digital currency wallet where digital currency can be securely stored [21]. In addition to web browsers, the wallet operates on Android and Iphone. Coinbase guarantees secure means of storage, protection of insurance, maintenance of absolute private keys control among others.

In March 2016, Coinbase was listed by Richtopia (a company based in UK) as the second most influential Blockchain organizations [22]. It offers API for the building of applications as well as payment acceptance in digital currencies by merchants and developers.

Some of the key functionalities of Coinbase platform are: *Mobile Wallet*, which serves as a platform for sending Bitcoin to friends and shopping with merchants that accept Bitcoin, *Insurance Protection*, in which the Coinbase platform is insured against any form of digital agreement and theft. It is worthy of note that the worth of Bitcoin and Ether this Coinbase platform holds at a particular period of time is less than the insured amount. Another key functionality of the Coinbase platform is *Secure Storage*. Appropriate measures are taken by Coinbase to provide adequate security against any form of theft and this is achieved by the addition of another security layer apart from the username and password.

It is worthy of note that the user value indicator of Coinbase platform is positive with regards to the user interface and user experience and it has a high process impact.

The other case study which is a company called *Blockstream* was founded by Adam Back and Mark Friedenbach in 2014 and is a company that has the development of Bitcoin applications and other applications as its focus [23]. One of the Bitcoin applications is *Sidechain*, which is an open source code as well as developer sidechains for the advancement of Bitcoin. Sidechain is the main innovative area of Blockstream.

In October 2015, the first commercial application of sidechain technology with liquid was announced by Blockstream [24]. This commercial application was to serve as a platform for Bitcoin payment processors, exchanges as well as brokerages [24].

It is worthy of note that the intention for the launching of Blockstream was for new ways of innovations in cryptocurrency, open assets and smart contracts to be developed [25]. Some of the key functionalities of Blockstream are: *Trustless and Permissionless Innovation* in which the Blockstraem platform aims to promote such environment for enabling new innovations and to work towards guaranteeing that developers, asset issuers and users have computing technology that provides both neutral and cryptographical assurance for their financial needs [25] and *Fairness*, *Openness and Accountability* in which its platform aims to power fair and accountable markets that are interoperable.

It is worthy of note that the user value indicator of Blockstream platform is positive with regards to the user interface and user experience and it has a high process impact.

1.7 Summary

In this Chapter, we looked at the introduction into Blockchain technology where we defined Blockchain technology to be a distributed public ledger or database of records of every transaction that has been carried out and shared among those participating in the network [2]. We also looked at Blockchain phenomena, where it was pointed out that there are Centralized and Decentralized Databases and Bitcoin was the first of the numerous possible lists of Blockchain technological applications. Furthermore, we discussed the four main key concepts of Blockchain technology, which are: Blockchain, Decentralized Database, Proof of Work (PoW) and Proof of Stake (PoS), and Smart Contracts.

Blockchain technology involves the distribution and encryption of database in an irreversible and incorruptible manner, then it is of utmost importance to the effectiveness of the financial sector as its benefits such as Trust, Openness, Independence, Speed, Robustness, Global Nature and Effectiveness are key to the development of the capital market, payment systems, trade finance and other areas of the financial and non-financial sectors.

It is paramount to note that this technology is spreading to the non-financial sectors as pointed out by the singer-songwriter and composer Imogen Heap at an event in London in 2015 where he stated that "The biggest problem for an artist right now is payment…[the blockchain] could spark up many new platforms and services that would enrich all our lives" [26]. To a large extent, the future of Blockchain technology is bright if well harnessed.

References

1. Wright A, De Filippi P (March 10, 2015) Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Available at SSRN: https://ssrn.com/abstract=2580664
2. Crosby M, Nachiappan N, Pattanayak P et al (2016) Blockchain technology: beyond bitcoin. Applied Innovation. 2:6–10
3. Frøystad P, Holm J (2016) Blockchain: powering the Internet of Value, EVRY Labs White Report, https://www.evry.com/globalassets/insight/bank2020/bank-2020—blockchain-powering-the-internet-of-value—whitepaper.pdf. Accessed 2nd January 2017
4. Lewis A, Larsen M, Goh C. Y et al (2016) Understanding Blockchain Technology And What It Means for Your Business, Asian Insights Office • DBS Group Research
5. de France B (2013) The dangers linked to the emergence of virtual currencies: the example of bitcoins. FOCUS No. 10–5 December 2013, pp. 1–6
6. Lewis A (2015) A Gentle Introduction To Blockchain Technology. Brave New Coin
7. GitHub I (2016) barisser/bitcrypt. In: GitHub, Inc. https://github.com/barisser/bitcrypt. Accessed 25 Aug 2016
8. BitFury Group (2015) Proof of Stake versus Proof of Work White Paper, Sep 13, 2015 (Version 1.0). http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf. Accessed 2nd January 2017
9. Farell R (2015) "An Analysis of the Cryptocurrency Industry". Wharton Research Scholars. 130. http://repository.upenn.edu/wharton_research_scholars/130.

10. Laurie B, Clayton R "Proof-of-work" proves not to work. In: Proceedings of The Third Workshop on the Economics of Information Security (WEIS), May 13–14, 2004, The University of Minnesota. http://www.cl.cam.ac.uk/~rnc1/proofwork2.pdf. Accessed 2nd January 2017
11. Tomorrow S (2016) Future of Blockchain. In: Collab. Connect. https://www.shapingtomorrow.com/home/alert/665529-Future-of–Blockchain. Accessed 25 Aug 2016
12. CoinDesk (2016) Bank of Japan: Blockchain could alter financial services. In: CoinDesk. http://www.coindesk.com/bank-japan-blockchain-alter-financial-services/. Accessed 25 Aug 2016
13. Finextra Research Ltd (2016) Banking on Blockchain: charting the progress of distributed ledger technology in Financial Services, A Finextra White Paper in association with IBM
14. Skinner C (2016) Applying Blockchain to trade finance. In: Chris Ski. blog. http://thefinanser.com/2016/08/applying-blockchain-trade-finance.html/. Accessed 25 Aug 2016
15. Szmukler D (2016) Applying cryptotechnologies to Trade Finance—Information Paper, Euro Banking Association (EBA) Working Group on Electronic Alternative Payments.Version 1.0, May 2016, pp. 1–23
16. Van de Velde, Jo, Scott A, Sartorius K et al (2016) Blockchain in capital markets—The prize and the journey, Euroclear Group and Oliver Wyman
17. Tuesta D, Alonso J, Cámara N et al (2015) Smart contracts: the ultimate automation of trust? Digital Economy Outlook-October 2015, BBVA Research
18. Counterparty Counterparty. In: Counterparty. http://counterparty.io/. Accessed 25 Aug 2016
19. Ethereum (2016) Ethereum. In: Ethereum found. https://www.ethereum.org/. Accessed 25 Aug 2016
20. Euromoney (2016) Getting to grips with Blockchain. In: Euromoney Institutional Invest. PLC. http://www.euromoney.com/Article/3501936/Getting-to-grips-with-blockchain.html. Accessed 25 Aug 2016
21. Coinbase (2016) Coinbase. In: Coinbase. https://www.coinbase.com. Accessed 16 Sep 2016
22. Richtopia (2016) Top 100 Blockchain organisations: from CoinDesk to BitPay, These are the most influential organisations in the distributed ledger space. http://richtopia.com/top-lists/top-100-blockchain. Accessed 5 Nov 2016
23. Cryptocoinsnews (2015) The first sidechain for Bitcoin exchanges. https://www.cryptocoinsnews.com/blockstream-announces-liquid-the-first-sidechain-for-bitcoin-exchanges/. Accessed 5 Nov 2016
24. News C (2016) Blockstream acquires Bitcoin wallet GreenAddress to advance sidechains project. In: Cryptocoinsnews. https://www.cryptocoinsnews.com/blockstream-acquires-bitcoin-wallet-greenaddress-sidechain/. Accessed 19 Sept 2016
25. Blockstream (2015) About us. In: Blockstream. http://www.blockstream.com/about/. Accessed 19 Sept 2016
26. Yessi Bello Perez (2015) "Grammy winner Imogen heap: Blockchain tech can empower artists," CoinDesk, December 9, 2015. http://www.coindesk.com/grammy-award-nominee-touts-benefits-of-blockchain-tech/. Accessed 18 Nov 2016

Blockchain Value System

2

Abstract

Long before the advent of the blockchain, digital cash had been conceptualized in a setting with a central server trusted to prevent double-spending with the help of public-key cryptography, whereby each agent is assigned a private key (kept secret like a password) and a public key shared with all other agents. In spite of major cryptographic advances, failure to ensure compatibility between centralization, anonymity and double-spending prevention, eventually put the viability of this new form of money into question. Recently, Bitcoin's blockchain model has been proposed as the backbone for a wide range of applications, from asset trading to real estate transactions, from escrow services to even a national income distribution system. A value system is a coherent set of values adopted by an organization, or society as a standard to guide its behavior in preferences in all situations. This chapter discusses blockchain as a value system and expounds the main fundamental principles behind blockchain technology, the way it works, advantages, limitations and challenges of blockchain and finally, some of its cutting-edge applications.

2.1 Introduction

Modern technologies allow people to communicate directly. Voice and video calls, emails, pictures and instant messages travel directly from the sender to the receiver over the internet, while maintaining trust between individuals no matter how far apart they are. However, when it comes to money, people have to trust a third party to be able to complete the transaction, thus, over the past decade; blockchain technology has been slowly invading the internet as a secured alternative digital paradigm. By using math and cryptography, blockchain provides an open decentralized database of any transaction involving value such as money, goods,

V. Morabito, *Business Innovation Through Blockchain*,
DOI 10.1007/978-3-319-48478-5_2

property, work or even votes. In other words, blockchain is a data structure that facilitates the creation, sharing and storing of a digital ledger of transactions among a distributed network of computers, which makes it decentralized and distributed architecture [1, 2]. This allows creating a record whose authenticity can be verified by the entire community, which makes blockchain a "trustless" technology. In this case, "trustless" means that the "value" over a computer network can be verified, monitored and enforced without the need for a trusted third party or central institution. Thus, third party trust organisations such as, e.g., VeriSign may no longer be necessary.

Consequently, the future economy will move towards one of distributed property and trust, where anyone with access to internet can get involved with blockchain based transactions. Blockchain technology can be thought of as wills and contracts that execute themselves. It will become a global decentralized source of trust. Accordingly, the ownership of the system does not belong to a certain company or a person yet everyone can use it and help run it. As a result, as long as one of the computers or "nodes" in the network is safe, the digital ledger is safe [3, 4].

The uses of blockchain technology are endless. Some expect that in less than 10 years, it will be used to collect taxes. Also, since every transaction will be recorded on a public and distributed ledger, it will make it easier for people to transform money to geographical areas where access to financial institutions is limited allowing for financial fraud to be significantly reduced. A huge proportion of trust services that range from banking to notaries will face challenges on price, volume and in some cases, their survival. Public authorities could find it more and more difficult to enforce traditional financial regulations due to the new possibilities offered by blockchain network to bypass traditional financial intermediaries. The organizations that don't adapt with new technological trends will lag and collapse as their success will depend on the strategic choices they make regarding the adoption of new technologies. However, whether the governments and financial and legal institutions will embrace blockchain or not is too soon to judge. It is predictable that not everyone is ready to embrace its features and advantages.

2.2 Fundamental Principles

As described in Chap. 1, Blockchain was developed as the main authentication and verification technology behind the Bitcoin, the first decentralized crypto digital currency. In Bitcoin, a transaction is initiated when the future owner of the coins (or digital tokens) sends his/her public key to the original owner. The coins are transferred by the digital signature of a hash. Public keys are cryptographically generated addresses stored in the blockchain. Every coin is associated with an address, and a transaction in the crypto-economy is simply a trade of coins from one address to another. In blockchain, the data used in the transactions is stored in an immutable public record, or giant spreadsheet, that is secured by concerned members who participate in a peer to peer network and act like verifiers of its

authenticity and credibility [5]. Blockchain technology provides a mechanism to enable "trustless" transactions that don't need intermediary agents to verify or monitor the integrity of the value exchanged through computer networks. Simply put, blockchain allows businesses to transact among each other without central financial institutions such as banks [1].

A blockchain transaction between two parties starts when one of the participants signals a message to the network about the terms and conditions governing the transactions between the two stakeholders. Then, the other participant broadcasts its acceptance to the network, which by default triggers the request for the network participants to authenticate and verify the transaction. Consequently, network members automatically play the role of authenticators that validate and guard the transaction against double spending through a validation system called "proof-of-work", which represents a competition among network members to validate the transaction [1]. At this point, when the transaction is validated, the public ledger (blockchain record) as well as the users of network will be collectively updated with the status of the recently added transaction. This mechanism helps in establishing trust between concerned stakeholders through the use of a decentralized public ledger as well as cryptographic algorithms that can guarantee approved transactions cannot be altered after being validated. The following points summarize the key attributes of blockchain technology:

- ***Decentralization***: It is one of the main characteristics of blockchain where participants are linked together in a market place where they can conduct transactions and transfer ownership of valued assets among them in transparent way and without the help from third party mediators, hence, the name *value network*.
- ***Trust and provenance***: Blockchain technology provides an indisputable mechanism to verify that the data of a transaction has existed at a specific time in the block. Moreover, because each block in the chain contains information about the previous block, then, the history, position and ownership of each block are automatically authenticated, and cannot be altered.
- ***Resilience and irreversibility***: Blockchain resilience stems from its structure since it is designed as distributed network of nodes (computers) in which, each one of these nodes store a copy of the entire chain. Hence, when a transaction is verified and approved by the participating nodes, it is highly impossible to change or alter the transaction's data.

2.3 How Blockchain Works

This section explains how blockchain works. Figure 2.1 illustrates the basic components in the blockchain technology [6].

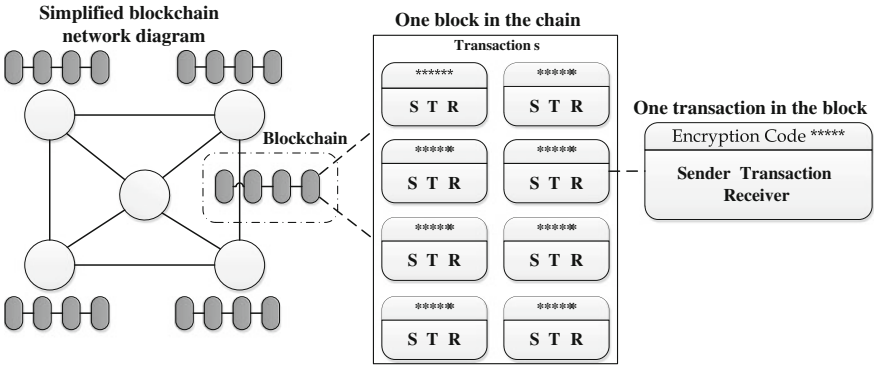


Fig. 2.1 Basic components of blockchain, adapted from [6]

In Fig. 2.1, the transaction is composed of the sender, the transaction information and the receiver, and it is secured by an encryption code. The block contains several transactions and the blockchain is constructed of several blocks. Figure 2.2 illustrates how the transaction is authenticated and how the block is created, chained and validated.

The following points provide descriptions for the steps illustrated in Fig. 2.2, which are:

- ***Transaction definition***: It is the first step where the sender creates a transaction that holds information about the receiver's public address, the value of the transaction and a cryptographic digital signature that verify the transaction's validity and credibility [6].
- ***Transaction authentication***: When the nodes in the network receive the transaction, they first validate the message by decrypting the digital signature and then the message is held temporarily until being used to create the block [6].
- ***Block creation***: One of the nodes in the network uses the pending transactions in order to update the ledger or the block. Then, at a specific time interval the updated block is broadcasted to the other nodes waiting for validation [6].
- ***Block validation***: When the nodes responsible about the validation in the network receive a request to validate an updated block, they go through an iterative process, which requires agreement from the other nodes in order to authenticate the block [6].
- ***Block chaining***: When all the transactions in a block are approved, then, the new block is attached "chained" to the current blockchain, resulting in broadcasting the new state of the block to the rest of the network [6].

These steps can take about 3 to10 s to finish, which gives blockchain a big advantage as a very fast technology for settling financial transactions.

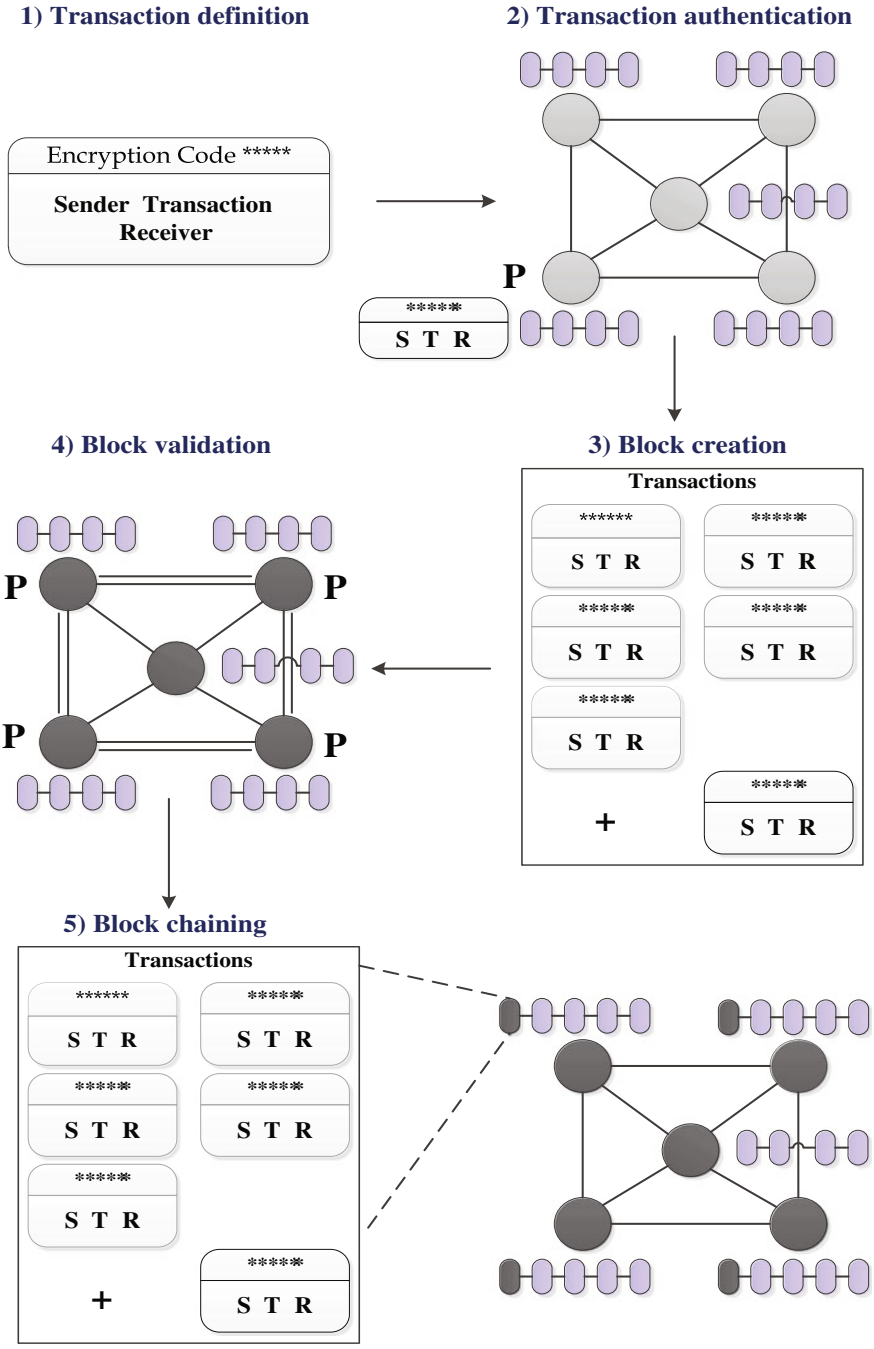


Fig. 2.2 Generalized overview of blockchain transaction, adapted from [6]

2.4 Blockchain's Challenges

Adopting blockchain as a unified method for conducting financial transactions over the Internet, requires a major redesigning task for the network of participating organisations as well as the practiced financial business processes, which is accompanied with many challenges. First, organisations have to come to an agreement that governs the fundamental rules of the new network. However, such arrangement can be a very daunting process, as different organizations and businesses have varying policies and protocols to perform their operations, and determining the best practice could take long and careful negotiations [7]. Additionally, security and privacy issues pose a big concern, since participating organisations need to be satisfied with security levels against attacks as well as regarding the trade information that needs to be known for each financial transaction to be verifiable throughout the network.

In order to overcome the aforementioned challenges, standards would be a good starting point to get the institutions within a certain industry on the same page. Standards promote an equal competitive playing field as well as reduce new technologies' time to market. Thus, the focus of blockchain implementation is more on the standardization of data flows and the intermediate language used to communicate within blockchain rather than the technology that supports its platform [8].

2.5 Advantages and Limitations of Blockchain

Blockchain technology is based on the idea of distributing transactional database into several nodes that are represented by computers. These nodes work together as one system that stores encrypted sequences of the transactional record as a single chained unit or block [2]. As discussed before, by using blockchain, parties can conduct exchanges without depending on a middleman or a third party to provide trust and validate the transaction. However, this is not the only advantage of blockchain. The following list highlights the most important benefits that blockchain can bring to the business world [9]:

- ***Empowered Users***: Blockchain provides the users with the ability to control their information as well as the transaction that they are part of [9].
- ***Durability, reliability and longevity***: Blockchain technology does not depend on a centralized computing architecture, thus, it will not fail because of a single failure [9].
- ***Process with integrity, transparency and immutability***: Transactions conducted using blockchain are viewable by public and cannot be altered, thus, their integrity, transparency and immutability are guaranteed [9].
- ***Faster and lower costs transactions***: Blockchain technology has the potential to radically reduce the time and costs for the transactions by eliminating the intermediaries or third party agents [9].

However, the introduction of a nascent technology such as blockchain technology to the business world faces several challenges because of the principles it is based upon. Thus, dealing with issues related to transaction verification process and data limits per transaction is very important to the adoption of this new technology in vital business sectors such as financial services. Moreover, the list below discusses some other challenges that might hinder the implementation of blockchain [9, 10]:

- ***The rules governing regulatory status***: Currencies currently used in financial transactions are governed by national governments and in order for blockchain to be widely adopted by financial institutions, agreement has to be reached by the those governments to regulate the use of blockchain, otherwise, its status remains unsettled [9].
- ***Security and privacy concerns***: Despite the existing security solutions with strong encryption algorithms, cyber security concerns are considered one of the main important factors that affect public's decisions on sharing personal data using blockchain systems [9]. Blockchain security system will be discussed in more details in Chap. 4 of this book.
- ***Software Vulnerability***: Bugs in software code always exist and poorly written software is especially vulnerable to malicious activity. As software gets more complicated and interconnected, its reliability goes down while the number of bugs goes up. Although we have huge and rapid advancements in technology, software is written by humans and therefore it will always be imperfect. Blockchain is no different. Additionally, the integrity of the software and network are fundamentally important in the evaluation of blockchain as an infrastructure technology. If the technology permeates every major financial system worldwide, the impacts of a glitch or hack could be catastrophic [10].
- ***Integration concerns***: When organisations adopt new technologies to streamline their business process, they face change management challenge to integrate new systems with legacy ones. In this situation, adoption of blockchain technologies is no different, since such projects impose big and difficult task to strategize the transition [9].
- ***To understand the technology***: One of the biggest operational risks with blockchain is that relatively few people understand how it works. Coders and hackers have the expertise to write the software, understand the basic functions and make it work. However, we should be concerned about deploying software when we are unaware of the unknowns. For example, recently, the German automobile manufacturer Volkswagen has admitted that the software programmed by the coders deceived the emission levels by their cars. Consecutively, international fury has been sparked against the company, which led the chief executive to resign [10]. Such software malfunction would have much bigger impact on the financial world if it happens with blockchain.

- ***The decentralized nature of blockchain***: It is true that blockchain is decentralized, which makes it more difficult for all participants to be attacked simultaneously. However, if it is an inside job by a developer with experience of the topology of the network, then, this might cause major disruption to the network [10].
- ***Cultural acceptance***: Public acceptance for the shift brought by the adoption of blockchain is important to the success of the blockchain implementation projects [9].
- ***Initial implementation cost***: The savings promised by the use of blockchain technology are encouraging, however, the initial implementation costs would be considered as an important factor that cannot be neglected [9].

2.6 Potential Applications of Blockchain Technology

Blockchain technology offers many opportunities for saving costs and time as well as increased security for online transactions of any kind. This part discusses some major applications of blockchain technology in financial services, healthcare sector as well as scientific research.

2.6.1 Blockchain Implementation in Financial Services

The interest in blockchain is growing rapidly because of many factors such as the inefficiencies caused by third party trust organisations, logistics processing time, streamlining cumbersome as well as costly and risky correspondent networks [11]. Thus, institutions in financial services sector are showing increasing interest in this technology as an alternative to the current approach for conducting transactions between those organisations [12]. The list of such institutions includes major banks like JP Morgan and Goldman Sachs, where they created a partnership to invest in blockchain technology and develop it according to their needs, standards and expectations. Such investment is vital for those financial institutions as Santander bank has estimated that blockchain technology has the potential to save banks $20bn as a result of eliminating centralized trust agencies and overcoming the aforementioned reasons for investing in blockchain technology [12]. Additionally, when it comes to leans, blockchain facilitates the process of checking check creditworthiness, which results in reducing friction and increasing transparency. Similarly, financial institutions can benefit from blockchain's ability to reduce settlement time required in financial exchanges where post-trade clearing and settling is part of the process [13].

The second use case is about ledger duplication in financial services since each financial institution maintains its own registers. The reconciliation process of these ledgers is costly especially in the case of large banks where they have hundreds of

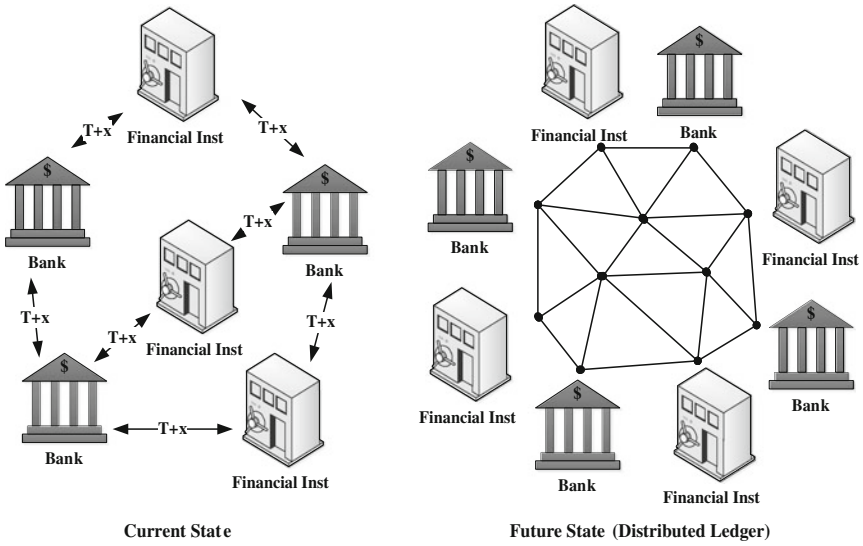


Fig. 2.3 Blockchain's impact on the financial Services, adapted from [14]

ledgers. Also, this process is usually performed by using primitive and unsecured tools such as Visual Basic for Applications (VBA) programming language, which makes it a risky process [14]. Consequently, the need for a technology like blockchain has emerged to tackle the delays caused by such fragmented architectures. Blockchain can deliver a unified ledger for the transactions among the participating financial institutions, resulting in transactions validated in near-real time (see Fig. 2.3).

Utilizing blockchain in the financial services sector could result in several advantages [14]:

- ***Cost reduction*** as a result of elimination of duplication as well as the reduction of post-trade processing such as settlement and reconciliation. It is estimated that banks could save about 15–20bn USD with seven years [14].
- ***Smart Contract*** is another advantage of blockchain since that the majority of financial assets exist in electronic form and smart contract have the ability to automate the existing logic, which could reduce remittance and initiation costs [14]. Smart contracts will be discussed in more details in Chap. 6 of this book.
- ***Risk Management*** can benefit from blockchain technology as well because of the increased speed of settlement, which results in an increased liquidity and decreasing balance sheet risk [14].
- ***Improved regularity compliance*** by having authorized regulator to view a transparent ledger that is distributed among financial organizations. This could also reduce the costs of anti-money laundry and fighting against terrorism financing [14].

2.6.2 Blockchain Implementation in Healthcare

The realization of blockchain benefits for the healthcare industry started to grow as many opportunities started to arise in such vital sector. New models for managing and sharing medical records have emerged using blockchain's ability to provide trust and security while cutting costs, time and resources required by traditional health management infrastructure. As a result, systems such as Health Information Exchange (HIE) and All-Player Claim Database (APCD) became useless [15]. For example, a partnership between the government of Estonia and a cyber-security firm called Guardtime (guardtime.com) in 2007 has emerged to replace HIE and APCD systems. The plan is to make use of blockchain's Keyless Signature Infrastructure (KSI) in order to authenticate and verify the integrity of the medical public data [15]. Additionally, technologies invested in nowadays' wearables provide rich sources for Patient-Generated Health Data (PGHD). However, since this data is not securely accessible, its potential is not yet harvested. Thus, digital health innovators such as Healthbank (healthbank.coop) and Netcetera (netcetera.com) in Switzerland as well as Noser (noser.com) in Germany have started an initiative to securely share personal medical data by investing in and making use of blockchain technology. The intention is to enable the personal to control his\her own data [15].

2.6.3 Blockchain as a Tool to Improve Trust in Scientific Research

Trust in scientific research is an important factor for the credibility of the outcomes especially in vital areas such as medical sciences. However, this factor has suffered trust issues cause by scientific data manipulations such as outcome switching, data cleansing and selective results publication. Thus, a study by Carlisle in 2014 has proved that blockchain can offer a low cost, independently verifiable method to audit and confirm the reliability of the results of scientific studies by using blockchain-timestamped protocols. Carlisle's study shows how blockchain provides an immutable record of the existence, integrity and ownership of a specific medical trial protocol [16].

2.6.4 Applications in Various Industries

Additionally, blockchain technology has applications across several industries. The following point group these application:

- ***Cryptocurrency***: Originally used for value transfer and payments, this blockchain application works by allowing different parties to transact among each other in a trusted manner without the need for third party intermediaries [11]. Additionally, organizations interested in the applications of the distributed

ledger are trying to make use of it for the post trade activities such as clearing, custody and cash management [11].

- ***Proof services***: Blockchain ability to store value at a very detailed level (identity, ownership, membership, etc.…) provides governments with the capability to provide services for citizens related to birth and death certificates, business licenses and property titles [11]. One real life example of this project is the one created by BitNation (bitnation.co) and aims to initiate decentralized governance at global scale such as World Citizenship ID [11].
- ***Smart Contracts***: Smart contracts can enable transactions to self-execute themselves without the involvement of any third party, by the use of the imbedded information such as predetermined terms and conditions, and execution rules [11, 17]. Some startup blockchain-based projects started to offer full featured smart contracts capabilities such as Ethereum project (ethereum.org). Smart contracts will be fully analyzed in Chap. 6.
- ***Decentralized autonomous systems/services***: This could be the most prominent role of blockchain, which is about establishing trust mechanisms between the human and the computer. This is also called Decentralized Autonomous Organizations (DAO) and it can autonomously hire agents on the Internet to perform specialized tasks. However, it is understandable that creating self-organizing and self-governing DAO is not an easy mission, but once properly implemented, it can have a major impact on various industrial sectors such as transportation, healthcare and cloud storage [11].

Table 2.1 illustrates a grouping for the key applications of blockchain technology according to the users of the technology.

Moreover, Fig. 2.4 provides a grouping for the key applications of blockchain technology according to technology sub-domains and time-to-delivery indicator.

2.7 Blockchain Adoption

The introduction of blockchain technology into the world of business promises massive change to organizations' IT infrastructure as well as to the way they transact and conduct business. This section explores the potential of blockchain technology as well as its benefits and obstacles that face its adoption.

2.7.1 Blockchain Potential as SWIFT Replacement

SWIFT stands for Society for Worldwide Interbank Financial Telecommunication and is considered as the most important aspects in banking industry since the 1970s. It is a global system that enables financial institutions to securely exchange information about their financial transactions. Swift is globally used by more than 9000 financial institutions in 209 countries to exchange $5 trillion a day. For all these

Table 2.1 Key blockchain applications groupings according to the users of the technology, adapted from [14]

Institutions	Regulators	Operations	Individuals
FX settlement	Compliance reporting	Client onboarding	Crowd-funding
Trade reconciliation	Risk visualization	Intra-company settlement	Virtual identity
Cross border payments	Basel III compliance	Normalize reference data	Credit scoring
Credit efficiency	Client fraud transparency	Time-stamping	Cross border remittance
Loan settlement	Know your customer/Anti-money laundering	Account portability	Vault/escrow services
OTC derivatives clearing	Trade reporting	Broker fraud identification	Customer deposit cost
Collateral management		Securities agreements as smart contracts	Peer-to-peer lending

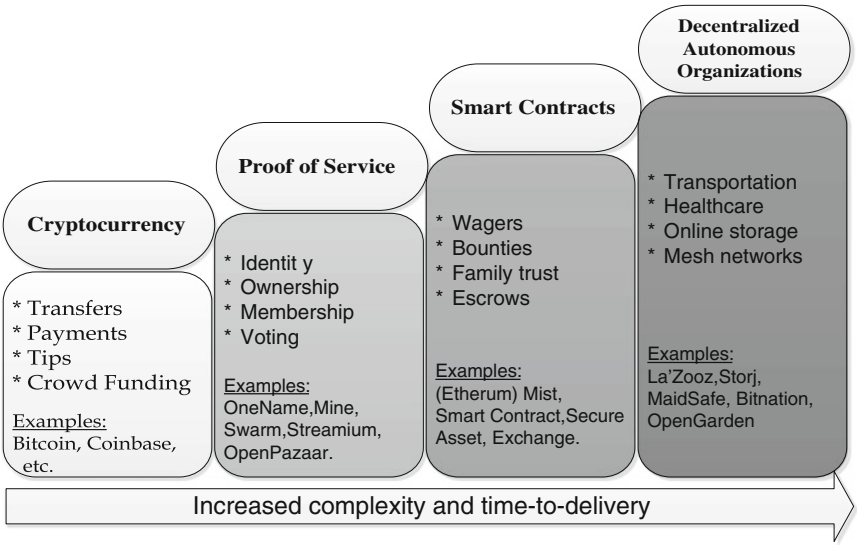


Fig. 2.4 Key blockchain applications groupings according to technology sub-domains, adapted from [11]

reasons, it is difficult for banks and other financial organizations to replace Swift with blockchain, and it is even more difficult for this transition to happen when bankers and executives lack the full understanding of what blockchain is, how it works or its capabilities. Blockchain abilities include recording digital value exchange such as payment or a marriage vows and record securities settlements [18].

2.7.2 Blockchain Adoption by Organizations

Many organizations started to realize the prospective advantages that can be achieved by adopting blockchain technology. IBM for example, is investing in this technology in order to shape the regulations that govern its implantation as well as to develop products that can be used by interested businesses. Additionally, IBM has joined a Chamber of Digital Commerce, which was jointly established by a group of blockchain startups, software firms, financial institutions and interested investors in 2014 in an effort to work closely with US government to set the standards for blockchain development and usage as well as to develop a legal framework that can lead its adoption.

In corporation with Digital Asset Holdings and the Linux Foundation, IBM's idea is to develop open-source blockchain-based software that can become the basis for any future blockchain implementation by interested organisations. Major firms such as JPMorgan Chase, ANZ Bank, Cisco, Accenture, Intel, London Stock Exchange Group, Mitsubishi UFJ Financial Group, IC3 and VMware have already started to invest in what IBM is developing [19]. Furthermore, Deloitte is another example of big organization that realized the potential of blockchain, as it started a partnership with five blockchain specialized firms in order to use the emerging technology effectively in its consulting business by developing blockchain based applications such as digital identities, digital banking, cross-border payments as well as loyalty and rewards [20].

Moreover, capital markets represent an important part of the financial system that uses shares, bonds, and other long-term investments to generate and raise companies' capitals. Figure 2.5 illustrates the benefits of blockchain adoption across the different trading stages within the financial markets. These stages cover pre-trade, trade, post-trade and finally custody and securities servicing.

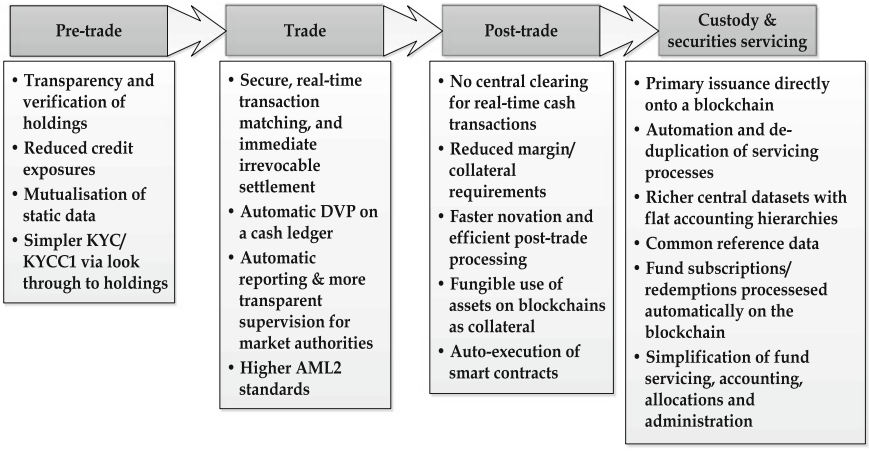


Fig. 2.5 Benefits of blockchain adoption for capital markets, adapted from [21]

Considering the impact of adopting blockchain in capital markets however, it is necessary to consider the obstacles that might hinder or affect its success. Thus, blockchain technology requires further investment in order to have an agreement on its common standards and in order to have scalable enough technology [21]. In the following Section, we outline an implementation timeline suitable to be addressed before widespread adoption will become feasible.

2.7.3 Blockchain Implementation Timeline

It is important for the developers behind new technologies such as blockchain to produce practical applications and solutions in order to ensure ongoing investment and to be able to scale the technology to real-life applications in live environments. Figure 2.6 illustrates the time to market timeline for the adoption and development of blockchain-based applications.

