Contents

Full table of contents

Additional information and references

About the author

Jean-Luc Verhelst is a Strategy Consultant working for Monitor Deloitte and is a founding member of BlockchainHub Brussels, a non-profit think tank and information hub part of the global BlockchainHub network. He holds an applied Bachelor's degree in Information Technology and a Master of Science in Business Administration.

In 2014, his master thesis on Bitcoin received the award for best financial thesis of Belgium by ING Bank. In 2016, he won the world's largest blockchain hackathon in Dublin. He is recognized as a global blockchain expert within the consulting firm Deloitte and has facilitated and conducted the first EMEA and US trainings. He is currently involved in the development of blockchain projects in multiple industries.

Finally, Jean-Luc is a well-regarded speaker within the Belgian Bitcoin and blockchain community. He is known for his ability to explain technical topics in an inspiring and understandable way, coming up with innovative use-cases while being knowledgeable on the more technical aspects.

Twitter:	@JLVerhelst
LinkedIn:	Jean-Luc Verhelst
Facebook page:	Jean-Luc Verhelst
YouTube channel:	jeanlucverhelst
Instagram:	BitcoinBlockchainBook

www.jeanlucverhelst.com
www.bitcoinblockchainbook.com

Contact is possible via www.jeanlucverhelst.com

Acknowledgments

"No man is an island,

Entire of itself,

Every man is a piece of the continent,

A part of the main."

~ John Donne

These verses from John Donne perfectly articulate how nothing can be achieved by one person alone. Everything we are and everything we do is shaped by our environment, the people inspiring us, the people surrounding us, the people helping us, and the people supporting us.

This book is no different.

You are holding in your hands the achievement of a four-year journey. It would, however, not exist had it not been for the many people involved in the process.

First, there are those who contributed to my environment. I am grateful to **my parents** who made it possible for me to study what I wanted and who respected the choices I made. I am thankful to **my professors** for their lessons in an academic environment fostering intellectual challenge. To **the Jury of the ING Thesis Award** and **Frederic Helsen**, who confirmed the quality and uniqueness of my message.

Then there are the people who inspired me. This list would be endless, and most of the people on it are people I have never met. These are world leaders in their domains, entrepreneurs, and people who changed things; those who hold a passion or a message and do not give up.

Finally, thank you to the people surrounding me, the many **colleagues** across all levels at Deloitte who were positive and interested in this adventurous project, and who welcomed my different initiatives with

enthusiasm and trust. To **my friends** in Belgium and the people I met in Dublin, for being there when I needed small “escapes” from the “overloaded life.”

Thanks to:

Moe **Adham** (Co-founder, BitAccess)
Dr. Adam **Back** (Co-founder and CEO, Blockstream)
Damian **Barabonkov** (Slimcoin)
Thomas **Bertani** (CEO, Oraclize – Founder, InsurETH)
Iddo **Bentov** (Cornell University)
David **Birch** (Director of Innovation, Consult Hyperion)
Michelle **Brinich** (Head of Marketing, Blockstream)
Francisco **Cabañas** (Monero)
Luke **Dashjr** (Bitcoin Core developer)
John **Frazer** (External Relations Lead, Ethereum Foundation)
Nick **Gogerty** (Solarcoin and MIT Media Lab)
Cedric **Hauben** (Lawyer, DLA Piper)
Haitch (member of forums.burst-team.us)
Eitan **Katchka** (Founder of La’Zooz and Commuterz)
Arnaud **Kodeck** (Founder, EBTM)
Claire **LaRocca** (Everledger)
Louis **Larue** (Basic income, Catholic University of Louvain)
Christophe **Lejeune** (Catholic University of Louvain)
Christoph **Jentzsch** (CEO, Slock.it)
Daniel **Kraft** (Namecoin)
Sunny **King** (Founder, Peercoin)
Gilles **Mitteau** (Founder, YouTube Channel Heu?reka)
Bach **Nguyen** (SatoshiLabs)
Jean-Grégoire **Orban de Xivry** (Co-founder, Solarly)
David **Osojnik** (CTO, Bitstamp)
John **Quinn** (Co-founder, StorJ)
Luca **Pensieroso** (Macroeconomics, Catholic University of Louvain)
Paige **Peterson** (Zcash)
Andrew **Poelstra** (Mathematician, Blockstream)