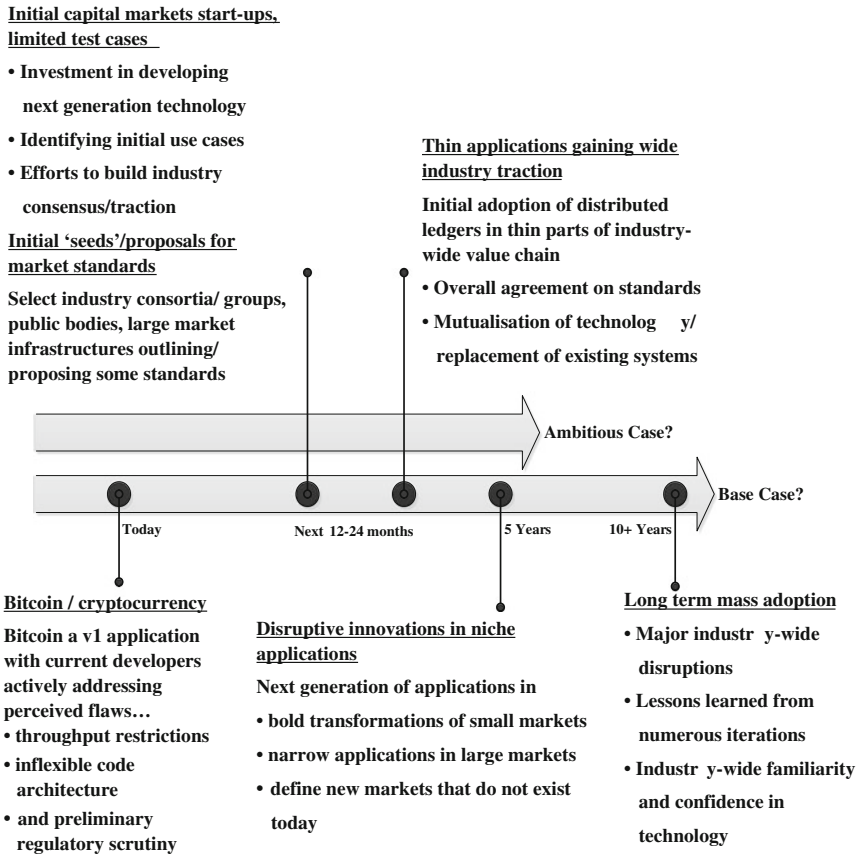


Fig. 2.6 Blockchain adoption and implementation timeline, adapted from [21]

Taking the timeline into account, it is key for organizations to realize the importance of keeping up to date with the emerging technologies, since falling behind, might result in loosing important share of the market or even leaving it. Thus, the following points list several suggestions related the adoption of blockchain for a successful adoption and implementation:

- ***Proofs of concept must be reliable and convincing***: Technology developers and innovators must present solid use cases by justifying how the distributed ledger will have a great and positive impact to the industry as well as to the clients [21].
- ***To understand the current status and the future impact***: Interested adopters or developers of blockchain have to understand the current situations with the current technological solutions and analyze the challenges, costs and benefits from adopting blockchain in the organization [21].
- ***New technology needs more time for success***: It is understandable that sometimes new technologies might not achieve their potentials fast, thus, innovators, developers and adopters need to continue driving the change in the industry by more engagement and collaboration [21].
- ***Mature and successful products need more time***: Technological innovations don't achieve success from the first versions, thus, it is important to consider those early versions as prototypes that help in uncovering the areas that need improvement [21].
- ***The importance of bridging the gap between technology and industry***: It is important to fully understand the domain knowledge that will be used to develop the new technology, and not to separate the development process from the business expertise [21].
- ***The important role of the regulators***: Technology development should be in full accordance with authorities' standards and roles. It is important to keep briefing these authoritative stakeholders about the development process in order to address their concerns regarding security, privacy and legal measures [21].
- ***Scalability of the Technology***: It is important for new technologies like blockchain to be able to handle large financial markets datasets while considering concerns related to security, robustness and performance [21]. This issue is especially important in order to manage the operational risks of the transition to the new technology during implementation.
- ***Agreement on common standards***: Industries need to have an agreement on the design issues of blockchain such as its openness (open or permissioned-base access systems). Moreover, they need to have common grounds on how to operate and manage blockchain infrastructure, which includes its governance, updates and responsibilities.

2.8 Case Studies

In this section we investigate two case studies showing the implementation of blockchain at work environment and we provide explanation about its role for the business success. However, because the business world is still discovering the hype and the potentials of a nascent technology like blockchain, the following use cases are still developing.

The first case study is about a futuristic plan or vision called "Energy union" set by the European Commission Energy Union Framework Strategy in 2014 [22]. This plan aims to give the power for the EU citizens to embrace the energy transition in order to reduce their bills, have more choices, actively participate in the energy market, and most importantly to protect the consumers [22]. However, such vision requires dealing with many critical issues. These are:

- *Delivering accurate information* regarding incurred costs and power consumption in order for the customers to realize possible opportunities in such fully-integrated continental energy market.
- *Appropriate ways to reward active participants* such as switching between contracts as well as managing demand and response according to current prices.
- *Ensuring interoperability* in the market while considering various aspects such as residential energy service providers and available options for the consumers as well as embracing possible gains from self and micro power generation.

These factors make it necessary for the European commission to invest in new technologies that can meet their expectations. Hence, the interest in blockchain and its distributed ledger as the technology that can improve the level of integration and development of the energy retail market. Thus, a European Commission called Joint Research Centre (JRC) for science and knowledge service, which provides scientific advice to EU policy, is practically investigating the applications for blockchain, such as micro-generation energy market and energy contract ledger. The first one is about consumers that are capable to produce energy locally and trade it with other local markets. Distributed ledgers and smart-metering can enable local energy generators to access the energy market, which until now remains a privilege for only the major energy suppliers. The later case, energy contract ledger, is another application context where distributed ledger can enable better management of the administrative complexities associated with changing the energy supplier such as closing the current contract, opening a new one with new supplier, and discussing new terms. Distributed ledgers can improve this process by allowing consumers to finalize the transition easily on the internet. Additionally, energy providers can save costs required for the administrative operations [22].

Point of Attention This case study shows how distributed ledgers (blockchain) can be utilized to develop more competitive energy retail market by empowering the consumers with more information that can enable them to have wide choice of action. The benefits of such vision are so promising, hence, that further investigation is required. However, there are still questions about the scalability, security and stability of such applications that need to be addressed.

The second case study discusses the use of Distributed Ledger Technologies (DLTs) in contexts different from its original purpose, Bitcoin, since the concepts and structures developed for distributed ledgers is extremely portable and extensible to other areas of economic and social interactions. It is about the ability of governments to use distributed ledgers for information sharing between economic entities, which helps to reduce market friction and would enable new forms of innovation to emerge. Consequently, SMEs can benefit from the reduction in transactions' costs to be able to move more freely within the market, which helps to lower overall operating expenditures. Additionally, by using DLTs to register companies' patents and Intellectual Property (IP), it is possible to reduce the overall number of contract disputes. These disputes make up 57% of all litigation in the UK, more than any other category of legal action [22].

Point of Attention This case study shows how distributed ledgers can help reduce transaction costs for SMEs and streamline cost of operations for local and national government. Additionally, having a trustworthy proof of ownership for digital assets such as IP will reduce the options for litigation, providing an overall social benefit for UK society.

DLTs can be used to register contracts and assets, which provide a robust and trustworthy method to prove the businesses ownership of the properties including Intellectual Properties (IPs) as well as patents. Moreover, they can handle micropayments, decentralized value exchange and transfer, token earning and spending. Thus, DLTs can help governments to improve the way businesses work in various ways. These include:

- Business licensing.
- Registration (e.g. properties, wills, intellectual properties, notary services, health data, etc.).
- Insurance transactions.
- Taxation management at different municipal and regularity levels.
- Pension related data.

Distributed ledgers provide opportunities for government to reduce operating costs, fraud, error and the costs of delivering services to underserved users. This can benefit SMEs by reducing the costs of the transactions.

2.9 Summary

Blockchain is a technology that is highly likely to change the way businesses will work in the near future, just like what the Internet did in the 1990s. It is a nascent technology, and the realization of its potentials to overcome the existing issues in the way businesses transact among each other as well as to improve current business practices encouraged large organizations such as IBM and major banks to greatly invest in it. Blockchain adopters, however, have to face several concerns such as the regulations that govern how it works, security and privacy issues, integration concerns and cultural acceptance. If these concerns are addressed properly, then, blockchain will successfully match its potentials as a value system and the possible advantages of shifting to blockchain technology will be promising for the adopting organizations.

In this chapter, comprehensive descriptions for blockchain and its features have been provided. Moreover, explanations for blockchain applications in several industrial sectors have been discussed. The discussion has proved the importance of blockchain technology in vital domains such as scientific research and healthcare. Additionally, it demonstrated the variety of implementation areas in the financial sector. Nevertheless, proper research, management and experience are required to successfully understand the business domain as well as how blockchain technology can fit and meet business requirements. Finally, the chapter has discussed two developing case studies, highlighting the significance and benefits associated with the adoption of blockchain in order to have more efficient businesses.

References

1. Kiviat TI (2015) Beyond bitcoin: issues in regulating blockchain transactions. Duke Law J 1:569–608
2. Lemieux VL (2016) Trusting records: is blockchain technology the answer? Rec Manage J 26:110–139
3. Batog C (2015) Blockchain: a proposal to reform high frequency trading regulation. Cardozo Arts Ent LJ 33:1
4. Watanabe H, Fujimura S, Nakadaira A, Miyazaki Y, Akutsu A, Kishigami JJ (2015) Blockchain contract: a complete consensus using blockchain. IEEE 4th global conference on consumer electronics, pp 557–578
5. Dorri A, Kanhere SS, Jurdak R (2016) Blockchain in internet of things : challenges and solutions. arXiv preprint arXiv:1608.05187
6. Froystad P, Holm J (2015) Blockchain: powering the internet of value
7. Kraft D (2016) Difficulty control for blockchain-based consensus systems. Peer-to-Peer Netw Appl 9:397–413

8. Reutzel B (2016) Why standards would aid blockchain's adoption. http://www.americanbanker.com/news/bank-technology/why-standards-would-aid-blockchains-adoption-1090219-1.html. Accessed 10 Oct 2016
9. Boersma J, Bulters J. Blockchain technology 9 benefits and 7 challenges. http://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html. Accessed 09 Oct 2016
10. Summers TC (2016) Hacking the blockchain. Mod Trader 82
11. Anonymous (2016) Blockchain: double bubble or double trouble? IT NOW 58–61
12. Walch A (2016) The bitcoin blockchain as financial market infrastructure: a consideration of operational risk. Public Policy, N.Y.U J. Legis 1
13. Tapscott D, Tapscott A (2016) How will blockchain change banking? How won't it? http://www.huffingtonpost.com/don-tapscott/how-will-blockchain-chang_b_9998348.html. Accessed 09 Oct 2016
14. Brennan C, Lunn W (2016) Blockchain: the trust disrupter, UK
15. Nichol PB (2016) Blockchain applications for healthcare. http://www.cio.com/article/3042603/innovation/blockchain-applications-for-healthcare.html. Accessed 12 Oct 2016
16. Irving G, Holden J (2016) How blockchain-timestamped protocols could improve the trustworthiness of medical science. F1000Research 222:1–6
17. Christidis K, Devetsikiotis M (2016) Blockchains and smart contracts for the internet of things. IEEE Access 4:2292–2303
18. Skinner C (2016) Will the blockchain replace swift? Accessed 12 Oct 2016
19. Macheel T (2016) IBM joins Washington Blockchain Trade Group. http://www.americanbanker.com/news/bank-technology/ibm-joins-washington-blockchain-trade-group-1081778-1.html. Accessed 11 Oct 2016
20. Yurcan, B. (2016). Blockchain Firms Team Up with Deloitte, http://www.americanbanker.com/news/bank-technology/blockchain-firms-team-up-with-deloitte-1080802-1.html. Accessed 15 Oct 2016
21. de Velde J Van, Scott A, Sartorius K, Dalton I, Shepherd B, Allchin C, Dougherty M, Ryan P, Rennick E (2016) Block chain in capital markets: the prize and the journey
22. Walport M (2015) Distributed ledger technology: beyond block chain. Government Office for Science, London

Blockchain Governance

3

Abstract

Blockchain governance is the provision of services in a potentially more efficient and decentralized way, without having to necessary rely on the state or government bureaucracy. In this chapter, the societal impact of decentralized Blockchain governance is discussed, describing their associated challenges. We further explain how banks are adopting Blockchain to improve upon their existing products and services with specific examples of some European-based banks. In addition, the impact of Blockchain governance on non-banking sectors such as financial institutions are well presented as well as techniques needed for adoption. The chapter concludes by an articulate summary on overall issues addressed, the risks Blockchain-based governance may produce and highlights a few methods to cope with such a huge technological disruption.

3.1 Introduction

Blockchain governance is the provision of services in a potentially more efficient and decentralized way, without having to necessary rely on the state or government bureaucracy [1]. This provides a more distributed diffusion of authority, in which the sources of authenticity are individuals themselves. Using the Blockchain as a permanent, encryption-secured public record storehouse, human agents as representatives can be replaced by smart contracts and decentralized autonomous Corporations [2].

Existing legal systems currently involves the invocation of various state-appointed mediators to improve the enforceability of contracts. Some contracts need to be notarized to prove that the parties really did sign the contract in the presence of a legislative officer, while others have to be registered in order for the transaction to be stored in the public records. When all contracts are put into a

V. Morabito, *Business Innovation Through Blockchain*,
DOI 10.1007/978-3-319-48478-5_3

Blockchain, a technological solution can be developed that does away with the need for human intermediation and establishes provenance [3].

With such a technological solution, Lawyers will no longer draft lengthy paper documents but will instead prepare self-executing legal documents that activate payments when certain pre-defined situations occur. The ownership of intellectual property rights would be easily demonstrated by referencing their time-stamped locations on the Blockchain [4]. In addition, many government operations can also be replaced by Blockchain equivalents. A Blockchain database of public records will ensure that birth certificates, land records, other records are automatically recorded in a format that is publicly verifiable. This would consequently diminish our investment in governance and offer greater accountability in the provision of public services. As noted above, record keeping is considered as an important function and feature of the blockchain technology. It enables easier and more trusted value transfer among individuals in both of its forms, short-term transfer such as money transfers, as well as long-term records retention such as land transfers. Considering the implications of having frauds committed in both of these use cases, however, it is important to understand the two dimensions—record retention requirements and evidential requirements—that characterize the different blockchain technology applications [5]. Figure 3.1 provides an illustration of the blockchain use cases considering these two dimensions.

It can be noticed from Fig. 3.1 that when both retention requirements and evidential requirements are low the use cases are most suitable for blockchain-based solutions. In contrast, when both retention requirements and evidential requirements are high, then the aforementioned technology is not suitable for such applications unless blockchain governance is well structured and can prevent fraud incidents [4].

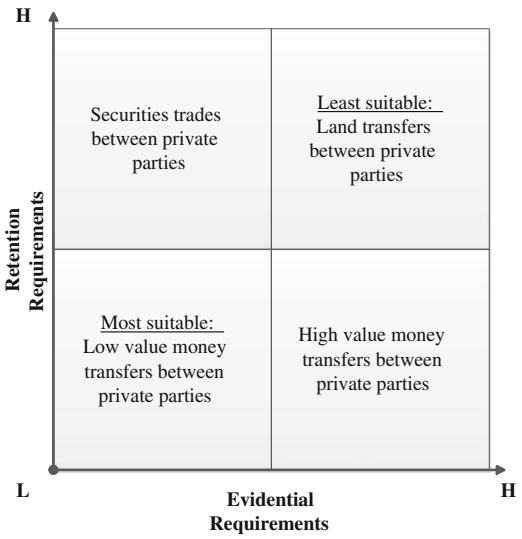


Fig. 3.1 Heuristic for thinking about the suitability of blockchain solutions for recordkeeping. Adapted from [4]

Considering the fact that blockchain technology is new and that it is still in the development phase, it is important to study the impact and the challenges of implementing decentralized blockchain-based applications and governance on the targeted society. Hence, the following section will address some of the predictable concerns that would most likely affect such a significance technological transformation on the adopting organizations.

3.2 The Impact of Decentralized Blockchain-Based Governance on Society

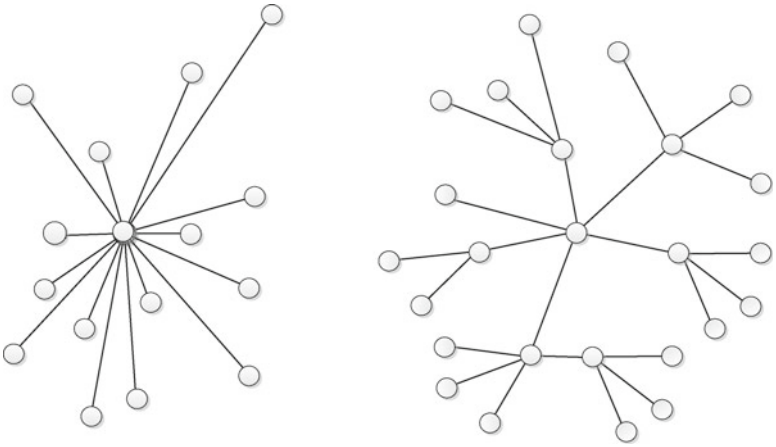
This section discusses some known issues that would be greatly impacted by the evolution of Blockchain-based governance and their respective challenges. The issues addressed include; reducing the need for centralized authorities, automated contractual negotiation, reducing resistance in capital markets and financing, the growth of the peer-to-peer economy and smart property and machine-to-machine communications.

3.2.1 Reducing the Need for Centralized Authorities

Before the evolution of Blockchain governance, a centralized government authority has been responsible for organizing business and state related activities such tallying votes of the populations, collecting taxes, maintaining property registries and enabling the creation of flexible political institutions as well as maintaining law and order [1, 6]. With the Blockchain, the need for these centralized authorities would be remarkably reduced. Users of the internet would be able to act as middlemen and manage their own affairs through a shared decentralized database [5, 7].

For example, users would be able to register any piece of content, data, or even property on the Blockchain in an encrypted form, enabling transactions to occur directly, immediately, and anonymously [6]. As a result, Blockchain technologies can actually make feasible what many Internet pioneers preconceived: more flexible interactions between a smaller number of centralized organizations whose functions are split into decentralized entities [8]. As depicted in Fig. 3.2, the differences between a centralized and a decentralized network are quite apparent. Yet, the anonymous nature of Blockchain governance introduces major regulatory challenges. It's extensive adoption could potentially weaken the ability of law enforcement agents to uncover and close down on criminal activities [8].

Furthermore, digital currencies can be used as tax havens. In case that an individual or a group are trying to evade paying taxes, they could very easily set-up multiple digital currency accounts and transfer funds between them. Furthermore, tax-evaders could use several anonymization methods, in their endeavor to avoid paying money to the government, thus making it more difficult for authorities to actually find the owner of these bank accounts [6]. It could be relatively easy to use



(a) Centralized Network (b) Decentralized Network

Fig. 3.2 Illustration of a centralized and decentralized network. Adapted from [3]

digital currencies and transfer money between bank accounts in a non-legitimate way without anti-money laundering (AML) rules or know your customer (KYC) practice implemented by payment mediators [9].

Moreover, as Blockchain technology enhances the encryption of communication, the adoption and utilization of anonymous decentralized communication channels could create severe obstacles to governments trying to intercept communications without consent. Data can be encrypted as it is transported between two points and the message content can also be stored in an encrypted form on the Blockchain; this means that the message can only be unlocked with a secret key, only known to the parties involved in the communication process. More importantly, in case that blockchain technology is broadly adopted, these communication networks could successfully interrupt mass surveillance currently performed by governments or corporate entities; but, on the other hand, the implementation of these networks could severely eradicate other important forms of surveillance that are being used for prosecution and law enforcement [6].

3.2.2 Automated Contractual Negotiation

Although Chap. 6 is fully dedicated to smart contracts and licensing, a brief explanation of this blockchain application is discussed here to place it within a governance context.

Blockchain governance has the potential of decreasing the minor cost of contracting; smart contracts have the prospective to radically reducing friction in both commerce and society by providing greater precision and swiftness to transactions [1]. As smart contracts are written using source code, they can be executed like any other programming language. As a result, it is expected that in the near future an

individual will be able to draft and execute his own smart contracts, eliminating the need of hiring a lawyer. This is expected to have a momentous impact on the legal profession. As above-mentioned, for example, lawyers may no longer need to focus on the drafting of long and standard legal provisions; such details would be left to a machine and thus they can concentrate on more complex legal work to recognize the main provisions of a contractual agreement that should be implemented into the code [10, 11]. In addition, smart contracts offer a significant advantage to existing contractual drafting practices by eliminating the inherent ambiguity of natural language. While words can be interpreted differently in various contexts, smart contracts combat this ambiguity by incorporating legal provisions into the source code.

Nevertheless, legal parties can use vagueness and poor drafting in order to step back from contractual conditions that they no longer want to honor. With blockchain technology, smart contracts offer an effective solution to this problem by incorporating legal provisions into code [4]. More specifically, smart contracts can provide a great amount of certainty to parties that a contractual condition will be undoubtedly be honored by forcing the parties to remain loyal to their respective obligations [12, 13].

Although smart contracts may facilitate the implementation of multifaceted agreements with better clearness, they also present a cycle of novel challenges. By default, smart contracts embed a zero-tolerance policy where parties are obliged to carry out the contract [6]. Existing legal structures establish a series of regulations that the parties involved must abide to based on provisions of the law. Nonetheless, there is freedom to breach these rules because legal enforcement takes place after the act. Unlike traditional contracts, where parties can choose whether or not to fulfill their obligations, a smart contract cannot be breached. Judicial enforcement is less needed in a system controlled by self-executing smart contracts as the manner in which the rules have been defined in the code matches exactly the manner by which they are enforced. Eventually, the only means that people can use in order to violate the law is to break successfully the code [4]. Therefore, this raises an issue on the differences between technically and legally binding contracts. Though contract law includes a series of security measures to protect consumers that may either quash the contract or make it non-enforceable, smart contracts operate within their own closed technological structure. Figure 3.3 shows in detail how smart contracts can be executed in practice by exploiting the dynamics of blockchain technology. At first, the terms of the smart contract are being predefined by the parties. Then an event is triggering the actual execution of the contract. While the contract is being executed and its value is transferred, settlement takes place—either in cases of digital assets or in cases of physical assets.

It becomes apparent, that although the implementation of essential contractual security measures and consumer protection provisions into smart contracts seems promising, it may prove to be rather complicated in practice given the formalized and deterministic character of the code [11, 14].

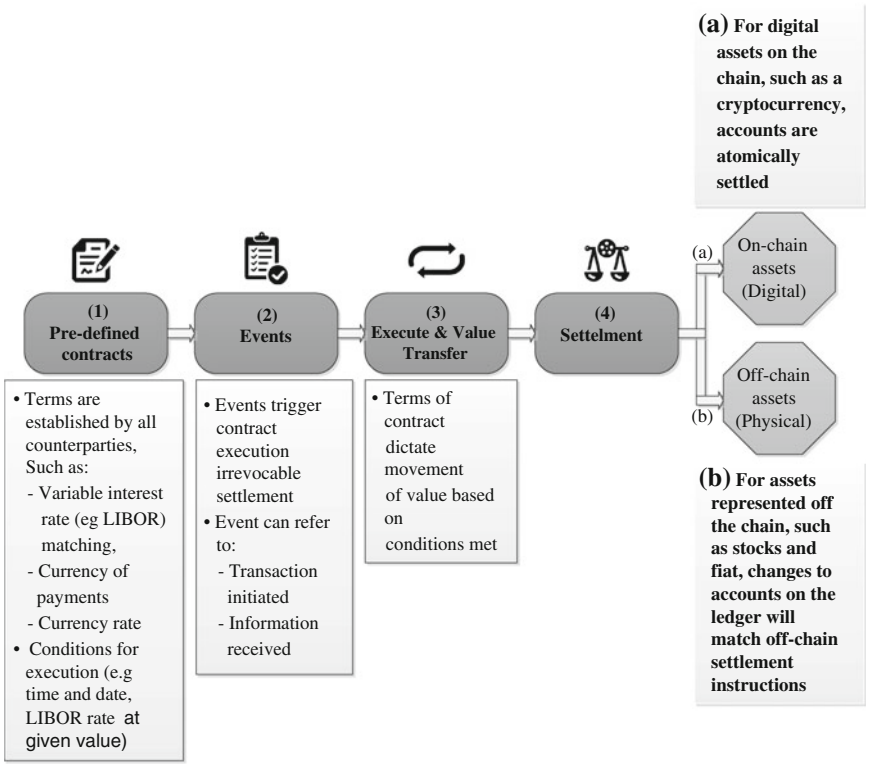


Fig. 3.3 Illustration of smart contracts' execution procedure. Adapted from [9]

3.2.3 Reducing Resistance in Capital Markets and Financing

Blockchain governance provides a practical framework to create digital assets and decentralized exchanges. Until today, it was very difficult to raise money and assign equity in an organization without hiring a lawyer. By exploiting the dynamics of Blockchain technology and using services such as Koinify and Swarm, nowadays a website can easily and quickly issue a cryptotoken to raise money to invest in various areas such as software development or reward new users [4]. By means of a few lines of source software code, an organization can generate its own cryptotoken to signify an ownership interest in a company or voting privileges. Just as the Internet and personal computers have invaded and conquered people's lives, Blockchain could offer to everyone the opportunity and authority to effortlessly issue financial instruments [9]. Eventually, centralized physical exchanges by financial corporations will be replaced by Blockchain-based, decentralized exchanges.

As settlements and payments can happen simultaneously, these exchanges will enable the trading of cryptotokens and securities that are recorded, transferred and

managed by the Blockchain [4]. The need for a licensed market decreases, because immediate settlement efficiently eliminates counterparty risk. On the other hand, the digitization of assets and securities could introduce several problems, particularly in the area of securities laws [15, 16]. When people conduct their businesses through decentralized methods, without complying to the rules instructed by the law they face a huge risk to be stopped down by regulatory agencies. Furthermore, this could result to technical challenges similar to those that surfaced after the introduction of file sharing.

As regulators were not successful in controlling the distribution of information, it is safe to assume that governments could fail to manage technological development in the digital finance ecosystem. While reasonable in the existing economical structure, security rules may need to be improved to better reflect and take into account the opportunities Blockchain has to offer in order to encourage new promising businesses to be created that may have never existed previously. Certainly, it may result to be more and more unpractical and ultimately lead to sluggish economic development. Therefore, it is important that people create extensive releases about the risks and potential rewards of a specific project before seeking to raise funds [10].

3.2.4 The Growth of the Peer-to-Peer Economy

Smart contracts and digital currencies may also revamp how individuals interact with the online world. Software developers are trying hard to integrate Blockchain technology into every Internet browser, so that websites will eventually employ these distributed data centers [1]. As a result, the implementation of a metered Internet, where actions are connected to small micropayments and accompanying smart contracts would be realized. As smart contracts can vividly lessen the costs financial transactions, authors and musicians, may soon use this technology to automatically collect royalties on their works whenever they are being purchased [6]. Apparently, this could result in the elimination of the dependency of artists and musicians on affiliate-based income models. If micropayments are effectuated and accepted, content creators will be adequately enthused to circulate their works extensively and persuade people to remix them; because the more these works are used or reused by third parties, the larger rewards they will obtain. Smart contracts and micropayments could then be used to realign the financial motivation structure of the Internet, redistributing wealth in a more effective manner [17].

Concurrently, Blockchain governance, through the deployment of smart contracts, could challenge the free nature of the current online world, as the system in effect can lead to a further development of current digital rights management (DRM) that could endanger the open nature of the Internet [9]. These evolving digital contracts have the influence to possibly manage access and utilization of

digital content. Content creation organizations could protect their materials by utilizing blockchain and smart contracts in order to guarantee that payment is being made as well as put boundaries on transferability and protect content that is available in the public domain [6]. By implementing self-executing contracts that can track every duplicate, distribution, unoriginal work, content creators could strengthen their position and eventually be able to recognize all of their content that is online, thus lessening the possibility for online copyright infringement [16].

3.2.5 Smart Property and Machine-to-Machine Communications

Due to Blockchain governance, Internet-connected machines also would be able to correspond and carry out real time transactions. Physical property can be maneuvered and guarded through source code, turning previously static, daily items into "smart property." Smart properties could be defined to embed digital capacities and intended to transact and correspond with humans and other machines and be managed either through human control, algorithms, or artificial intelligence [1, 6]. Soon, in the near future, people will be able to immediately search, utilize, and pay for available resources [14]. For instance, people will be able to order self-directed cars through their smartphones. Each order could be recorded onto a Blockchain which can be scanned and inform the self-directed car of the transaction. We would then be able to pay for a trip, like a normal taxi, with our charge deposited into the car's own bank account (apparently a digital currency account) [6].

On the other hand, the mass deployment of smart property also introduces new challenges that cannot be effortlessly addressed within the existing legal framework [9]. Nowadays, it is commonly assumed that an individual or a group that owns a property has received some rights and those rights can be transferred to another party by legal regulation mechanisms such as seizure, divestiture, or judicial action. In the case of smart property, things are very different as ownership could be both described and managed by source code. A person who qualifies as the technological owner—and not the legal owner- of the smart property, actually has the complete self-governance over that resource, which cannot be objected by anyone unless particularly stated in the code [6, 10]. In addition, this code can also be used to carry out a series of technological arrangements that might ultimately limit the exercise of property rights over a particular object. For instance, access to property can be restricted to specific users or device, or even be allowed only to a specific person who is recognizable in a record that is stored on the Blockchain. In the extreme case, every piece of property could be disabled or deprived distantly with the click of a button or the execution of a computer algorithm [6, 18].

This section has highlighted the areas that will be affected by the evolution of Blockchain-based governance and it discussed their respective challenges. Table 3.1 summarizes all the challenges explained in this section.

Table 3.1 Summary of the challenges facing blockchain governance

The affected area	The challenge
Reducing the need for centralized authorities	Elimination of legitimate forms of surveillance
Automated contractual negotiation	Integrity concerns
Reducing resistance in capital markets and financing	Risks of failing to abide by regularity and financing
The growth of the peer-to-peer economy	Threat to the open nature of the internet
Smart property and machine-to-machine communication	Limits on the exercise of property rights

3.3 The Synergy of Blockchain-Based Governance and the Banking Sector

Many bankers have been pondering about their Blockchain strategy in boardrooms around the world over the past year. Some big banks are now becoming gradually more active with Blockchain and investing notable resources to advance their existing banking infrastructure [19]. Moreover, no other industry is setting aside as much financial resources researching Blockchain as the one that Bitcoin was created to circumvent the finance industry.

Blockchain governance has attracted the interest of banks due to its potential to simplify the industry's multifaceted and wide-ranging payment and agreement networks, and in such process they concurrently lessen risks and expenses. Advocates of Blockchain argue that because it eliminates mediators and is faster, more secure and dependable than today's legacy systems it could save banks billions of dollars in costs [16]. The discovery of Blockchain governance has driven banks in numerous directions; from exploring entirely decentralized systems that integrate bitcoin or other virtual tokens to function, to ones where only authorized and investigated users are given access to a network. Although the exact model likely to be adopted by the industry is not clear, it is evident that numerous big global banks are working towards harnessing the Blockchain technology [2].

One method carried out by many big global banks is the creation of innovation laboratories where investor communities, startup firms, and banks work collaboratively in an effort to speed up innovation opportunities, including the improvement of a Blockchain solution that is well-organized, scalable, secure, and reliable. For instance, Citi bank launched a global network of innovation laboratories in Singapore, Dublin, and Tel Aviv; UBS opened innovation laboratories in London, Singapore, and Zurich; Deutsche Bank in Berlin, Silicon Valley, and London; Barclays in London [9].

UBS is one of the most active banks adopting Blockchain governance. They explore a variety of use cases for Blockchain technology, including settling trades and issuing bonds. During a global CEO panel debate on the opportunities

Blockchain technology provides for trade settlement, Dr. Axel Weber, chairman of UBS, explained that, "With these Blockchain technologies, if you can settle in two hours instead of two days, you can turn over your balance sheet in the same activity 24 times. Just imagine the profitability that this will bring to financial institutions that are payment focused and transaction focused I see this as a huge opportunity for the banking industry" [10]. The organization is researching across a large number of distributed ledger systems with the hope that it will be well equipped to rapidly implement the most favorable one for its business model as well as the industry. UBS' Oliver Bussmann considers the technology's disruption in diverse areas of finance will actually begin to be felt by the end of the decade [10].

Similarly, Deutsche Bank has also invested a substantial amount of resources exploring the possible business uses of the Blockchain. According to the bank's reply to a call for facts on virtual currencies and distributed ledger technology by the European Securities and Markets Authority, Deutsche Bank has identified numerous possible uses for the technology in finance, together with fiat currency payment and settlement, securities issuance, transfer, clearing and settlement, enforcing derived contracts, asset registries without the need for a central administrative authority, anti-money laundering supervision, and know your customer as well as creating clearness and facilitating distinguished customer and regulatory reporting [9].

The perception of Blockchain's potential is also seen in investment trends. Certainly, financial institutions invested US$75 million in Blockchain technology in 2015, according to the Aite Group, a financial services research organization (see Fig. 3.4) [15]. That is more than twice the amount invested in 2014, and Aite calculates approximately that financial institutions will be investing five times that amount annually by 2019.

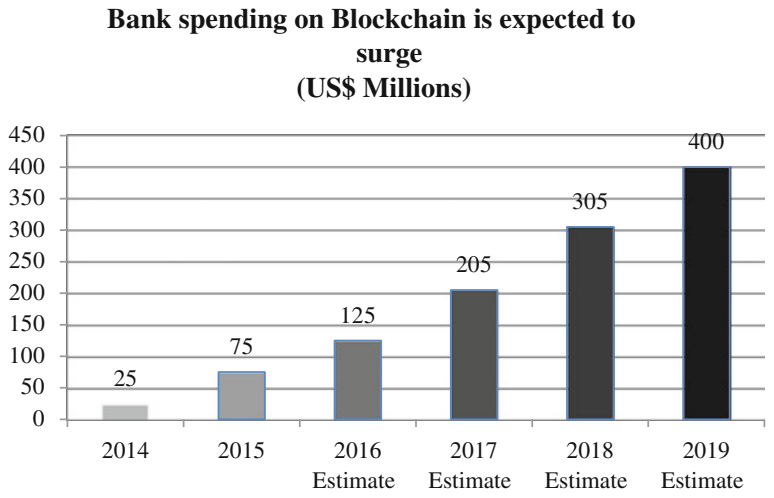


Fig. 3.4 Bank spending on blockchain is expected to surge. Adapted from [20]

Financial institutions are spending a great amount of time and resources in order to explore and identify the potential applications of blockchain technology in order to exploit its opportunities at the maximum level. They have been investing in several different ways in this radical technology such as in start-ups where Goldman and Sachs have invested $50 m in only one startup company as well as Visa and NASDAQ giving $30 m in Chain.com. In addition, banks have been creating common initiatives in their endeavor to understand the underlying idea of blockchain technology and search for unified solutions with the most prominent example being the collaboration of the most powerful banks globally: Goldman Sachs, JP Morgan, Credit Suisse, Barclays, UBS, Commonwealth Bank of Australia, RBS and BBVA have invested millions of dollars in order to create a common standard to connect banks across the globe through a network of a shared infrastructure [21]. Moreover, just recently UBS made an agreement with Santander, BNY Mellon and interdealer broker ICAP to create a pioneering blockchain digital currency that they can use in order to speed up settlements and clear trades [22].

3.4 Blockchain and Financial Services

In addition to the outburst of banks in the Blockchain ecosystem, conventional financial services firms, including the New York Stock Exchange, Visa, and NASDAQ are also discovering innovative ways to leverage the technology. For instance, in October 2015, NASDAQ, the world's second major exchange in terms of market capitalization, launched Linq, a Blockchain-enabled platform [23]. According to the organization's press release, the new platform enables the "issuance, categorization, and recording of transfers of shares of privately-held organizations on The NASDAQ Private Market." Linq customers, which presently include ChangeTip, Chain, PeerNo-va, Synack, and Tango, are provided access to a "wide-ranging, historical record of issuance and transfer of their securities, offering amplified auditability, issuance governance and transfer of ownership capabilities" [23]. Consequently, this will develop the existing painstaking procedures where even the most clear-cut trades may necessitate weeks to complete due to the fact that paper certificates are still being utilized (ref).

NASDAQ is also investigating the likelihood of employing Blockchain-like ledgers to enhance the speed and reduce the price of trading in several other markets; as a result, facilitating the reduction of the counterparty risk of unfulfilled trades by diminishing the time delay between the implementation and settlement of a trade, and also releasing the insurance or collateral capital used to support business transactions. In a recent forum with investors, the organization's CEO, Robert Greifeld, mentioned, "Blockchain technology holds an enormous potential in allowing capital markets to operate more efficiently while at the same time providing greater clearness and security, all of which are essential to the public interest" [9].

Another financial firm, New York Stock Exchange (NYSE), has also been active in the implementation of Blockchain; they are a minority stakeholder in Coinbase and introduced the NYSE Bitcoin Index (NYXBT). NYXBT is the first exchange-calculated and distributed bitcoin index. A good example of non-bank financial services firms' activity in the Blockchain governance ecosystem includes Visa and NASDAQ's investment in Chain [24]. Chain's platform enables organizations to plan, install, and activate Blockchain networks that can power any kind of asset in any market and it is based on open source procedures to guarantee interoperability across systems and networks. In an attempt to speed up the implementation of Blockchain governance in the mainstream economy, NASDAQ and Visa alongside other key investors are setting up an operational group at Chain that is committed to researching and testing the technology in diverse markets [24].

A 2015 survey carried out by Swiss Fintech (see Fig. 3.5), an association that aims to serve as the hub for the Swiss fintech scene, found that among 265 respondents, the majority believes that Blockchain technology will most likely form the future of financial services (55), followed by payments innovations (37) and robo-advisors (35). Robo-advisors are online wealth management platforms that utilize technology to offer automated, algorithm-based portfolio management recommendation, reducing the need for intervention by humans [25].

As clearly seen, the benefits and practical applications of Blockchain governance are extensive: reliability, decentralization, simplification, transparency, traceability, cost saving, reduced room for error, faster transactions and improved data quality [26]. However, it is important to examine the specific use cases as Blockchain will change the Financial Services industry; hence the following subsection will discuss several use cases that represent challenges to such a vital industry sector.

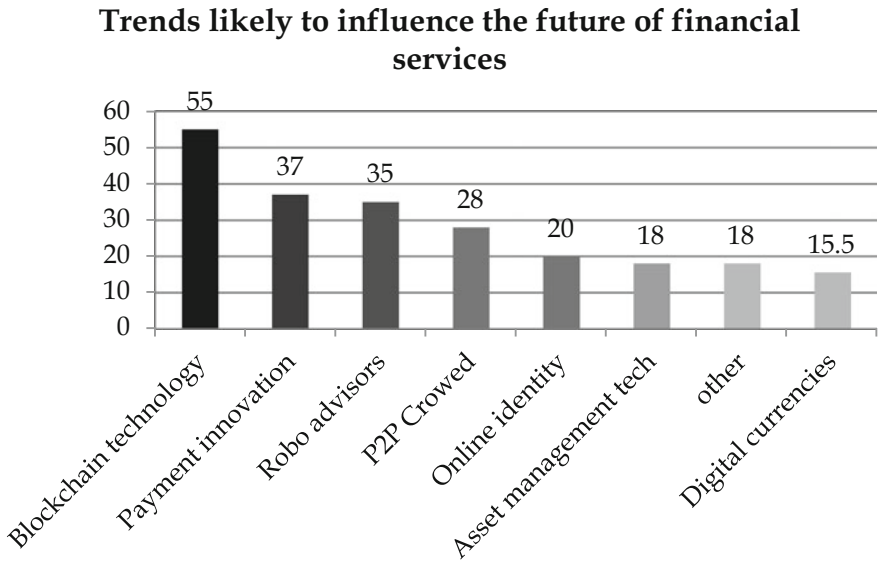


Fig. 3.5 Trends likely to influence the future of financial services. Adapted from [25]

3.4.1 Use Cases Challenging the Financial Services Industry

The following use cases describe the challenges that face financial services industry.

3.4.1.1 Use Case: Settlements

Traditional procedures of trading within asset management are relatively slow, burdensome and packed with risks when reconciling and matching. They are getting more intricate with cross border transactions and for non-standard investment commodities such as loans. Broker dealers, intermediaries, custodians and clearing teams in the trade lifecycle presently keeps their own copy of the same record of a transaction, creating major inefficiencies and room for inaccuracy. Blockchain technology would simplify this entire process, providing an automated trade lifecycle where all parties in the transaction would have access to the exact same data about a trade [27]. This would lead to considerable infrastructural expenditure savings, efficient data management and transparency, quicker processing cycles, least reconciliation and the possible removal of brokers and intermediaries in general [27].

3.4.1.2 Use Case: Claims Processing

Some of the major challenges experienced in the insurance sector today are falsified claims, labor-intensive processes, fragmented data sources, and legacy underwriting models, which results to extremely low customer satisfaction. Creating policies as smart contracts on the Blockchain is an ideal use case for insurance. It offers absolute control, precision and traceability for each claim and could lead to automatic payouts. Blockchain governance would also improve risk modeling for the sector, and significantly reduce fraudulent claims by capturing the origin and ownership of diamonds, paintings, homes, cars and other assets to be insured [27].

3.4.1.3 Use Case: Trade Finance

One of the most motivating opportunities for smart contracts and Blockchain is the revolution of the supply chain and trade finance. Existing supply chains are complex, time-consuming, scattered, involve many parties across the world and lack trust; thus the need for trusted third parties such as banks and clearing houses to intervene [18]. By implementing Smart Contracts automatically on the Blockchain to transfer descriptions to goods and money eliminates the necessity for banks to offer products such as Letters of Credit, significantly reduces costs by cutting out the middlemen and their associated fees as well as creating a trusted network of assured authenticity and origin of products being supplied [17].

3.4.1.4 Use Case: International Payments

The international payments sector is extremely large, however slow, expensive, prone to error and not entirely traceable which often results in money-laundering [27]. There is a desperate need for a stir and Blockchain is already providing

solutions for the financial industry. Lately Santander became one of the first banks to apply Blockchain to a newly released payments app, allowing customers to make international payments 24 h a day, clearing the next day [19]. However these little steps are; Blockchain will in due course enable banks to provide instantaneous payments at the same time reducing working costs, human fault and scam. Head of customer and innovation at Santander Sigga Sigurdardottir mentioned that Blockchain is the key to future services and the technology will play a transformational responsibility in the manner goals are achieved, customers are served and brand value is enhanced by creating more choice and convenience [27].

3.4.1.5 Use Case: Know Your Customer (KYC)

Financial organizations around the world are responsible for conforming and reporting on a number of business requirements from their local authority. One of the requirements, "Know Your Customer" (KYC) is incredibly time consuming and lack the automated customer identification technology and integration essential by teams to economically execute their work. Blockchain could provide a digital single source of identity data that allows for the flawless exchange of documents between banks and external agencies. This would possibly result in automated account opening, reduced resource and cost, though preserving the privacy of data that is lawfully required [27].

3.5 Case Studies

In this section, we provide a detailed description of two case studies for blockchain governance issues, which are Fatcom and Dash.

Factom (*factom.com*) is a very motivated Blockchain project undergoing development. The organisation is working on a system that secures and proves the legitimacy of records, documents or other vital data types. Factom consists of a four-tier structural design intended to produce confirmed chains of information and secure data inside the Blockchain [28]. They have a diversity of use cases, which includes producing trustless audit chains, maintenance of records for sensitive personal, medical and corporate materials, and identity management as a Know Your Customer (KYC) solution [28]. So far Factom have raised $1.7 m in their succession of funding, and presently valued $11 m [29].

One of the founders of Factom, Paul Snow mentioned that they are proposing to develop a node network with an infrastructure that can hold huge volume of transactions [9]. In addition, the structural design of the node network would consist of full nodes proficient of replicating all the data, and partial nodes replicating only the data essential in specific chains. Its preliminary Use case is a land registry idea developed in collaboration with the government of Honduras. Honduras has a history of land rights misuse, where fraud and unprofessional behavior have influenced a conflict over land civil liberties which have existed for decades.

Factom expects to develop a system that would enable the ease of storing proof of ownership in countries where government registries are missing or else lacking, but that their solution can extend to the rest of the world if successful [30].

Point of Attention Data integrity in governmental sector is an important issue that attracts great attention from many technological companies. To address the concerns surrounding this issue, a significant number of startup firms are investing in blockchain technology as it increasingly proves itself as a solution to improve the integrity of the governmental sensitive data.

Dash (*dash.org*), a new cryptocurrency that is based on Bitcoin and provides several privacy features, has lately included a decentralized governance system directly into its Blockchain. Similar to all Bitcoin-based cryptocurrencies, Dash creates new coins also known as "block rewards" on a usual basis, with the utilization of mathematical algorithms to decide who receives these new coins [31]. In Bitcoin, all the block rewards go to miners, i.e., those who program their computing systems to perform complex mathematical computations towards securing the Blockchain.

One of the immense challenges for open-sourced, decentralized projects is funding. Payments are needed for development, marketing, legal services and in the past, such projects depended on devoted volunteers or corporate funding. However, there are flaws both situations. In the first case, the whole project depends on the devotion and resources of a little group of supporters. Nevertheless they need to solve their personal financial challenges, just like everyone else. In the event that their devotion, or their bank account, runs dry there would be severe limitations in raising funds using this technique. The other likelihood—corporate sponsorship—has its risks as well. In this situation the apparently decentralized project is subject to the stockholders, of a centralized company. Their idea for the project may be different from that of the mainstream of the system's users.

Whereas with Dash the project factually funds itself; at present there is a budget proposal which pays for the salary of the core development team. As a result, on a monthly basis, if approved, the Dash protocol generates a set number of Dash which pays the core developers. It is far more ground-breaking than it first appears. Dash technology funds its own development. Projects other than core development can be funded as well. A healthy cryptocurrency environment involves numerous products and services that encircle the protocol itself. After all, if mobile wallets did not exist, for instance, the use of Bitcoin would not be very attractive. Using the Dash Bitcoin System, community members can recommend their own projects for funding. A good illustration of this was the creation of a Dash-powered soda machine ("Dash N' Drink"), which was introduced at the 2016 North America Bitcoin Conference [31]. This project allowed Dash's instant transaction attribute ("InstantX") to be highlighted in a real-world point-of-sale system. It was partly funded from the Dash Bitcoin System.

Point of Attention From this case, it is clearly seen that the practical applications of Blockchain-based governance are endless: marketing, new wallets, point-of-sale systems and much more could be funded straight from the Dash Blockchain.

A project needs not to rely on the selflessness of volunteers or the unfamiliar idea of corporate puppeteers in order to be successful. Dash, more or less like a living being, has the inherent capability to naturally develop on its own.

3.6 Summary

Blockchain governance has a tremendous transformative potential for our societies. However, the risks and benefits associated to its practical applications must be cautiously evaluated, avoiding un-realistic hopes, as well as the drawbacks of technocratic way of thinking. If correctly managed, decentralization of government services through permission Blockchain is promising and desirable, since it can amplify public administration functionality [19]. Decentralization of governance through open, distributed Blockchain like Bitcoin, nevertheless, presents severe risks and drawbacks, which offset the benefits. While initially designed as disintermediation tools, the environment of fully distributed Blockchain are categorized by a huge amount of third parties and money-making businesses contributing intermediation services, with strong asymmetries of information and power between developers and users [15].

The free nature of existing distributed networks call into question factors such as digital divide, unaccountable power of core developers, and lack of clearness in decision making process, thus making some Blockchain advocates' expectations overestimated and unrealistic [20]. There are hence reasons to investigate the role of the Blockchain-based governance as a large catalyst of individual power, in a complete sense. Furthermore, the promise of empowering individuals is likely to stay unfulfilled, due to the prevailing role of markets and the tentative verification systems of fully distributed Blockchain. On the other hand, the process of undermining public institutions, the superiority of economics over politics, and the change of citizens into costumers with the promise of more autonomy, effectiveness, and fairness may conceal yet an additional dangerous process of corporatization of politics, which perpetually empowers markets to the disadvantage of citizens. Far from being innovative, such transfer of power from public to private sector has been ongoing in different forms for decades, with vast social and economic costs.

Blockchain is paving the way for tech-driven financial innovation that is by now disrupting the banking and financial sectors. It is enticing to analogize this change to the computer processing revolution of the 1980s, but doing so would devalue the degree of the impending changes. When computers replaced paper in the back

offices of financial institutions, the fundamental processes stayed unaffected. For instance, the steps necessary to complete a securities trade are basically the same today as they were 50 years ago; computers only improved the trading speed. In contrast, Blockchain primarily reorganizes the operations of financial transactions in ways that was not envisioned just a few years ago.

In order for institutions to completely account for the profits and risks that Blockchain-based governance offers it will take some time; although few organizations cannot afford to wait for total clearness as the technology evolves and is deployed by their competitors. The swiftness of innovation will go faster as technology and financial services continue to come together, and success will repeatedly be determined by the ability to take sensible action founded on knowledgeable experience. Consequently, it is crucial for institutions to vigorously partake in this cycle of innovation and disruption to guarantee that they comprehend how technology is dynamically influencing the sector and that they are well-positioned to recognize and track opportunities as it evolves. Equally, it will be essential to realize that working to build up a perfect solution will be pointless if the challenge changes prior to the implementation of a suitable solution.

In the nearest future, we predict a reasonably multitude of changes and developments from Blockchain-based governance solutions. At the moment, the dawn of the Blockchain revolution produces challenges that lie ahead for financial services that will require new and innovative thinking. Blockchain is a radical technological innovation that offers a great amount of potential and opportunities to organizations. Success will depend on the risks that firms are ready to take as well as on the speed of their actions and decisions. It becomes apparent that the most successful firms will be those that will be able to outperform and distinguish among competitors during this Blockchain revolution [17].

In this chapter, the societal impact of decentralized blockchain governance and the associated challenges have been discussed. Moreover, it explained how banks and financial institutions are adopting and implementing blockchain-based solutions to improve their processes and the way they transact while explaining how this is reflected upon their existing products and services. Finally, the above conclusive remarks have provided an articulated summary of the overall issues and risks that Blockchain-based governance may produce and highlights a few methods to cope with such a huge technological disruption.

References

1. Atzori M (2015) Blockchain technology and decentralized governance : is the state still necessary ? Accessed 16 Sept 2016
2. Peters GW, Panayi E, Science C (2015) Understanding modern banking ledgers through blockchain technologies : future of transaction processing and smart contracts on the internet of money, pp 1–33. Accessed 16 Sept 2016
3. Lundström VK, Lundström VK (2016) Impact from the blockchain technology on the Nordic capital market capital market. http://uu.diva-portal.org/smash/get/diva2:937451/FULLTEXT01.pdf. Accessed 16 Sept 2016

4. Walport M (2015) Distributed ledger technology: beyond block chain. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. Accessed 16 Sept 2016
5. Lemieux VL (2016) Trusting records: is blockchain technology the answer? Rec Manag J 26:110–139. Accessed 16 Sept 2016
6. Wright A, De Filippi P (2015): Decentralized blockchain technology and the rise of lex cryptographia. Soc Sci Netw 4–22. Accessed 17 Sept 2016
7. Kiviat T (2015) Beyond bitcoin issues in regulating blockchain transactions. Duke Law J 65:569–608. Accessed 17 Sept 2016
8. Yermack D (2015) Corporate governance and blockchain. http://www.nber.org/papers/w21802. Accessed 17 Sept 2016
9. Froystad P, Holm J (2015) Blockchain: powering the internet of value. https://www.evry.com/globalassets/insight/bank2020/bank-2020—blockchain-powering-the-internet-of-value—whitepaper.pdf. Accessed 17 Sept 2016
10. Byström H (2016) Blockchains, real-time accounting and the future of credit risk modeling. In: Working paper/department of economics, school of economics and management. Lund University. Accessed 17 Sept 2016
11. Swan M (2016) Blockchain temporality: smart contract time specifiability with blocktime. In: International symposium on rules and rule markup languages for the semantic web, pp 184–196. Accessed 17 Sept 2016
12. BCS (2016) Blockchain—double bubble or double trouble? http://www.bcs.org/content/conWebDoc/55926. Accessed 18 Sept 2016
13. Christidis K, Devetsikiotis M (2016) Blockchains and smart contracts for the internet of things. IEEE Access 4:2292–2303. Accessed 18 Sept 2016
14. Manski S (2015) Building the blockchain: the co-construction of a global commonwealth to move beyond the crises of global capitalism. http://www.democracy.uci.edu/newsevents/events/gradconference16/CSDpaper%20-%20SarahManski.pdf. Accessed 18 Sept 2016
15. Silverberg K, French C, Ferenzy D et al (2015) Banking on the block chain reengineering the financial architecture, The Institute of International Finance (IIF), Inc., November 16, 2015
16. Peters GW, Panayi E, Chapelle A (2015) Trends in crypto-currencies and blockchain technologies: a monetary theory and regulation perspective. Available SSRN 2646618, pp 1–36. Accessed 18 Sept 2016
17. Petrasic K, Bornfreud M (2015) Beyond bitcoin: the blockchain revolution in financial services. http://www.whitecase.com/publications/insight/beyond-bitcoin-blockchain-revolution-financial-services. Accessed 18 Sept 2016
18. Philippon T (2016) The FinTech opportunity. http://pages.stern.nyu.edu/~tphilipp/papers/FinTech.pdf. Accessed 18 Sept 2016
19. Macdonald TJ, Allen D, Potts J (2016) Blockchains and the boundaries of self-organized economies: predictions for the future of banking, pp 1–16. https://www.weusecoins.com/assets/pdf/library/Blockchains%20and%20the%20Boundaries%20of%20Self-Organized%20Economies%20-%20Predictions%20for%20the%20Future%20of%20Banking.pdf. Accessed 19 Sept 2016
20. Lee S, Wang G (2015) Demystifying blockchain in capital markets: innovation or disruption? http://aitegroup.com/report/demystifying-blockchain-capital-markets-innovation-or-disruption. Accessed 19 Sept 2016
21. Deloitte (2015) Blockchain disrupting the financial engaging services industry? https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/IE_Cons_Blockchain_1015.pdf. Accessed 19 Sept 2016
22. Stafford P (2016) Banks struggle to make blockchain fast and secure. https://www.ft.com/content/e0a32840-4f68-11e6-8172-e39ecd3b86fc
23. Nasdaq (2015) Nasdaq Announces inaugural clients for initial blockchain-enabled platform "Nasdaq Linq". http://ir.nasdaq.com/releasedetail.cfm?releaseid=938667. Accessed 19 Sept 2016

24. Perez B (2015) New York Stock Exchange launches bitcoin price index. http://www.coindesk.com/new-york-stock-exchange-launches-bitcoin-price-index/. Accessed 19 Sept 2016
25. Finanzprodukt (2015) Swiss Fintech survey: blockchain tech will shape the future of financial services. http://www.finanzprodukt.ch/finance-2-0/swiss-fintech-survey-blockchain-switzerland-fintech/. Accessed 19 Sept 2016
26. Tapscott D, Tapscott A (2016) How will blockchain change banking? How won't it? http://www.huffingtonpost.com/don-tapscott/how-will-blockchain-chang_b_9998348.html
27. Chris Skinner (2016) The five major use cases for financial blockchains. http://bravenewcoin.com/news/the-five-major-use-cases-for-financial-blockchains/. Accessed 20 Sept 2016
28. Das S (2016) Bitcoin blockchain startup factom raises $4.2 million in equity funding. https://www.cryptocoinsnews.com/bitcoin-blockchain-startup-factom-raises-4-2-million-in-equity-funding/. Accessed 20 Sept 2016
29. Blockchaincan: blockchain can register physical assets. http://blockchaincan.com/project/case-25-blockchain-can-register-physical-assets/. Accessed 20 Sept 2016
30. Dale B (2016) Three small economies where land title could use blockchain to Leapfrog the US. http://observer.com/2016/10/benben-factom-bitfury-ghana-georgia-honduras/. Accessed 20 Sept 2016
31. Sammons E (2016) Rise of the machines: blockchain-based governance. https://medium.com/@EricRSammons/rise-of-the-machines-blockchain-based-governance-91d05a332cdb#.x4tcew1yy. Accessed 20 Sept 2016

The Security of Blockchain Systems

4

Abstract

The blockchain technology has been under intense research in the last decade. It is expected to revolutionize the nature of information sharing and transaction processing across computer systems. However, numerous issues have been made as to the security of and confidence in the blockchain architecture. Also, a series of cyber-attacks coordinated against various blockchain research centers and companies has highlighted areas of the blockchain technology that may be vulnerable to attacks in cyberspace. This chapter discusses the architecture supporting the blockchain and describes in detail how the data distribution is done, the structure of the block itself, the role of the block header, the block identifier, and the concept of the Genesis block. It then discusses that blockchain has security incorporated at main layers: Consensus, Mining, Cryptography, Propagation and Semantics. Subsequent sections discuss the challenges, advantages and limitations of blockchain from a security point of view.

4.1 Introduction

The blockchain is a form of technology combining peer-to-peer file sharing and key cryptography. Information systems in modern society are intact distributed and the network structure of the internet itself is a distributed system. Distributed systems are characterized by *geography*, *parallelism*, *reliability*, *availability*, and *mistrust*. The blockchain is a distributed ledger of blocks that hold valid transactions that have been executed in a network. Each block contains a timestamp of creation and a hash or pointer to the previous block which links it to the previous block. The continuous linking of blocks forms a chain.

V. Morabito, *Business Innovation Through Blockchain*,
DOI 10.1007/978-3-319-48478-5_4

Every peer in a decentralized peer-to-peer network has a copy of the latest version of the transaction ledger. Blockchain systems have an algorithm for scoring different versions of the transaction ledger so that the highest scoring version takes precedence. Peers in the network keep the highest scoring version at all times (which they currently know of) and overwrites their old version when a new version has a higher score. Each block is identified with a key hash using a crypto hash algorithm. It also has a reference to the previous block called its *Parent Block* [1]. Although each block can be linked to just one parent block and parent key hash, a parent block can have many children and all its children bear the same parent key hash.

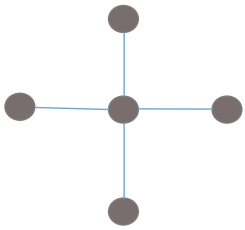
A blockchain can be seen as a container where data is stored. Everyone can verify that an individual owns the information inside the container because it has a signature on it but only the owner can access the information inside the container. In theory the blockchain behaves like conventional databases except that information stored is publicly visible but only privately accessible.

Mary wants to arrange dinner with Lian, and since both of them are very reluctant to use the "call" functionality of their phones, she sends a text message suggesting to meet for dinner at 6 pm. However, texting is unreliable, and Mary cannot be sure that the message arrives at Lian's phone, hence she will only go to the meeting point if she receives a confirmation message from Lian. But Lian cannot be sure that his confirmation message is received; if the confirmation is lost, Mary cannot determine if Lian did not even receive her suggestion, or if Lian's confirmation was lost. Therefore, Lian demands a confirmation message from Mary, to be sure that she will be there. But as this message can also be lost, you can see that such a message exchange continues forever, if both Mary and Lian want to be sure that the other person will come to the meeting point!

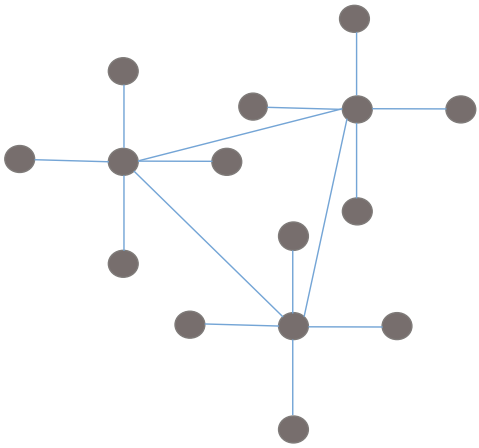
Similar to those configurations shown in Chap. 3, Fig. 4.1 shows the various networking paradigms; distributed networks, de-centralized networks and centralized networks. Distributed Networks, or in some cases, distributed computing network systems are systems where data and computer resources to be used in operational tasks are spread out on various hardware nodes or computer devices. This may also be seen as many computers working together towards a common goal. This is usually implemented over a network and all computers connected to that network play a specific role in delivering the final tasks.

In a centralized network, shown in Fig. 4.1a, all resources, computing servers and variables are stored on a single computer hardware. All other systems would have to connect to this single system to access these computing resources whenever they need it. Although this model gives a little bit more control in terms of administration, it has been criticized as not being transparent, stringent and un-inclusive. Moreover, centralized servers are high risk data breach targets as attackers not only expect to get all the information they need by hacking into a single node, but it is also time and cost effective from an attacker's perspective. It is simply less time to breach a single node than it is to write exploit for more than one node.

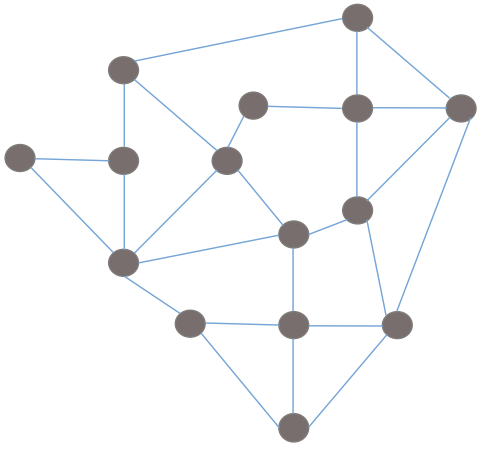
Fig. 4.1 Types of networks



(a) centralized



(b) de-centralized



(c) distributed

Decentralized computing allocates resources, hardware, software, computing power to individual work stations. Majority of functions are split between individual nodes and there is no need for everyone to access a single node to get a simple task done. The major difference between distributed and decentralized computing is in the manner of task distribution. The tasks are split up between nodes in a distributed network and all nodes are up-to-date with the current state of all other nodes. However, in decentralized computing, the resources are split up between nodes and each node queries for a resource and finds respective node on which needed resource exist.

An attacker's virus may probably spread faster on a decentralized network as he only needs infect one node and hope other nodes unknowingly copy these viruses to other systems via the resource sharing process. In a distributed network, nodes do not necessarily share resources but share tasks. In other words, they operate independently as part of a whole. Each node on a distributed network only needs information regarding the current state of all other nodes. This network infrastructure has been criticized as being underlying decentralized in its implementation but claiming to be distributed. If the synchronization mechanism is a copy and paste mechanism, then the idea of distributed is defeated.

Decentralized, distributed and centralized networks are all networking frameworks that work effectively in various business or industrial scenarios. The distributed architecture of the block chain network provides for independent exchange of information between nodes where one node does not depend on other nodes for information required. All nodes need only ensure they are up-to-date by syncing with all other nodes. Resources and computing power are not shared but are independently distributed across all node.

4.2 The Blockchain Architecture

The following paragraphs describe how the data distribution is done in an blockchain, the structure of the block itself, the role of the block header, the block identifier, and the concept of the *Genesis block*.

4.2.1 Data Distribution and Structure of a Block

Data distribution in a blockchain system is done using a peer-to-peer architecture. In peer-to-peer networks, each peer has a complete version of the data and the same data is replicated many times, one per peer. Every update creates a chain of communication across peers; however, each peer is independent of other peers and can continue to operate without the other peers. Most importantly, from a security perspective, given the decentralized nature of peer-to-peer networks, the absence of a central server makes it difficult for the network to experience attacks such as denial of service attacks or other client/server related attacks [6].

Considering now a *block*, it is a data structure that records transactions to be included in a public ledger. A block comprises of a *header*, which contains metadata of the block details, a list of valid transactions, the key hash of the previous block and its own key hash. A single block can contain more than 500 transactions and the number of transactions in each block is termed the "Block Height". The block header is 80 bytes and the average size of one transaction is 250 bytes [1] (Table 4.1).

As for the *block header*, if a block is altered, the hash of that blocks changes and the corresponding hashes of all other blocks in the chain changes as well. This cascading model of key hashes ensures that a block cannot be modified without forcing a change in at least 80% of the blocks in the chain. The huge computation required for a recalculation of every block in the chain makes the blockchain immutable which is a major factor of the blockchain security. It would seem as more blocks are added to a chain, the more secure it becomes as becomes difficult to alter. Cawrey noted that as the length of the blockchain decreases, the probability of a block being altered decreases [10] (Table 4.2).

As for *block identifiers*, the block header contains three sets of metadata; a reference to the previous block, information relating to the mining competition of the block and a summary of all transactions or entries in the block. Information related to the mining competition details the timestamp, difficulty and a proof of work. These concepts would be discussed later in this section [1]. It is worth noting now that the *genesis block* was established in 2009 [13] and refers to the first block in any blockchain. It is the ancestor of all blocks in a chain. The genesis block acts as a secure root to every node in a blockchain network and every node knows the key hash and block structure of the genesis block [1].

Taking the above issues into account, each new block added to a blockchain is placed on top of the previous and is one position higher than the previous block. Therefore, every block in a blockchain can be identified in two ways: its

Table 4.1 The structure of the blockchain, adapted from [1]

Size (bytes)	Name	Description
4	Block size	The size of the block
80	Block header	Information from the block header
1–9	Counter	How many transactions?

Table 4.2 The structure of the block chain header, adapted from [1]

Info size (bytes)	Field name
4	Version tracker
32	Previous block hash
32	Hash of block transaction summarization
4	Timestamp
4	Difficulty target
4	Proof of work by miners

cryptographic hash and its block height. Although the primary unique identifier of a block is its cryptographic hash created by the SHA256 algorithm, the position of the block in the chain or its distance from the genesis block can also be used to identify a block. This is however not unique due a concept called "blockchain forking" [4]. Two or more blocks can have the same height, which may also be stored in the blocks metadata or an indexed database.

Figure 4.2 represents a blockchain fork. Here, more than one chains, with the same genesis block get a forking point where they exist in parallel. If either one of these parallel chains are completely abandoned, a completely new network is formed. Whereas at block 6 in Fig. 4.3, a brand new network is formed as block 6 becomes the new genesis block. An accidental forks occurs as a result of incompatible coin mergers or coin software version control problem. Participants in a network may use various versions of the same software of which a problem is created when a bug in the previous version is encountered that does not happen the newer version. In such circumstances, the coin developer must decide how to quickly synchronize the chain by resolving the incompatibilities.

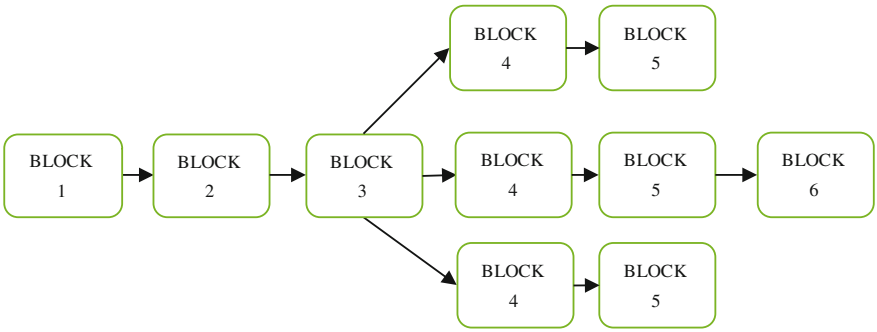


Fig. 4.2 Occasional blockchain forking [2]

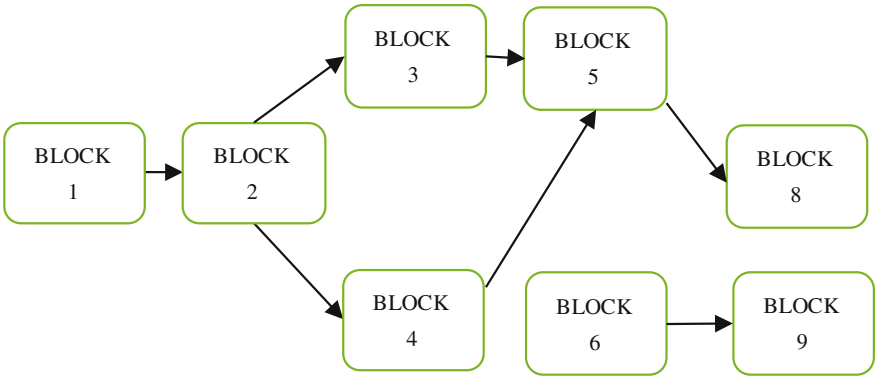


Fig. 4.3 Occasional blockchain forking: A new chain is formed; adapted from [2]

A hard fork occurs when compulsory changes need to be made to the programming or underlying technology of the block chain or transaction coins. After changes have been made, all users have to agree to make these changes for consistency and to continue to use the block chain properly. In cryptocurrencies, when two different blockchain exists, only one can in the end, be correct. This causes a controversy as this leads to an uncertainty as to which chain would eventually resolve to be the correct one. Eventually, coins in transactions in the wrong chain could ultimately be lost. During a forking event, participants are warned not to make transactions until the fork is resolved. For companies, organization and industries, forks are unfriendly as transactions could be lost in a forking event, so businesses using the cryptocurrency are immobile. Additionally, forks cause an enormous amount of workload as all participants' software, Coinbase, ledgers, miners, exchanges and associated resources have to be updated to the latest versions.

Any probability of lost coins can make cryptocurrency seem unattractive to users. Theoretically, if a forking event remains unresolved, this would lead to two different versions of the coin which may affect the value of the cryptocurrency. This is usually unacceptable in the world of cryptocurrencies and users frown upon currencies that are victims to occasional forking. Any potential for lost transactions make the block chain participants uncertain about the value of their coins or if some or all of their coins may get lost in the fork reconciliation process. A particular cryptocurrency might begin loosing a lot value if block chain forking becomes a regular phenomenon in its processes. Therefore, a permanently forked cryptocurrency would eventually become worthless as it would loose customers and its trust-worthiness. Alternatively, a fork can be a good buying opportunity if the fork puts in the currency's long term survival risk into consideration. The coin value falls during a forking event, however it gives if the coin stability and risk assurance is improved over time, investors may buy coins at low value with hopes of a value pump when the currency gains momentum.

Finally, the blockchain is designed to run a *peer-to-peer network* on top of the Internet. A peer-to-peer network means that computers talk to each other directly without the need of a central server for information exchange. In this model there are no special nodes or hierarchy and each nodes requests information directly from respective nodes. Peer-to-peer networks are therefore decentralized and open. The "Blockchain Network" is therefore simply a collection of nodes running a block chain system protocol with decentralization of control as its core principle. Nodes in a peer-to-peer network may be decentralized but in a traditional blockchain system, they take up different roles depending on their respective functions in the blockchain. A blockchain network mainly has to route information across nodes, manage a database of stored information, perform mining tasks and maintain a service for user interfaces e.g. a wallet service. To this effect, each node in a blockchain may act as a miner or a database or a wallet and a routing node. All nodes perform the routing functionality to participate effectively in the blockchain.

4.3 Layers of Security in a Blockchain Network

Security and privacy in a blockchain network is implemented via a layered approach. These layers include *Consensus*, *Mining*, *Propagation and Semantics*. Recently, a series of cyber-attacks on digital currencies has drawn attention to the vulnerabilities of the blockchain technology. The blockchain as a technology eliminates the need for a central verification during communication within a network. After the DAO and Bitfinex was robbed of $50 m and $150 m respectively during a series of cyber-attacks, the security concerns of the blockchain technology became apparent. Some of the causes identified by Stefan Thomas the CTO of Ripple is the newness of programming code behind the technology. Therefore, it is difficult to anticipate or track possible attacks as these methods would be relatively new.

As said above, blockchain technology as it exists today, has security incorporated at the already mentioned main layers: Consensus, Mining, Cryptography, Propagation and Semantics. However, it is important to define a process at the center of blockchain technology; *transactions* and message transmission on the Internet. These are explained in the next subsections.

4.3.1 Transactions

In terms of digital currencies, transactions occur when certain member/members of a blockchain network authorize the transfer of digital currencies to another within the same blockchain network or another. The authorization of transfer of digital currencies may also be seen as the authorization of transfer of ownership. Blockchain transactions are similar to what one finds in a standard double-entry ledger [5]. Every transaction contains at least one input or debit request and at least one output which credit requests are. Transaction operations move digital currencies or values of digital currencies from one input to output or form sender to receiver. When an owner authorizes a change of ownership on digital currencies, the transaction output receives this message and assigns a new owner (the receiver) to the digital currency by associating it with a key [1]. Credits from one transaction cab be propagated as inputs of another transaction thereby creating a transaction chain or a chain of ownership. How is data transmitted in cyberspace? On the physical layer of cyberspace, the wireless and wired connections hold the infrastructure that supports communication on the internet. The network manages node addressing and routing between different nodes in the network. The transport layer manages transmissions and connection states and protocols e.g. TCP, HTTP, HTTPS, SSH [15]. Similarly, the blockchain network works in the same fashion. However, unlike in a standard internet network where central nodes may be assigned for specifically performing these tasks, in a blockchain or a distributed network, participating every node perform all of these functions needed to keep the network running.

4.3.2 Consensus

A consensus algorithm allows for users to securely update states using pre-defined state transition rules where the rights to state transitions is distributed to all nodes in a securely decentralized network [12]. Consensus provides a protocol by which new blocks are allowed to be added to the ledger. For the concept of consensus to be effective, three things are needed: (i) common acceptance of laws, rules, transitions and states in the blockchain; (ii) common acceptance of nodes, methods and stakeholders that apply these laws and rules; (iii) a sense of identity such that members feel that all members are equal under the consensus laws. The basic parameters of a consensus mechanism are as follows:

- *Decentralized governance*: No single central entity or authority can finalize any transaction or process.
- *Quorum structure*: Nodes in a consensus mechanism exchange messages in a pre-defined set of stages or steps.
- *Authentication*: This protocol provides means to verify the participants' identities.
- *Integrity*: It enforces the validation and verification of process integrity.
- Nonrepudiation: This provides means to verify that the supposed sender really sent the message.
- *Privacy*: This protocol ensures that only intended recipients of a message have access to and can read the message.
- *Fault tolerance*: The speed and efficiency of network operations in such a way that network operations are not dependent on the non-failure of any specific node or server [16].

Taking these parameters into account, the main types of consensus are briefly discussed in what follows.

4.3.2.1 Proof-of-Work Consensus

With Proof-of-Work Consensus, the miners create a proposed block with transactions and calculate the hash of the block headers. Then, the miners match this hash to the intending target or the last block of the desired blockchain. If the hash does not match, it repeats the calculation but with an adjusted cryptographic pseudo-random number called a '*nounce*'. Nounces are used to vary the input of the cryptographic function until a match is achieved. A nounce can only be used once and is usually updated by simply incrementing by one. The new block may be added to chain when a match is found.

4.3.2.2 Proof-of-Stake Consensus

With Proof-Of-Stake Consensus, stakeholders with the highest incentives in the system are identified and only these stakeholders participate in mining [15]. Active participation in the blockchain networks gives participants the rights to generate new blocks for the chain. Blocks are generated similarly to the Proof-of-Work

methodology except hashing operation is done in a limited search space rather than the computationally intensive unlimited search space [8]. This lack of need for computational capacity creates a free pass on the need for possible hardware centralization.

4.3.2.3 Practical Byzantine Fault Tolerance

The Byzantine fault tolerance can be attributed to a form of distributed consensus and is peculiar to distributed networks. In a blockchain network, each node broadcasts a public hashed key. Transmissions flowing through each node is signed and verified by the node in relation to formats and content. Once a considerable amount of responses to the transmission as it passes through is reached, a consensus is achieved and the transmission is deemed valid. This method eliminates the hashing protocol and works well with low-latency storage systems. This architecture can manage digital assets little throughputs but large number of transactions [20]. Also, trust or mistrust is independent of resource ownership making the relative size or power of ownership irrelevant.

4.3.3 Mining

Mining in blockchain technology, refers to the distributed computation performed on each block of data in a chain that allows for the creation and addition of new blocks to the chain [7]. Beside the creation of new blocks, miners also serve the following purpose:

(a) Secure the blockchain against fraudulent or unverified usage.
(b) Miners provide processing power to the blockchain network.
(c) In the case of digital currencies, miners are solely in charge of validating new transactions and adding them to a global ledger.

For their mining activities, miners receive new currencies and transaction fees as rewards. To complete a task, miners have to solve a difficult mathematical problem based on a hashing algorithm. The solution is called the "proof-of-work" and this is included in the new block created. Since each miner has to work to solve mathematical problems before rewards are given, a competition is created. The mining process creates new currencies in each block. Transactions are propagated through the network but are not added to the blockchain until verification has occurred. Mining ensures trust by ensuring that sufficient computational is devoted to the creation of each block. Therefore, the number of blocks, the complexity of computation and the level of trust are all directly correlated. A transaction usually all information necessary for processing itself, therefore it does not matter where on the network it is transmitted through.

4.3.4 Information Propagation and Immutability

How is information or data propagated through a blockchain network? Propagation is the distribution of a transaction or block throughout the network. It is like-broadcast or replication model. Node1 may send a message or transaction to Node2, which is any of the other nodes in the network. Node1 does not have to be directly connected to Node2. Any network node that receives a new transaction or message forwards it to all other nodes on the network it is directly connected to, thus propagating the new transaction across all nodes in the network. In this area, the question of propagation speed is raised [11].

Thus, while the propagation from, e.g., Ade to Yu in the diagram in Fig. 4.4 may occur within seconds, the speed at which this propagation occurs has also been studied by researchers and adversaries for possible vulnerabilities. In typical block chain architectures, security is built at the consensus layer by ensuring that the node cannot be fooled into accepting a version of the ledger that is not true [14].

As for immutability, the term 'immutable' means that something cannot be changed over time or the values remain the same over a specific period of time. In the context of block chains, data already written into data blocks cannot be changed by anyone even an administrator. The process of a single rewrite is tedious and would require a consensus from every member of the chain. One would have to persuade every single participating member to make a single change. Collaborative consensus of every participating member is needed. Any attempt to modify the contents of any single block or transaction in a block would require a re-calculation of the block's key hash. A recalculation of the any block's key hash would also lead to a break in the entire chain as blocks are linked via their key hashes.

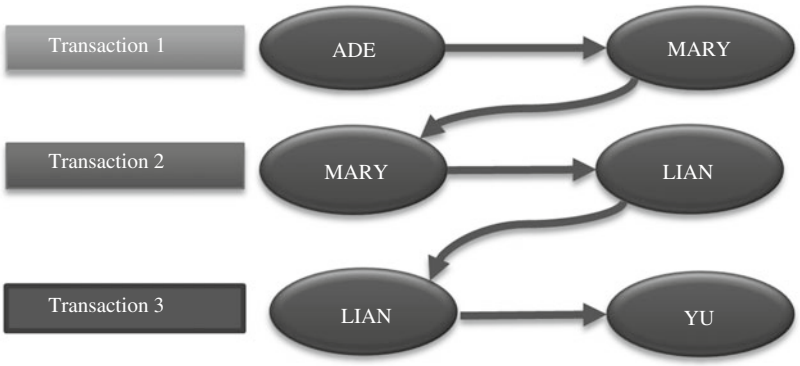


Fig. 4.4 Example of propagation as distribution of a transaction or block throughout the network. Adapted from [9]

4.4 Blockchain Security Challenges

The blockchain is a distributed file system or a shared data structure built on the concepts of "mistrust". Its architecture provides a solution to the management of transaction files across multiple systems. A transaction ledger is created and propagated throughout the network and each participant has an exact copy of the ledger at all times. Participants do not need to know or trust each other. This public log of digital transactions is called the blockchain. The blockchain is secured by a chain of cryptographic puzzles solved by organized miners. The miners are little algorithms in charge of recording transactions in the blockchain. When a miner solves a puzzle, it is given permissions to record a set of transactions in the shared ledger. The blockchain stores transactions in blocks where each block has a unique ID and the unique ID of the previous block. A valid block contains a solved crypto puzzle, the hash transactions of the previous and current blocks and a transaction address to be rewarded for mining. Taking these issues into account, a set of blockchain security challenges is outlined in what follows.

4.4.1 Distributed or Replicated?

One major criticism of the blockchain infrastructure from field engineers is the issue of replication and duplication. A distributed system or network relies on two processes mainly to ensure consistency across all participating members of the network; replication and duplication. While duplication searches across all nodes for changes to a shared file in all nodes, replication on the other hand recognizes one node as the master and updates all other nodes with reference to that node. The replication process has been criticized as being over-whelming complex, computationally intensive and time consuming. The duplication processes however an easy fix for the criticisms of the replication process may cause further problems when put in context of blockchain networks. During the implementation of a blockchain infrastructure, the duplication process simply identifies one node at any given time as a master node. This would therefore revert back to the idea of disguised central databases [17].