Joseph **Poon** (Lightning network)
Veena **Pureswaran** (IBM)
Jeremy **Rand** (Namecoin)
Ripple
Ted **Rogers** (President, Xapo)
Pavol **Rusnak** (SatoshiLabs)
Fabian **Schuh** (BitShares)
Matthew **Spoke** (Co-founder and CEO, Nuco)
David **Schwartz** (Member of bitcoin.stackexchange.com)
Martin **Swende** (Ethereum Developer)
Alan **Szepieniec** (Cryptographer, KU Leuven)
Ryan **Taylor** (CEO, Dash)
Susanne **Tarkowski Tempelhof** (Founder, Bitnation)
Stephan **Tual** (COO, Slock.it)
Roger **van de Berg** (Lawyer, Baker & McKenzie)
Patrick **van der Meijde** (Founder, BitKassa)
James **Walpole** (BitPay)
Tyler **Welmans** (Deloitte Digital)
Bas **Wisselink** (Nxt Foundation)
Lon **Wong** (President, NEM.io Foundation Ltd)
Vasja **Zupan** (COO, Bitstamp)

For their help, insights, content review, and feedback to this book.

Special thanks to **Mallory Miles** and **Vidya Vijayan**, for helping in the editing process and answering my endless requests. Your feedback and work have truly made a difference and contributed immensely to the quality of this book. Thanks to the **teachers** of universities who trusted me to be a guest lecturer and to **Deloitte** for bringing me to the executive boards.

To my dear friends: **Gerard Salvador** for his continuous and extreme enthusiasm: every author needs someone like you around. To **Jérémie Denis**, for his feedback, ideas, positivity, and the time he invested voluntarily. To **Quentin Nederlandt** for his feedback.

Thanks to **Kim Bracke** and **Lieven Verbrugge** for their personal time investments in creating the first YouTube video.

On an almost final note, I would like to thank many people in the Bitcoin and blockchain **community** who helped me in the writing of my thesis during 2013–2014. The **developers** of the community who make things real as well as the **connectors** for connecting, opening doors, and giving me opportunities. To all the people who believed I was not crazy after receiving my speeches and who welcomed my opinions with great enthusiasm and challenge.

A huge thank you to **all those who like, follow, share, and subscribe** to my social media pages for spreading the message! Your impact is much larger and more valuable than you would expect. I will be extremely grateful if you post a picture of this book and let me know what you think!

Finally, I would like to thank **you as a reader** for believing this work is worth your time. I am grateful and humbled by your attention, and I hope this book will meet your expectations.

Notes

1. Original title in Dutch: “Innovatie en disruptie in het economisch recht”
2. The paper was shared via the Cryptography Mailing List and can be viewed at: http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html
3. https://bitcointalk.org/index.php?topic=195.msg1617#msg1617
4. Nakamoto’s first post is visible on the P2Pfoundation forum: http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source. He later became active on the Bitcointalk forum: https://bitcointalk.org
5. http://www.coindesk.com/information/who-is-satoshi-nakamoto/
6. A function is a programmed procedure that performs the same algorithm every time it is called. It can receive information to treat as input and returns a value as output.
7. This is called a collision in cryptography. All functions in cryptography can have collision; the art of a strong hashing function resides in the enormous number of guesses one must make before finding a collision, and thus this unlikelihood of finding a collision.
8. Open source means that the code is publicly available and can be reviewed by anyone. It is 100% transparent.
9. Based on testing conducted in August 2010 with IBM, https://usa.visa.com/run-your-business/small-business-tools/retail.html
10. A bit is a zero or one in computing language. Together, 256 bits offer 2^{256} (roughly 1 followed by 77 zeros) possible combinations.
11. Addresses are inspired from https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses (consulted July 10, 2016) where you can also find further information on the used functions.
12. In fact, there will be a signature for every transaction input. More on transaction inputs in Chapter 6.
13. Going short in finance consists of betting that the price of something will go down
14. July 2017
15. GHash.IO, *Bitcoin mining pool GHash.IO is preventing accumulation of 51% of all hashing power* https://ghash.io/ghashio_press_release.pdf
16. Bershidsky L., *Did Ukrainians Almost Take Over Bitcoin?*, http://www.bloombergview.com/articles/2014-01-14/did-ukrainians-almost-take-over-Bitcoin- April 23, 2014