4.4.2 Monopoly of Miners

The process of mining is run and managed by participants in a group. Although the system assumes a decentralized model where participants are unknown to each other, researchers, [21], Eval and Sirer [9] have strongly argued with the monopolization of mining and the creation of numerous malicious miners by a cooperating group of individuals. Furthermore, recent contributions from industrial research have shown that the blockchain network is not totally incentive-compatible (see, e.g. [17]). That is, the network creates an incentive for miners to follow set

protocols thereby working under the assumption that they would be honest or accept such incentives. While minority groups cannot own a huge percentage of the computational power, rational miners would prefer to join selfish miners. This process occurs gradually until the minority group becomes a majority and eventually controls a huge percentage of the computational power.

4.4.3 Double Spending

A double spend is as a result of an inconsistent node state. A double spend is a situation where nodes attempt to create multiple transactions on the same output or credit [19]. A double-spend may be unintentional or intentional. When multiple nodes co-own the same outputs however only one transaction can be valid for that output. In an intentional double-spend attack, an attacker may transfer an output to the victim only to create another transaction with the same output back to itself. By default, a node considers the first transaction to be valid when two conflicting transactions are seen. However, the order in which the transactions propagate may not be same for all nodes. Therefore, a conflict resolution mechanism is adopted.

4.4.4 Gossip Networks versus Point-to-Point

Richard Gendal Brown, chief technology officer at R3, points out that the start-up was building a blockchain-style distributed ledger for regulated financial institutions, where everyone has to be identified with keys on the network [22]. Although authentication is a challenge for every network, according to Brown R3 aims to address it by limiting the spread of information about transactions. “We took a very different design choice and said, ‘we are not a gossip network where we send data to everyone’. We have more traditional architecture point-to-point messaging, sending information only to those who need to validate the transaction” [22].

4.4.5 Permissionless Versus Permissioned Consensus

In a permissionless consensus, in order to contribute to the processing of transactions and vote, a person does not need a previous relationship with the ledger and each vote does not depend on some prior identity for the vote owner within the ledger. In a permissioned consensus, only those already validated and recognized within the ledger are allowed to participate in the validation processes of transactions within the chain. Although both models have their pros and cons, the permissioned consensus operates a closed model where only participants are allowed to make decisions on what happens within the chain. Only participants have control over the decisions and validation of transactions within the chain.

4.5 Case Studies

In this Section we investigate two case studies that highlights the security vulnerabilities of the block chain technology. The first case study is about the DAO, a Decentralized Autonomous Organization that focuses on the creating codes for rules and decision making activities of an organization. The second case study is about *ransomeware*. These are detailed next.

The DAO focuses on the creating codes for rules and decision making activities of an organization. This process eliminates the need for documents and people in governing creating a true decentralized organizational structure. The idea behind the DAO is a system that is independent of people or document influence in the decision making of company structures especially with regards to finances (Figs. 4.4 and 4.5 shows an example of how the DAO works). To this end, tokens give the rights to vote but do not represent equity shares as the DAO, for most of its parts belongs to no single entity. During the DAO's initial launch, it raised over $150 m through crowdfunding. Hackers were able to exploit a 'recursive calling bug' to withdraw money from the DAO's account. At the end of this hacking exercise, $40 m dollars had been stolen and the price for DAO tokens fell 70%. The exploit most importantly, discredited the notion of 'immutability' of block chains [23].

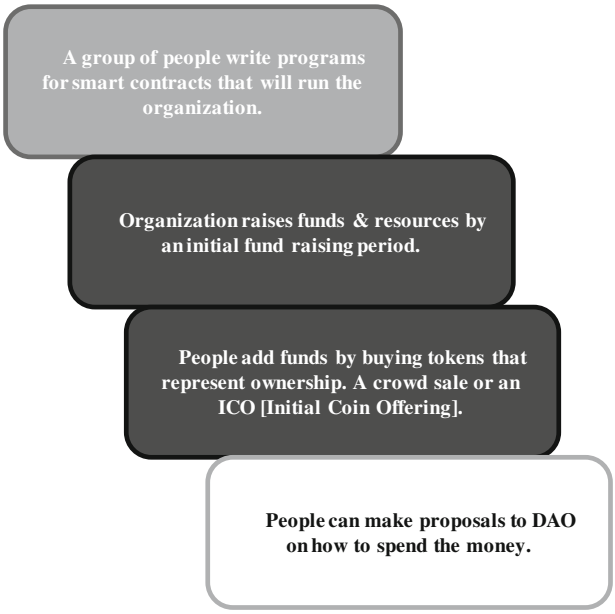


Fig. 4.5 How the DAO works

Point of Attention This case study shows how distributed ledgers (blockchain) can be utilized to develop more competitive energy retail market by empowering the consumers with more information that can enable them to have wide choice of action. The benefits of such vision are so promising, hence, they further investigation is required. However, there are still questions about the scalability, security and stability of such applications that need to be addressed.

The exploit allowed the hacker the move funds into another smart contract from where he can start up a parallel process of exchange and bidding. As for the attack, [18], analyzed the details of the attacker's steps in manipulating the information of the block chain. A subset of the token holders in the DAO's chain decided they wanted to split either to withdraw their funds of did not agree with the current proposal. The way to implement this is by using split proposals in the block chain [3]. Split proposals create a mini version of the mother chain and participants are allowed to create their own splits once they acquire voting rights and vote 'yes'. The split occurs and all coins and rewards controlled by the participants of the new split would be sent to the new split chain.

The attacker was able to exploit this process by creating a split, transferring tokens and voting 'yes' multiple times. With every step, he is able to use the same tokens to restart this process.

Not only has the blockchain technology been a victim of cyber-attacks, it has also been used as an attack vector in propagating cyber-attacks. A ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid [24]. Interestingly, ransomwares have become an effective cyber-attack tool especially in cases of cyber hacktivism or cyber warfare. in Its present form, it has mostly been targeted at individuals, however researchers have predicted that these tactics will definitely be targeted towards businesses and organization if not checked. This scam is perfectly explained in Gavin and McDonald's 2012 paper "*Ransomware: a growing menace. Symantec Corporation*" [25].

Blockchain technology is now also used as a payment mechanism for demanding digital ransoms from individuals and organizations. A version of such ransomwares emerged recently, with the sole purpose of encrypting websites. Although researchers report that this has not been as successful as the attackers had hoped, the possibilities and relentlessness is glaring [25].

The CTB-Locker for websites is a variant of ransomwares focused on compromising, accessing, manipulating and encrypting servers and configuration files that keep a website online [26]. The CTB-Locker for websites uses the blockchain technology in implementing its extortive capacities. In 2014, a new feature was introduced to the blockchain technology which made the technology applicable to other fields besides digital currency [26]. This feature allows small blocks of

metadata to be included in OP_RETURN field which is a scripts used to invalidate invalid transactions. This feature, although irrelevant to the blockchain itself.

What makes CTB-Locker for Websites interesting, however, is the fact that it uses blockchains, which are chains of verified transactions used in the Bitcoin world, to transmit decryption keys. Since blockchains are public, they can be tracked by anyone, and specialized services exist that allow users view Bitcoin blockchains.

Point of Attention "Even smart use of a new technology is not a guarantee of success when you are porting a tried-and-true business model from one niche to another. The devil is in the details" [26]. Your blockchain technology can be a target victim of cyber-attacks and also used as an attack vector (relevant to insider threats and blockchain breach). This process is open and transparent and can be targeted at any organization or individual.

The ransomware authors start by creating a new bitcoin wallet with a unique address for each hijacked website and publish this address to the ransom demand page. The wallet's blockchain is appended with a new transaction when the victim pays the ransom sum. The OP_RETURN field of the new transaction contains the decryption key to put the website back online [26]. The OP_RETURN transaction is validated and propagated through distributed nodes of the Bitcoin system, and it also becomes visible in services that provide information on blockchains.

This method becomes popular as the use of blockchains to transmit decryption keys is more reliable and secure than using third party services or third party websites. Moreover, the CTB-Locker for websites also reads the keys directly from public, which makes the entire process transparent, also keeping things anonymous and not traceable to real IPs.

4.6 Summary

This chapter starts by examining the architecture supporting the blockchain by looking at how the data distribution is done, the structure of the block itself, the role of the block header, the block identifier, and the concept of the Genesis block. It then discusses that blockchain technology, as it exists today, has security incorporated at main layers: Consensus, Mining, Cryptography, Propagation and Semantics. These two set the basis for looking at the challenges facing this technology.

The block chain security is a complex multi-layered inter-connected problem. Like every transaction payment, it is vulnerable to problems of authentication, verification and authorization and transaction propagation speed. The computational resources required to pull-off of a blockchain mining exercise that ensures no

self-miners is cumbersome and may not be feasible for everyday consumers of the technology. Distributed networks also have the tendency to be 'overly connected' with limited management of the 'need-to-know' information model. This may seem like a transparent system, however information regarding certain processes in the chain needs to be managed and dissemination properly.

References

1. Antonopoulos, Andreas M (2014) Mastering bitcoin: unlocking digital cryptocurrencies. O'Reilly Media, Inc
2. Pilkington M (2016) Blockchain technology: principles and applications. In: F. Xavier Olleros and Majlinda Zhegu (ed) Research handbook on digital transformations. Edward Elgar, Cheltenham, UK, p. 225
3. Croman K et al (2016) On scaling decentralized blockchains. In: Proceedings 3rd workshop on bitcoin and blockchain research
4. Vukoli M: The Quest for scalable blockchain fabric : Proof-of-Work versus BFT replication. In: Lecture notes in computer science (including subseries Lec)
5. Sompolinsky Y, Zohar A (2013) Accelerating bitcoin's transaction processing. Fast money grows on trees, not chains. IACR Cryptol ePrint Arch 881: 1–31
6. Ben-Sasson E et al Zerocash: practical decentralized anonymous e-cash from bitcoin. In: Proceedings of the 2014 IEEE symposium on security and privacy
7. O'Dwyer KJ, Malone D Bitcoin mining and its energy footprint. In: 25th IETIrish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014), pp. 280–285
8. King S, Nadal S (2012) PPCoin : peer-to-peer crypto-currency with proof-of-stake. Ppcoin Org
9. Eyal I and Sirer EG (2014) Majority is not enough: bitcoin mining is vulnerable. International conference on financial cryptography and data security, Springer Berlin, Heidelberg
10. Cawrey D (2014) Are 51% attacks a real threat to bitcoin?, http://www.coindesk.com/51-attacks-real-threat-bitcoin/. Accessed 19 Nov 2016
11. Decker C, Wattenhofer R (2014) "Information propagation in the Bitcoin network," IEEE P2P 2013 Proceedings, Trento, 2013, pp. 1–10. doi: 10.1109/P2P.2013.6688704
12. Buterin, V: A next-generation smart contract and decentralized application platform. Etherum. January, 1–36 (2014)
13. Barber S et al (2012) Bitter to better—how to make bitcoin a better currency. In: Financial cryptography and data security, pp 399–414
14. Babaioff M et al (2012) On bitcoin and red balloons. ACM SIGecom Exch 1(212):56–73
15. Crosby M, Nachiappan Pattanayak P, Verma S, Kalyanaraman V (2015) BlockChain Technology—bitcoin, beyond. Sutardja Center for Entrepreneurship & Technology, Berkeley, US
16. Samman G, Sigrid S (2016) Consensus immutability for governance of the internet of value
17. Biella M, Zinetti V Blockchain technology and applications from a financial perspective, Unicredit technical report (2016). Available at http://www.the-blockchain.com/docs/UNICREDIT%20-%20Blockchain-Technology-and-Applications-from-a-Financial-Perspective.pdf. Accessed 19 Nov 2016
18. Vessenes P Deconstructing the DAO attack: a brief code tour, http://vessenes.com/deconstructing-thedao-attack-a-brief-code-tour/. Accessed 19 Nov 2016
19. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. Accessed 4th January 2017
20. Castro M, Barbara L (1999) Practical byzantine fault tolerance. OSDI

21. Decker C, Seidel J, Wattenhofer R (2016) Bitcoin meets strong consistency. In: Proceedings of the 17th international conference on distributed computing and networking. ACM
22. Kuchler H (2016) Cyber attacks raise questions about blockchain security. [online] Financial times. Available at: https://www.ft.com/content/05b5efa4-7382-11e6-bf48-b372cdb1043a. Accessed 29 Oct 2016
23. Siegel D (2016) Understanding the DAO attack. Available at http://www.coindesk.com/understanding-dao-hack-journalists/. Accessed 19 Nov 2016
24. Zvelo (2016) Definitions of the malicious web—malicious software. Available at https://zvelo.com/wp-content/uploads/2015/11/zvelo-Definitions-of-Malicious-Web.pdf. Accessed 19 Nov 2016
25. O'Gorman G, McDonald G (2012) Ransomware: a growing menace. Symantec Corporation. Available at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf. Accessed 19 Nov 2016
26. Sinegubko D (2016) Website ransomware—CTB-locker goes blockchain, Sucuri Blog. Available at https://blog.sucuri.net/2016/04/website-ransomware-ctb-locker-goes-blockchain.html. Accessed 19 Nov 2016

Part II
Bitcoin Phenomenon and Trends

Digital Currencies

5

Abstract

Digital currencies are an innovation in payment systems. They are an internet-based medium that serves as an alternative medium of exchange. Many experts and advocates of this technology argue that this innovation in payment systems could have an immense significance on the financial system and the economy at large. There are various examples of digital currencies such as Litecoin. Litecoin is a recognized digital currency that uses peer-to-peer technology in its operation. It is entirely decentralized and has easier mining compared to others. Bitcoin is another example of digital currencies and could be said to be one of the most widely used innovative payment network. It is known to be easily convertible and the creation of accounts is free of any form of charge. Furthermore, the mode of operation of Bitcoin is referred to as 'peer-to-peer technology'. More examples of digital currencies include; Chinacoin, which can generate 462.5 million coins and Devcoin, which can generate 7.2 million coins daily. Despite the uniqueness of digital currencies such as Litecoin, Bitcoin and other digital currencies, some risks could be involved in its use. Such risks as well as the advantages of the usage of digital currencies should be analyzed in order for organizations to guard against such risks and embrace the advantages. This Chapter thoroughly examines the concept of Digital currencies as well as its advantages, limitations and risks.

5.1 Introduction

With the present growth and developments in mobile technology and software, there have been extensions in the meaning of money. Money has been seen to not only be a form of physical tender, but has now included digital currencies and mobile form of payment [1]. Some years ago, digital currencies were seen as

V. Morabito, *Business Innovation Through Blockchain*,
DOI 10.1007/978-3-319-48478-5_5

innovations for the future. Now, digital currencies have been embraced by a wide range of businesses from public trading companies to online businesses [2]. However, the evolution of payment technologies has been outstanding. Before the emergence of digital currencies as a payment technological innovation, there have been several other innovations. One of such innovation is *mobile money*, which converts money as mobile credit and is hugely dependent on national currency.

The digital currencies mainly those that make use of the distributed ledger (in which their mechanism of payment is decentralized) could be said to be an immense technological innovation that would have tremendous effect on so many areas of finance as it relates to the economy. The interruption to the usual flow of existing business systems as well as business models could be said to be one of such tremendous effects [3].

Furthermore, some other effects of digital currencies are to help bring about fresh economic exchanges, associations as well as relationships and help make transactions faster and more cost effective for the consumers and other end users. All these tremendous effects brought about by digital currencies have been as a result of the concept of 'distributed ledger' that has been incorporated by digital currencies and this makes it possible for digital currencies to work in an entirely decentralized payment system as Ali et al. [4] pointed out that distributed ledger has been the key ingredient behind the success of digital currencies.

In addition, there are lots of examples of digital currencies. Such examples include; Bitcoin, Altcoin, Ethereum, Feathercoin, Ripple, Namecoin, Litecoin, Chinacoin, PPcoin, Groupcoin and Zen. These aforementioned examples and other examples of digital currencies would be critically looked into later in this book.

Any form of currency including digital currencies must have its specific features. Moreover, digital currencies such as Bitcoin have some features such as ability to have no intrinsic value (in which demand and supply are the determining factors of its value), its increasing ability to be used as a medium of exchange, its ability to serve as an asset among other features.

There has been an increasing market for digital currencies especially Bitcoin as digital currencies have free entry characteristic. As much as the market for digital currencies is increasing, there is an urgent need to look critically at its advantages and disadvantages as well as the risks and limitations brought about by its use. This Chapter provides a detailed view on these topic ideally completing what discussed in Morabito [5].

5.2 Understanding the Concept of Digital Currencies

In economics the ability of any currency (both digital and physical currencies) to serve as a medium of exchange for goods and services rendered, as an asset and as transferrable assets makes such currency acceptable.

Digital currencies came to being in the 1990s and E-Gold, was operated by a sub-division of E-Gold Ltd called Gold and Silver Reserve Incorporation came to being in 1996 as the first set of digital currencies to ever exist. On the E-Gold website, E-Gold permitted intending users to open an account [6]. Based on grams of precious metals such as gold, these accounts were designated. Also, Liberty Reserve, which is one of the first set of digital currencies to ever exist, came into being in 2006. Liberty reserve allows the conversion of Euros or Dollars to its form in Euros or Dollars by its users. This form of Liberty reserve is referred to as Liberty Reserve Euros and Liberty Reserve Dollars. It should be noted that both Liberty Reserve and E-gold offered centralized services. Moreover, in 2005, QQ coins emerged and it served on the Tencent QQ's platform for messaging as digital currency. They were highly efficient to the extent that they made Yuan unstable as a result of assumptions.

Thereafter, Bitcoin came to being. Bitcoin initiated its operation in 2009 and has not looked back since then. It is the leading and most widely accepted digital currency compared to other examples of digital currencies such as Litecoin, Chinacoin, Namecoin, Devcoin and a host of other digital currencies. The scheme of Bitcoin is based on the concept of 'Distributed Ledger'. Bitcoin is not left alone in the use of this scheme as hundreds of the other forms of previously existing, presently existing and presently developed digital currencies make use of this scheme (Distributed Ledger) [3]. A 'Distributed Ledger' is an electronic financial record that is loaded with information that is encrypted with regards to the transfer of digital currencies and then propagated via a congested network system [7]. This encrypted electronic financial record is made up of a lot of blocks that are connected and is otherwise called 'Blockchain' [7]. Before we go further into this book, it is of utmost importance to look into the categories of digital currency as well as some of the various examples of digital currencies to ideally complete what was discussed in [5].

5.3 Categories of Digital Currency

There are basically two categories of digital currency as highlighted by the European Central Bank. These two categories are: Electronic Money (*E-money*) and *Virtual Currency*. Both E-money and Virtual Currency have various different characteristics. Table 5.1 shows the characteristic similarity and differences between E-money and Virtual Currency as specified by the European Central Bank. As can be seen from Table 5.1, both E-money and Virtual Currency have various varying characteristics but only share one similarity. This similarity is the digital format of both E-money and Virtual Currency. With regards to their varying characteristics, it can be seen from Table 5.1 that with respect to unit of account, E-money is characterized by the use of traditional currency such as Euros, US Dollars, Pounds, Yen, Australian Dollar, Dirham, Rupee and a host of other

traditional currencies while virtual currency is characterized by the use of invented currencies such as Linden Dollars, Bitcoins and other invented currencies.

Furthermore, E-money has legal tender status which makes it function like physical currencies (physical money) whereas virtual currency has no legal tender status. E-money can be regulated and supervised while virtual currency can neither be regulated nor supervised. Also, E-money is guaranteed and can be issued by legally established electronic money institutions while virtual currency is not guaranteed and can be issued by non-financial private companies.

5.4 Examples of Digital Currencies

There are various examples of digital currencies. Some of these examples are discussed as follows.

Litecoin was launched in 2011. It was created by Charles Lee. It is a Bitcoin fork and it uses "*scrypt*" algorithm as a function for the 'proof of work'. Its coin limit is 84 million. It has a mean block time of 2.5 min (150 s).

Furthermore, another example of digital currencies is Peercoin, which came into being in 2012. It has a higher speed than Bitcoin. It uses the 'proof of stake' protocol, which demands less computation compared to the 'proof of work' protocol used by Bitcoin. The 'proof of stake' protocol permits participants on the Peercoin platform to have a share of the rewards obtained through mining without being a part of the mining pools. The protocol used by Peercoin makes it less prone to collusive attack since there are no mergers of miners into larger pools [8].

Table 5.1 European central bank categorization of digital currency

Characteristics	Electronic money schemes	Virtual currency schemes
Money format	Digital	Digital
Unit of account	Traditional currency (British Pounds, US dollars, Euros and so on) with legal tender status	Invented currency (Litecoin, Ripple, Bitcoins and so on) without legal tender status
Acceptance	By undertakings other than the issuer	Usually within a specific virtual community
Legal status	Regulated	Unregulated
Issuer	Legally established electronic money institution	Non financial private company
Supply of money	Fixed	Not fixed (depends on issuer's decisions)
Supervision	Yes	No
Type(s) of risk	Mainly operational	Legal, credit, liquidity, and operational

Adapted from [5]

Also, PPcoin is another example of digital currencies. PPcoin came into being in 2012. It maintains the properties of Bitcoin and serves as a form of cryptocurrency that is energy-efficient. Rather than making use of the Bitcoin 'proof of work' protocol for mining, PPcoin makes use of the 'proof of stake' protocol. It uses peer-to-peer technology.

Furthermore, another example of digital currencies is Linden Dollars, which is a digital currency that is platform-based and used for the game Second Life. Linden Dollars are earned by players through the trading for virtual goods with other players [9]. Feathercoin is a digital currency that was launched in April, 2013. It uses a scrypt-based algorithm for mining. The number of coins Feathercoin produces is four times that produced by Litecoin (See [10]). Its coin cap and block time are 336 million and 150 s respectively.

Ethereum, on the contrary, is a decentralized platform with the functionalities of smart contract. It was previously described by a programmer Vitalik Buterin in a white paper [11]. Vitalik Buterin was involved with Bitcoin.

Also, another example of digital currencies is Qcoin. Qcoin was introduced by Tencent. Tencent is a well-known site for social networking in China. It allows its users make payments on the site for virtual goods. Qcoin cannot be redeemed, but can either be earned or purchased. Also, it can be transferred within the Qcoin platform from one user to another. The initial intent of Qcoin was for it to be used as a means to buy virtual goods and services, but it then began to serve as a means of payment that does not require a middleman. Due to its growing popularity, the Ministry of Commerce in China made an announcement in 2009 that digital currencies should not be exchanged for real goods and services.

Furthermore, Primecoin is a digital currency that was developed by the main developer of Peercoin. It makes use of a recently made 'proof of work protocol' that reduces the time of confirmation to 60 s. It achieves this by finding prime numbers.

However, this 'proof of work protocol' has some requirements it should satisfy. These requirements are:

- *It should be difficult to compute in order for no one to create a proof in no time*
- *The level of difficulty required to solve the proof should be capable of been adjusted linearly*
- *The verification process should be simple in order for ease of checking the validity of the proof*
- *Prevention of the multiple use of proofs should be possible* [12].

Also, Chinacoin is a form of digital currency based on litecoin. It was launched in May, 2013. It uses the key derivation function password based on scrypt. It generates 88coins per block and 462.5 million coins.

Furthermore, Zen is an example of digital currency that is used to purchase various items or goods for specific extended capabilities of games from the Zen market. Moreover, it advertises itself as a fixed digital currency as well as an anti-bitcoin digital currency. It is neither pegged to any good or currency. It performs its functions without any centrally authorized institution. Zen can as well be

used as a means of exchange for Astrial Diamonds, one of the currencies in the game Neverwinter [13]. In addition, Zen was designed to have centralized properties but it has centralized properties as well as decentralized properties [13, 14].

Dogecoin is another example of digital currency. It was designed by Billy Markus. Dogecoin is a digital currency that was introduced in 2013 and in January 2014, it attained a market capitalization of USD 60 million. Its market capitalization was USD 22.2 million as at March 2016 [15].

Moreover, 100 billion Dogecoins were meant to be produced at the initial launch of Dogecoin, but a later announcement indicated that unlimited number of Dogecoins will now be produced.

Furthermore, Terracoin was first mined in October 2012. It is a digital currency created to produce a maximum of 42 million coins. It has a transaction confirmation time of 120 s.

Also, Namecoin is a digital currency that works based on Bitcoin cryptocurrency [10]. It was the first fork of Bitcoin. It uses peer-to-peer technology and is decentralized.

Devcoin is a Bitcoin fork that was created to give inspiration to programmers as well as developers for their projects. The process of mining Devcoin is easy and each Devcoin block generates 50,000 Devcoins. Out of the 50,000 Devcoins generated, 5000 Devcoins are for the miners while the other 45,000 Devcoins are for the developers. On a daily basis, about 7.2 million Devcoins are generated [10].

Novacoinis a digital currency similar to PPcoin except that it employs the use of a marginally distinct emission model [10]. It is based on both 'proof of stake' and 'hybrid scrypt proof of work' protocols (see also Chap. 1).

In 2011, Ixcoin was created. This form of digital currency is open source digital currency that is decentralized and operates as a low cost peer-to-peer digital currency. Each block of Ixcoin generates 96 Ixcoins [10].

Emercoin is a digital currency that was launched as a hybrid of both Namecoin and PPcoin in 2013. It makes use of both proof-of-stake and proof-of-work protocols (see also Chap. 1). It makes use of SHA-256 hashes.

Vertcoin is a digital currency and software project that uses peer-to-peer technology. It is like Bitcoin and it has other capabilities such as the stealth address technology.

BBQCoin is a scrypt-based digital currency. It is founded on the original source code of Bitcoin. This implies that BBQcoin is a peer-to-peer means of payment via the Internet and Bitcoin protocol is its backbone. Either BBQ or BQC is its usual abbreviation.

Just after Litecoin came into being, BBQcoin was launched [16]. The BBQ block time is one minute with a coin cap of 88 million [16].

Groupcoin is a digital currency that was made and launched as a backup digital currency for Devcoin. It uses peer-to-peer technology and is decentralized. Each block of Groupcoin generates 50coins.

Darkcoin was launched in April 2014 and was later renamed Dash. It alters the Bitcoin code in order to make anonymity to users greatly possible [8]. Transaction using Dash platform are deliberately made to create more confusion.

Finally, Auroracoin is a digital currency that was launched in February 2014. It is Iceland based only and it helps the people of Iceland avoid exchange controls in Iceland.

5.5 Advantages of Digital Currencies

There are immense advantages of the use of digital currencies. These advantages include; faster payment alternative, independence, global nature, cost-effectiveness, ease of use and privacy of data. We discuss them in what follows:

- *Faster Payment Alternative*: Time is saved when digital currencies are used compared to traditional currencies. The payment system of digital currencies such as Bitcoin does not require entering a lot of payment information (such as card numbers, card issue dates, card expiry dates and so on) and as such it saves transaction time [17].
- *Independence*: Digital currencies such as Bitcoin are designed not to be dependent on government, banks or any other institution. This fact makes digital currencies less subject to regulations from government, banks or any other institution. Thus, this makes digital currencies more enticing for transactions. As such, more users embrace digital currencies.
- *Global Nature*: The network for payment mediation is global. This implies that payments can be made locally as well as globally [17]. In other words, it means that payments can be made from one country to another without putting the traditional currencies (dollar, euro, pounds and so on) of such countries into consideration. This allows a global embrace of digital currencies.
- *Cost-effectiveness*: Digital currencies such as Bitcoin are more cost-effective when compared to traditional (physical) currencies in some cases. Such cases are the transfer of funds from one traditional currency to another. During the transfer of these funds, the conversion rate is considered and service charges are incurred but this is not the case for digital currencies. Digital currencies reduce cost and therefore serve as a means of savings [17]. This helps users of the digital currencies and the digital currency platforms to save more. As a result of the cost-effectiveness of the digital currencies, they are used by more users across the globe.
- *Ease of Use*: The ability to easily use any system or mechanism is important in any technology as it has a lasting effect on the acceptability of such system or mechanism. The digital currency system is easy to use and there are few steps required for transactions to be completed. As a result of the ease of use of the platforms of the digital currencies, more users embrace the use of digital currencies.

- *Privacy of Data*: 'Distributed ledger-based' digital currencies have the ability to permit the non-disclosure of vital information during transactions. As a result of its ability to permit the non-disclosure of vital information during transactions, users believe their details as well as accounts are secure and not vulnerable to hacking and online crime (money laundering and fraud).

5.6 Limitations and Risks of Digital Currencies

As much as digital currencies have advantages, there are some limitations of and risks attached to the use of digital currencies.

Vulnerability is one key issue when talking about the limitations and risks of digital currencies. The consumers and merchants that make use of digital currencies are vulnerable to possible hacking, money laundering and fraud. As such, this poses a big threat to institutions and customers that transact via the use of digital currencies. This could hinder potential users from making use of digital currencies. Also, this could make present users to stop using digital currencies as they might have the fear that their accounts may be hacked.

Volatility is another key issue when talking about the limitations and risks of digital currencies. Digital currencies are highly volatile. This high volatility in the rate of exchange gives room for loss of currency value. As a result of the loss of currency value, funds are lost by users.

Another key issue when talking about the limitations and risks of digital currencies is *Anonymity*. Transactions via digital currencies are prone to criminal activities such as fraud as a result of the level of anonymity during transactions.

Furthermore, *Crime* is another key issue when talking about the limitations and risks of digital currencies. The use of digital currencies gives room for criminal activities such as money laundering, fraud, purchase of illegal goods and services; financing terrorism and extortion [18].

Another key issue when talking about the limitations and risks of digital currencies is *Lack of Measures*. As a result of the lack of measures put in place for users to recover funds, lots of users loose funds and such funds are irrecoverable [18]. This could hinder potential users from making use of digital currencies. Also, this could make present users to stop using digital currencies.

5.7 Factors Determining the Development of Digital Currencies

As a new and widely used payment technology, digital currencies that operate on the basis of distributed ledger have some factors that initiated its development. This new development in payment technology offers reduction in cost of transactions

and increase in the transaction speed. Technological advancement as pointed out in the innovations in retail payments report by CPMI is one of the core factor for the changes in services of payment, with a significant influence on the demand and the supply of these services [3]. The factors on the demand side as well as the supply side will be discussed next.

There are various factors that influence the demand for digital currencies. These factors include:

- *Cost*: That 'distributed ledger-based' digital currencies make it possible for lower fees of transaction to be charged compared to other methods of payment has been debated over the years. In a couple of the schemes used, transaction fees are not charged but could be measured in terms of the sovereign currency units [3]. As a result of this, the schemes employed by digital currencies could be an enticing option especially for entities that require cross-border transactions that require the payment of high service charges by the providers. However, fees could be charged as a result of the conversion between the digital currency and the desired currency.
- *Ease of Use*: The ability to easily use any system or mechanism is important in any technology as it has a lasting effect on the acceptability of such system or mechanism. In this case, the number of steps required for transactions to be completed and the ease of use of the platform by users are the main factors to be considered. At present, the improvement to facilitate the ease of use of the scheme is of high necessity to a considerable number of providers.
- *Security*: This factor is vital to end-users as they always want their specific information to be kept securely without any form of hacking. The confidence of users may dampen if their details are not kept securely as there are no measures for recovery of lost funds.
- *Irrevocability*: Since distributed ledger is the basis of digital currencies, payments are irrevocable. This disables reversal of payments made and can dampen the confidence of end users as they could be defrauded without any payback.
- *Volatility*: Users tend to encounter losses as a result of risks associated with liquidity and prices. As a result of market dislocations and volatility that some digital currencies witness, the risks associated with liquidity and prices are essential. Some users could benefit while some could lose as there are noticeable variations in the rate of exchange.
- *Transaction Speed*: That 'distributed ledger-based' digital currencies are faster in completing transactions than traditional mechanism has been a point of dispute. However, the speed of processing transactions varies with respect to technicality [3].
- *Privacy of Data*: 'Distributed ledger-based' digital currencies have the ability to permit the non-disclosure of vital information during transactions. As a result of vulnerability to online crime (money laundering and fraud), users prefer privacy of data in some cases of transactions.

- *Global Reach*: The network for payment mediation for 'distributed ledger-based' digital currencies is global. This implies that payments can be made locally as well as globally. It should be noted that the transaction speed is independent on the location of the parties involved in such a transaction. Moreover, it is a herculean task for authorities to impose any form of restriction on transactions [3].

Furthermore, the supply of digital currencies is also influenced by various factors. These factors include:

- *Technical Factor*: There has to be an agreement among the participants of the network in order for a single version of the ledger to be used. If such an agreement is not reached, the level of acceptance of such digital currencies will decrease [3].
- *Sustainability*: Extending over a relatively long period of time, the sustenance of the model for some of the 'distributed ledger-based' digital currencies could be a difficult task.
- *Anonymity*: The level of anonymity that mechanisms employed by digital currencies provide could be discouraging to financial institutions [3].
- *Fragmentation*: At present, there are over 600 digital currencies in circulation having distinct transacting and confirmation protocols [3]. The distinction in the transacting and confirmation protocols of the digital currencies may serve as a stumbling block to the approval and use of the mechanisms employed by digital currencies.
- *Efficiency*: As a result of the faster speed of completing transactions as well as the advancements in processing power, digital currencies may be more widely used and accepted.

The advantages as well as the limitations and risks of involved in the use of digital currencies have been considered; therefore the possible regulatory roles will now be discussed.

5.8 Possible Regulatory Role

The role of regulation in the use and acceptance of digital currencies schemes by consumers is paramount. In recent time, the technological advancement in the design and schemes of digital currencies may prove slightly impossible to be regulated.

However, there are basically two main regulatory influences that are associated with the use and acceptance of digital currencies. These regulatory influences are; *limitation of crime* (as the use of digital currencies gives room for criminal activities such as money laundering, fraud, purchase of illegal goods and services; financing terrorism and extortion and this has hindered the growth of digital currencies) [18]

Table 5.2 Regulatory categories and potential actions required

Category	Potential actions required
Regulation of some particular entities	Through institutional approach, a limited number of regulatory measures could be put in place by authorities
Interpretation and explanation of present regulatory measures	A number of authorities could access the present regulatory measures and verify if such regulatory measures could be put in place for digital currencies and their agents
Extension and reformation of present regulatory measures	Issues of jurisdiction could pose as a challenge, but the reformation of the present regulatory measures to traditional payment systems could be of essence
Prohibition	Authorities could prohibit the acceptance and use of digital currencies in their jurisdictions

Adapted from CPMI [3]

and *consumer protection laws* (as the lack of protection for consumers have hindered investment from such consumers). It is envisioned that for consumers to be motivated to accept and consistently use digital currencies schemes, regulatory measures have to be put in place as such regulatory measures could assure consumers that their monies are safe.

Moreover, various digital currency operators have to cooperate with the government of the countries involved in order to lower the rate of or put an end to criminal activities. Anonymity in transactions has been a thing of concern to some consumers as this can also serve as a medium for crime activities to take place. Thus, this calls for cooperation among digital currency operators and the governments of countries involved.

There are about four basic possible regulatory categories that should be acted upon in order to put regulatory measures in place for the operation of digital currencies. Table 5.2 shows the possible regulatory categories and the potential actions required. These categories as well as the possible actions required to be taken can motivate the acceptance and use of digital currencies.

5.9 Case Studies

In this Section, we will take a good look at three key case studies of digital currencies, which are *Bitcoin*, *Ripple* [22], and *Scanergy project* [23].

Bitcoin could be said to be one of the most widely used digital currency that initiated its operation in 2009 and has not looked back since then. It is an innovative payment network, which is a form of virtual currency built on a transaction log circulated across participating computers in the network. It employs the use of the 'Distributed Ledger' scheme. Furthermore, the purpose of the design of Bitcoin was to perform three basic functions of traditional money. These basic functions are:

- *To serve as a means of facilitating exchange commercially*
- *To serve as a means of storing value by users for the purpose of use in the future and*
- *To serve as the basic unit for measuring the values of market goods and services rendered* [19].

As mentioned in previous Sections, there are numerous numbers of Bitcoin forks some of which include; Litecoin, Primecoin and Peercoin (Table 5.3).

Bitcoin operates using a virtual currency scheme. This scheme is decentralized and its flow is in two directions. Bitcoin was designed not to be dependent on government, banks or any other financial or non-financial institution and the manner of operation of Bitcoin is like that of electronic cash [17]. Moreover, it can be exchanged for the currency of nations such as Dollars after been bought on dedicated websites across the globe. However, demand and supply in the market are the determining factors of the rate of exchange of Bitcoin. A software referred to as 'wallet' is the software platform for which payments of Bitcoins are made. This software platform (wallet) must first be in operation on the computers to be used. Furthermore, when payments are made, the accounts of the senders are debited while the receiving accounts are credited. These payments been made are done via the exchange of messages, which are encrypted and are authenticated within the network of the users. The authentication is carried out by miners providing solution to a mathematical question. It is worthy of note that it is hard to provide solution to the mathematical question and pretty simple to authenticate when the solution is provided.

Bitcoin has intrinsic value and as with the financial sector, the value of any form of currency is measured by its ability to be changed into legal type of payment [7]. This value of Bitcoin is highly volatile with regards to its rate of exchange with the US Dollar. Table 5.4 shows the Bitcoin and the US Dollar rate of exchange on a monthly basis from April, 2013 to December, 2014. Furthermore, Table 5.5 shows the Bitcoin and the US Dollar rate of exchange on a monthly basis from January, 2015 to July, 2016. It should be noted that the US Dollar rate of exchange highlighted in Tables 5.4 and 5.5 is the average US Dollar rate of exchange per Bitcoin on the closing day (last day) of each month.

However, Fig. 5.1, which shows the graphic representation of the rate of exchange of US Dollar per Bitcoin further buttresses Tables 5.4 and 5.5.

From Table 5.4, it can be seen that there are highly noticeable variations in the rate of exchange of US Dollar per Bitcoin. Moreover, between April 2013 and May 2013, the difference in the rate of exchange of US Dollar per Bitcoin increased by

Table 5.3 Characteristics of some of the Bitcoin forks

Digital currency	Mining time (min)	Maximum volume
Bitcoin	10	21 million
Litecoin	2.5	84 million
Primecoin	1	No limit
Peercoin	10	No limit

Adapted from Sprankel [12]

Table 5.4 The Bitcoin and the US dollar rate of exchange [20]

Year	Month	US dollar average price per Bitcoin
2013	April	120.87
	May	128.10
	June	89.03
	July	101.46
	August	137.57
	September	133.03
	October	206.72
	November	1019.95
	December	772.53
2014	January	835.89
	February	566.61
	March	476.87
	April	454.09
	May	642.24
	June	649.84
	July	591.77
	August	479.72
	September	384.02
	October	330.27
	November	380.74
	December	316.90

Table 5.5 The Bitcoin and the US dollar rate of exchange [20]

Year	Month	US Dollar Average Price per Bitcoin
2015	January	218.81
	February	252.94
	March	244.53
	April	236.12
	May	227.58
	June	260.73
	July	283.04
	August	230.32
	September	238.59
	October	318.43
	November	368.28
	December	433.38
2016	January	373.83
	February	436.22
	March	417.77
	April	453.02
	May	534.75
	June	677.35
	July	636.88

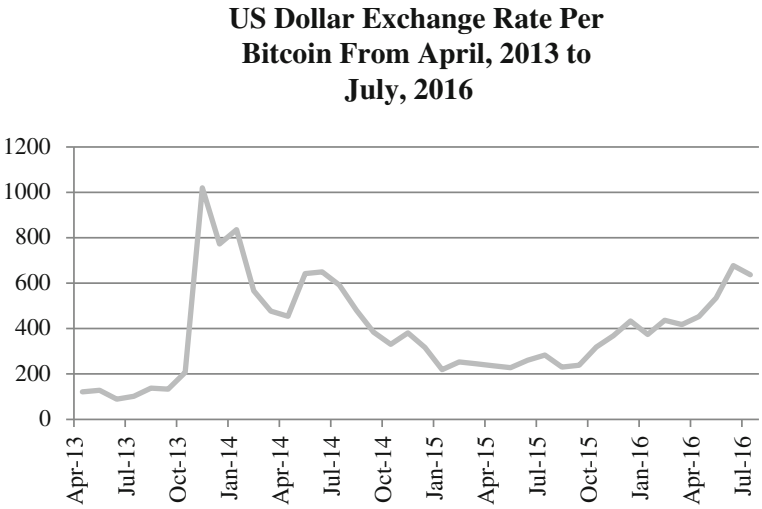


Fig. 5.1 Graphic representation of the rate of exchange of US Dollar per Bitcoin. Adapted from Bitcoin Average [20]

$7.23, which indicates a percentage increase of 5.98%. At the end of June 2013, this rate of exchange dropped by $39.07, which is a percentage decrease of 30.5%. In the following month (July 2013), an increase of $12.43, which indicates a percentage increase of 13.96% was noticed and in the following month (August 2013), an increase was noticed as well, which was $36.11 more than the rate of exchange in the preceding month. This implies a percentage increase of 35.59%.

Subsequently, a decrease was experienced in September of the same year where the rate of exchange dropped by $4.54 indicating a percentage decrease of 3.30%. In the month of October of 2013, there was a sharp increase of $73.69 thereby indicating a percentage increase of 55.39% (well over an increase of 50% compared to the rate of exchange in September 2013). The rate of exchange in November of the same year closed at $1019.95, which has been the highest rate of exchange per US Dollar since 2013 till July 2016. This shows a huge increase of $813.23 and a percentage increase of 393.4%. This increase was over thrice the value of the rate of exchange for the preceding month (October 2013).

Furthermore, after this huge increase came a drastic decrease of $247.42 and a percentage decrease of 24.26% in the month of December. January 2014 then ushered in an increase of $63.36, which signifies 8.20% increase in percentage. From February 2014 to April 2014, consistent decreases of $269.28, $89.74 and $22.78 respectively in terms of the rate of exchange were noticed. This implies that percentage decreases of 32.22, 15.84 and 4.78% were experienced in the months of February, March and April in the year 2014 respectively.

Subsequently, the months of May and June of 2014 both experienced increases of $188.15 and $7.6 in the rates of exchange respectively. This also implies that percentage increases of 41.44 and 1.18% were experienced in the months of May

and June in the year 2014 respectively. Also, in July, August, September and October, there were decreases in the rate of exchange of US Dollar per Bitcoin. There were decreases of $58.07, $112.05, $95.7 and $53.75 in July, August, September and October respectively. This signifies that the percentage decreases of 8.94, 18.94, 19.95 and 14.00% were experienced in July, August, September and October respectively. Also in 2014, the months of November and December witnessed an increase of $50.47 (percentage increase of 15.28%) and a decrease of $63.84 (percentage decrease of 16.78%) respectively.

In 2015, the months of January and February witnessed a decrease of $98.09 (percentage decrease of 30.95%) and an increase of $34.13 (percentage increase of 15.6%) respectively, while the months of March, April and May experienced decreases of $8.41 (percentage decrease of 3.33%), $8.41 (percentage decrease of 3.44%) and $8.54 (percentage decrease of 3.62%) respectively. Then, the months of June and July experienced increases of $33.15 (percentage increase of 14.57%) and $22.31 (percentage increase of 8.56%) respectively. August 2015 witnessed a decrease of $52.72 (percentage decrease of 18.63%). However, there were increases of $8.27 (percentage increase of 3.59%), $79.84 (percentage increase of 33.46%), $49.85 (percentage increase of 15.66%) and $65.10 (percentage increase of 17.68%) in September, October, November and December respectively.

In 2016, the rate of exchange of US Dollar per Bitcoin for the months of January, February and March were a decrease of $59.55, which implies a percentage decrease of 13.74%, an increase of $62.39, which implies a percentage increase of 16.69% and a decrease of $18.45, which implies a percentage decrease of 4.23%. Subsequently, there were increases of $35.25, which implies a percentage increase of 8.44% in April, $81.73, which implies a percentage increase of 18.04% in May and $142.60, which implies a percentage increase of 26.67% in June. However, July witnessed a decrease of $40.47, which implies a percentage decrease of 5.98%.

However, with regards to Tables 5.4, 5.5 and Fig. 5.1, it can be said that Bitcoin is highly volatile as there were hugely noticeable variations in the rate of exchange of US Dollar per Bitcoin since April, 2013 till date; thus, this high volatility could be said to be one of the limitations of Bitcoin.

Point of Attention Nearly 120,000 units of Bitcoin digital currency worth about USD72 million was stolen from Bitfinex (an exchange platform) in Hong Kong. This came as a surprise to the Bitcoin global community as it is the second-biggest breach of security of such an exchange [21].

The second case we consider is *Ripple*, a digital currency issued by the for-profit enterprise Ripple Labs. It is a digital currency and a system of payment that was totally developed without any form of dependence on Bitcoin. It had its first trade in August 2013. It is independent on any mining protocol and has a publicly shared ledger.

In addition, Ripple's system of payment is decentralized and its code is an open source (made readily available to the public). Recently, ripple became the digital currency with the second highest market capitalization after Bitcoin [22]. Moreover, an additional USD 30 million funding for the growth and development of Ripple Labs were finalized. However, Ripple made an affirmation to not only act as a digital currency alone but also as a means of exchange between currencies in its network [22].

The distributed ledger used by Ripple helps to monitor and record all transactions across the Ripple system. The following are the constituents of a Ripple distributed ledger:

- Transaction set
- Details of account such as total balance and account settings
- Timestamp
- Ledger number, and
- A status bit to indicate the validity of the ledger.

Each validating server in the Ripple system authenticates any assumed change to the last closed ledger otherwise called the most recently validated ledger and the changes that half or more of the servers agree upon are put into a new assumption before being sent to the other servers within the network [22]. This process Is then repeated and the requirements for the vote is then increased to 60% of the servers, then 70% of the servers then 80% of the servers. After this process, the server then authenticates the changes before alerting the network of the closure of the most recently validated ledger [22]. Any transaction that has initially taken place but was not indicated in the ledger is then discarded at this stage. Such discarded transactions are then considered to be invalid by the users of the Ripple system.

Point of Attention In the Ripple system, each server that validates keeps a list of trusted servers referred to as Unique Node List (UNL) and each server only trusts the votes issued by the servers listed on the UNL [22].

The third case we consider is *Scanergy project*. Europe's power grids could be saved by Bitcoin-style virtual currency from attaining a breaking point as more consumers that put energy back into the network from solar panels [23]. These consumers that put energy back into the network are referred to as prosumers. The European Union (EU) has a target to attain a reduction of 80% in greenhouse gases by 2050. However, the European energy distribution networks are systemized in a top-down manner for large energy distributing providers to consumers either by direct means or indirect means (via the use of smaller local energy distributing providers) [23].

An increased number of consumers are fast becoming prosumers. They produce a percentage or all of their own renewable energy. They also willingly trade energy with others. Between 8 and 12% of households in Belgium are now prosumers and this development is expected to continue [23]. Furthermore, the European power grids is required to be made to become "smart grids" that allow the production and consumption of energy locally and this cuts down the transmission loss that take place during transmission over long distances [23].

Point of Attention Scanergy won the best demo award at the International Conference on Autonomous Agents and Multiagent Systems in Instanbul, Turkey in May 2015 [23].

Enter Scanergy (a scalable and modular system for trading energy between prosumers) is a project funded by the European Union's Seventh Programme for research, technological development and demonstration. It is centered on an intelligent multi-agent system, which has the ability to manage produced and consumed electricity both lower level, which consists of dwellings and neighborhoods and higher level, which is mainly the cities. The smart energy trade between prosumers is made possible by the Scanergy system while dealing with the intrinsic simultaneous dynamism in the demand and supply of electricity [23].

Furthermore, this Scanergy project recommends an online currency (digital currency) to boost local trade between the producers and the consumers of energy. As reported by [23], according to a researcher at the AI lab of the Vrije Universiteit Brussel (VUB), Mihail Mihaylov: "prosumers create decentralized digital money themselves and want to know what their return on investment (ROI) is". He also pointed out that "the recommended concept addresses the ROI problem. We lower the risk of policy change" [23].

The Scanergy trading system checks the supply of renewable and the overall demand for electricity in a given neighborhood through its smart meters every 15 min. Those that feed energy back into the system would be paid a Bitcoon-like digital currency called NRGcoin [23].

NRGcoin offers various benefits over fiat currency. It is generated by injecting energy into the grid rather than spending energy on computational power.

5.10 Summary

In this chapter, we looked at Digital currencies by highlighting the consequent extensions in the meaning of money, especially with regard to the present growth and developments in mobile technology and software. We further highlighted that tremendous effects such as fresh economic exchanges, faster transactions among

others were brought about by digital currencies and these have been as a result of the concept of 'distributed ledger'.

Also, we looked at the concept of digital currencies where we pointed out that the ability of any currency (both digital and physical currencies) to serve as a medium of exchange for goods and services rendered, as an asset and as transferrable assets, makes such currency acceptable. It was also pointed out that digital currencies came to being in the 1990s. Moreover, it was pointed out that Liberty Reserve was one of the first set of digital currencies to ever exist and it came into being in 2006. We also highlighted that Bitcoin initiated its operation in 2009 and has not looked back since then and is the leading and most widely accepted digital currency compared to other examples of digital currencies such as *Litecoin*, *Chinacoin*, *Namecoin and Devcoin.*

Thereafter, we have discussed the two categories of digital currencies, which are E-money and Virtual currency. Here, we pointed out the various characteristics of each of the two categories of digital currency, we further noted that the legal status for E-money is regulated while the legal status for Virtual Currency is *unregulated.* Also, we pointed out that the supply of money for E-money is *fixed* while that for Virtual Currency is *not fixed*. Moreover, it was highlighted that E-money is characterized by the use of traditional currency such as Euros, US Dollars, Pounds, Yen and a host of other traditional currencies while virtual currency is characterized by the use of invented currencies such as Linden Dollars, Bitcoins and other invented currencies.

Furthermore, we discussed the examples of digital currencies where we highlighted *Litecoin*, *Peercoin*, *PPcoin*, *Linden Dollars*, *Ethereum, Primecoin, Chinacoin* and so on as the examples of digital currencies. Also, we looked at the advantages of digital currencies which include; *faster payment alternative, independence, global nature, cost-effectiveness, ease of use* and *privacy of data*. Also, we discussed the limitations and risks of digital currencies which include; *vulnerability, volatility, anonymity, crime* and *lack of measures*.

Moreover, we highlighted the factors that determine the development of digital currencies, which include; the factors that influence demand (*cost, ease of use, security, irrevocability, volatility, transaction speed, privacy of data and global reach*) and the factors that influence supply (*technical factor, sustainability, anonymity, fragmentation and efficiency*).

Afterwards, we discussed the possible regulatory role where we pointed out limitation of crime and consumer protection laws as the two main regulatory influences associated with the use and acceptance of digital currencies.

Finally, in this chapter, we looked at three case studies which are *Bitcoin*, *Ripple* and *Scanergy Project*. It was highlighted that Bitcoin is one of the most widely used digital currency that initiated its operation in 2009 and has not looked back since then. We also pointed out that the basic functions of Bitcoin are; to serve as a means of facilitating exchange commercially, storing value for users and for measuring the values of market goods and services rendered [19]. Furthermore, it was noted that Ripple is a digital currency issued by the for-profit enterprise Ripple Labs and is a system of payment that was totally developed without any form of dependence on

Bitcoin. Ripple distributed ledger consists of *transaction set, details of account, time stamp, Ledger number* and a *status bit* to indicate the validity of the ledger. For the third case study, which was Scanergy Project, we highlighted that (i) it is a scalable and modular system for trading energy between prosumers and (ii) it is a project funded by the European Union's Seventh Programme for research, technological development and demonstration.

Digital currencies are an innovation in payment systems. They are an internet-based medium that serves as an alternative medium of exchange. This innovation of Digital currencies could prove to be a stunning, accepted and widespread technology as it could have a huge impact on payment systems as it is more cost effective, independent of any authority, has a global reach and has faster transaction processing time. This huge impact will as well tell on the financial system and the economy at large. Unlike traditional E-money, digital currency does not serve as a liability of any individual or institution and are not dependent on any governmental or institutional authority.

However, the limitations and risks attached to the use of digital currencies (*high volatility, susceptibility to crime and fraud*, *irrevocability* among others) could pose a threat to the use and acceptance of digital currencies.

References

1. Peng S (2013) BITCOIN: Cryptography, Economics, and the Future. Available at https://www.cis.upenn.edu/current-students/undergraduate/courses/documents/EAS499BitcoinThesis-StarryPeng.pdf. Accessed 20 Nov 2016
2. Hoelscher JL (2014) Digital currency risks. Intern Audit 71:24–25
3. CPMI (2015) Digital currencies, Committee on Payments and Market Infrastructures, Bank for International Settlements (BIS), ISBN 978-92-9197-384-2 (print), ISBN 978-92-9197-385-9 (online)
4. Ali R, Barrdear J, Clews R, Southgate J (2014) Innovations in payment technologies and the emergence of digital currencies. Bank of England Quarterly Bulletin, 2014 Q3. Available at https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2499397. Accessed 20 Nov 2016
5. Morabito V (2016) Digital Currencies and Distributed Ledgers. In: Futur. Digit. Bus. Innov. Springer International Publishing, Switzerland, pp 43–60
6. E-gold e-gold Corporate (2016) https://web.archive.org/web/20041014062818/http://www.e-gold.com/unsecure/aboutus.html. Accessed 3 Nov 2016
7. Allen & Overy (2015) Virtual currencies. http://www.allenovery.com/SiteCollectionDocuments/Virtual%20Currencies.pdf. Accessed 20 Nov 2016
8. White LH (2015) The market for cryptocurrencies. Cato J 35:383–402. doi:10.2139/ssrn.2538290
9. Fung B, Halaburda H (2014) Understanding platform-based digital currencies. Bank Canada Rev 12–20
10. Siluk S (2013) What other digital currencies are there? In: CoinDesk. http://www.coindesk.com/what-other-digital-currencies-are-there/. Accessed 20 Nov 2016
11. Buterin BV (2013) A next generation smart contract and decentralized application platform. 1–36. Ethereum White Paper. Available at http://www.fintech.academy/wp-content/uploads/2016/06/EthereumWhitePaper.pdf. Accessed 20 Nov 2016
12. Sprankel S (2013) Technical basis of digital currencies. Available at http://www.coderblog.de/wp-content/uploads/technical-basis-of-digital-currencies.pdf. Accessed 20 Nov 2016

13. Ziff Davis (2014) Zen. In: Ziff Davis, LLC. http://www.ign.com/wikis/neverwinter/Zen. Accessed 20 Nov 2016
14. Truong A (2013) Zen—Bitcoin's polar opposite. In: CoinDesk. http://www.coindesk.com/zen-bitcoins-polar-opposite/. Accessed 18 Aug 2016
15. CoinMarketCap Crypto-Currency Market Capitalizations. In: CoinMarketCap. http://coinmarketcap.com/. Accessed 3 Nov 2016
16. CryptoSource (2016) BBQCoin, http://cryptosource.org/coins/alt-coins-other/bbqcoin-bqc/. Accessed 4th January 2017
17. Segendorf B (2014) What is bitcoin? Sveriges Riksbank Econ Rev 1–7
18. HM Treasury (2015) Digital currencies: call for information. In: Gov.UK. https://www.gov.uk/government/consultations/digital-currencies-call-for-information/digital-currencies-call-for-information. Accessed 19 Aug 2016
19. de France B (2013) The dangers linked to the emergence of virtual currencies: the example of bitcoins. FOCUS No. 10–5 December 2013, pp. 1–6
20. Bitcoin Average (2016) Bitcoin price index. In: Bitcoinaverage. https://bitcoinaverage.com/charts#USD-averages-1d. Accessed 18 Aug 2016
21. Baldwin C (2016) Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong. Reuters technology news. http://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP. Accessed 20 Nov 2016
22. Armknecht F, Karame GO, Mandal A, Zenner E (2015) Ripple: overview and outlook. In: Conti M, Schunter M, Askoxylakis I (eds) Proceedings of International Conference on Trust & Trustworthy Computing (TRUST), Crete, Greece, 2015
23. Prisco G (2016) An energy Blockchain for European prosumers. In: Bitcoin Mag. https://bitcoinmagazine.com/articles/an-energy-blockchain-for-european-prosumers-1462218142. Accessed 3 Nov 2016

Smart Contracts and Licensing

6

Abstract

Contracts are agreements, which involve moving certain assets or value from one owner to another based on a condition or set of conditions between people or things. Considering the fact that institutions and central organizations are commonly fundamental as trusted authorities, part of their central operations can be condensed into smart contracts that are controlled by decentralized consent on a blockchain. The idea behind smart contracts and smart licensing of proprietary material (e.g., software, music and digital art) is that the contractual control of transactions between two or more entities is confirmable programmatically through the blockchain instead of through a central gatekeeper or arbitrator. Smart contracts eliminate the need for two parties to depend on a central authority because they 'can agree' between themselves, define the terms and implications of their agreement programmatically and conditionally, with automatic asset releases when fulfilling services in a sequential manner, or incur penalties if not fulfilled. Due to the ability of the blockchain technology as an indisputable endorser of dealings, each peer can go ahead and have trust in each other because the framework of governance, contracts, trust, and agreements dwell on top of the technology. To this end, this chapter will describe how organizations can leverage the smart contract technology by integrating smart contract code and the blockchain for the purpose of overseeing agreements and licensing. It then explains the benefits, the down sides as well as realistic case studies on the use of smart contracts in various industries.

6.1 Introduction

The focus of this chapter is on the provision of more specific definitions of the terms Contract and License. A contract provides parties with a set of rights and obligations, which are used among other things to encourage long-term relationships [1]. This is

V. Morabito, *Business Innovation Through Blockchain*,
DOI 10.1007/978-3-319-48478-5_6

very useful in environments where relationships thrive upon trust. Licenses on the other hand are used to grant permission for parties to carry out activities with products or properties that would otherwise be illegal. A license may be granted by a party ('*licensor*') to another party ('*licensee*') as a form of an agreement between those parties [2]. For example, a licensor may grant permission to a licensee to copy and distribute copyrighted works such as software or digital art.

Among the diverse definitions [3], a contract is a voluntary, deliberate and legally binding or valid agreement between two parties. The law will consider a contract to be valid if it contains all of the following elements:

- Offer and acceptance;
- An intention between the parties to create binding relations;
- Consideration to be paid for the promise made;
- Legal capacity of the parties to act;
- Genuine consent of the parties; and
- Legality of the agreement.

An agreement that lacks one or more of the elements listed above is not a valid contract [3]. Contracts are normally enforceable whether or not in a written form, although a written contract protects all parties to it. Some contracts, (such as for sale of real estate, rental, car finance installment plans, or home insurance policies) must be in writing to be legally irrevocable and enforceable [3, 4]. When there is a breach of contract, e.g., non-performance, poor-performance, or part-performance the unhappy party or parties in most cases rely on the courts or a third party to enforce the contract. However, the latest disruption in the technology world, the blockchain, has meant that *some* legal contracts can now become 'smart' [5]. The hype over smart contracts has resulted in headlines such as *blockchain smart contracts to disrupt lawyers* [5]. The idea of smart contracts dates back to 1994, when Szabo [6], a cryptographer widely praised with laying the groundwork for bitcoin, first formulated the term 'smart contract' [7]. These automated contracts basically work like any other computer program's if-then statements. *If this happens*, *then do that*.

6.1.1 Smart Contracts

There are various definitions of what a smart contract is and we shall look at a few of these. According to Idelberger et al. [8], a smart contract is a computer program that holds the terms of a contractual accord and also implements the accord while ensuring trust, transparency and understanding between parties. Also, a smart contract can be considered just a decorative name for computer code that runs on a blockchain, and interacts with that blockchain's state [9]. Therefore, in the context of blockchains, smart contracts are [9, 10]:

- Pre-written and self-executed computer program.
- Saved and mirrored on a shared storage platform (i.e., a blockchain).

- Accomplished by a network of computers (usually those running on the blockchain network).
- Set off by blockchain transactions.
- Interprets and records data in a blockchains database and can give rise to ledger updates (e.g., cryptocurreny remittances).

In uncomplicated terms, these definitions imply that smart contracts are computer codes that reside in the blockchain and implement *if this then do that*, run and are confirmable by a number of computers to ensure truthfulness. There is no need for a middleman or company sitting in the middle of agreements or transactions and amassing fees [11] with the use of computer code (embedded in a blockchain) to articulate, verify, and enforce an agreement between parties. Some authors have chosen to call this a 'smart legal contract' [12, 13]. Others have emphasized that these programs may replace lawyers and banks for handling certain reoccurring financial transactions in future [7, 14]. If blockchains give us distributed trustworthy data storage then smart contracts give us distributed trustworthy judgments [10]. According to [8] examples for applying smart contracting and licensing are *programmatic banking functions* (e.g. Automated Escrow, Savings), *decentralized markets* (e.g. OpenBazaar—www.openbazaar.org), *prediction markets* (Augur—www.augur.net), *distribution of music royalties* (Ujo—www.ujomusic.com) and *encoding of virtual property* (Ascribe—www.ascribe.io).

Blockchains are able to run code. The first type of blockchains were made to perform digital currency (currency-like tokens) transactions, techniques have emerged which have enabled the blockchain to perform complex tasks defined in full-fledged programming languages [15]. The fact that these programs are run on a blockchain makes them dissimilar to other types of software. First, the program itself is registered on the blockchain, thus having its blockchain's unique permanence and censorship defiance [15]. Then, the software can on its own manage blockchain assets, in other words, it can actually store and allocate chunks of cryptocurrency. Finally, the program is triggered *by* the blockchain, meaning it will always work as designed and no one can obstruct or change its operation [15]. To most developers, the term 'smart contracts' is often used to refer to this blockchain code. This presents a challenge because almost everyone who understands English can read a paper contract written in English but not everyone will be able to read and fully understand a smart contract [15] as not every English speaker is a software developer.

Szabo's original theories about how these smart contracts could work remained unrealized because there was no technology to support programmable agreements and transactions between parties. His example of a contract was the vending machine that holds onto goods until money has been received and then the goods are released to the buyer. The machine holds the property and is able to enforce the contract [12]. There were two main issues that needed to be addressed before smart contracts could be used in the real world. Firstly, the control of physical assets by smart contracts to be able to enforce agreements. Secondly, the lack of trustworthy

computers that are reliable and trusted to execute the contract between two or more parties [12].

However, the widespread adoption of Bitcoin is changing that, solutions to both problems have emerged and as a result Szabo's idea has now come to life. The first use of the blockchain technology was the digital currency Bitcoin. Computer programs can now execute agreements and trigger payments between parties.

The potential for the Blockchain technology and smart contracts goes beyond the transfer of money from one party to another. Smart contracts could be used to unlock the door of a car by connecting smart contracts to the Internet of things (IoT). With smart contracts we could see a reduction in mortgage rates, update our will at ease without a lawyer and ensure that our friends are not able to weasel out of paying up on a bet. That and much more is the promise of smart contracts, a technology that is getting closer and closer to reality thanks to digital currencies and encryption [7]. But as always with this cutting edge of financial technology, major questions abound: the thought of how this will all align with our current legal system remains and whether anyone will actually make use of it [7].

Whereas a traditional legal contract defines the rules around an agreement between multiple people or parties, smart contracts go a step further and actually enforce those rules by controlling the transfer of currency or assets under specific conditions [16]. Smart contracts and licenses would decentralize the model of who needs to be trusted. And in doing so, it would cut out hefty fees by brokering services like Airbnb.

Smart contracts do not have to unsettle existing business models, instead they can also help them to develop. Szabo [6], explained the idea that smart property might be created by implanting smart contracts in physical objects. He chose as an example a car loan, defining that if you miss a car payment, the smart contract could automatically invalidate your digital keys to operate the car. Car dealerships are likely to find this idea interesting.

In order to bring transparency and auditability to real-world objects, software developers (e.g., Germany-based Internet of Things company Slock.it) are already engaged on ways to associate the Internet of Things with the bitcoin framework so that something like a bitcoin can actually represent a real item. That token is what these developers call smart property.

Using the example of renting a house, lets say all the door locks are internet-enabled and have working connections. When a Bitcoin transaction for the rent is made, the smart contract allows the tenant to have access to the flat by unlocking the house and the tenant can go in using 'smart' keys stored on his or her smartphone. When there is a smart contract in place, it will be trivial to set up dates for when the keys would expire. According to Cassano [7], it sounds like Airbnb without the need for Airbnb. Actually, the current Airbnb system makes the tenant and host to put their trust in Airbnb if the guest does not pay up or the host does not leave the keys. However, carrying out the same sublet with smart contracts would eliminate a business model like Airbnb's. The homeowner and renter still do not

need to trust each other; they only need to trust the smart contract [11]. Another example is online shopping. You could have a smart contract that verifies parcel tracking data and only makes a payment to the seller upon verifying that the goods have been delivered to your address [7].

6.1.2 Smart Licensing

Sandy Ressler at Bitcoin Magazine, states that automatic contributions to network services (walking into a WiFi hotspot); remittance to reporters for single articles or paragraphs, software subscriptions; remittance to content producers of all categories are certainly feasible with the adoption of smart contracts embedded in the blockchain [17]. Smart contracts have the capability of disrupting the way licensing is presently done in the Art, Journalism and Music industry and also has the potential to revolutionize the software industry. For example, using smart contracts the mass distribution of software products under a smart license from the developer can be monitored. Upon expiry, the software product stops working based on the terms of the smart contract and the users renew their software license by purchasing tokens on the blockchain network. Other users who are no longer interested in using particular software could also re-sell their license on such distributed networks [17].

This could lead to a whole new era of creativity, just like the economy that was launched 400 years ago by the *Statute of Anne* (also known as the Copyright Act established in the year 1710 by the Parliament of Great Britain which bestows the sole liberty of printing or reprinting books to the authors or purchasers of copies, thus enforcing copyrights) [18]. This Statute gave books, plays or song writers the right to earn a royalty when they were copied. An micropayment system would permit content creators to be able to sell digital copies of their articles, songs, games, and art by the piece. In other words personally grant people the license to use their intellectual property in a 'smart' way. This is what is referred to as 'smart licensing'. In addition to allowing them to pay the rent, it would have the worthy benefit of encouraging people to produce content valued by users rather than merely seek to aggregate eyeballs for advertisers [18]. The historic licensing of digital art is gray and usually relies on physical materialization—paper certificates, printed, limited edition prints and endorsed licenses—conceiving scarcity, a pre-requisite for market value [19].

Falsification is widespread in the art scene and artists are also probing how the blockchain technology can cater for methods to trail and verify ownership authenticity through tools like smart contracts and licenses authenticated by cryptographic information. Traditional ways of licensing would create a tradable commodity. Buyers could not be certain the license was authentic nor would they be able to assert whether the author had created multiple copies of the piece [19]. Just like bitcoin can replace banknotes, it can replace the piece of paper with the license text on it. Once its usage rights have been converted into a legally limited and tradable virtual asset using blockchain technology; as for this issue, [19] points out the case of the German-based artist Stephan Vogler, whose pieces are published

under a smart license [20]. Furthermore, Samuel Miller, a London-based artist, presents an imaginary way of how the Blockchain (distributed ledger technology) works. He presents smart contracts as a wizard sitting in a room of people talking and taking down notes. Then after they have finished talking, everything each person is said is read back to everyone [19].

Austria's Museum of Modern Art (MAK) made the headlines [21, 22] when it became the first museum to purchase a piece of art with Bitcoin [19]. Berlin-based Ascribe oversees galleries, artists and collectors allowing them enroll or transfer a compilation of digital art with the use of time-stamped cryptographic ownership certificates on its blockchain-based Ownership Registry. Besides Ascribe, Monegraph, a collaborative venture between a New York University professor and a technologist also enables artists to secure digital property on the Namecoin Blockchain [19].

Two companies presently using the Blockchain technology to revolutionize the music industry are Ujo and PeerTracks [23]. PeerTracks' CEO Eddie Corral says that each song uploaded with be associated with a smart contract that will then automate the sharing of earnings gained from trading the song between contributors and intellectual property owners (for example, the lyricist, the composer and performer) based on their real-life agreement [23]. Ujo is attempting to tackle two major problems. The first is a reflection of PeerTracks, the allocation of funds to artists and rights holders. The other is resolving who owns a creative work. In a situation whereby songs can have ten or more co-writers attached, licensing becomes difficult. With smart contracts and licensing, creators such as software developers, artists, musicians and journalists can trail and collect royalties on their digital work [23].

6.1.3 Smart Contract Types

Blockchain networks like Ethereum and Bitcoin have input and output limitations due to their security constraints that limit access to external data (e.g., price, weather, location, etc.) which are needed for contractual performance and forms of payment preferred by parties involved in these contracts. Because of this, trusted links to external data sources are required for some smart contracts to be executed. Thus smart contract can be further divided into deterministic and non-deterministic smart contracts.

Deterministic smart contracts are smart contract codes that do not depend on outside information other than information on the blockchain in which they live into be triggered and work effectively. In other words, the blockchain network facilitating the smart contract has sufficient information to make decisions. E.g., peer-to-peer lottery: the funds are held on the blockchain network and random numbers are also generated by the smart contract code. At the end of the lottery, the funds are transferred the winners account via his or her address on the blockchain network [24].

In *Non-Deterministic smart contracts* the network facilitating the smart contract code does not have sufficient information to make decisions. Thus an outside party is needed, usually called an 'Oracle' in the computer science domain. E.g., Decisions about value flow based on human behavior, events (price drop or hike) or predictions. However, research has shown that using external state does not always introduce the need for trusting an additional party [25]. For example, in a driving license renewal scenario, the government is a trusted party anyway, thus, we use government as a validation oracle that injects external state into the blockchain [25].

Oracles are known in computer science for their ability to provide information from outside a system that the system itself cannot acquire. When applied to smart contract networks, oracles act as programmable agents that provide a smart contract with the data it requires (inbound oracles) and act on its behalf by releasing payment or informing your internal systems what a smart contract has concluded (outbound oracles) [26]. Oracles also store the data and only pass the important and relevant data to the smart contract. This ensures the security and high privacy of the network and improves efficiency.

Usually the desirable applications of smart contracts contain some degree of non-determinism. In any case, if Oracles are federated, the smart contract still reduces the risk of fraud. An example of a source of trusted information feeds is the Bloomberg terminal thus non-deterministic smart contracts map well into legacy systems.

A canonical example of non-deterministic smart contract would be the sports betting scenario where the system cannot exactly know what team has won the game. Participants must agree on a trusted third party (Oracle) to supply an outcome. Thus the security of the system is reduced in a sense to the reliability of the source [26]. Because smart contracts are computer programs, it would not be necessary to add more complex betting elements like odds and score differentials into the mix [7]. However, they can determine the rule, odds and conditions of transfer of value. We can use carefully thought out processes for undesired behavior such as federating the oracle or creating an arbitration process [24]. Companies like Augur and TruthCoin are analyzing ways of improving the trust model for Oracles using Principal component analysis (PCA).

6.1.4 Smart Contract and Career Disruptions

Although the concept of 'smart contracts' is still in its early stages, the future potentials are visible. Seeing the potential of smart contracts, one cannot doubt the fact that smart contracts will disrupt the legal and banking industries but it will still be early to conclude that smart contracts can replace legal documents. However, what lawyers and the banks do are repetitive tasks but we still pay them huge fees for carrying out these tasks. Some of these tasks could be automated so that people can save financial resources as well as time.

Firstly, considering the Banks. When we take out a mortgage from the Bank, the Bank does not hold onto it for the number of years it lasts; it is usually sold to an investor [27]. However, we do not pay the investor directly but the Bank for processing the monthly payments and other things such as home insurance and tax. The Bank usually takes a large chunk of the mortgage for just processing and forwarding your payments to the right places. If smart contracts are used when it comes to mortgaging, processing fees could be eliminated making it cheaper to own a home.

Now, considering the legal angle of the 'smart contract' concept. According to Cassano, if a simple enough user interface were developed it could remove so many legal headaches, like updating your will [7]. Imagine if designating personal assets in a will was as easy as moving an adjustable slider that determines who gets control of what asset. It has been suggested that smart contracts will never significantly replace natural-language law [12]. It will not replace the legal system as much as provide an intermediate layer between transacting and going to court [7].

The role that lawyers play might look very different in the future. Instead of having lawyers adjudicate individual contracts, their role might shift to produce smart contract templates on a competitive market. Contract selling points would be their quality, how customizable they are, and their ease of use. It sounds a bit like an e-commerce website for website themes [12, 28] where people will develop smart contracts that do different things and sell these for others to customize and use or deploy according to their needs. So for example companies can charge for access to really good equity agreements that have a bunch of different functionality.

There are plenty of agreement types that can never be fully expressed in code or executed by a computer. For example, those involving human performance [12]. Fully self-executing contracts alike will sooner or later demand referencing legal terms and theory that will decide entities rights when relationships lead to litigation. The evolution of smart contracts will give rise to a re-assessment of usual practice, as lawyers and their clients alike identify which types of agreements and terms are appropriate to code, which should be left to natural language, and how to associate each to derive the best of both worlds. Smart contracts are still science fiction but for the first time there is a technology that could bring them into commercial use. It will be wise of legal professionals to consider how smart contracts could have an impact on their business. By the time smart contracts become 'legally' viable to a large extent, law firms should hope that they have lawyers that can fully understand and use the technology [12].

In summary, Sect. 6.1 has introduced the concept of smart contracts and licenses and some mind provoking questions around industry disruptions and the future of smart contracts. Section 6.2 will discuss the implementation of smart contracts and briefly compare several blockchain platforms available for developing and deploying smart contracts.

6.2 Implementation

In Sect. 6.1, the smart contract technology has been introduced with some examples. The aim of this section is to introduce the platforms that can be and have been applied in the development and deployment of smart contracts. The various aspects that need to be considered when developing smart contracts as well as sources of documentations and tutorials will be outlined in this section.

6.2.1 Platforms

Platforms (Eris, Ripple, Ethereum, Nxt, and a few others [25]) and programming languages (e.g., *Solidity* and *Serpent* [29]) have emerged for people to build decentralized applications (DApps). However, not all of these blockchain platforms offer enough flexibility for developing smart contracts [10]. Table 6.1 shows a comparison of a selection of some of these blockchain platforms, after which the platforms are discussed in more detail.

Bitcoin's platform is great for processing cyptocurrency transactions but with a low compute capability. Within Bitcoins scripts there is a limited ability to add or implement any advanced logic [30]. For example, in Bitcoin it is possible to add logic requiring multiple signatories to a transaction before payment but changes will have to be implementedto the mining functions and mining incentive schemes to enable smart contracts on Bitcoins blockchain. However, Sidechains (blockchains that are connected to Bictoins blockahin) could enable smart contracts with an ability to transfer value from the main blockchain to the sidechain. According to Back et al. [31] a sidechain enables bitcoins and other ledger assets to be transferred between multiple blockchains. This gives users access to new and innovative cryptocurrency systems using the assets they already own.

NxT is a public blockchain platform that contains smart contracts that are already live. However, it is not 'Turing-complete' in the sense that it does not allow customized smart contracts to be developed, existing templates have to be used.

Table 6.1 Smart contract enabled and disabled (public and private) blockchains

	Blockchains without smart contracts	Blockchains with smart contracts	Blockchains with turing-complete smart contracts
What?	Dispersed storage	Dispersed compute: holds the capacity to compute pre-defined logic	Dispersed compute: holds the capacity to compute any logic
Examples	Bitcoin (public) Litecoin (public) Multichain (private)	NXT (public)	Ethereum (public) Eris (private) Clearmatics (private)

Adapted from [10]

On the other Ethereum is a public blockchain platform, which is currently the most, advanced 'Turing-complete' coding system. Ethereum contains smart contract implementation functionality [32, 33]. Customized smart contracts can be developed and deployed on a whole blockchain network. Lewis states that there are mechanisms in place to prevent abuse, and you have to pay for compute power in Ethereum, by passing in 'ether' tokens which act as payment for the miners who run your code [10, 29].

According to Ethereum co-founder, Vitalik Buterin, Ethereum is a platform that is specifically designed for people to build and deploy trustworthy and decentralized applications (DApps). The questions is what will you build on top of Ethereum? [34, 35] Companies like American Express, Deloitte, Goldman Sachs, MasterCard and the New York Stock Exchange, have also poured millions of dollars into blockchain firms, particularly Ethereum [32].

In a peer-to-peer financial ledger, it is a must for every dealing to maintain the absolute amount of funds, otherwise entities will have the ability to freely allocate as much money as they want to themselves. Various ways of enforcing these rules can be imagined but at the moment, there are two leading paradigms inspired by Bitcoin and Ethereum for expressing these rules [9]. The Bitcoin method, checks every transaction based on: (a) the database entries removed by that transaction and (b) the entries generated. In a financial ledger, the rule states that the total portion of funds in the removed entries must be equal to the total number of those generated.

The second paradigm that emanates from Ethereum is smart contracts. This states that a smart contracts' program must carry out all changes to the contract's data. In traditional databases, this can be identified as an enforced stored procedure.

Smart contracts' data is modified by user requests sent to its code. Whether and how to fulfill these requests is resolved by the smart contracts' code as shown in Fig. 6.1. As in this example, the smart contract code for a financial ledger performs the same three operations as the controller of a centralized database: checking for satisfactory funds, withdrawing from one account and adding to the balance of another account. These two paradigms are adequate, and each has its merits and demerits. In a nutshell, superior concurrency and performance is catered for by bitcoin-style transaction constraints, enormous flexibility is catered for by Ethereum-style smart contracts [9].

Koulu [33] presents an example of a non-deterministic smart contract between two parties developed using the Solidity programming language and deployed on an Ethereum blockchain network is presented. His example has demonstrated that a simple contract between two parties can be translated into code lines, a 'smart contract code' [8, 33, 35]. This transformation, however, differs significantly from the impression a lawyer has about contracts. This example raises questions on the boundary between law and the blockchain architecture. It can be noticed that legally relevant occurrences take place in smart contracts: they accommodate to predictable expectations that are, somehow, linked with those created by the legal system [12, 33].

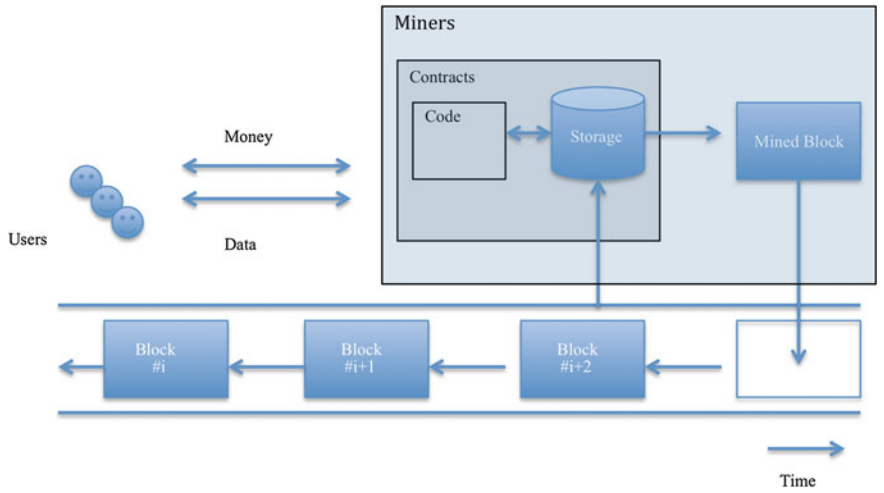


Fig. 6.1 A view of a decentralized cryptocurrency system with smart contracts. Adapted from [13]

6.3 Smart Contracts for Decentralized Autonomous Organizations (DAO)

According to Matt Levine at Bloomberg [11], the best opportunity for smart contracts is embedded in business organizations. The capability of the blockchain to eliminate the need for trust will allow people to stop working for aged style organizations, instead each individual will be an entity in a commercial system operating on the blockchain. The functions of a company's leaders and board can be reduced to smart contracts implemented in computer programs. Investors can make decisions over e-voting and such a decentralized organization will be exempt from external influence because it will operate just the way it has been programmed to.