17. Curtis J., *Mining pool 'in control' of Bitcoin hit by DDos attack*, http://www.cbronline.com/news/social/mining-pool-in-control-of-Bitcoin-hit-by-ddos-attack-4293920, consulted June 20, 2014
18. Quentson A., *Bitcoin Mining Pool Ghash.io DDos-ed in Response to threat of 51% attack?*, http://www.cryptocoinsnews.com/news/Bitcoin-mining-pool-ghash-io-ddos-ed-response-51-attack/2014/06/15, consulted June 06, 2014
19. Buterin V., *Bitcoinmagazine.com,* https://Bitcoinmagazine.com/articles/Bitcoin-is-not-quantum-safe-and-how-we-can-fix-1375242150 - consulted June 2016
20. Further reading on Lamport Signatures: https://gist.github.com/karlgluck/8412807
21. Buterin V., *Bitcoinmagazine.com,* https://Bitcoinmagazine.com/articles/Bitcoin-is-not-quantum-safe-and-how-we-can-fix-1375242150 - consulted June 2016
22. Alan Szepieniec (PhD Researcher in Cryptography at the KU Leuven), July 2016
23. Alan Szepieniec (PhD Researcher in Cryptography at the KU Leuven), July 2016
24. Pieter Wuille at the Scaling Blockchain conference in Hong Kong, December 7, 2015 - https://www.youtube.com/watch?v=zchzn7aPQjI
25. Off-chain bitcoin payments are bitcoin payments that happen on alternative platforms and require only a limited number of re-transactions in the Bitcoin Blockchain.
26. Technically speaking, Johanna is rewriting a transaction waiting for John's signature to be broadcasted. The new transaction uses the same input but sends a higher amount to John. The transaction will be broadcasted once the channel is closed.
27. The complete white paper can be found at: https://blockstream.com/sidechains.pdf
28. Written by Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille
29. Peer-review with Luke Dashjr, May 2017
30. Routing tables facilitate communication on networks. In this case, they would keep track of the different existing channels and how to transfer cryptocurrencies across channels.
31. https://lightning.network/lightning-network-paper.pdf
32. https://bitinfocharts.com/comparison/bitcoin%20cash-hashrate.html
33. https://blockchain.info/charts/hash-rate

34. https://www.coindesk.com/bitcoin-cash-closes-profitability-parity-original-blockchain/
35. https://www.coindesk.com/bitcoin-cash-returns-profitability-amid-mining-adjustments/
36. August 15, 2017
37. April 2017
38. http://www3.weforum.org/docs/WEF_Internet_for_All_Framework_Accelerating_Internet_Access_Adoption_report_2016.pdf, consulted August 16, 2017
39. https://motherboard.vice.com/en_us/article/xy5evk/meet-the-man-running-the-only-bitcoin-node-in-west-africa, consulted August 16, 2018
40. https://blockstream.com/satellite/howitworks, consulted August 16, 2017
41. https://blockstream.com/satellite/faq/, consulted August 16, 2017
42. https://blockstream.com/satellite/blockstream-satellite, consulted August 16, 2017
43. https://en.bitcoin.it/wiki/Thin_Client_Security
44. The initial chaincode at the master level is an input generated from random data. As from the next level, the chaincode is generated from a function hashing the parent key, the previous chaincode, and the index of the child key.
45. *Mastering Bitcoin*, Andreas
46. Coin Desk, how to store your Bitcoin – consulted June 1, 2016 - http://www.coindesk.com/information/how-to-store-your-bitcoins/
47. Coin-mixing is a method of mixing Bitcoin transactions in order to make them less traceable. A mixing service receives different transactions from different users (the initial owners), then sends the funds of these transactions to multiple addresses before sending them back to an address controlled by the initial owner. The multitude of transactions splitting and merging bitcoins recorded on the Bitcoin Blockchain is supposed to increase the difficulty in retracing transactions.
48. Near-field communication (NFC) is a technology allowing devices to communicate in a contactless way.
49. Blockchain is the technology behind Bitcoin but there is also a wallet company based in Luxembourg, called Blockchain, which operates the website Blockchain.info. In this case, we are referring to the wallet provider.
50. “A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a

large number of consecutive guesses as to the value of the desired data." - https://www.techopedia.com/definition/18091/brute-force-attack
51. You can generate a paper wallet online at https://bitcoinpaperwallet.com/
52. Some offline generators can be downloaded at https://github.com/cantonbecker/bitcoinpaperwallet
53. https://en.bitcoin.it/wiki/Paper_wallet#Generation_of_secure_keys
54. https://ihb.io/paper-wallet
55. In this case, we use the term digital currencies instead of cryptocurrencies because a few currencies are not backed by a distributed ledger or by cryptography and, as a consequence, do not fall under the denomination of cryptocurrencies.
56. Dougherty C. and Huang G., *Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss*, http://www.bloomberg.com/news/2014-02-28/mt-gox-exchange-files-for-bankruptcy.html, consulted May 2, 2014
57. Wilson S., *Mt. Gox finds 200,000 Bitcoins in 'forgotten' wallet*, http://www.telegraph.co.uk/finance/currency/10713243/MtGox-finds-200000-Bitcoins-in-forgotten-wallet.html n, consulted May 26, 2014
58. http://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html
59. https://cdn.omise.co/omg/whitepaper.pdf
60. http://www.coindesk.com/reality-chinese-trading-volumes/
61. http://in.reuters.com/article/china-bitcoin-idINL3N0JX2FH20131218
62. Automated teller machines
63. Phone Interview, Jean-Wallemacq, Belgian Bitcoin Foundation
64. Phone Interview, Moe Adham, BitAccess
65. Phone Interview, Moe Adham, BitAccess
66. http://www.ebtm.be/buy-sell
67. Phone interview with Arnaud Kodeck, EBTM
68. Phone interview with Arnaud Kodeck, EBTM
69. Phone Interview, Moe Adham, BitAccess
70. Wikipedia, *Silk Road*, http://en.wikipedia.org/wiki/Silk_Road_(marketplace) – consulted May 18, 2014
71. Kar I., *What companies accept Bitcoins?*, http://www.nasdaq.com/article/what-companies-accept-Bitcoin-cm323438 - consulted June 6, 2014
72. http://www.coindesk.com/tesla-model-3-bitcoin/
73. https://spectrum.mit.edu/continuum/mits-bitcoin-experiment-is-underway/ consulted August 14, 2016