The old way was that a group of individuals came together to set up an organization for commercial purpose, another group brought the investment to run it, others ran the business and others worked for it and decisions on how to share the benefits or profit at the end of the day were difficult to make [11]. The new way is that a group of individuals put their money into a company organized with smart contracts without any difficult decisions to make in the future apart from how and whether to retrieve their money if a hacker steals it. Research has shown that people agree with the premise that the smart contract approach is better than the previous approach which requires human activity [11].

The biggest challenge facing the potentials of smart contracts in organizations is likely the human element [36]. Individuals like their freedom, and the blockchain has to find a way to detach them from organizational hierarchies and not making them subject to a new leader; the blockchain itself. However, smart contract should

not be underrated. Some ideas for using smart contracts are amazing. Toyota Financial services has played with the idea of connecting blockchain smart contracts to cars such that if people miss their car finance payments, the car will not turn on and the ownership of the car can be reassigned to a new owner. But people would rather use this option to finance their car because they will get a better deal at a cheaper rate without the need a bank or for an investor acting as a middleman [36], they will pay directly to Toyota and this will reduce finance interests.

Smart contracts act in real time and reduce the chance of human error and cases of fraud prone processes, increase privacy and trustworthiness. These are no doubt features of smart contracts that can be added on top of existing business processes for improved efficiency. A company based in San Francisco called SmartContract [26] has developed technology capable of connecting smart contracts to external data feeds, internal infrastructure and external payments.

Sections 6.3.1 and 6.3.2 will elaborate on how smart contracts can be used to build internal and external organizational relationships while enforcing business rules, improving efficiency and performance within (between departments) and outside organizations (for example or between suppliers or shareholders and the business).

6.3.1 Internal Relationships for Organizations

Inter-departmental communication and partnership is crucial in organizations to improve knowledge sharing and organizational efficiency. Departments should posses build and manage relationships based on trust and commitment [37].

In a centralized organization several setbacks exist with inter-departmental intelligence. Inadequate inter-departmental relationships can cause inadequate customer service, trust issues and clashes within the organization [38]. Research is on-going in the area of inter-departmental conflict management and resolution in organizations [39].

When departments rely on each other to deliver factual information, this removes the extra fact-checking process that slows down productivity. When inter-departmental transmission is poor, customer service can deteriorate. For example, if because the accounts receivable department is not communicating properly with accounts payable and a client continues to get a bill for an invoice that has already been paid for, then there is the risk of losing the customer. If your sales department loses business because the manufacturing group was unaware of an increase in product demand, then your company suffers a loss of revenue. If the shipping department is not advised of an essential shipment in time to make next day delivery, this can cause a clash between several departments in an [38].

Taking all these scenarios into consideration, it is rather clear to see the colossal potential of smart contracts in promoting synergy between departments. If departments transact with each other on a blockchain network (a network of decentralized departments in an organization), then smart contracts can be used to implement and monitor day-to-day business processes in the form of *if this*, *then do this*.

For example, if there is an unusual increase in product demand, notify manufacturing department to step up production. This will immediately eliminate human errors and oversight. More complex and changing environments create a greater need for functions to interact and this means working together to build new forms of customer value [40].

6.3.2 External Relationships for Organizations

It is important for business to maintain a good relationship between other businesses, suppliers, vendors and investors who provide credit facilities necessary for running an organization. This is where smart contracts come in. Organizations can connect their existing infrastructure to smart contracts, keep using existing IT systems for off-chain data and reports, but connect those systems with smart contracts [26]; allowing them to trigger steps in a smart contract's lifecycle. Different applications within enterprise software systems (e.g., SAGE, SAP ERP, etc.) can be connected with a smart contract reducing the staff work load while allowing staff to focus on the customers rather than carrying out repetitive tasks which reduce staff motivation, restrict staff attention to running the systems and verifying records manually allowing room for fraud. Enterprise systems will be able to automatically check inventory based on stored data retrieved from an 'Oracle' and procure from suppliers if and when supplies are low for production.

Imagine speaking to a contract and asking it questions about a particular supplier or vendor such as whether the vendor complete a supply within time and budget or how a supplier has performed in the past [41]. These thoughts can now become a reality because the building blocks exist with smart contract enabled blockchains. Smart contracts can further automatically make direct payments to suppliers without the need to wait for Bank processing times when the delivery of goods have been verified depending on the business rules of an organization programmed in the smart contract code.

The World Economic Forum states that since the blockchain allows irrevocable transactions to take place in real time then it means that counterparty risk can be eliminated and transaction costs can be greatly reduced [42]. Suppliers will be able to get paid in real time and procurement will become faster for business organizations. Smart contracts in turn can be used to develop 'smart securities': smart bonds, equities and other financial instruments that could service themselves throughout their life cycle, for example paying their own coupons and dividends and acting as their own custodians. This could enable members of staff within an organization to become shareholders of the organization, thus motivated to see that the organization succeeds and reaches its full potential: 'a decentralized and efficient organization' [42].

The efficiencies created by smart contracts in industries where accurate monitoring and execution of high-value contracts is critical will be the first to benefit from this technology. Insurance [43, 44], derivatives [45], and trade finance are among the early adopters who will see large gains in profit due to the extremely low

cost of servicing a fully automated smart contract. According to San Francisco based SmartContract, instead of multiple people from different departments to call a data source or check a website for information such as price, location and weather for proof of performance, the contract itself can automatically check for proof of performance [26].

Smart contracts can also be referenced by multiple private systems at the various companies that are contract participants, making the smart contract a single point of truth that is tamper resistant and can be relied upon to trigger payment, accounting and compliance events for internal systems [26]. An association of seven banks including CIBC and Santander is asserting a breakthrough, ranking among the first financial institutions in the world to have transferred real money beyond borders with the use of a blockchain-based [46].

The Banks convert money into Ripple's (the platform they use) digital currency and complete transactions in real time, as opposed to the three to five days that it normally takes. It is worth to consider that the global financial system is composed by a large number of computers that indicates how much money everyone has, and a cross-border payment just updates the computers to indicate that one bank has more money and the other has less; a process that *shouldn't take five days*. The fact that it does take much time, makes it easy to understand why people are so excited for the blockchain, despite all the hacks [46].

Researchers have found some of the benefits of constructing smart contracts in organizations. In a study on corporate governance, Yermack [47] states that smart contracts on a blockchain could reduce the costs of trading and bring about more clear ownership records for shareholders, while allowing crystal-clear real-time shares transfer from one owner to another [47].

Managerial ownership could become much more transparent, with insider buying and selling detected by the market in real time, and chicanery such as the backdating of stock compensation becoming much more difficult, if not impossible. Corporate voting could be more precise and activities such as empty voting would become harder to carry out secretly. Any and all of these changes could dramatically affect the balance of power between directors, managers, and shareholders [47].

This leads us to the example of an organization that requires a loan from a financial institution. It takes much time and paper work to transfer a loan from a financial institution to an organization [48]. Thus, in a report on the future of financial infrastructure, the World Economic Forums (WEF) imagines the process like this [56]:

- A firm applies for a loan from a financial institution (FI) acting as the lead arranger.
- Taking advantage of the Companys' digital identity, the FI performs KYC (know your customer) activities very quickly through the distributed ledgers' (blockchain) record-keeping component that also provides regulators with a crystal-clear view of activity.

- The financial records and risk tolerance of the investor stored on the DLT automates the selection process; minimizing the time it takes to form an association.
- Making use of financial information about the firm and project plan data accessible through the DLT, diligence activities are mechanized via a smart contract.
- Important features from the diligence process are added into the underwriting template Key attributes from the diligence process are populated into the underwriting template, consolidating the process and minimizing time through the DLT's transfer of value capability.
- Smart contracts take out the need for a third party to fund the loan, disperse funds and facilitate the loan servicing process.
- Enclosed regulation facilitates the review of financial details to ensure that procedures are followed appropriately.

The World Economic Forum's vision for loan application and transfer seems to reduce privacy for organizations, as their data will be globally visible to investors and financial institutions. However, it will achieve the main goal which is the timely availability of funds to run organizations and smooth running of businesses while reducing interest rates and loan servicing and processing costs currently charged by Banks (the middlemen).

6.4 Organizational Benefits of Smart Contracts

In previous sections, some of the advantages of smart contracts have been highlighted, such as privacy, disintermediation, self-enforcement and trust [5, 16, 33, 35, 49, 50]. In this section, some of the reasons why organizations should deploy smart contracts are presented. Smart contracts decentralize a centralized or federated service in order to improve transparency, reduce the need for trust and sometimes gain economic efficiency because you no longer have to pay a central arbitrator to do a particular task. Having a central party governing contracts poses so many risks, such as; data privacy, reliability, trust, monopoly, expensive, privacy, and authenticity [50]. In summary, the following are guaranteed with smart contracts:

- Anonymity: participants can be completely anonymous but transfer of value from one party to another is guaranteed. In a commerce scenario, because the system ensures that the buying party has the ability to pay, the seller does not need to know the identity of the person buying. The smart contract ensures that the funds reach the account of the seller upon fulfilling a pre-agreed condition. This ensures that peoples credit card information is protected and cannot be stolen or used for fraud [49].
- Value can only be spent or transferred the way parties intended.

- No central actor has to be paid as the system is decentralized [16, 33, 34].
- Trust model is understandable prior to the flow of value from one party to another.
- Self-enforceable. Smart contracts can automatically execute the contract, e.g., allocate resources autonomously regardless of trust between parties. There is no need to trust third parties such as escrow services or credit card companies [33].
- The cost of changing the rules is extremely low. Computer code can 'easily' be re-written depending on programmers experience.
- The network hosting the smart contract can always take custodial risk instead of an improbable third party.
- None of the communication or transactional anonymity developed for blockchain platforms has to be sacrificed to use smart contracts. For example, anonymous voting system or lottery system.
- Atomicity: because of the mining concept of the blockchain where each node in the network is rewarded for carrying out a transaction, an entire operation runs or nothing does [24].
- Synchrony: no two operations can interfere with each other.
- Immortality: According to Hoskinson, objects can never be deleted—unless they commit 'voluntary suicide' [24].
- Immutability: objects cannot be changed [51].
- Permanence: objects are permanent and stored on a blockchain (history of linkable and traceable transactions) [5].

6.5 Organizational Challenges of Smart Contracts and Licensing

Despite the enormous potentials of smart contracts, several challenges that need to be addressed still lie in the pipeline. In order for smart contracts to be 'complete' to a large extent, authors have highlighted some of these challenges and some have also gone further to advocate possible solutions. These challenges are discussed in what follows.

6.5.1 Enforcement and Variations

For smart contract code, the key requirement is that the code should execute successfully and accurately to completion, within a reasonable time. If the execution platform is in complete control of all of the actions that the smart contract code wishes to perform, then these actions should be executed faithfully and with reasonable performance. Things that can go wrong (and therefore require 'enforcement') might either be technical issues within the platform, or issues that take place outside of the execution platform.

In a system with enforcement by tamper-proof network consensus, there would be no 'execute override' provisions. Currently, agreements once deployed as smart contract code, could not be varied. But it is quite common for provisions of an agreement to be varied dynamically. For example, allowing a regular client to defer paying interest by a few days, or to permit a paid holiday for a hardworking member of staff in an organization. Unless every possible foreseen variation is coded in advance, none of this would be possible in a tamper-proof system. Smart contracts only focus on pre-programmed execution [52].

An obvious example of something that could go wrong outside the execution platform would be the processes in the physical delivery of goods [52]. As an example, Mike does not like to go shopping physically but instead likes to shop online. Mike purchases an item online from a seller and chooses a delivery date. The money is then taken from Mike and held by the smart contract enabled system, which has been programmed to pay the seller if Mike receives his goods on the agreed delivery date or return the money to Mike if he does not receive the goods on the agreed date. However the courier company the seller uses to send the Goods to Mike fails to deliver the goods on time but instead deliver the goods a day after the chosen date. The smart contract however, based on its construction decides that the seller failed to deliver the goods and sends the money back to Mike's account. Nonetheless, the goods arrive the following day at Mikes address. The smart contract has no way of identifying that this was not the intention or fault of the seller but that the fault of courier company adopted by the seller.

In real-world situations, the initial agreement is usually not the final say. Agreements are sometimes negotiated if possible and modified to cater for unforeseen circumstances that were difficult to predict at the beginning. The self-enforcement characteristic of pre-written logic (smart contracts) means that the current smart contracts in distribution are not flexible to changes in the real world.

6.5.2 History of Hacking

Chapter 4 has discussed in full the security issues around blockchain. In this section we will discuss particular security issues related to smart contracts.

The limitations of relying on smart contracts have been exhibited by the attack on the Distributed Autonomous Organization (DAO) [33], which drained $53 million before changes were made to the computer code to restore the funds. The DAO is a collection of smart contracts, a new early-stage investment fund without manager (see also Chap. 4). Instead of having a manager, investors vote on which projects they decide to fund and the software does the rest. The DAO promoted itself as a smart contract that is borne from immutable, unstoppable, and irrefutable computer software, operated in its entirety by its members. Expressed in a different way, the DAO was intended to be like the digital currency Bitcoin in that it would operate without any governmental intervention.

The transfers made did not infringed the smart contract but exploited weaknesses in the computer code. If the code is seen as the law, as some smart contract

proponents have asserted, what happened with DAO was within legal parameters. The organizations running the software voted to restore the funds to the original investors in late July 2016 [14]. The DAO code was incomplete because it did not foresee the possibility that software errors could result in unexpected wealth transfers from participants to others. It cannot be argued, however, that this gap in the code emerged because of an event that could not have been anticipated. Even though the hack and movement of funds was not anticipated, Gideon Greenspan, founder and CEO of Coin Sciences, the company behind the MultiChain platform for private blockchains, argues that any large piece of computer code will usually contain bugs that are not easily detected during testing [9].

6.5.3 Smart Contracts' Code

Reviewing a smart contract code can be time consuming for a lawyer who is not a programmer [14]. The use of smart contracts requires programming skills, but web-based applications can bring the technology within everyone's grasp. The question of digital literacy, however, remains as this new model of contractual relations relies on a different technological functionality that varies significantly from the traditional understanding of contract law and dispute resolution [33]. Everyone reads English, so in some ways it's easier to read a traditional paper contract. But this is still very introductory technology, so no one can tell what kind of user interface improvements will be made eventually [7].

The interdisciplinary nature of blockchain technology, and 'smart contracts' in particular, lead people to see the technology as primarily belonging to their own discipline, at the expense of the others. Lawyers often look at smart contracts and see marginally improved legal agreements, without appreciating the fuller potential of smart contract code to extend beyond law's reach. Developers, on the other hand, consider smart contracts and see the limitless possibilities of software, without appreciating the subtleties and commercial realities reflected in traditional legal agreements. As with any interdisciplinary field, both must learn from the other [15].

6.5.4 Dispute Resolution Complexity

A substantial quantity of low intensity online disputes takes place in relatively simple realistic circumstances. For instance, a common e-commerce dispute regarding whether the paid goods have been delivered or not can easily be verified through a delivery note. The resolution of simple cases like the one previously exposed is likely to benefit from automation through smart contracts. We need to see, however, how more complex disputes can be automated. For example, the quality of delivered goods is something that may not be that simple. The question is not whether all forms of dispute resolution can be solved by technological means but which dispute categories can—and should-be automated [33]. One question is

how dispute resolution could be organized through a blockchain infrastructure. Another question is what mechanisms exist or should exist for smart contracts that are irreversible by default [33].

6.6 Recommendations for Organizations

The first step in designing smart contracts is to understand the problems being solved by any existing paper contracts or legal documents. If a smart contract is to replace the paper contract, then it should be able to solve all the problems or provide benefits to parties that exceed the costs of not solving all the problems.

The second step would be to develop smart contracts that preserve some of the abilities of traditional paper contracts. For example, implementing the ability for parties to renegotiate at any point in time in cases whereby the parties increase or decrease or want to reveal their identities. The replacement of one smart contract with another should also not pose any difficulties. This also applies to the use of smart contract templates—the smart contract should be easily editable to provide some flexibility for reuse [12].

Finally, the people aiming to implement smart contracts should also give serious consideration to what happens in those circumstances where renegotiation is convenient but the parties cannot reach an agreement. There are examples of appealing to the relevant community for a decision in the paper world, but it is relatively rare. The problem with these types of approaches is that participants in the decision may make a decision based on their own personal interests. What the parties to most contracts are looking for, however, is to place jurisdiction over the contracts in a place where the parties have confidence that their case will be fairly determined by a disinterested court applying well-developed legal standards [14, 33].

Therefore, smart contracts can have an optimistic future but face some problems that must be addressed beforehand, such as dealing with the potential for coding errors. However, to reach their potential fully, smart contracts are going to have to be flexible and adaptable to real life situations because in the real world the initial contract or agreement is not always the final say [14, 33].

6.7 Case Studies

This section outlines and discusses real-world examples of the implementation of smart contracts in various industries.

Barclays bank recently tested a way to trade derivatives using smart contracts and a blockchain-like technology being developed by a consortium of the world's leading banks [15, 45].

A derivative is essentially a trading contract between two or more parties that can take many forms and is based on an underlying asset [53]. Currently, the contracts are made up of three main parts with a body called the International

Swaps and Derivatives Association (ISDA) creating the standards across the financial world for derivative trading. But the process is arduous with current paper contracts in the form of computer documents still being issued [15, 45].

Point of Attention This case study shows how smart contracts have been adopted in the financial sector to reduce data redundancy, while ensuring that transactions are done in real time. This was something that was not achievable in the past by human efforts.

A smart contract on the other hand can automatically execute the terms of a contract when certain conditions are met, potentially taking a lot of the human involvement out of completing a deal. Using smart contracts on a blockchain, all the banks will have the same document that will not vary slightly from bank to bank, and something that can cause delays and unnecessary human intervention. Currently, each party has their own version of the legal documents. By having centralized documentation storage all parties will be able to settle trades quicker and cheaper.

Also, insurance companies will be able to provide temporal liability insurance. For instance, using smart contracts, an insurance company could charge rates differently based on where and under what conditions customers are operating their vehicles. For example, a car driven on a clear day, gathering information about the weather conditions from a weather service, in an area where all the roads are repaired, having verified with information about road repairs supplied by the Department of Motor Vehicles, for instance, would be charged a lower rate compared with a car that's being operated in bad weather, perhaps on pothole-filled roads [16].

Germany-based insurance giant Allianz successfully used blockchain-based smart contracts to handle catastrophe swaps and bonds and they reported that the technology could boost marketability of the financial instruments [43, 44].

'Cat swaps' and bonds are instruments that protect insurers against huge potential losses following a major catastrophe, actually, activated under predefined parameters. In other words, cat swaps and bonds allow risk transfer from one insurer to another [54].

Point of Attention From this case study, it is evident that smart contracts can make insurance rates flexible. This has the potential of increasing income for insurance firms, as customers will likely be interested in a flexible insurance rather than one with fixed prices. Smart contracts can be used to reduce the number of fraudulent claims going on in the insurance industry. Prevent double claims by customers from two different insurers.

However, the payments between insurers and investors can drag on for weeks or months after a disaster. According to Allianz, automating the process via smart contract technology, though, has the potential to reduce that time to as low as a few hours [44]. Other industries where the potential usefulness of smart contracts have been speculated include supply chain and logistics [16, 55].

6.8 Summary

Smart contract programs are self-enforceable and for this reason many prefer the term 'smart agent', corresponding to the more general concept of a software agent. Sooner or later the use of this term will fade as the blockchain technology evolves. Developers will prefer to refer to a programming language (e.g., solidity) as opposed to a general terminology that describes a complicated operation that works on the blockchain ('smart contracts') [15].

Part of the uncertainty of meaning around 'smart contracts' results from the relationship between the legal concept of contract and the element of 'smart', i.e. the fact that the contract could be embedded within and defined by software [33]. Despite unforeseen pitfalls, the promise of smart contracts is clear [12, 16, 33, 34].

The task at hand for legal scientists is to map out the legal implications of the blockchain architecture and to conceptualize it for future policy recommendations. The inevitable fact is that the technology has a tendency to develop faster than the legal system can react. Technological innovations and applications do not wait for the legal system to catch up [33].

Long-term research may lead from existing disjointed computer code and natural language legal documents to source languages which can be automatically translated into both executable code and legal documents, with the both being admissible in courts. Even longer term research could result in formal languages which themselves are admissible in court [52]. The appearance of legal programming is near [33]. The technology has the potential to change our understanding of contractual law, of dispute resolution and enforcement and the divide between public and private use of power.

Forward-thinking law firms should future-proof by tooling up and building in-house capabilities for developing and deploying smart contracts. Students with legal ambitions should gain coupled skills of law and programming those who can close that gap between law and computer science will be highly needed in the near future [10].

The contracts in use today are static files managed by individuals. In our world today where airplanes and cars drive themselves, its definitely time for contracts that are managed and executed by themselves [41]. The days of a contract being read, interpreted, acted upon and managed by contracting personnel seem to be nearly over. Actually, smart contracts may imply that in a near future we probably do not need people to manage contracts, because contracts can be self-enforced.

References

1. Hart O, Moore J (2002) Contracts as reference points. Q J Econ CXVII:1–48
2. Taylor R (1984) Licensing in theory and practice: licensor-licensee relationships. Antitrust Law J 53:561. 1
3. The Law Handbook: What is a contract? Available online at: http://www.lawhandbook.org.au/07_01_01_what_is_a_contract/. Accessed 25 Aug 2016
4. BusinessDictionary: Contract. Available online at: http://www.businessdictionary.com/definition/contract.html. Accessed 23 Aug 2016
5. Lim C, Saw T, Sargeant C, Smart contracts: bridging the gap between expectation and reality. Available online at: https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality. Accessed 25 August 2016
6. Szabo N (1997) Formalizing and securing relationships on public networks. First Monday 2 (9)
7. Cassano J, What are smart contracts? Cryptocurrency's Killer App. Available online at: http://www.fastcompany.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app. Accessed 25 Aug 2016
8. Idelberger F, Governatori G, Riveret R, Sartor G (2015) Evaluation of logic-based smart contracts for blockchain systems. In: Alferes JJ, Bertossi L, Governatori G, Fodor P, Dumitru R (eds) Rule technologies. research, tools, and applications 10th international symposium, RuleML 2016, Stony Brook, NY, USA, July 6–9, 2016. Volume 9718 of the series lecture notes in computer science, pp 167–183, Springer, Switzerland
9. Greenspan G, Why many smart contract use cases are simply impossible. Available online at: http://www.coindesk.com/three-smart-contract-misconceptions/. Accessed 28 Aug 2016
10. Lewis A, A gentle introduction to smart contracts. Available online at: https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/. Accessed 28 Aug 2016
11. Levine M, Herbalife deals and blockchain dreams. Available online at: https://www.bloomberg.com/view/articles/2016-08-26/herbalife-deals-and-blockchain-dreams. Accessed 29 Aug 2016
12. Stark J, How close are smart contracts to impacting real-world law? Available online at: http://www.coindesk.com/blockchain-smarts-contracts-real-world-law/. Accessed 24 Aug 2016
13. Delmolino K, Arnett M, Kosba AE, Miller A, Shi E (2015) Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab. IACR Cryptol ePrint Arch 460
14. Wall L, "Smart contracts" in a complex world. Available online at: https://www.frbatlanta.org/cenfis/publications/notesfromthevault/1607. Accessed 29 Aug 2016
15. Stark J, Making sense of blockchain smart contracts. Available online at: http://www.coindesk.com/making-sense-smart-contracts/. Accessed 24 Aug 2016
16. Troy S What is a smart contract and what's it good for? Available online at: http://searchcio.techtarget.com/feature/What-is-a-smart-contract-and-whats-it-good-for. Accessed 24 Aug 2016
17. Ressler S, Bitcoin micropayments, a new enabling technology. Available online at: https://bitcoinmagazine.com/articles/bitcoin-micropayments-new-enabling-technology-1398880834. Accessed 29 Aug 2016
18. Isaacson W, How bitcoin could save journalism and the arts. Available online at: http://time.com/3476313/can-bitcoin-save-journalism/. Accessed 29 Aug 2016
19. Perez YB, How blockchain tech is inspiring the art world. Available online at: http://www.coindesk.com/blockchain-technology-inspiring-art/. Accessed 27 Aug 2016
20. Stephan Vogler: Introduction. Available online at: http://www.stephanvogler.com/en/. Accessed 3 Sept 2016
21. Ghorashi H, Mak Vienna becomes first museum to use bitcoin to acquire art, a harm Van Den Dorpel. Available online at: http://www.artnews.com/2015/04/24/mak-vienna-becomes-first-museum-to-acquire-art-using-bitcoin-a-harm-van-den-dorpel/. Accessed 24 Aug 2016

22. Emory S, Here's the first museum to buy art with bitcoins. Available online at: http://thecreatorsproject.vice.com/en_uk/blog/heres-the-first-museum-to-buy-art-with-bitcoins. Accessed 28 Aug 2016
23. Gottfried G, How "the blockchain" could actually change the music industry. Available online at: http://www.billboard.com/articles/business/6655915/how-the-blockchain-could-actually-change-the-music-industry. Accessed 24 Aug 2016
24. Hoskinson C, A brief introduction to smart contracts. Available online at: https://www.youtube.com/watch?v=3bY66Zgr8Cs. Accessed 29 Aug 2016
25. Xu X, Pautasso C, Zhu L et al (2016) The blockchain as a software connector. 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA 2016), Venice, 2016, pp. 182–191
26. SmartContract: Smart contract oracles. Available online at: http://about.smartcontract.com
27. Ellis L (2013) Housing and mortgage markets: the long run, the short run and the uncertainty in between 8:1–16
28. Benson E (2013) Mockup driven web development. In: Proceedings of the 22nd international conference on world wide web companion, pp 337–341
29. Delmolino K, Arnett M, Kosba A et al (2015) A Programmer's guide to ethereum and serpent acquiring the virtual machine, Available at https://www.cs.umd.edu/∼elaine/smartcontract/guide.pdf. Accessed 4th January 2017
30. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. 9. www.Bitcoin.Org
31. Back A, Corallo M, Dashjr L, Friedenbach M, Maxwell G, Miller A, Poelstra A, Timón J, Wuille P (2014) Enabling blockchain innovations with pegged sidechains, pp 1–25
32. Brown C, How companies are using ethereum as an advanced version of bitcoin. Available online at: https://due.com/blog/ethereum-advanced-version-bitcoin/. Accessed 2 Sept 2016
33. Koulu R (2016) Blockchains and online dispute resolution : smart contracts as an alternative to enforcement. Scripted A J Law Technol Soc 13
34. Schneider N, Meet Vitalik Buterin, the 20-year-old who is decentralizing everything. Available online at: http://www.shareable.net/blog/meet-vitalik-buterin-the-20-year-old-who-is-decentralizing-everything. Accessed 24 Aug 2016
35. Buterin V (2014) A next-generation smart contract and decentralized application platform. Etherum 1–36
36. Coy P, Kharif O, This is your company on blockchain. Available online at: http://www.bloomberg.com/news/articles/2016-08-25/this-is-your-company-on-blockchain. Accessed 29 Aug 2016
37. Blomqvist K, Levy J (2006) Collaboration capability–a focal concept in knowledge creation and collaborative innovation in networks. Int J Manag Concepts …. 2:31–48
38. Root GN, The importance of communication between different departments in an organization. Available online at: http://smallbusiness.chron.com/importance-communication-between-different-departments-organization-11901.html. Accessed 13 Sept 2016
39. Walton RE, Dutton JM (2016) The management of interdepartmental conflict : a model and review 14:73–84
40. Hulland J, Nenkov GY, Barclay DW (2012) Perceived marketing-sales relationship effectiveness: a matter of justice. J Acad Mark Sci 40:450–467
41. Chesebro R (2015) A contract that manages itself: the time has arrived, Defense AT&L: January–February 2015
42. Lehmann A, Why banks shouldn't fear blockchain. Available online at: https://www.weforum.org/agenda/2016/06/why-banks-shouldn-t-fear-blockchain/. Accessed 29 Aug 2016
43. Allianz Press Release: Blockchain technology successfully piloted by Allianz Risk Transfer and Nephila for catastrophe swap. Available online at: http://www.agcs.allianz.com/about-us/news/blockchain-technology-successfully-piloted-by-allianz-risk-transfer-and-nephila-for-catastrophe-swap-/. Accessed 3 Sept 2016

44. Palmer D, Allianz tests blockchain to boost catastrophe bond trades. Available online at: http://www.coindesk.com/allianz-blockchain-smart-contracts-boost-catastrophe-bond-trading/. Accessed 3 Sept 2016
45. Kharpal A, Barclays used blockchain tech to trade derivatives. Available online at: http://www.cnbc.com/2016/04/19/barclays-used-blockchain-tech-to-trade-derivatives.html. Accessed 1 Sept 2016
46. Levine M, Conflicted deals and stress tests. Available online at: https://www.bloomberg.com/view/articles/2016-06-23/conflicted-deals-and-stress-tests. Accessed 29 Aug 2016
47. Yermack D (2015) Corporate governance and blockchains. NBER Working Paper Series December. Available at http://www.nber.org/papers/w21802. Accessed 20 Nov 2016
48. Levine M, Kitten hugs and the blockchain heart. Available online at: https://www.bloomberg.com/view/articles/2016-08-12/kitten-hugs-and-the-blockchain-heart. Accessed 29 Aug 2016
49. Fairfield J (2014) Smart contracts, bitcoin bots, and consumer protection. Wash Lee Law Rev Online 71:35–50. Accessed 3 Sept 2016
50. Wood G, DEVCON1: ethereum. Available online at: https://www.youtube.com/watch?v=U_LK0t_qaPo. Accessed 29 Aug 2016
51. Cuomo J, How businesses and governments can capitalize on blockchain. Available online at: https://www.ibm.com/blogs/think/2016/03/16/how-businesses-and-governments-can-capitalize-on-blockchain/. Accessed 9 Sept 2016
52. Clack CD, Bakshi VA, Braine L (2016) Smart contract templates: foundations, design landscape and research directions, pp 1–15
53. Parsons JE (2013) Hit or Miss: regulating derivative markets to reduce hedging costs at non-financial companies, MIT Center for Energy and Environmental Policy Research, CEEPR WP 2013-002, January 2013
54. Teh T-L (2015) Counterfactuals for the appraisal of disaster risk financing and insurance strategies. Br Actuar J 20:241–256
55. Camerinelli E, Blockchain in the supply chain. Available online at: https://www.finextra.com/blogposting/12597/blockchain-in-the-supply-chain. Accessed 3 Sept 2016
56. McWaters J (2016) The future of financial infrastructure—an ambitious look at how blockchain can reshape financial services, An Industry Project of the Financial Services Community | Prepared in collaboration with Deloitte, World Economic Forum. Available at http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf. Accessed 20 Nov 2016

Blockchain and Enterprise Systems

7

Abstract

Enterprise systems (ES) are large-scale application software packages that support business processes, information flows, reporting, and data analytics in complex organizations. While ES are generally packaged enterprise application software (PEAS) systems, they can also be bespoke, custom developed systems created to support a specific organization's needs. An integrated enterprise will need more than one specialized use case and will need to drive synergy to exploit the promises of enterprise blockchain fully. For example, an integrated enterprise system will generally handle more than one operation for a company to facilitate its business and management reporting needs. The success of blockchain consumption should initially focus on technology play, and enterprises should consider integration with existing enterprise systems. This will create ease in the collective understanding of this technology, while establishing a path of least disruption and accelerating enterprise adoption. The blockchains' main advantage is the concept of 'trustless' systems. A system that does not need a trusted party. However, in the 'Enterprise' world, the trusted party is already there, it's the 'Enterprise' itself. Blockchain technology can be inserted into and can be subsumed by larger systems, and it's best to think of blockchains in terms of what will eventually surround them. They will not stand alone, but will function within the core of multiple, increasingly distributed ecosystems. This Chapter will explain in detail how the blockchain technology can fit into the world of Enterprise Systems (ES) by comparing the value system of existing enterprise systems to that of the blockchain technology. The Chapter will also address the issue of where the blockchain can fit in and whether it is time to replace existing enterprise systems with the blockchain or rather make them work with the blockchain.

V. Morabito, *Business Innovation Through Blockchain*,
DOI 10.1007/978-3-319-48478-5_7

7.1 Introduction

In the 1970s due to the small capacity of computers and programming languages, when organizations identified a new problem, they developed discrete new information systems to manage the problem. If the new system had similar features with existing systems, they were often manually integrated. This meant that, for example combining information about sales and manufacturing was error prone [1] and detailed record analysis required manual record inspection. Organizations began to pursue the dream of one company, one system [1]. Software entrepreneurs began developing software packages, which shared a common database. These packages then became more advanced with the introduction of new technologies and improvement in the capacity of computers and programming languages and later became what we now refer to as *enterprise systems* (*ES*) [1, 2].

Since then, enterprise systems have emerged as the core of successful information management and the enterprise backbone of organizations [3]. An effective business strategy emphasizes on the use of information technology and information.

Enterprise systems (ES) include enterprise resource planning (ERP; transaction automation), customer relationship management (CRM; facilitate customer relationship management [4]), supply chain management (SCM; provide more sophisticated planning capabilities [4]), and product life cycle management (PLM). However, ERP is the most important class of ES [5]. ERP software integrates management information and processes, such as financial, manufacturing, distribution and human resources, for the purpose of enabling enterprise-wide management of resources [5].

Research has shown that ERP implementation enabled a 70% reduction in accounting personnel by eliminating duplicate data entry and many consolidation tasks [1]. An ERP is packaged business software that integrates solutions to support organization's business processes, efficient and effective use of resources as well as business processes standardized across the enterprise. According to Nah et al. [3], the most important attributes of ERP are its abilities to:

- *Automate and integrate* an organization's business processes;
- *Share common data and practices* among the enterprise. A seamless integration of all the information flow through a company [1, 2, 6]. However, it is possible that some organizations implement enterprise systems and configure them to exclude integration. For example, an organization may customize or only install the financial modules of the system thus depriving itself of the benefits of integrating accounting data with sales, and production or manufacturing [6]. Others might permit different departments to use different ERPs;
- *Produce and access information in a real-time environment* [3] enabling real-time business decision making.

Despite the benefits of ERP systems, some companies have failed to achieve the hoped-for financial returns on the ERP investment [1, 2, 6] and research has been on-going in the area of risk management during ES implementation in organizations [7]. Organizations that use enterprise systems have options to choose from during the implementation phase. They either bring in a consultant to carry out the implementation from start to finish, do it themselves with some assistance. Table 7.1 shows the technical reasons for adopting ERPs while Table 7.2 shows the business reasons why small and large organizations implement ERPs. However, some reasons for the non-adoption of ERPs include: dynamic company strategies, decentralized organizational structure, and a lack of features that fit organizations business goals or requirements in the market. More commonly, organizations may only choose to adopt parts of the ERP or modify the enterprise system to fit their goals [1].

According to Maas [2], the business benefits of implementing enterprise systems include the following:

- *Cycle time reduction*. Time reduction in business processes such as the time it takes to deliver products to customers and financial closing times.
- *Faster information transactions*. Crediting customers for returned items is now faster with ERPs.
- *Better financial management*. Reducing the time taken to carry out financial reporting and procurements from vendors.
- *Laying the groundwork for electronic commerce*. Offering customers web-based access to ordering, tracking and delivery processes.

One of the reasons for non-implementation of enterprise systems is a decentralized organizational structure [1]. Therefore, there is a potential for enterprise systems to leverage upon the decentralized aspect of blockchain technologies to support decentralized organizational structures. The following Sections will discuss 'enterprise blockchains'; factors to consider when moving from traditional

Table 7.1 Technical reasons for adopting enterprise systems, adapted from [1]

Small companies/Simple structures	Large companies/Complex structures
Integrate applications cross-functionality	✓
Replace hard to maintain interfaces	✓
Eliminate redundant data entry and difficulty analysing data	✓
Decrease computer operating costs	✓
Ease technology capacity constraints	✓
	Consolidate multiple different systems of the same type (e.g., general ledger packages)

Table 7.2 Business reasons for adopting enterprise systems, adapted from [1]

Small companies/Simple structures	Large companies/Complex structures
Accommodate business growth	✓
Improve formal and/or inefficient business processes	✓
Clean up data and records through standardization	✓
Reduce operating and administrative expenses	✓
Reduce inventory carrying costs and stockouts	✓
Eliminate errors and delays in filling out customer orders for merged businesses	✓
	Provide integrated IT support
	Standardize different numbering, naming and coding schemes
	Standardize procedures across different business locations
	Present a single face to the customer
	Improve companywide decision support

centralized ERPs to blockchain enabled ERPs. Furthermore, the benefits and likewise the challenges of implementing 'enterprise blockchains' will be discussed, followed by recommendations for organizations and lastly, a summary of the chapter.

7.2 Blockchain-Enabled Enterprise Systems

The core values of the blockchain technology include immutable transaction records, consensus (using the network to verify and validate transactions), decentralization and disintermediation. Research has shown that the packages in todays' ES rely on a central database which collects information from a series of applications as well as feeds information to these diverse applications while supporting various business functions [6, 8], as shown in Fig. 7.1.

According to Davenport [6] configuring a enterprise system included balancing the way you want to work with the way the system lets you work. You decide which modules to install and configure them to fit business processes including internal as well as external business objectives.

Learning from organizations that have implemented ES, it has been observed that enterprise systems are configurable, as firms have configured ES to suit their business strategies, enabling them to remain competitive [3, 6]. For example in the early 1990s, after a series of mergers, Elf Atochem North America, a chemicals branch of the French company called Elf Aquitaine, discovered that its business processes were hindered by the disconnect between its business software systems.

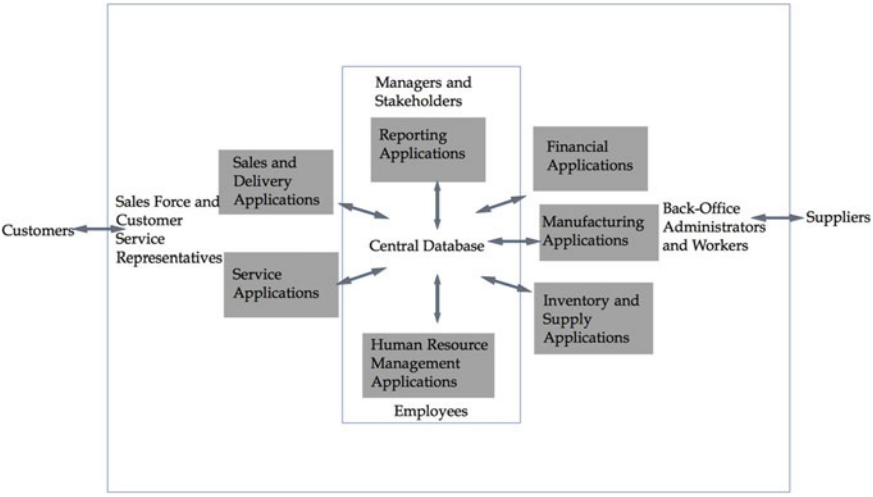


Fig. 7.1 The structure of an enterprise system, adapted from [6]

Their sales systems were not linked with their budget systems; this was the same for ordering and manufacturing systems. Each system handled its reports independently. As a result of the disconnected systems and in order to be more customer-focused the company chose to install only those Germany-based SAP Enterprise Resource Planning (ERP) modules required to support customer-oriented processes. It did not for example install modules without a direct impact on customers such as plant maintenance and human resource planning modules [6].