74. Gill R., Video: Holland's Bitcoin Boulevard Celebrates Two Successful Months, http://www.coindesk.com/video-hollands-Bitcoin-boulevard-celebrates-two-successful-months/ - consulted May 27, 2014
75. "Exchange risk exists (…) when a financial transaction is denominated in a currency other than that of the base currency of the company. (…) The risk is that there may be an adverse movement in the exchange rate of the denomination currency in relation to the base currency before the date when the transaction is completed." Wikipedia, consulted August 14, 2016.
76. Skype interview with Patrick van der Meijde, December 2016
77. https://www.cryptocoinsnews.com/bitcoin-boulevard-bitcoin-part-everyday-life-dutch-neighbourhood/
78. Skype interview with James Walpole, BitPay. January 6, 2017
79. Skype interview with James Walpole, BitPay. January 6, 2017
80. Skype interview with James Walpole, BitPay. January 6, 2017
81. Email exchange with James Walpole, BitPay. January 17, 2017
82. Skype interview with James Walpole, BitPay. January 6, 2017
83. Smallest storage unit on a computer, represented by 0 or 1
84. Beattie A., *The History of Money: From Barter to Banknotes*, consulted June 4, 2014, http://www.investopedia.com/articles/07/roots_of_money.asp
85. Moffatt M., *Money*, consulted June 4, 2014, http://economics.about.com/od/termsbeginningwithm/g/money.htm
86. Weatherford J., *The History of Money*, New York, Crown Publishers, 1997, p22
87. Weatherford J., *The History of Money*, New York, Crown Publishers, 1997, p31
88. Weatherford J., *The History of Money*, New York, Crown Publishers, 1997, p32
89. Weatherford J., *The History of Money*, New York, Crown Publishers, 1997, p199-203
90. http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ecofin/136487.pdf
91. https://www.usatoday.com/story/money/business/2013/07/29/bank-of-cyprus-depositors-lose-savings/2595837/
92. https://www.rt.com/business/cyprus-crisis-bailout-deposit-631/
93. The European troika is a decision group formed by the European Commission (EC), the European Central Bank (ECB) and the International Monetary Fund (IMF).
94. *Russia Today*, https://www.rt.com/business/cyprus-crisis-bailout-deposit-631/ - consulted July 2013

95. Andresen G., *Gavin Andresen on the Present and Future of Bitcoin*, 2014, http://www.econlib.org/cgi-bin/fullsearch.pl?query=Andresen%20on%20Bitcoin, (EconTalk, Posdcast)
96. Author's experience in the Philippines
97. In Keyna, more than 45% of money transaction are done through M-Pesa (a cellphone-based money transfer service) while 30% are done by hand.
    Source: The World Bank, *Mobile payments go viral: M-PESA in Kenya*, http://web.worldbank.org/WBSITE/EXTERNAL/COUNTRIES/AFRICAEXT/0,,contentMDK:22551641~pagePK:146736~piPK:146830~theSitePK:258644,00.html - consulted June 17, 2014
98. Messenger call, Jean-Gregoire Orban de Xivry
99. A full report from Deloitte concerning supply chain challenges for retail banks and their structure can be found at: http://www.deloitte.com/assets/Dcom-Canada/Local%20Assets/Documents/Insights/Innovative_Thinking/2013/ca_en_insights_optimizing_the_retail_bank_supply_chain_102913.pdf, - consulted June 15, 2014
100. Unlike standard formatting, zero-fill formatting overwrites every bit on a hard drive to zero. It is estimated that a hard drive has to undergo three cycles of zero-fill formatting to make it impossible to recover any data.
101. Weatherford J., *The History of Money*, New York, Crown Publishers, 1997, p25-27
102. https://en.wikipedia.org/wiki/Superdollar#Confirmed_sources
103. Galt J. *BitcoinMagazine.com,* https://bitcoinmagazine.com/articles/is-bitcoin-headed-for-a-break-in-fungibility-1450823559 - consulted June 2016
104. Galt J. *BitcoinMagazine.com,* https://bitcoinmagazine.com/articles/is-bitcoin-headed-for-a-break-in-fungibility-1450823559 - consulted June 2016
105. Thousand millions of millions in the American system.
106. Campbell D., *Trust in politicians hits an all-time low*, http://www.theguardian.com/politics/2009/sep/27/trust-politicians-all-time-low - consulted 6/8/14
    Pew Research center, *Public Trust in Government: 1958-2013*, http://www.people-press.org/2013/10/18/trust-in-government-interactive/ - consulted July 7, 2014
107. https://rbi.org.in/Scripts/NotificationUser.aspx?Id=10683&Mode=0
108. Author's personal experience in India

109. http://timesofindia.indiatimes.com/india/2-die-in-country-wide-rush-to-junk-banned-notes/articleshow/55374158.cms
110. http://indianexpress.com/article/india/india-news-india/arvind-kejriwal-lashes-out-at-bbc-reporter-questioning-him-on-demonetisation-4384031/?campaign_id=A100
111. http://www.dnaindia.com/india/report-demonetization-with-no-cash-on-hand-4-lakh-trucks-stranded-on-highways-2273414
112. http://www.firstpost.com/business/demonetisation-farmers-fear-loss-of-crops-and-income-after-currency-ban-3111694.html
113. http://www.cnbc.com/2016/11/15/india-rupee-restriction-boost-bitcoin-digital-currency.html
114. https://www.theguardian.com/world/2016/dec/15/venezuelans-on-the-removal-of-the-100-bolivar-note-thoughtless-dangerous
115. https://www.washingtonpost.com/news/global-opinions/wp/2016/12/15/declaring-war-on-common-sense-venezuela-bans-its-own-money/?utm_term=.c969f12e0b6f
116. http://www.coindesk.com/assange-bitcoin-wikileaks-helped-keep-alive/
117. https://europa.eu/newsroom/highlights/special-coverage/eu_sanctions_en - consulted September 10, 2016
118. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/135804.pdf - consulted January 08, 2017
119. Verhelst J., The Bitcoin e-currency : historical genesis, current situation and empirical analysis compared to traditional currencies and commodities
120. https://www.cryptocoinsnews.com/ghostsec-isis-bitcoin-wallet-worth-3-million/
121. http://www.wienerzeitung.at/_em_daten/_wz0/2016/01/25/160125_1356_europol_dokument_aenderungen_in_der_verfahrensweise_mit_is_terroranschlaegen_pdf_englisch.pdf + http://europeanmemoranda.cabinetoffice.gov.uk/files/2017/07/10977-17-ADD-2.pdf
122. http://www.wsj.com/articles/alternative-currencies-flourish-in-greece-as-euros-are-harder-to-come-by-1439458241
123. http://www.investopedia.com/terms/s/seigniorage.asp
124. http://www.worldbank.org/en/news/video/2016/03/10/2-billion-number-of-adults-worldwide-without-access-to-formal-financial-services
125. https://www.ft.com/content/c5d08c5c-339c-11e6-bda0-04585c31b153
126. http://bruegel.org/wp-content/uploads/2016/06/pc_2016_10-1.pdf

127. Recent events include the transatlantic trading agreement. On the other hand, the Ukrainian conflict tends to reinforce old trading barriers.
128. For example, credit cards offer not only a faster payment method but also extra protections to their users at the cost of higher transaction fees.
129. Getting smart on smart contracts, CFO Insights, Deloitte Development LLC.– June 2016
130. https://www.youtube.com/watch?v=GplUE1NGqgA
131. Denoël T., *Pourquoi Albert Frère investit dans les terres agricoles*, http://www.levif.be/info/actualite /belgique/pourquoi-albert-frere-investit-dans-les-terres-agricoles/article-4000304793506.htm – consulted May 17, 2014
132. The blockchain is one of the more secure and world's more widespread database. Some people use the blockchain to store valuable information (i.e., Dutch notaries for storing the hashtag of documents).
Source : Spaes T., *De pro's en contra's van de Bitcoin*, http://deredactie.be/cm/vrtnieuws/videozone/programmas/devrijemarkt/2.31526?video=1.1838058 – consulted April 6, 2014
133. http://www.forbes.com/sites/katiegilbert/2014/09/22/why-local-currencies-could-be-on-the-rise-in-the-u-s-and-why-it-matters/#3e56201e27b0
134. http://www.forbes.com/sites/katiegilbert/2014/09/22/why-local-currencies-could-be-on-the-rise-in-the-u-s-and-why-it-matters/#3e56201e27b0
135. http://www.lemonde.fr/economie/article/2015/05/22/en-complement-de-l-euro-les-monnaies-locales-seduisent-de-plus-en-plus_4639088_3234.html
136. http://www.euskalmoneta.org/fr/ensemble-soutenons-leuskara-grace-a-leusko/
137. https://www.youtube.com/watch?v=mpE8UMMZa9w
138. http://www.euskalmoneta.org/fr/ensemble-soutenons-leuskara-grace-a-leusko/
139. http://www.euskalmoneta.org/fr/ensemble-soutenons-leuskara-grace-a-leusko/
140. https://letstalkpayments.com/which-countries-are-close-to-a-cashless-world/
141. http://www.worldatlas.com/articles/which-are-the-world-s-most-cashless-countries.html
142. De Redactie, *Terzake*, http://deredactie.be/permalink/2.32224?video=1.1892263 – 27/2/14