However, the design goals of adopting blockchain in any enterprise should focus on disrupting the incumbent system as little as possible. One way to go about this is to harmonize the blockchain technology and the enterprise system, thereby taking advantage of the blockchains features including its transaction processing techniques together with the enterprise systems of record as the channel for other applications such as business intelligence, reporting, regulatory interactions, and data analytics [9]. This points towards the decentralization of the legacy enterprise system structure depicted in Fig. 7.1. Thus allowing each application therein to communicate directly with each other and external applications. This will speed up system response times which will then speed up business decisions [10].

Looking at at Fig. 7.1, one can only wonder how enterprise systems can be transformed to 'enterprise blockchains'. The following Sections include factors that organizations need to take into serious consideration when making plans to implement this transformation. The dream of integrating enterprise systems with business processes can become a nightmare if a business rushes to implement them without having an understating of their implication on its business [6]. This is when enterprise systems and business strategies have a misunderstanding [6]. When an enterprise system, by its very nature, imposes its own logic on a company's strategy, organization, and culture.

7.2.1 Public or Private Blockchain Network

In Chap. 1 we analyzed the features of public and private blockchain. This section aims to describe how these two modalities can fit within the Enterprise Systems Context.

Organizations have to decide on whether to integrate existing ES with public or private blockchains depending on their objectives. According to Cuomo who is the IBM Vice President, Blockchain Technologies "*blockchain technologies must be enhanced to meet the needs of businesses*" [11]. The technology at the heart of the blockchain must be enhanced to be able to handle any security and privacy issues that might arise during its use—creating an 'enterprise-ready blockchain'. Furthermore, to be able to deal with the immense volume of transactions per second, minute or day, computer systems and networks must be designed constructed so that they can be adjustable and scale up to handle the growing number of transactions as industries and governments begin using the technology to handle their core organizational processes and complete their tasks in real-time rather than minutes [11]. "*Those companies that stress the enterprise, and not the system, gain the greatest benefits*" [6]. Davenport outlined the scope of enterprise systems [6]; some of the functions offered by Germany-based SAP's ERP package are as follows:

- **Financials**. Accounts receivable and payable; Asset accounting; Cash management and forecasting Cost-element and cost-center accounting Executive information system; Financial consolidation; General ledger; Product-cost accounting Profitability analysis; Profit-center accounting; Standard and period-related costing.
- **Human Resources**. Human resources time accounting; Payroll; Personnel planning; Travel expenses.
- **Operations and Logistics**. Inventory management; Material requirements planning Materials management; Plant maintenance; Production planning; Project management Purchasing; Quality management; Routing management; Shipping; Vendor evaluation.
- **Sales and Marketing**. Order management; Pricing; Sales management; Sales planning.

Software connectors can be referred to as the foundation of software interactions [12]. According to [12] a connector is an interaction instrument for software components and the services provided by a connector can be partitioned into four groups: communication, coordination, conversion and facilitation. This definition of software connectors implies that the blockchain can serve as a software connector between several applications in enterprise systems. The blockchain can provide communication via a decentralized shared ledger or database [13], coordination via transactions, smart contracts and validation oracles [14–16], conversion and facilitation (cryptography-based secure payments, transaction validations and permission management) [12].

Each node in a blockchain network consists of two layers, application or enterprise layer and the blockchain layer. Components of the application are implemented inside the blockchain connector in terms of smart contracts. The part of the application that lives outside the blockchain is usually used in hosting off-line data and application logic, and communicates with the blockchain through transactions [12].

One of the main constructive resolutions for software connectors is to decide what processes are achieved in the connector and what processes are is implemented in the component. In the case of the blockchain, the burden of this resolution lies in which data and computation should be situated on-chain or kept off-chain (Application Design Decision 1 in Table 7.3). Another decision concerns the access scope of the blockchain: public, private or consortium/community (Application Design Decision 2 in Table 7.3) [12].

The scope of enterprise systems (ES) as outlined by Davenport [6] gives an indication that blockchain enabled enterprise systems will require private blockchain networks. This is because of the functions provided by the ES, protecting business strategies from external forces such as business competitors and for the security of the transactions that take place within ES. For example, it will not be advisable to use a public blockchain platform for an organizations ES as this will expose their financial data and reports. Public blockchain platforms such as Ethereum has had its share of the unpleasant hacking experience [17]. Organizations such as Airbus, IBM, Sany, Samsung SDS [18] and a number of sponsors and members (from the healthcare, finance, Internet of Things, and other industries [19]) of the Hyperledger project have been highly interested in private blockchains because what can be achieved by organizations with the blockchain technology is restricted with public blockchains [20].

The Hyperledger Project, with support from it members such as IBM, Intel, and Accenture, is a collaborative effort to establish, build a sustainable open, distributed ledger enterprise platform [21].

The Hyperledger project's blockchain is a Linux-led 'private' blockchain initiative [18]. This project is different from 'public' blockchains in three major ways. Each posted item be encrypted and also permissions can be put in place to determine who can view the item. Additionally, each item can be digitally signed to identify who posted it [22]. The project is a collaborative effort, which aims to advance the blockchain for intra and inter-organizational transactions by identifying, and addressing important features for a cross-industry open standard for distributed databases that transform the way transactions are carried out around the world. The project is a Linux Foundation collaborative project and will be an enterprise-grade, open-source distributed ledger technology. The project once completed can be used to help companies manage the flow of goods and related payments or enable manufacturers to share production logs with original equipment manufacturers (OEMs) who make part or subsystems used in other companies end products and regulators to reduce product recalls [23].

From Table 7.3, considering the goal and services offered by enterprise systems and the quality attributes offered by the public and private blockchain types; the

Table 7.3 Design decisions developers need to contemplate when adapting the blockchain technology as a software connector and their reciprocal impacts on software quality attributes, adapted from [12]

Blockchain Design Decision 1
Techniques for Scaling up the Blockchain for Transaction Processing Carry out transactions off-chain; Carry out transactions in bit without signatures; Scalable protocol; Increase the size of blocks on the blockchain
Blockchain Design Decision 2
Mechanisms of selecting blocks to append to the blockchain Proof-of-stake, Proof-of-burn, Proof-of-work, Proof-of-retrievability
Application Design Decision 1
Capacity: on-chain Enable verification of computational result, limited computation power and data storage Examples: Metadata (V-A), Negotiable value (V-B) **Capacity: off-chain** More computation power and data storage, less cost, additional trust required Examples: Raw personal data (V-A), Sensitive information (V-B)
Application Design Decision 2 (Public blockchain vs. Privacy)
Public chain Growth potential to larger scale, Information transparency, trustworthy, existing user base Examples: V-A **Private chain** Restricted access, Mutability, Easier management, better privacy Examples: Consortium blockchain (V-B)
Application Design Decision 3
Single blockchain Easier chain management and permission management, harder data management and isolation Examples: V-A, V-B. **Multiple blockchains** Information isolation, harder chain management and permission management
Application Design Decision 4 (Internal or External Validation Oracle)
External Validation oracle Introduce a third party that will be trusted by the whole network Examples: Arbitrator (V-A) **Internal Validation oracle** Periodically injecting external state into the blockchain might introduce latency issues. The source of external state also needs to be trusted
Application Design Decision 5
Permissionless versus Permissioned blockchain Trade-offs: Performance, cost, censorship, reversibility, finality, flexibility in governance Permissions: Read/Join network, submit transaction, mine, create assets Example: Permissioned (V-A, V-B)

blockchain type that best suits ES services and goals is undoubtedly private blockchains (Application Design Decision 2, Public blockchain versus Privacy in Table 7.3). Public blockchains offer 'trustworthiness', however, in the 'Enterprise' world, the trusted party is already there, and it's the 'Enterprise' itself.

Currently, International Business Machines Corporation (IBM) is developing capabilities that can make the blockchain fit for business processes ('enterprise friendly blockchains') [20]. This implies for example, developing blockchains networks that are private and can be used within and between financial institutions. A step taken by a number of others, along with Swiss bank UBS. In comparison, bitcoin and other cryptocurrencies tend to rely public ledgers or blockchain networks [20].

7.2.2 Auditing and Logging

Auditing and logging is a must to satisfy regulations regarding regulated systems for purposes of non-repudiation, technology root cause analysis, fraud analysis, and other enterprise systems [24].

IBM's chief architect in charge of Internet of Things security Tim Hahn identified auditing and logging as one of the areas for improvement as part of his work to improve security by integrating blockchain and IBM Watson [25]. Transaction tracking, auditing and reconciliation processes are essential capabilities of business-to-business (B2B) processes [26]. The traditional business-to-business exchange models are one of the foundations of modern commerce. Traditional platforms allow these capabilities by the use of an implemented centralized transaction-trailing model that only lets businesses from one endpoint follow-up and record transactions. This can be slow and ineffective especially when it concerns with operations such as auditing, B2B transactions and reconciliation. A decentralized ledger can be a trusted way to allow business to track B2B transactions without the need for a central authority. This also comes with security abilities of the blockchain for more complicated auditing procedures.

7.2.3 Enterprise Integration

Integration with Incumbent Information storage systems or *System of Record* (*SoR*) is important to support existing and incumbent systems such as CRM, business intelligence, reporting and analytics, etc. Enterprise synergy (regulated data transfer between applications in Enterprise Systems, e.g., CRM, SRM, ERP, PLM). The blockchain as a transaction processing system will preserve the SoR as an interim approach to adopt a blockchain. The path of least disruption will accelerate the enterprise adoption [24]. It is advisable to create connectors to existing information storage systems to offload the reporting and regulatory requirements until the blockchain is enterprise aware, or rather, the enterprise software is blockchain aware [9]. This is because it is still unclear how the blockchain technology can be

used process and store business related data efficiently. Projects are on going to refine the blockchain technology for enterprises.

Furthermore, monitoring the 'enterprise blockchain system' is a must, to satisfy regulations and generally accepted IT practices for purposes of high availability, capacity planning, fault identification, and pattern recognition [24]. To be adopted in enterprise settings, the blockchain community needs to come up with solutions that can actively monitor the health of a blockchain network and recover from unexpected failures. These capabilities will allow organizations to monitor the runtime behavior of integrated blockchain solutions [26]. In other words, there is the need for programming frameworks that allow software developers to build applications against the blockchain. Such applications can be tailored to monitoring and fault prevention, whereby the state of enterprise blockchains state is logged at specified time intervals.

Besides monitoring the whole blockchain network and performance, each node on an enterprise blockchain network can be monitored independently and if the network is scalable, the fault from one node should not have ripple effects on the whole enterprise blockain network. For example, if one out of a group of organizations enterprise system on a shared blockchain network is compromised in terms of security, this should not affect the other organizations and such errors should not be a nightmare to fix as quickly as possible. Monitoring is necessary in an enterprise setting where system runtime is crucial to the performance of a business. Business transactions need to be processed in real time and blockchain enabled enterprise systems must live up to their expectations by providing flexibility, scalability and dependability. On the flip side, if this cannot be achieved with the blockchain then its integration with enterprise systems might not be necessary after all.

7.2.4 Enterprise AAA (Authentication, Authorization and Accounting) Requirements

Unlike the permissionless world of most crypto currency based blockchain networks, for example, the public Bitcoin blockchain, in a permissioned enterprise world all participants are to be identified and tracked. This is a measure aimed at safeguarding the enterprises data and business strategies from the general public, and competitors alike. A private blockchain's write permission is owned conserved by one institution. Using a private blockchain introduces the necessity for having a permission management element to permit the participants within the network. There are various platforms such as Multichain and Eris that enable the development of consortium chains and private chains [20].

In addition, roles are defined to play a part in the blockchain ecosystem [24]. Traditionally, in enterprise systems, different users are responsible for operating different applications (such as human resource, accounting, procurement, production, etc.) related to different business processes and departments within an organization. Staff members are trained in operating applications in enterprise systems and there are also certifications specific to enterprise systems, for example the SAP

ERP certifications that organizations look out for during recruitment. An 'enterprise blockchain' will need to ensure that users are verified to ensure that the blockchain is trusted and unauthorized persons do not tamper with financial reports or any form of sensitive data in general.

Sensitive data can include clients' credit card details, budget, revenue and future projects that are to take place in an organization. The loss of such data is not loosely connected to loss of customers, revenue and partners and sometimes lawsuits and fines imposed on businesses by regulatory bodies and government. The need for enterprise systems to be permissioned cannot be over emphasized. Thus it is important that enterprise blockchain technologies are fully ready to deal with user authentication issues that might arise and that they are implemented in a different manner compared to public blockchains. Current blockchain systems are not very scalable in terms of transaction handling. This can be problematic, as the current public blockchain platforms will not fully meet organizations accounting requirements. This is one of the reasons for which organizations need to work together to identify the best way to implement and adopt a particular blockchain architecture that they can all understand and work with to ensure data consistency.

If a blockchain enabled enterprise system is not scalable in terms of data storage and transaction handling, data might be hashed and stored off-chain. This leads to placing trust in external data storage. Organizations must ensure that they understand what data needs to be protected and such an external storage is safe and is implemented with layers of security and encryption technologies. Data needs to be encrypted before it is distributed over insecure networks. Nowadays, companies allow staff to work remotely in various locations spread across the globe, from their own computers, laptops and tablets rather than on the 'secure' company technology infrastructure. Therefore, once the data leaves the premises of the organization it becomes vulnerable. This means that even if a blockchain enabled enterprise system is permissioned, the endpoint being the point at which the data is accessed from and used might be vulnerable. Organizations must understand the difference between data at rest and data in transit, and train staff on endpoint security and ensure that they are cyber security aware.

7.3 Advantages, Opportunities and Challenges

According to Nitin, the Director at IBM Blockchain Labs [24] the success of blockchain should be focused, at least initially, on how this technology could be integrated with existing enterprise systems. This will create comfort in the collective understanding of this technology, while at the same time establishing a path of where there is the minimum disruption possible whilst accelerating enterprise adoption. Section 7.2 has also shown that it is more efficient for organizations to integrate existing enterprise systems with private blockchains rather than public blockchains [22]. Public blockchains are also inefficient in terms of number of transactions processed (3–20 transactions/s) per second [12]. Therefore, combining

private blockchains with enterprise systems applications will bring about return on investment from investment in 'enterprise blockchains' and the following organizational benefits:

- *Reduced errors in manual data entry*. This means more focus on customers because staff will be less busy with manual data entry tasks, they will have more time to focus on customer needs.
- *Data Archiving*. Decentralized and autonomous data archives models, such as the ones provided by the blockchain, can be an interesting alternative to centralized data storage solutions in use by legacy enterprise systems [6]. This model will eliminate the dependency on a centralized authority and will allow distributed and trusted storage across nodes (applications) in a blockchain network (blockchain-enabled enterprise systems). More importantly, using the blockchain as a data archive will allow any nodes to validate the authenticity of the archived data without relying on a central hub [26].
- *Privacy and Security*. Private blockchain network is non-permissionless reducing any threats of fraud in financial data and assets. In a decentralized organization, shareholders assets will be protected in real-time.
- *Consensus*. This means the validation of business processed and transactions by applications that makeup the blockchain network as well as the ES. Business rules will be complied with. If one application derails, the others will be notified and without a consensus the transaction will be cancelled.
- *Smart contracts for automatic procurement* of items as well as vendor payments. Releasing funds in transactions only when certain conditions are met, e.g., when a document is filed appropriately or a third-party consents. Organizations invest heavily in their ERP and accounting systems, but the actual payment itself is usually not connected to these commerce engines [9]. Payment systems that cannot provide automated, up-to-date and globally accessible tracking information, can disseminate inefficiencies to all areas of a business. When a company moves from paper to electronic checks, they gain the chance to add value to their transactions with rich data that can be synchronized between ERP, CRM and vendor-facing websites. They can begin to make connections between procurement, accounts payable and payments, with the chance to discover inefficiencies, double-payments and even fraud along the way.
- *Smart contracts for self-enforced business rules* are business terms embedded in a transaction database and executed with transactions. This is a rules component, as needed by any business to define the flow of value and state of a transaction [9].
- *Decentralized Business-to-Business (B2B) Auditing*. Business-to-Business, also known as B2B exchange models are one of the core activities of modern trade. In those scenarios, the essential features of B2B processes are auditing, reconciliation processes and transaction tracking. Traditional B2B platforms allow these capabilities by providing a centralized transaction-tracking model that only allows a business at one endpoint to record relevant transaction events. This has proven to be slow and inefficient in addressing many of the reoccurring

challenges of B2B transaction trailing operations in activities such as auditing and reconciliation. Taking advantage of the blockchain as a decentralized, trusted and secured trusted transaction record keeping data store could be a more adequate model to cater for the challenges of B2B transaction tracking solutions. Using the blockchain, each party at both endpoints in a B2B process could independently verify and track the events related to a B2B transaction without the need to rely on a centralized authority that might not be fully trusted. Additionally, the security capabilities of the blockchain will facilitate the implementation of more sophisticated reconciliation and auditing processes [26].

Taking the above advantages and opportunities into account the major challenges of integrating the blockchain technology and enterprise systems are outlined as follows:

- **External Oracle**. 'Oracles' are still needed for non-deterministic smart contracts. Non-deterministic smart contracts are smart contracts that cannot determine the outcome of an agreement by themselves, in other words they require a third party or external application to determine the outcome of the contract. For example, verifying that goods procured from a vendor have been delivered by querying a couriers website to track the goods before automatically paying the vendor. More research is needed to reduce the theoretical downsides [27] which include security, and putting trust in third parties which is what the blockchain technology was built to avoid. However, carefully thought out processes for undesired behavior such as federating the oracle or creating an arbitration process can be applied in order to minimize the risks [16]. As mentioned in Chap. 6, companies like Augur and TruthCoin are exploring ways of improving the trust model for Oracles using Principal component analysis.
- **Organizational Changes**. Smart contracts are not yet dynamic. An 'enterprise blockchain' will need to 'keep up' (be maintained) with any rapid changes in organizational strategies. If the development of an enterprise system is not judiciously controlled by organizations, organizations may find themselves under the control of the system [6]. Strategies as well as business rules are dynamic but we are yet to see how the blockchain can be enterprise aware. As the technology matures, it is hoped that this will become a reality. The blockchain technology is still maturing and subject to change. Hence, organizations are being cautious in implementation. According to Eyre, As this is a new but rapidly maturing field (technology integrated with business processes) there can be significant internal challenges in getting such a project off the ground [28].

7.4 Case Studies

As discussed in most of the chapters of this book, Blockchain is a classic emergent technology. It advertise to have a large set of uses and benefits, but it is very different from what people are used to, and consequently, many business and

governments are adopting a wait-and-see attitude [11]. Thoughtful caution is encouraged, but it is believed that organizations and institutions can fall behind if they do not quickly assess the potential of blockchain and begin experimenting with its risk [11].

Considering first the case of consortia and collaboration between companies, the implementation or integration of the blockchain technology and enterprise systems (ES) is still at early stages. With the believe amongst financial institutions that a go-alone approach is not the right way, in 2016 there have been a number of collaborative initiatives including R3CEV, Hyperledger project, China Ledger and of various strategic alliances between fintechs, blockchain platforms and financial institutions [29]. There has also been knowledge sharing on the blockchain technology with workshops and startup incubation going on across the globe. The blockchain technology is constantly maturing and getting better as newer ideas are uncovered.

To automatically settle transactions, smart contracts need to be connected to the real world banking systems and it is expected that smart contracts will grow in popularity and become more feasible for real world enterprise transactions. For banks it is thus important that blockchain will be integrated with their banking systems [29].

It has been foreseen by some that a single leading open-source (software which its program or source code can be freely redistributed and modified), flexible; enterprise ready; distributed ledger will emerge, which will be significantly enhanced for private blockchain with full support for smart contracts. A number of organizations have already started making massive investments and efforts at implementing this type of blockchain [29].

New blockchain consortia and strategic partnerships will emerge and we will see an accelerated deployment of private blockchain networks. Multiple networks of trusted platforms each connecting a subset of industry players [19, 21, 29]. This however will ask for an overall distributed ledger that will be open source with common standards and protocols, enabling interoperability via APIs. For example, the Hyperledger Project [19, 21, 23, 29].

Point of Attention This case study shows that the blockchain technology needs to be regulated as well as enterprise to be ready in order to be integrated with enterprise systems. This is to ensure data integrity, less redundancy and trust between parties. Thus, we might see a situation where the enterprise system and company data in enterprise systems are private, but inter-company transactions on the blockchain are visible to collaborating companies in a 'closed' network.

The second case study we consider, concerns 'Enterprise Blockchain' Startups. A few blockchain-focused start-ups' have emerged in the enterprise blockchain domain. Recently, Ernst & Young announced that six startups will participate in its

first-ever startup contest focused exclusively on blockchain. The startups will work with mentors at Ernst & Young's Canary Wharf, London, offices to build products that are aimed to ensure intellectual property rights can be more easily managed and to make it easier for new business models to evolve in the energy trading space [30–32]. Interestingly, there are five enterprise related startups among the six shortlisted startups. The sixth startup JAAK (www.jaak.io) is focusing on using the blockchain to manage and commercialize digital media. In other words, JAAK is transforming digital rights management [31].

Point of Attention This case study shows that the blockchain technology is not fully enterprise ready yet. However, with the rise in startups and incubators, newer ideas will materialize and the potentials of the blockchain technology when integrated with or embedded in enterprise systems will only become clearer.

The five enterprise related startups among the six shortlisted startups by [30–32] are:

- **Adjoint** (www.adjoint.io). Adjoint aims to make smart contract reliable and verifiable and the startup is building a new messaging and consensus protocol with an easy-to-use interface that allows enterprises to quickly deploy, maintain, and analyze smart contracts. At the core of their application is a mathematically verified, cryptoledger fabric born out of cryptography research efforts. Their API will allow programmers to integrate their solution with enterprise systems and financial and banking platforms.
- **BitFury** (www.bitfury.com). The Bitfury Group develops and delivers software and hardware solutions for organizations, governments, businesses and individuals to digitize assets and transact them over the Internet safely and securely. This allows the movement of assets from one node to another, in a secure fashion across Blockchain networks. The platform will enable assets to be transferred and verified between individuals and businesses quickly without the need for a central authority.
- **BlockVerify** (www.blockverify.io). BlockVerify focuses on provenance. Their solution allows businesses to track and indicate where their products are in the supply chain. This allows customers to verify the source of the products they purchase, their authenticity and generally track the product from its production to the shelf. BlockVerify emphasize that they have introduced an anti-counterfeit solution that will be of significant importance in various industries, it is impossible to duplicate products making each product on the system unique.
- **BTL Group LTD** (www.btl.co). BTL offers blockchain solutions to businesses across a number of industries, and has recently built a prototype that uses a blockchain based interbank payment network built on their core settlement and

asset trading solution, Interbit. The startup also works with businesses by providing advice on integrating enterprise systems and the blockchain technology for those that do not know where to begin or what decisions to take, for example some of the decisions outline in Table 7.3.

- **Tallysticks** (www.tallysticks.io). Tallysticks makes use of the distributed functionality of the blockchain technology to deliver transparent invoicing for B2B transactions. This speeds up the transactions and payments between businesses, as there is no central authority responsible for verifying invoices and payments, thus delivering efficiencies across financial workflows. Tallysticks system is integrated into the enterprise systems of businesses, accounting systems and plugging them into electronic payment rails.

In a nutshell, the case has shown that organizations are eager and ready to let the blockchain technology disrupt the way businesses are operated as well as enterprise systems (ES). Investors are also willing to invest in the technology that is still maturing because of the potentials this technology holds for business organizations. How soon this will happen however cannot exactly be predicted with high precision at this moment.

7.5 Summary

This Chapter has discussed the present state of enterprise systems in relation to the blockchain technology; factors to be considered before coupling the blockchain and enterprise systems and how the blockchain can further improve business transactions, processes and enforce business rules on a daily basis.

Enthusiasts of the blockchain technology will be concerned with whether enterprises are ready for blockchain, as well as if a consideration of blockchain adoption should focus on the integration with legacy systems. An integrated enterprise will need several use cases to drive the enterprise towards the full exploitation of enterprise blockchain. The success of blockchain adoption should initially focus on how this technology integrates with the different organizational systems. This will create ease in the collective understanding of this technology, while establishing a path of least disruption and accelerating enterprise adoption [9].

The blockchain technology has extensive possibilities and together they differ from core features when measured individually. Enterprise blockchain provide a layout channel through which value, transaction data and state are close to the business process and a more community process, bringing about a layer of trust and the scalable processing of transactions, with an satisfaction over the security of the execution of business transactions. There are merits of using a blockchain as a technology alternative that is permissioned and conforms to all the regulatory platforms that have evolved over time. The blockchain promise is to solve long-standing industry concerns such as modernizing the financial and trade system and speeding up securities and trade settlements [24]. It is hoped that the blockchain

technology will fully understand and become feasible for a majority of the ongoing business transactions; processes; rules and regulations; and will find its way into organizations' enterprise systems (ES) as soon as possible.

References

1. Markus ML, Tanis C (2000) The enterprise system experience—from adoption to success. Fram Domains IT Manag Proj Future Through Past 173–207
2. Maas J (2000) Mission critical: realizing the promise of enterprise systems. Sloan Manage Rev 41:102–103
3. Nah FF-H, Lau JL-S, Kuang J (2001) Critical factors for successful implementation of enterprise systems. Bus Process Manag J 7(3):285–296. doi:http://dx.doi.org/10.1108/14637150110392782
4. Hendricks K, Singhal V, Stratman J (2007) The impact of enterprise systems on corporate performance: a study of ERP, SCM and CRM system implementations. J Oper Manag 25:65–82
5. Shang S, Seddon PB (2002) Assessing and managing the benefits of enterprise systems: the business manager's perspective. Inf Syst J 2000:271–299
6. Davenport TH (1998) Putting the enterprise into the enterprise system. Harvard Bus Rev 1–12
7. Scott JE, Vessey I (2002) Managing risks in enterprise systems implementations. Commun ACM 45:74
8. Fan M, Stallaert J, Whinston B (2000) The adoption and design methodologies of component-based enterprise systems. Eur J Inf Syst 9:25–35
9. Gaur N, Considering blockchain for an enterprise? Available online at: http://infocastinc.com/industries/considering-blockchain-for-an-enterprise/. Accessed 11 Sept 2016
10. Deloitte, Deloitte launches ExaLink, a multi-services platform that transcends legacy enterprise systems. Available online at: http://www.prnewswire.com/news-releases/deloitte-launches-exalink-a-multi-services-platform-that-transcends-legacy-enterprise-systems-30032-6929.html. Accessed 13 Sept 2016
11. Cuomo J, How businesses and governments can capitalize on blockchain. Available online at: https://www.ibm.com/blogs/think/2016/03/16/how-businesses-and-governments-can-capitalize-on-blockchain/. Accessed 12 Sept 2016
12. Xu X, Pautasso C, Gramoli V, Ponomarev A, Chen S (2016) The blockchain as a software connector. In: Proceedings of 13th working IEEE/IFIP conference on software architecture, WICSA 2016, pp 182–191. http://dx.doi.org/10.1109/WICSA.2016.21
13. Weisfield N, The leading distributed ledger and blockchain business and technology advisory organisation. Available online at: http://www.gft.com/int/en/index/discovery/innovation/blockchain-and-distributed-ledger-technology.html. Accessed 3 Sept 2016
14. Idelberger F, Governatori G, Riveret R, Sartor G (2015) Evaluation of logic-based smart contracts for blockchain systems. 9202:167–183
15. Stark J, Making sense of blockchain smart contracts. Available online at: http://www.coindesk.com/making-sense-smart-contracts/ Accessed 24 Aug 2016
16. Hoskinson C, A brief introduction to smart contracts. Available online at: https://www.youtube.com/watch?v=3bY66Zgr8Cs. Accessed 29 Aug 2016
17. Ore J, How a $64M hack changed the fate of Ethereum, Bitcoin's closest competitor. Available at http://www.cbc.ca/news/technology/ethereum-hack-blockchain-fork-bitcoin-1.3719009. Accessed 20 Nov 2016
18. Higgins S, Hyperledger Blockchain Project adds 17 new members. Available online at: http://www.coindesk.com/hyperledger-project-adds-17-new-members/. Accessed 12 Sept 2016
19. Mizrahi A (2016) China's Wanda Group joins Hyperledger Project after 170% growth in H1 2016

20. Finnegan M, Blockchain needs Linux-style open community to succeed in the enterprise, says IBM CTO. Available online at: http://www.computerworlduk.com/applications/how-ibm-plans-push-blockchain-into-enterprise-3626741/. Accessed 11 Sept
21. Vaughan-Nichols S, Apache Software Foundation founder to lead blockchain Hyperledger Project. Available online at: http://www.zdnet.com/article/apache-software-foundation-founder-to-lead-hyperledger-blockchain-project/ Accessed 12 Sept 2016
22. Hall C, Wrapping your head around private blockchains. Available online at: http://windowsitpro.com/industry/wrapping-your-head-around-private-blockchains. Accessed 11 Sept 2016
23. Hyperledger Project (2016) What is the Hyperledger Project. Available at https://www.hyperledger.org/. Accessed 20 Nov 2016
24. Gaur N (Director at I.B.L), A blockchain for the enterprise—a technical perspective. Available online at: http://infocastinc.com/industries/a-blockchain-for-the-enterprise-a-technical-perspective/. Accessed 12 Sept 2016
25. del Castillo M, IBM Watson is working to bring AI to the blockchain. Available online at: http://www.coindesk.com/ibm-watson-artificial-intelligence-blockchain/. Accessed 12 Sept 2016
26. Bitcoin Magazine, Beyond Bitcoin: how the blockchain can power a new generation of enterprise software. Available online at: https://bitcoinmagazine.com/articles/beyond-bitcoin-how-the-blockchain-can-power-a-new-generation-of-enterprise-software-1443635470. Accessed 11 Sept 2016
27. Greenspan G, Why many smart contract use cases are simply impossible. Available online at: http://www.coindesk.com/three-smart-contract-misconceptions/. Accessed 28 Aug 2016
28. Eyre J, Blockchain: creating a blueprint for business change. Available online at: https://www.gtnews.com/blogs/blockchain-creating-a-blueprint-for-business-change/. Accessed 13 2016
29. De Meijer CRW, Blockchain: what to expect for 2017? Available online at: https://www.finextra.com/blogposting/12995/blockchain-what-to-expect-for-2017. Accessed 12 Sept 2016
30. del Castillo M, 6 blockchain startups accept new ernst & young “challenge”. Available online at: http://www.coindesk.com/ernst-young-selects-6-startups-to-blockchain-challenge/. Accessed 12 Sept 2016
31. Kastelein R, Six companies picked to participate in EY blockchain startup challenge. Available online at: http://www.the-blockchain.com/2016/09/09/six-companies-picked-to-participate-in-ey-blockchain-startup-challenge/. Accessed 12 Sept 2016
32. Econotimes, EY startup challenge selects six blockchain entities. Available online at: http://www.econotimes.com/EY-Startup-Challenge-selects-six-blockchain-entities-274349. Accessed 12 Sept 2016

Part III
Blockchain Business Innovation

Blockchain Practices

8

Abstract

This Chapter focuses on examples of innovation solutions in practice, providing fact-sheets of eight interesting ideas in the field of blockchain technology worldwide in 2016. The underlying rationale in order to select those ideas was twofold. First, the aim was to present innovative solutions on the areas that this book has already discussed in previous chapters. Second, most of the selected ideas are based on innovative research projects that have successfully become start-ups and/or spin-offs and have already reached the market. In accordance with my previous volume, each innovation is described by an introduction, highlighting the main characteristics of the application or software, some general information about its developers and their motivation behind their solution is provided, accompanied by the main company competitiveness indicators for time-to-market as well as indicators of user value in terms of perception, such as the user experience and the so called «Wow» effect.

8.1 Introduction

Blockchain technology has been vastly characterized as the world's game changer [1]. By creating a distributed digital ledger that records and stores all transactions in a decentralized network of computers, blockchain technology is offering high transparency along with trust, security and speed [1]. As of today, almost $1.1bn has been invested in venture capitals to startup companies for research and development of innovative solutions that could potentially transform the way businesses operate around the globe [2]. Attempting to revolutionize current processes and expecting to escalate enterprise adoption by early 2017, this disruptive innovation has already been applied on numerous use cases that span from financial services, trade finance and smart contracts to healthcare, supply chain and identity

V. Morabito, *Business Innovation Through Blockchain*,
DOI 10.1007/978-3-319-48478-5_8

management [3]. So far, the previous chapters of this book have explored different areas related to blockchain technology as a value system, and covered its governance as well as the security concerns surrounding its implementations in different scenarios such the creation and execution of smart contracts. This Chapter will elaborate on the discussion presented in the previous chapters by providing interesting examples of innovative solutions that are utilizing blockchain technology and are available worldwide in 2016.

The ideas that were selected in the current chapter constitute successful research projects that received both attention and funds from investors and managed to build up startup companies in order to develop innovative solutions utilizing the blockchain technology. The first case study belongs to the financial services field and more specifically in the loyalty rewards sector. Having established a partnership with Deloitte, Loyyal introduces a platform that offers interoperability between loyalty programs and vendors, such as credit card providers, airline companies and hotel businesses, through one digital wallet. Everledger is the second presented case study that attempts to combat insurance fraud and jewelry theft by recording the transaction history and provenance of high value goods such as diamonds, luxury goods and fine art in the distributed digital ledger of blockchain. The third case study, GemHealth, brings innovation to the healthcare industry by offering a radical patient centric solution that allows the interoperability of healthcare data across the continuum of care so that different stakeholders, such as patients and clinicians, can have access to. Attempting to revolutionize the supply chain process, the fourth case study describes Wave, a platform that can be used by shipping companies in order to achieve faster, safer and simpler trade finance. In the financial services industry and more specifically in the international payments sector, the fifth case study, Align-Commerce offers a solution that aims to modernize current business-to-business payment processes. Civic, the sixth case study in this Chapter, is an identity management company that aims to protect consumers from identity theft by alerting them in real time manner when a transaction is using their social security numbers. In a similar area, the next case study, ShoCard, is focusing on providing blockchain based solutions to securely store customer's information, which they can use to verify their identities whenever they need it. The last case study in this chapter, Factom, is about a startup company that aims to build on the advantages of blockchain technology to secure and verify the integrity of the data transacted between and within enterprises as well as governmental agencies.

8.2 Loyyal

Loyyal, recently named as one of the most influential blockchain companies, is a Fintech start-up offering a loyalty and rewards platform built with blockchain and smart contract technology. Loyyal can benefit both loyalty program providers and their customers. The start-up aims to unify the currently fragmented loyalty industry by introducing interoperability of data between loyalty programs, allowing for

multivendor alliances, enabling dynamic issuance and redemption options to each customer while at the same time maintaining consumer privacy [4]. By leveraging the decentralized solution of blockchain technology, the platform offers a personalized added value service to customers by enabling the creation, redemption and exchange of loyalty points across vendors, programs and industries in near real-time and through one digital wallet ultimately aiming to improve customer experience [5].

8.2.1 Developer

Originally founded in 2014 as Ribbit.me, the New York based start-up was recently rebranded to Loyyal in order to better reflect the underlying industry and meet the company's business objectives [6].

Loyyal was co-founded by Greg Simon, who is currently the CEO of the start-up and also serves as a Founding member and current president of the Bitcoin Association as well as a member of the Dubai Global Blockchain Council [7]. He holds an MBA from Columbia and is a Certified Blockchain Professional. Having been working in the financial services industry for the last 15 years, Simon's aspiration was to provide customers with a fuller and more personalized experience as "*loyalty should be about enriching the individual's life experience, not simply rewarding repeat behavior*" [8]. Simon's co-founder, Sean Dennis, is also the Founder of the Nicaragua Bitcoin Association. Both of the co-founders share a business educational background and a genuine interest in the applications of blockchain and distributed ledger technology [7].

According to the Chief Operating Officer (COO) of Loyyal and Chairman of Wall Street of Blockchain Ron Quaranta, recent studies have shown that current loyalty programs are ranking very poorly both in terms of innovation and customer satisfaction. Loyyal is aiming to 'cure' this ailment of the loyalty industry by bringing in a creative and innovative solution that will attract and retain customers by introducing a more personalized experience to the user while at the same time increasing the reputation of financial institutions [9].

Table 8.1 depicts the representation of the competitiveness indicators for time to market and a growing demand of the market. The startup has a large market to tap. There are some competitors in the rewards market but Loyyal has established strong partnerships that could differentiate it amongst the others. The enabling infrastructure is currently used on beta version on the Dubai initiative and the developers are aiming for continuous improvements.

8.2.2 Application

Loyyal was one of the five start-up companies that Deloitte, one of the largest accounting firms in the word, teamed up a partnership with in the first quarter of 2016. By utilizing blockchain technology, Loyyal aims to apply the loyalty network

Table 8.1 Loyyal competitiveness indicators for time-to-market

Solution	Loyyal
Founded	2014
No. of products	1
Clients	Financial Institutions, Enterprises and Individuals
Partners	Different levels of partnership
Market dimension	Growing
Competitors	Some
Enabling infrastructure	Beta

platform in the financial services sector that will benefit both individuals and companies and will result in: unification of the fragmented loyalty industry, near real time transparency, cost savings, fraud and abuse prevention and overall enhanced customer retention and satisfaction [5]. For example, when Alice buys her airline tickets from London to Paris, her credit card transfers the awarded points into her digital wallet in a real-time manner. In that way, Alice can instantly use the points she just earned in order to upgrade her booked room at a local hotel in Paris. Thus in this example, the customer can enjoy an enhanced experience while at the same time the airline and hotel companies have gained a happier and satisfied customer that is very likely to return [5].

Loyyal has also recently joined the Dubai Future Accelerators program and will be collaborating with Dubai Holding in the industries of food and beverages, hospitality and real estates. Moreover, Loyyal has just launched the Dubai points program which is focusing on the tourism industry and aims to incentivize tourists to visit local attractions. By using the loyyal smartphone app, the user earns points every time he performs specific activities such as travelling, visiting museums or staying in hotels. In that way, the earned points can be used by the user to offset the cost of the promoted places of attraction [10].

Table 8.2 depicts the measure of *User value* of Loyyal solution based on current feedback as well as experience of the solution. The process impact is medium as the implementation of the solution by financial institutions and enterprises will not severely affect their processes.

Table 8.2 User value indicators for Loyyal

Fast learning	Medium
User interface	Positive
User experience	Positive
Process impact	Medium
User feedback	Positive
«Wow» effect	Medium

8.3 Everledger

Utilizing the distributed ledger technology, Everlegder was created in an endeavor to combat insurance fraud as well as diamond theft by facilitating diamond certification and tracing of its transaction history [11]. The platform can be used by insurance companies, owners and law enforcement to track diamonds' provenance in a more robust and reliable way compared to using paper certificates that can be easily lost or modified [12]. Everledger is built on blockchain technology and can track any asset with unique identification. By creating the first of its kind global digital legder, Everledger collects thousands of data points for each recorded diamond and creates a digital fingerprint in the immutable distributed ledger [13]. According to the founder of the company, every single tiny detail of a diamond is being recorded as "*All of the angles and the cuts and the pavilions and all of the crown … as well as the serial number, … the four Cs, and we put all that into the blockchain*" [12].

8.3.1 Developer

Leveraging the notion of smart contracts within blockchain technology, Everledger startup was founded in 2015 in London by current Chief Executive Officer (CEO) Leanne Kemp. Having been working for 20 years in emerging technologies and 10 years in the jewelry and insurance industry, Kemp's idea was triggered while discussing with insurers about diamond fraud and seeking potential solutions that could combat the problem [12]. The team is also comprised of Gaurav Rana, the Chief Technology Officer (CTO) of the startup who is working on the underlying blockchain technology of the platform [12].

Since the first presentation of Kemp's idea at the Aviva hackathon in 2015, Everledger has won numerous awards with the most prominent ones being the 2016 Winner European Fintech for best blockchain company as well as the 2015 Meffy award for Innovation Fintech [11]. Recently, Everledger has been announced as one of the top 50 Fintech companies in Europe [14]. Until today, it has digitized almost 980,000 diamonds and embedded them into the distributed ledger of the blockchain.

Table 8.3 depicts the representation of the competitiveness indicators for time to market and a growing demand of the market. The startup is solid with few competitors in the market who are following a more traditional approach. The company has established strong collaborations in order to grab the attention of the market. Both the law enforcement and insurance sector have shown interest in the application, which already looks promising. The enabling infrastructure is running on a beta version at the moment but is continuously evolving.

Table 8.3 Everledger competitiveness indicators for time-to-market

Solution	Everledger
Founded	2015
No. of products	1
Clients	Insurance companies, Law enforcement, Individuals
Partners	Different levels of partnership
Market dimension	Growing
Competitors	Few
Enabling infrastructure	Beta

8.3.2 Application

Everledger focuses on introducing transparency into the diamond market as well as on eliminating criminal activity. The system includes three stages [15]:

1. Establish an electronic ID by collecting thousands of reference-able data points of each diamond and recording them on the global digital ledger.
2. Assign a digital passport to each diamond that will record each transaction history and provenance.
3. Detect, guard and prevent illegal activities associated with diamond fraud and theft.

The company has been commercially supported by Allianz, Barclays and BBVA and only recently it has established a strategic cooperation with Jeweltree Foundation, a non-profit diamond certification organization [14]. Currently, the major implementation of Everledger includes its collaboration with several major certification companies and also with the four largest insurance companies in London. Police organizations such as Interpol and Europol have expressed their interest in utilizing the platform in order to prevent and detect criminal activity [12].

According to Kemp, her future goal is to extend her idea from diamonds to high value, luxury goods, fine art and electronic devices. The ultimate vision of the start-up is to combat counterfeiting which can be applied in online retail marketplaces such as Amazon and eBay in order to detect the authenticity of the products being sold to customers [13]. Figure 8.1 depicts the future goals of Everledger.

Table 8.4 User value indicators for Everledger

Fast learning	Medium
User interface	Positive
User experience	Positive
Process impact	High
User feedback	Positive
«Wow» effect	High

Fig. 8.1 Everledger goals

Table 8.4 shows a good level of perceived *User value* of Everledger solution as user feedback is very positive, the solution exhibits great novelty and the "wow" effect is high.

8.4 GemHealth

GemHealth is a platform built by a startup called Gem, a provider of enterprise blockchain solutions [16]. GemHealth enables the collaboration of different stakeholders into the sharing and transferring of healthcare data. GemHealth gives the ability to different healthcare operators to have access to the exact same information with transparency through a universal data infrastructure [17]. By exploiting the dynamics of blockchain technology, GemHealth introduces a robust and flexible healthcare ecosystem that guarantees data integrity and security amongst collaborating parties. The system represents a decentralized architecture that is tamper-proof and allows for an immutable and secure library of healthcare data [18].

8.4.1 Developer

Gem, that kickstarted 2016 with a funding of $7.1m and has totally received $10.4m till today, was founded in 2014 by its current CEO Micah Winkelspecht [17]. Gem's focus is on providing enterprise solutions utilizing the blockchain technology and the underlying idea of data exchange through a shared infrastructure. Winkelspecht found a gap in blockchain market as most of the spotlight until

Table 8.5 Gem competitiveness indicators for time-to-market

Solution	Gem
Founded	2014
No. of products	2
Clients	Enterprises and Individuals
Partners	Different levels of partnership
Market dimension	Growing
Competitors	Very few
Enabling infrastructure	Yes

now has been on applications for the financial industry [17]. According to him, blockchain could be applied to numerous non-financial use cases and this is how his idea about GemHealth was actually born. The founder's goal was to introduce a patient centric model for healthcare to ensure security of clinical data. He believes that it is about time to leave behind the idea of silos and separate views and move forward to a more united world of data regarding patient care [17].

In Table 8.5 the time to market competitiveness indicators appears to be high, with a solid company and a growing demand of the market. The company is on a continuous development aiming to provide more pioneering solutions for enterprises in the continuum of care. Enabling infrastructure is ready and the demand is really high.

8.4.2 Application

Gem has just started a partnership with Philips Healthcare focusing on further research and development of the GemHealth platform. The healthcare application is aiming to fill an important gap in the market where for many years both patients and clinicians were yearning for a digital shared unified patient record [18]. Medical record repositories and closed book keeping create important obstacles in the effective facilitation of health services offered to patients. This is because data exchange and collaboration between different healthcare providers—private or not-is not entirely feasible. This becomes quite apparent in cases where a patient relocates or gets sick while travelling abroad. GemHealth facilitates electronic health record (EHR) operability, replacing the classic paper patient record, through which physicians, clinicians, patients and payers can have access to the same shared data. An illustration of the application can be depicted through the following: Adam faints and hits his head while hiking in Oregon. As his primary doctor is unavailable, his friends drive him to the emergency room where he is accepted by Dr. Yang. Adam can grant read access through his wearable device to Dr. Yang for his medical records, latest laboratory results as well as the list of current and previous medications. In that way, GemHealth enables information exchange between different parties so that all users are connected to a universal library of health data across the continuum of care [18].

Table 8.6 User value indicators for Gem

Fast learning	Medium
User interface	Positive
User experience	Positive
Process impact	High
User feedback	Positive
«Wow» effect	High

The potential use cases of GemHealth span from wellness applications, electronic medical records, global patient id software to medical inventory management, rehabilitation incentive programs, billing and claims processing targeted both to users and healthcare providers [16].

GemHealth runs on GemOS, which is the infrastructure that supports the implementation of the decentralized servers, applications, and of course the platform. In other words, it is the technology that can be used to implement blockchain network.

Table 8.6 depicts the measure of *User value* of GemHealth solution. User feedback is quite positive and the process impact is important enough as the platform offers a quite innovative solution for healthcare that will severely affect current processes of adopting companies.

8.5 Wave

Innovation in the trade finance sector is deemed as crucial nowadays as this particular banking area is facing a huge amount of challenges and competition from newly founded Fintech companies entering the industry. Having graduated from Barclays TechStar Accelerator Program in 2015 and recently created a partnership with the bank, Wave claims to be the first company that has executed a global trade transaction through blockchain technology [19]. By dematerializing paper documents, Wave aims to reduce costs in supply chain management, eliminate disputes and forgeries and ultimately offer simpler, safer and faster trade finance. The application makes it feasible to connect all carriers, banks, forwarders, traders and any other parties involved in the international trading supply chain into one decentralized network [20].

8.5.1 Developer

Formerly called as OgyDocs, Wave was founded in 2014 by current CEO Gadi Ruschin, who has 12 years' experience in the international trade sector in the shipping industry [21]. The rest of the team includes Or Garbash, the Chief Technical officer of the startup and Yair Sappir, Chief Product Officer both of whom are experts in information security [20]. The Tel Aviv based company is

Table 8.7 Wave competitiveness indicators for time-to-market

Solution	Wave
Founded	2014
No. of products	1
Clients	Enterprises
Partners	Different levels of partnership
Market dimension	Growing
Competitors	Few
Enabling infrastructure	Yes

currently comprised of only three members but is eager to expand and build a much bigger local team. According to Garbash, the trade finance sector can be transformed globally as blockchain solution technologies can successfully outperform pen-and-paper processes that have been utilized for almost 200 years by shipping companies and make sure that no fraud or falsified documents are being used in the way [22].

The first global trade transaction utilizing the Wave application was executed between Ornua, formerly known as the Irish Dairy Board that owned the brands Kerrygold and Dubliner cheese, and the Seychelles Trading Company in the beginning of September 2016. Barclays Bank, Wave's partner, is currently seeking to convince other banks to adopt the Wave application to execute their trade finance processes [19].

In Table 8.7 the time to market competitiveness indicators appear to be medium, as Wave has just recently performed the first pilot transaction in the market. There is relatively growing demand but the company needs more team members and partners. The startup has announced that it will continue research and development of the application with some select trade finance clients.

8.5.2 Application

The Wave platform can have applications in almost all of the industries, as the majority of companies are involved in imports and exports at some level. Currently, trade transactions involve a high number of participants in the process, such as banks, insurance companies and government customs inspectors, and a significant amount of paperwork has to be signed and transferred between one another. Lack of trust is a huge challenge between the parties involved in every trade process. By replacing documents with their electronic versions that are stored in the distributed ledger of the blockchain, Wave allows all involved parties to view, transfer titles, submit shipping documents and other original trade documentation through a secure decentralized network [20]. Unlike regular electronic files, such as PDFs, documents saved in the blockchain have to be approved by all involved parties and any

Table 8.8 User value indicators for Wave

Fast learning	Medium
User interface	Positive
User experience	Positive
Process impact	Medium
User feedback	Positive
«Wow» effect	Medium

changes can be detected immediately. As a result, the application fosters trust between participants as well as eliminates the risk of documentation fraud, reduces errors in documents and most importantly increases the speed of the overall document transfer process [22].

Since the seventeenth century, nothing has actually changed in the processes of the shipping industry as shippers have been using the exact same producers in selling, shipping and delivering goods. Aiming to optimize the antiquated methods of global trade finance, Wave's goal is to revolutionize the supply chain process. By replacing the printed bill of lading (BOL), a document that includes information about the shipment and more specifically about the type of goods being transferred, their quantities and their destination, an electronic version of the document will be stored in the blockchain that all interested parties can have access to [21].

Table 8.8 depicts the measure of *User value* of Wave solution. User feedback, coming from the first executed transaction, is very positive at the moment as it seems that the platform offers a very good user experience. Process impact is evaluated at medium level as the platform can easily be implemented and combined with existing processes of the adopting company.

8.6 AlignCommerce

In an age where electronic payments have taken over the world, the business-to-business (b2b) payment landscape seems to be living in the past. According to a recent survey, paper checks are the predominant method of payment for 97% of today's organizations with most of them being small and medium businesses (SMB) [23]. As a result, due to the lack of automation of payments, businesses are facing numerous difficulties and challenges including lack of transparency, inability to tracking their transactions and slow processing times. Having recognized this need of urgent modernization of the b2b payment process, AlignCommerce aims to change current payment processes by combining blockchain technology with traditional banking transfers and treasury operations [23]. It offers a solution that can significantly improve customer satisfaction, reduce costs, protect from fraud and ultimately increase the company's efficiency [24].

8.6.1 Developer

Having partnered with Silicon Valley venture firm KPBC and raised $12.5m in funding, AlignCommerce aims to revolutionize the global b2b payment industry. It was founded in early 2014 in San Francisco by current CEO Marwan Forzley, former general manager of Western Union and founder of eBillme, and Aldo Carrascoso, current COO of the company. The startup is comprised of a big team of almost 40 people sharing several years of industry experience in payments, payment processing and banking IT infrastructure management [25].

Going after the small business market, AlignCommerce's goal is to change the legacy financial payment system and offer an innovative solution that will significantly simplify cross borders payments. By exploiting bitcoin's blockchain, the platform is designed to reduce times and high transaction costs and offer a better overall customer experience [23].

In Table 8.9 the time to market competitiveness indicators show that the company is stable and ready to tap a large market as it has received funding from a wide range of investors such as Silicon Valley Bank, Pantera Capital, Digital Currency Group and Pivot Investment Partners [24]. The platform is already available in 60 countries around the world and the demand is currently growing.

8.6.2 Application

Currently, cross border payments are both time consuming and expensive for small businesses as usually when a company sends a payment to a vendor overseas, the money needs to pass through several intermediaries till it reaches the destination bank. These co-operating intermediary banks are charging additional fees for their services which are translated into more costs for the company that initiated the payment. AlignCommerce aims to renew cross-border payments by offering a solution that small businesses can use to pay their vendors at a much lower cost than before. The main difference from current used processes is that AlignCommerce bypasses any intermediaries in the process, reduces forms and fees and offers much simpler transactions characterized with transparency and high security. This is achieved by utilizing blockchain technology and the idea of a digital distributed ledger [23]. With AlignCommerce, a company can send a payment in Euros and the

Table 8.9 AlignCommerce competitiveness indicators for time-to-market

Solution	AlignCommerce
Founded	2014
No. of products	1
Clients	Enterprises
Partners	Different levels of partnership
Market dimension	Growing
Competitors	Few
Enabling infrastructure	Yes

Table 8.10 User value indicators for AlignCommerce

Fast learning	Medium
User interface	Positive
User experience	Positive
Process impact	Medium
User feedback	Positive
«Wow» effect	Medium

vendor can receive the money in US dollars. Both parties are still using traditional bank accounts but the platform converts the euros into bitcoins and sells the digital currency at an exchange rate for the desired currency of the recipient [24].

Furthermore, another very appealing feature of the platform is that it offers timely information about the transaction and both parties can track at any moment the status of the ongoing payment. Similar to package tracking in UPS or FedEx websites, with AlignCommerce both the sender and the receiver can track all money movements, from invoice generation to completion of the payment process [23].

Table 8.10 depicts the measure of *User value* of AlignCommerce solution. The platform offers a very unique feature in the cross border payment system, tracking of the payment through a dashboard, that has received very positive feedback from users and greatly enhances the overall experience of the solution [23]. The design is simple and easy to grasp and doesn't require any special training in order to use it.

8.7 Civic

Till today, 13.1 million fraud victims have been recorded in the US and only last year a 113% increase was reported for new account fraud. To make things worse, more than $112 billion dollars have been stolen by fraudsters during the past 6 years [26]. As hacks and data breaches are continuously increasing, identity theft is a very crucial issue that needs to be tackled.

Attempting to combat this ongoing serious problem, Civic offers an identity management service in order to protect people from identity theft. The identity protection application ensures that a user's personal information and more importantly his social security number is secure, not compromised and not used by someone that attempts to impersonate him. By leveraging blockchain technology, where the system is tracking all transactions in the distributed ledger, Civic prevents identity replication and blocks access to a user's data from unauthorized users [27].

8.7.1 Developer

Based in Palto Alto and currently comprised of 14 members, Civic was co-founded in 2015 by the South African Internet entrepreneur and the CEO of the startup, Vinny Lingham, former co-founder of gift card application Gyft that was sold for

Table 8.11 Civic competitiveness indicators for time-to-market

Solution	Civic
Founded	2015
No. of products	1
Clients	Individuals, Enterprises
Partners	Different levels of partnership
Market dimension	Growing
Competitors	Some
Enabling infrastructure	Beta

$54m in August of 2014 [28]. Lingham had been working for several years in the e-commerce industry when he noticed that although hacks of digital information have been on the rise there was still no universal solution found yet.

As a result, the idea about developing and implementing a global solution for combating identity fraud came along. He believes that the only way to keep our sensitive information safe is to watch carefully how this information is being used [29]. Jonathan Smith, expert in banking and security, is the current CTO and second co-founder of the company [29]. At the moment, the application has been launched in the US but according to Lingham, during the next year Civic will be running globally [30].

Having already raised $2.75m, Civic has partnered with startups GoodHire and Onfido which are focusing on background check verification as well as with TransUnion in order to provide real time alert to its customers [31]. Moreover, it is seeking for more partners to collaborate with such as financial institutions, online lenders, wireless and cable providers and employee verification services [27].

In Table 8.11 the time to market competitiveness indicators show that the company is solid as it has created strong partnerships with big investors, such as Digital Currency Group and Social Leverage, and is continuously seeking for more partners and clients from a variety of industries [32]. Recognizing that there is a very large market to tap, the startup has adopted a very good strategy by offering the application for free to consumers. Although there are some competitors in the market, Civic offers a proactive feature of alerting the user in real-time manner, an element that is missing from similar applications.

8.7.2 Application

Civic aims to provide a solution that can help customers gain more control over their personal information by connecting them to a network of businesses such as banks, financial institutions and healthcare organizations who will alert users when any transaction is attempting to access or use their social security number. At the same time, Civic saves a significant amount of costs from financial services providers such as banks and credit card companies as they are the ones who take responsibility of these incurred costs in case of fraudulent activities [28].

Table 8.12 User value indicators for Civic

Fast learning	Medium
User interface	Positive
User experience	Positive
Process impact	Medium
User feedback	Positive
«Wow» effect	Medium

Characterizing its application as proactive, Civic differentiates itself from other competitors in the market by detecting transactions in real-time manner, meaning that the user is alerted the exact moment that his personal information is being used. The user is notified by email, text or a pushup notification on his smartphone. At this point, the user can immediately either accept or deny the transaction in case he suspects fraudulent activity. As a result, Civic can prevent fraud before it can actually happen [28].

The application is using a two-way authentication process between users and financial institutions so that both parties can be sure that they are communicating with each other and no fraudster has compromised the transaction [26]. Civic is currently on a beta version and users can download the application for free. The application offers its users credit report alerting, $1m fraud coverage in case of fraudulent activity and 24/7 fraud call support [27].

Table 8.12 depicts the measure of *User value* of Civic solution. The application is currently on beta version but the user feedback is positive as the interface looks promising and easy to use.

8.8 ShoCard

In the current digitized world, where smart handheld devices are the norm, people need easy, simple and secure ways to verify their identities upon request. The situation gets even more crucial in cases of identity theft and fraud where such acts bring huge losses to individuals, institutions, businesses and merchants. For example, the airline industry requires secure and costumer friendly identity verification systems for people to be able to clear security check-in and to board airplanes [33]. Having proven its merit to secure Bitcoin transactions over the internet, blockchain can be the ideal technology to provide people with a secure and simple way to use digital identity card platform, which consumers can use through a mobile app built on the top of the public Blockchain data layer. ShoCard aims to leverage the security features of blockchain technology to provide personal digital identity that can replace the traditional methods such as passports, driving licenses or user names and passwords [34]. The startup, based in Palo Alto, CA, recently struck a partnership with the travel technology provider SITA to develop a prototype platform to implement the idea of a mobile travel identification mechanism that facilitates identity verification during traveling [35].

8.8.1 Developer

With a desire to have a consumer friendly and secure method to verify personal identity, the founder and the CEO of ShoCard, Armin Ebrahimi a Ph.D. holder, has founded the startup on 2015. His motivation is to offer an application that people can use in order to verify their identities whenever it is necessary without sharing their personal and sensitive information with the verifiers [36]. The basic concept is to utilize blockchain infrastructure to encrypt and store personal identification data where it cannot be tampered or falsely modified in order to be used to verify someone's biometric data when it is required [37]. The founder's vast experience in scalable platforms, online services, mobile-development and digital advertising, gained from working at big technology firms such as Yahoo, AOL, AT&T and Verizon, has enabled him to successfully establish ShoCard to achieve his vision of having an identity for a mobile world [36].

According to the founder of ShoCard, the trend of people using their digital assets in their daily life will continue to prevail because of the increased crossover between the digital life and the physical life. Thus, there is an emerging need for a solution that enables easy and secure access to the desired resources and ShoCard was developed to fill in this gap [38].

Table 8.13 provides a representation for competitiveness drivers on a time-to-market basis, demonstrating continuous growing interest in the application of blockchain in the field of personal identity verification. It can also be noticed from the table that the technology is considered nascent and promising in different application contexts where identity verification is essential for both industries and people.

8.8.2 Application

The developers at ShoCard are looking to use blockchain for online identity by providing a simple and intuitive mobile application that people can use in conjunction with biometrics data (finger prints and face recognition information).

Table 8.13 ShoCard competitiveness indicators for time-to-market

Solution	ShoCard
Founded	2015
No. of products	1
Clients	Travel industry and other industries where identity verification is a necessity to enable access
Partners	Travel technology provider SITA
Market dimension	Growing
Competitors	Few
Enabling infrastructure	Development and evaluation phase

Table 8.14 User value indicators for ShoCard

Fast learning	Yes
User interface	Positive
User experience	Positive
Process impact	Medium to High
User feedback	Positive
«Wow» effect	Medium to High

The goal is to provide the ultimate user authentication while protecting their private information. Such a solution can open the door for many use cases such as login services without the need for a username and password, digital signature, financial transaction authentication to prevent fraud, and governmental transactions in order to protect people's sensitive information [35].

ShoCard has partnerned with SITA, a travel technology provider and together aim to utilize blockchain to enable "*single secure travel identification across border*" [39]. They are working on developing a prototype that uses a mobile app and face recognition technologies that keep the private information safe in the blockchain network. When needed, the traveler and her/his data can be quickly and securely verified by the concerned stakeholders in this industry such as airlines, airports and other agencies, by reading the data from the dedicated blockchain network without compromising traveler's information privacy.

Table 8.14, presents the *User Value* measure of using blockchain based solutions for user identity authentication, which reflect a positive users' experience. This positive feedback can be measured as a result of the "simplicity" and "security" gained by utilizing ShoCard's solution as well as the value they offer for both the traveler and the airline industry.

8.9 Factom

Trust is considered one of the most important factors in nowadays' business world. Guarantying the integrity of the data used in business or governmental transactions requires huge investments in order to audit and verify financial or governmental records. This situation poses a considerable reduction in efficiency and return on investment, which affects the prosperity of organizations [40]. Factom, as a technology company, has a vision to harness the power of blockchain's distributed ledger and its ability to secure data and make it verifiable and independently auditable, in order to provide platforms that can be used by organizations to ensure their data is secured and cannot be manipulated or falsely altered. Factom provides its customers with different solutions to verify the integrity of the data being used in the organization's business processes as well as the integrity of data generated from the Internet of Things (IoT) devices including users' entries, identity, reputation, origin and manufacturer [41].

8.9.1 Developer

Factom is located in Austin, Texas and founded in 2014 with the mission of making the world's information systems more transparent and secured against fraud and unauthorized modification. The team of founders, which includes Peter Kirby, David Johnston, Paul Snow, Tiana Laurence, Brian Deery and Abhi Dobhal, depicts the perfect example of combining wide range of expertise that covers entrepreneurship, leadership and management as well as the passion about blockchain technology [42]. Peter Kirby, who is also the CEO of the company, expressed that the motivation behind Factom was to develop a software that can guarantee the integrity of the data by not allowing to change past entries.

At Factom, the founders believe that honest systems can improve the world by allowing businesses to grow and by unlocking the tapped potential of the people—resulting in having a future that is free from fraud corruption and forgery [43]. Table 8.15 provides a representation for competitiveness drivers on a time-to-market basis. The information in the table demonstrates an advanced development of the technologies behind Factom's products and a growing demand of the market based on the value that can be acquired by having honest systems with immutable data. Moreover, the continuous growing interest in secured applications and data accompanied with the advantages provided by utilizing Factom's solutions, the time-to-market competitiveness measures look very high.

8.9.2 Application

Factom based its idea on the fact that Bitcoin's blockchain is the most trusted and immutable database ever existed on the internet [40]. Thus, it developed a general purpose data layer on top of Bitcoin's blockchain, allowing users to have full access to the features offered by blockchain technology without having to deal with the complexity associated with crypto-currency. Therefore, users can make use of Factom's solutions without the regulatory risks of a Money Service Business or Money Transfer Business [44].

Table 8.15 Factom competitiveness indicators for time-to-market

Solution	Factom
Founded	2014
No. of products	3
Clients	Enterprises and Governmental Organizations
Partners	Different levels of partnership
Market dimension	Growing
Competitors	Very few
Enabling infrastructure	Ready

Table 8.16 User value indicators for Factom

Fast learning	Medium
User interface	Positive
User experience	Positive
Process impact	Medium to High
User feedback	Positive
«Wow» effect	High

In essence, Factom's goal is to create a faster, cheaper, and bloat-free way to develop blockchain based applications. Factom offers three products that are built for enterprises and governmental organizations [45]:

- ***Apollo***: This solution aims to provide tools to verify the integrity of the data used in their transactions.
- ***Iris***: This platform uses a "Distributed Network of Authority" to create authenticated digital identities that is almost impossible to alter, which provides more authenticity for the data generated by the IoT devices.
- ***Hera***: It is considered as a complete security solution for the implementing organization as it combines security features offered by blockchain technology with the typical advantages of the permissioned databases.

From Table 8.16, it can be noticed that the measures that replicate the *User Value* of Factom's blockchain based solutions reflect a positive users' experience. This positive feedback is based on the "trust" gained by utilizing Factom's products as well as the value they offer for the adopting enterprises and governmental departments [46].

8.10 Summary

This Chapter has provided 8 interesting examples of innovative solutions that are utilizing blockchain technology and are available worldwide in 2016. The main rationale for the selection of these cases studies was to present innovative projects that have already had some impact in their domains and that are somehow related to the topics studied in this book.

Blockchain is the most innovative and disruptive technology that was introduced to the world since the establishment of the Internet. It entails tremendous potential to modernize and transform current processes used by organizations all around the globe covering the majority of industries [1]. The case studies described in this Chapter show an increased interest in the blockchain technology and its applications in various industrial and governmental sectors. They also discuss the readiness of blockchain technology to meet the existing market demand as well as the competition between several startups to harvest its potentials.

The innovation practices presented in this chapter cover several implementation areas such as financial services, smart contracts, security and healthcare. The financial services industry is represented by Loyyal, Wave and AlignCommerce. Loyyal is a loyalty and rewards platform that aims to offer a universal solution to users through one digital wallet. Wave appears to be a radical solution to the supply chain industry by dematerializing and storing shipping documents in the distributed digital ledger while AlignCommerce offers a platform that aims to simplify the cross border payment process for small businesses.

By utilizing the dynamics of blockchain and smart contracts, Everledger attempts to tackle the diamond fraud and theft problem that is overgrowing nowadays. Similarly, in the area of security, Civic provides an application that can protect a user's identity from being compromised or stolen while Shocard is developing solutions to protect people's private and sensitive information, which can be used by several industries including airline companies. Finally, within the domain of security, Factom, as a startup company, focuses on protecting the data transacted by enterprises or governmental organisations in order to promote the trust in the data.

The last area covered in this chapter, healthcare, is represented by GemHealth which constitutes an innovative solution in its industry by facilitating the collaboration of different stakeholders in the continuum of care in order to access and share the same healthcare data.

Considering the aforementioned areas and the wide variety of applications that can benefit from implementing blockchain based solutions, it can be concluded that the trend of investing in blockchain will keep growing in order to address the increased market demands.

References

1. Kelly B, Weinswig D (2016) Blockchain technology: the world's Game changer ? https://www.fbicgroup.com/sites/default/files/Blockchain%20Report%20by%20Fung%20Global%20Retail%20Tech%20Apr.%2019%202016.pdf. Accessed 18 Oct 2016
2. Hileman G (2016) State of blockchain Q1 2016: blockchain funding overtakes bitcoin. http://www.coindesk.com/state-of-blockchain-q1-2016/. Accessed 18 Oct 2016
3. Bogart S, Rice K (2015) The blockchain report: welcome to the internet of value. http://www.the-blockchain.com/docs/The%20Blockchain%20Report%20-%20Needham%20(Huge%20report).pdf. Accessed 18 Oct 2016
4. Loyyal (2014) http://www.loyyal.com/. Accessed 14 Oct 2016
5. Fromhart S, Therattil L (2016) Making blockchain real for customer loyalty rewards programs. https://www.finextra.com/finextra-downloads/newsdocs/us-fsi-making-blockchain-real-for-loyalty-rewards-programs.pdf. Accessed 14 Oct 2016
6. Blockchain Startup Ribbit.me Rebrands As Loyyal (2016) http://www.econotimes.com/Blockchain-Startup-Ribbitme-Rebrands-As-Loyyal-200254. Accessed 14 Oct 2016
7. Loyyal (2014) http://loyyal.com/team.html. Accessed 14 Oct 2016
8. Ogden J (2016) Banks should be experience providers, and blockchain can help. https://www.mx.com/moneysummit/banks-should-be-experience-providers-and-blockchain-can-help. Accessed 14 Oct 2016

9. PMNTS (2016) Loyalty programs, the blockchain way. http://www.pymnts.com/blockchain/2016/topic-tbd-loyalty-programs-blockchain-loyyal/. Accessed 14 Oct 2016
10. Parker L (2016) Loyyal helps make Dubai the global leader in blockchain technology. http://bravenewcoin.com/news/loyyal-helps-to-make-dubai-the-global-leader-in-blockchain-technology/. Accessed 14 Oct 2016
11. Everledger (2015) http://www.everledger.io/. Accessed 14 Oct 2016
12. Lomas N (2015) Everledger is using blockchain to combat fraud, starting with diamonds. https://techcrunch.com/2015/06/29/everledger/. Accessed 14 Oct 2016
13. Price R (2015) Everledger builds a ledger of diamonds using blockchain tech. http://uk.businessinsider.com/everledger-ledger-diamonds-blockchain-tech-theft-fraud-2015-8. Accessed 14 Oct 2016
14. JeweltreeFoundation (2016) Jeweltree Foundation and Everledger join forces to preserve the authenticity of diamond certification. https://jeweltreefoundation.org/blog/everledger/. Accessed 15 Oct 2016
15. Walport M (2015) Distributed ledger technology: beyond block chain. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. Accessed 15 Oct 2016
16. Gem (2014) https://gem.co/health/. Accessed 15 Oct 2016
17. Prisco J (2016) The Blockchain for healthcare: Gem launches Gem Health Network with Philips Blockchain Lab. https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938. Accessed 15 Oct 2016
18. Burniske C, Vaughn E, Shelton J, Cahana A (2016) How blockchain technology can enhance EHR operability. http://research.ark-invest.com/hubfs/1_Download_Files_ARK-Invest/White_Papers/ARKInvest_and_GEM_Blockchain_EHR.pdf. Accessed 15 Oct 2016
19. Barclays (2016) Barclays and Wave complete world first blockchain trade finance transaction. http://www.newsroom.barclays.com/r/3396/barclays_and_wave_complete_world_first_blockchain_trade. Accessed 16 Oct 2016
20. Wave Bill of Lading with the BlockChain (2015) http://wavebl.com/. Accessed 16 Oct 2016
21. Ritzo P (2015) Wave brings blockchain trade finance trial to Barclays. http://www.coindesk.com/wave-blockchain-trade-finance-barclays/. Accessed 16 Oct 2016
22. Shamah D (2015) Israeli start-up's bitcoin-based tech raises a mast for shippers. http://www.timesofisrael.com/israeli-start-ups-bitcoin-based-tech-raises-a-mast-for-shippers/. Accessed 16 Oct 2016
23. Parker L (2015) Align Commerce could modernize the B2B payments industry with bitcoins blockchain. http://bravenewcoin.com/news/align-commerce-could-modernize-the-b2b-payments-industry-with-bitcoins-blockchain/. Accessed 16 Oct 2016
24. Rizzo P (2015) KPCB leads $12.5 million round for blockchain firm Align Commerce, http://www.coindesk.com/blockchain-kpcb-align-commerce-12-5-million-series-a/. Accessed 16 Oct 2016
25. Align Commerce—ReThink Wire Transfers (2016) https://www.aligncommerce.com/. Accessed 17 Oct 2016
26. Shabshak T (2016) Identity Service Civic launches, offers $1m ID theft insurance. http://www.forbes.com/sites/tobyshapshak/2016/07/19/identity-service-civic-launches-offers-1m-id-theft-insurance/2/#51d98e405ad5. Accessed 17 Oct 2016
27. Civic Identity Protection (2016) https://www.civic.com/. Accessed 17 Oct 2016
28. Redman J (2016) Civic's $1million identity fraud protection. https://news.bitcoin.com/civic-identity-fraud-protection/. Accessed 17 Oct 2016
29. Civic Identity Protection (2016) https://www.civic.com/about. Accessed 17 Oct 2016
30. Van Der Merwe M (2016) Vinny Lingham's new Civic, http://www.dailymaverick.co.za/article/2016-01-28-vinny-linghams-new-civic/#.WAkkq5MrIb0. Accessed 17 Oct 2016
31. Brown B (2016) Startup civic protects against identity theft. http://www.digitaltrends.com/mobile/civic-identity-theft-blockchain-technology/. Accessed 17 Oct 2016

32. Rizzo P (2016) Vinny Lingham leaves Gyft, raises $2.75 million for identity startup. http://www.coindesk.com/gyft-founder-raises-2-75-million-for-id-startup-civic/. Accessed 17 Oct 2016
33. ShoCard (2016) https://shocard.com/wp-content/uploads/2016/05/ShoCard-release-v1.5.pdf. Accessed 17 Oct 2016
34. ShoCard (2015) https://shocard.com/. Accessed 16 Oct 2016
35. Shocard (2016) Identity for a Mobile World. http://www.sita.aero/globalassets/docs/events/2015-sita-innovation-day/shocard-armin-ebrahimi.pdf. Accessed 16 Oct 2016
36. ShoCard (2015) https://shocard.com/about/#team. Accessed 16 Oct 2016
37. Shrier D, Wu W, Pentland A (2016) Blockchain & infrastructure (identity, data security). MIT Connect Sci Eng. http://cdn.resources.getsmarter.ac/wp-content/uploads/2016/05/MIT_Blockchain_Infrastructure_Report_Part_Three_May_2016.pdf. Accessed 16 Oct 2016
38. ShoCard (2015) https://shocard.com/news/. Accessed 16 Oct 2016
39. ShoCard (2015) https://shocard.com/downloads/. Accessed 16 Oct 2016
40. Snow P, Deery B, Lu J, Johnston D, Kirby P (2014) Factom. http://bravenewcoin.com/assets/Whitepapers/Factom-Whitepaper.pdf. Accessed 18 Oct 2016
41. Factom (2016) https://www.factom.com/products/iris. Accessed 18 Oct 2016
42. AngelList (2016) https://angel.co/factom-for-profit. Accessed 18 Oct 2016
43. Factom (2016) https://www.factom.com/about. Accessed 18 Oct 2016
44. Kastelein R (2016) Peter Kirby—CEO and Founder Factom. http://www.the-blockchain.com/team/peter-kirby-ceo-factom/. Accessed 18 Oct 2016
45. Factom (2016) https://www.factom.com/products. Accessed 18 Oct 2016
46. Factom (2016) https://www.factom.com/. Accessed 18 Oct 2016

Conclusion: The B^3 Perspective

9

Abstract

The book has discussed challenges, benefits, and practices related to Blockchain. In this Chapter, conclusive remarks are provided and the B^3 Perspective is discussed as a way to exploit Blockchain for Digital Business Innovation.

9.1 The B^3 Perspective

In this book we showed the potential of Blockchain by presenting the main challenges and developments for the future implementation of this technology. Now we want to explain what is the B^3 perspective regarding the future innovations within this field.

B^3 is the acronym of *Blockchain Business Board*: these three words are bound together for a reason. Today Companies across the world are facing some major IT challenges and the latest one might reshape the economic world as we know it: that is the Blockchain technology. As we have seen through the Chapters of this book, the word *Blockchain*, at first, described the peer-to-peer distributed ledger, which is at the basis of the Bitcoin protocol. Blockchain helps in enforcing integrity of transactions by acting as a repository that holds records of every transaction executed in the Bitcoin network.

But this technology, as we discussed, is far more than that and this brings us to the second term, which is *Business*. Blockchain is not only about keeping a ledger of currency transactions but it goes beyond that. B^3 wants to explore how business can leverage the blockchain in several industries: financial institutions, insurance companies, healthcare, the energy sector are some of the areas which could be improved by adopting and implementing blockchain based technologies. In the last 20 years it has been clear that the IT sector is one of the most important business units for every company that wants to compete, improve and progress in the new

V. Morabito, *Business Innovation Through Blockchain*,
DOI 10.1007/978-3-319-48478-5_9

digital economy. Blockchain, as pure IT innovation, needs to be studied and embraced by the business world since this technology does not relate to IT world alone: it's a cross-industry technology which is going to be implemented in a variety of fields.

It seems therefore necessary to understand how business and technology can walk together, in order to make sure that, when this innovation will take place, anyone will be ready to change, adapt and adopt it rather soon. This technology could turn into a differentiating factor for adopting businesses, enabling them to process transactions and share information with more efficiency, security and reliability. Managers should not convert to blockchain initiatives right away. A robust strategic planning is essential for every company that wants to understand whether the blockchain is transformative or not.

Businesses have a huge challenge to face before this technology takes off. The time is right for pilot projects, experiments and proof-of-concepts that show and make possible to see how this technology works under the hood. The point is that the blockchain could support financial instruments like equity, securities and derivatives; smart contracts and smart property; new voting systems; identity and reputation systems; distributed databases; and even the management of assets and resources like energy and water [1].

Finally, we have the word *Board:* there is a need of bringing the business world to discuss and discover the technology potential and this can be done when all stakeholders are brought together to explore the many different technology implementations. The sharing part is fundamental because being at its early stages no standards are already in place.

This is the reason behind the Blockchain Business Board (B^3) perspective, which is worth developing as an international research program, aiming to see how business models could evolve in line with blockchain technology innovation.

9.2 Three Main Areas of Development

How is it possible to develop such a program? The main areas considered when discussing blockchain at a higher level imply:

- *speeding up the awareness* that blockchain technology exists and works;
- *providing the right services*;
- *promoting ecosystem connections*.

As for the first pillar, which happens to be fundamental, much can be said. To recognize the potential of a technology is not always easy and to predict trends in the tech industry is a challenging task. The astronomer Clifford Stoll made a prediction on the Internet that couldn't be more wrong: back in 1995 he stated that

"The truth in no online database will replace your daily newspaper, no CD-ROM can take the place of a competent teacher and no computer network will change the way government works". There are many examples of wrong predictions about many technologies but the point is to study them and analyze them before doing anything with them.

Is the blockchain going to be fundamental in the future? Bitcoin, so far the oldest blockchain running experiment, has a 10-billion-dollar market capitalization and has triggered several other blockchain based projects. Being an open source project, anybody could start a similar project and improve it, and actually that is what happened. After being considered a geek niche, Bitcoin reached quite a big recognition, especially because of the underlying technological innovation, which is at the basis of its protocol.

The point here, is that there's a need of speeding up the awareness on blockchain, since industry heavyweights are actually sponsoring a wide range of blockchain use cases supported by industry consortiums as well as innovative fintech startups. Thus, Blockchain Business Board perspective and programs are suitable to be developed as an advisory organism, which help companies to take the most informed decisions about what steps to take to get onboard the blockchain train.

Taking the above issues into account, *education* seems to be the best driver of innovation once again and that's one of the main pillar of the B^3 perspective. Education does not only refer to *learning by studying*, but also to *learn by discussing and sharing insights* with technology influencers and academics. Through communities and seminars stakeholders will get valuable insights and practical knowledge about how blockchain could innovate further.

What are the other means to speed up this awareness? A high-level strategic outlook through widely recognized International Strategic Partners who have developed specific experience in business management and consulting is what is needed the most to provide services which will help companies in the speed up process. Guided proof-of-concepts are the key in this stage because blockchain shows its best side when it stops to be a buzz word and has a chance to show how it works in real world application. As said above, many industries are worth being explored in this sense: financial institutions, insurance companies, telecoms, healthcare institutions and the energy sector are some of the most important areas which have seen the first attempts to implement blockchain.

Finally, all these efforts have to contribute creating a wider ecosystem which will leverage from all the that has been mentioned so far. Actually, experts, lecturers, startups, entrepreneurs and investors should work and learn together to enhance and speed up blockchain adoption. The B^3 perspective has been created to facilitate connections among the aforementioned stakeholders in order to build strong relationships and improve companies' interactions.

It's certainly a huge challenge to drive the change about blockchain and to make innovations within this field real, but the first step is what matters the most.

Reference

1. O'Dwyer R (2015) The Revolution will (not) be decentralised: Blockchains, 23 March 2015. http://commonstransition.org/the-revolution-will-not-be-decentralised-blockchains/. Accessed 20 Nov 2016

Index

V. Morabito, *Business Innovation Through Blockchain*,
DOI 10.1007/978-3-319-48478-5