143. http://www.tijd.be/nieuws/archief/Opnieuw_cyberdiefstallen_via_banken_platform_Swift.9804437-1615.art?highlight=swift
144. http://www.tijd.be/nieuws/archief/Bankenplatform_Swift_heeft_cyberveiligheid_verwaarloosd.9799381-1615.art?ckc=1&ts=1484491732
145. IOCTA 2016, *Internet organized crime threat assessment*, Europol report, the Hague, p.44. (https://www.europol.europa.eu/activities-services/main-reports/Internet-organised-crime-threat-assessment-iocta-2016)
146. This has been the case in the Netherlands, from where Bitcoin start-ups are interested to operate but the national bank has warned companies not to work with Bitcoin start-ups. Source: Skype interview with Van de Berg R. *Tax Lawyer at Baker & McKenzie Amsterdam N.V.* (2014) following publication "Fiscaal beleid overheid rond bitcoin remt innovatie", Dutch Financial Times, June 17, 2014.
147. https://www.asfi.gob.bo/images/ASFI/DOCS/SALA_DE_PRENSA/Notas_de_prensa/2017/N_20_Nota_Prohibici%C3%B3n_de_uso_y_circulaci%C3%B3n_de_monedas_virtuales.pdf
148. https://bitcoinmagazine.com/articles/bolivian-authorities-arrest-60-cryptocurrency-promoters/
149. Perkins Coie report, Virtual Currencies: International Actions and Regulations
150. http://fortune.com/2017/02/12/bitcoin-markets-china-regulation/
151. http://calvinayre.com/2016/12/07/business/russias-finance-ministry-delaying-bitcoin-bill-late-2017/
152. http://www.cnbc.com/2017/06/01/bitcoin-russia-regulation.html
153. Perkins Coie report, Virtual Currencies: International Actions and Regulations
154. http://uk.reuters.com/article/us-venezuela-bitcoin-idUKKCN0HX11O20141008
155. https://bitcoinmagazine.com/articles/venezuela-seems-be-cracking-down-bitcoin/
156. https://bitcoinmagazine.com/articles/venezuela-seems-be-cracking-down-bitcoin/
157. http://www.newsbtc.com/2017/02/23/surbitcoin-business-next-week/
158. http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf
159. http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf
160. http://data.consilium.europa.eu/doc/document/ST-15605-2016-INIT/en/pdf
161. Roger Van de Berg, email exchange July 2017

162. https://bitcoinmagazine.com/articles/regulation-bitcoins-germany-first-comprehensive-statement-bitcoins-german-federal-financial-supervisory-authority-bafin-1391637959/
163. http://www.cnbc.com/id/100971898
164. Financial Crimes Enforcement Network (FinCEN), *History of Anti-Money Laundering Laws*, http://www.fincen.gov/news_room/aml_history.html [hereinafter AML History]. – consulted June 5, 2014
165. https://cointelegraph.com/news/property-money-or-currency-what-is-bitcoin-and-why-it-matters
166. IRS Notice 2014-21
167. https://www.irs.gov/irb/2014-16_IRB/ar12.html
168. Rubin R. and Dougherty C., *Bitcoin Is Property, Not Currency, in Tax System: IRS,* http://www.bloomberg.com/news/2014-03-25/Bitcoin-is-property-not-currency-in-tax-system-irs-says.html - consulted June 7, 2014
169. Van de Berg et al., *Decision on Landmark Case Regarding the VAT Treatment of Bitcoin,* Bloomberg BNA - Tax Planning International (Indirect Taxes) - Volume 13
170. http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128en.pdf
171. Moore A. G., Crossing the Charm, New York, PerfectBound, 1991 – page 9
172. https://blockchain.info/fr/charts/hash-rate, consulted May 13, 2017. One Gigahash is equal to 1 billion hashes.
173. http://www.nytimes.com/2016/10/12/business/dealbook/central-banks-consider-bitcoins-technology-if-not-bitcoin.html?_r=0
174. https://www.cryptocoinsnews.com/european-central-bank-is-open-to-blockchain-technology/
175. https://bitcoinmagazine.com/articles/bank-of-england-chief-economist-blockchain-based-digital-currency-issued-by-central-banks-could-replace-cash-1443028299
176. Assuming no legal measures decide to ban the Internet.
177. Numbers on July 22, 2016. Source: https://cryptolization.com/
178. https://www.youtube.com/watch?v=fE_oWNEDh_k
179. August 15, 2017
180. Coinmarketcap.com, consulted August 15, 2017
181. The “pump and dump” of altcoins is similar to the pump and dump of penny stocks; both having relatively small market capitalization. You can buy a lot of coins at a cheap price, and then create a buzz about the coin to attract other investors willing to buy the coin. As more and more

investors buy in, the price increases (pump). While the price increases, the initial buyer starts selling his coins (dump). Ultimately, people realize that there was a lot of buzz about nothing, and the price decreases.

182. January 2017
183. https://peercoin.net/assets/paper/peercoin-paper.pdf
184. https://chainz.cryptoid.info/slr/
185. The full list of metadata posted in the transaction can be consulted at https://solarcoin.org/en/viewing-transactions-on-the-solarcoin-blockchain/
186. Facetime interview with Jean-Gregoire Orban de Xivry, Early adopter of Solarcoin and Founder of Solarly, a start-up bringing solar energy to African villages.
187. Email exchange Ryan Taylor, February 28, 2017
188. Email exchange Ryan Taylor, March 5, 2017
189. https://www.dash.org/team/
190. Email exchange with Bas Wisselink, Nxt Foundation, February 27 2017
191. Francisco Cabanas, Monero, Email exchange March 14, 2017
192. https://blockchainhub.net/blog/infographics/monero-in-a-nutshell/ consulted December 29, 2016
193. https://en.wikipedia.org/wiki/Monero_(cryptocurrency) consulted December 29, 2016
194. Ripple.com December 29, 2016
195. https://ripple.com/xrp-portal/
196. https://pando.com/2014/08/15/ripple-settles-with-estranged-founder-jed-mccaleb-outlining-a-metered-sale-of-his-xrp-holdings/
197. https://ripple.com/xrp-portal/, consulted March 14, 2017
198. Email exchange with Daniel Kraft, February 27, 2017.
199. https://nameid.org/?
200. http://bitcoin.stackexchange.com/questions/273/how-does-merged-mining-work
201. Remember, the coinbase transaction is the transaction in which the miner allocates newly generated bitcoins to himself.
202. Or another cryptocurrency backed by many times more computing power.
203. http://bitcoin.stackexchange.com/questions/3472/what-is-the-story-behind-the-attack-on-coiledcoin
204. https://bitcointalk.org/index.php?topic=56675.msg678006#msg678006
205. This example is inspired from Peercoin
206. https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/

207. https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/
208. https://solarcoin.org/en/important-update-to-solarcoin-currency-wallets/
209. Email exchange with Nick Gogerty, Founder of Solarcoin
210. http://docs.bitshares.org/bitshares/dpos.html#:
211. https://www.nem.io/NEM_techRef.pdf
212. https://cointelegraph.com/news/proof-of-importance-nem-is-going-to-add-reputations-to-the-blockchain
213. As explained https://bytecoin.org/blog/proof-of-activity-proof-of-burn-proof-of-capacity/
White paper can be found at https://eprint.iacr.org/2014/452.pdf
214. Iddo Bentov (Cornell University)
215. https://bitcointalk.org/index.php?topic=731923.0
216. https://en.wikipedia.org/wiki/Proof_of_Space
217. Email exchange with Nick Gogerty, May 12, 2017
218. This was the case for Chancecoin, one of the first altcoins to experiment with burning.
219. This assumes that the mechanism to go from private key to address is the same on both chains.
220. http://www.coindesk.com/everledger-blockchain-tech-fight-diamond-theft/
221. https://techcrunch.com/2015/06/29/everledger/
222. https://blog.oraclize.it/understanding-oracles-99055c9c9f7b, consulted April 16, 2017
223. Martin Swende, peer-review, May 2017
224. https://github.com/DavidJohnstonCEO/DecentralizedApplications/blob/master/README.md
225. http://blockchainhub.net/dapps/
226. https://techcrunch.com/2016/12/21/uber-losses-expected-to-hit-3-billion-in-2016-despite-revenue-growth/
227. www.lazooz.org
228. http://bitcoinwiki.co/using-the-blockchain-for-decentralized-ride-sharing-with-lazooz/
229. https://www.indiegogo.com/projects/la-zooz-real-time-social-ridesharing-app#/
230. https://storj.io/
231. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/
232. http://www.altcointoday.com/ethereum-classic-funds-of-the-dao-hack-are-moving/

233. https://www.youtube.com/watch?v=LVlT4sX6uVs
234. See https://t.co/mAMFrXCTiX for more technical details
235. Find demo at https://youtu.be/U1XOPIqyP7A
236. https://www.youtube.com/watch?v=49wHQoJxYPo
237. See Blockcharge
238. Find demo at https://youtu.be/U1XOPIqyP7A
239. https://www.youtube.com/watch?v=qlBQfv85g6I
240. https://en.wikipedia.org/wiki/Passport
241. https://en.wikipedia.org/wiki/Identity_document#History
242. https://shocard.com/cpt_news/identity-management-on-the-blockchain/
243. https://e-estonia.com/component/x-road/
244. https://www.youtube.com/watch?v=9PaHinkJlvA
245. https://bravenewcoin.com/news/e-estonia-initiative-progresses-with-blockchain-partnerships/
246. http://pwc.blogs.com/health_matters/2017/03/estonia-prescribes-blockchain-for-healthcare-data-security.html
247. https://www.genome.gov/sequencingcostsdata/
248. Tyler Welmans, Blockchain and Digital Identity specialist Deloitte, Email exchange May 2017
249. https://www.youtube.com/watch?v=zpO7eH5FYdo
250. http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf
251. http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf
252. https://www.youtube.com/watch?v=IoQqchIoA-k
253. https://www.youtube.com/watch?v=hS15p5V3slg
254. http://www.businessinsider.com/elon-musk-universal-basic-income-2017-2
255. http://www.businessinsider.com/bill-gates-basic-income-2017-2
256. http://www.doorbraak.be/nl/etienne-vermeersch-men-schijnt-onvoldoende-te-beseffen-wat-er-op-ons-afkomt
257. https://medium.com/basic-income/why-milton-friedman-supported-a-guaranteed-income-5-reasons-da6e628f6070#.modlnxi4s
258. https://www.weforum.org/agenda/2017/01/why-we-should-all-have-a-basic-income?
259. https://www.youtube.com/watch?v=_wYywEW9aTY
260. https://www.swissinfo.ch/eng/cantons-and-municipalities/29289028
261. https://www.youtube.com/watch?v=_wYywEW9aTY
262. http://direct-democracy.geschichte-schweiz.ch/
263. http://direct-democracy.geschichte-schweiz.ch/

264. https://www.youtube.com/watch?v=PJy8vTu66tE
265. https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.sy4Wm32Kp#.jh30ARMge
266. http://www.pcworld.com/article/3142412/windows/just-how-partisan-is-facebooks-fake-news-we-tested-it.html
267. http://www.journalism.org/2016/12/15/many-americans-believe-fake-news-is-sowing-confusion/
268. http://www.independent.co.uk/voices/facebook-fake-news-fact-check-google-ad-save-journalism-a7645706.html
269. http://www.independent.co.uk/life-style/gadgets-and-tech/news/us-election-rigged-hillary-clinton-hacked-donald-trump-russia-edward-snowden-a7437181.html
270. http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA(2016)581918_EN.pdf
271. https://www.youtube.com/watch?v=UajbQTHnTfM
272. https://blockgeeks.com/blockchain-voting/
273. https://e-estonia.com/estonian-government-and-bitnation-begin-cooperation/
274. https://www.youtube.com/watch?v=M4Dg3mO3cAc Susanne Tarkowski Tempelhof
275. https://bitnation.co/refugee-emergency-response/
276. https://www.youtube.com/watch?v=fEfgCdy1mwE
277. https://www.bloomberg.com/view/articles/2015-12-01/i-attended-the-first-official-digital-wedding
278. https://www.bloomberg.com/view/articles/2015-12-01/i-attended-the-first-official-digital-wedding
279. https://www.bloomberg.com/view/articles/2015-12-01/i-attended-the-first-official-digital-wedding
280. http://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct

In this book, you will learn:

- What is Bitcoin and what is blockchain
- How it works, step-by-step
- Why it is important
- What is “mining”
- The security threats that plague it
- The challenges it faces
- The solutions to these challenges
- How to acquire bitcoins
- How to store your bitcoins safely
- Four characteristics and six types of wallets, their advantages, and disadvantages
- How and where to spend your bitcoins
- The ecosystem landscape
- If Bitcoin is, or can become, money or currency
- Political, economic, and social implications
- Regulations
- Other cryptocurrencies
- Different consensus mechanisms
- What are smart-contracts, Dapps, and DAOs
- Concrete examples of blockchain applications
- What it means for business and financial audits
- What it means for identity, basic income and democracies
- The promises of blockchain
- The pitfalls of blockchain