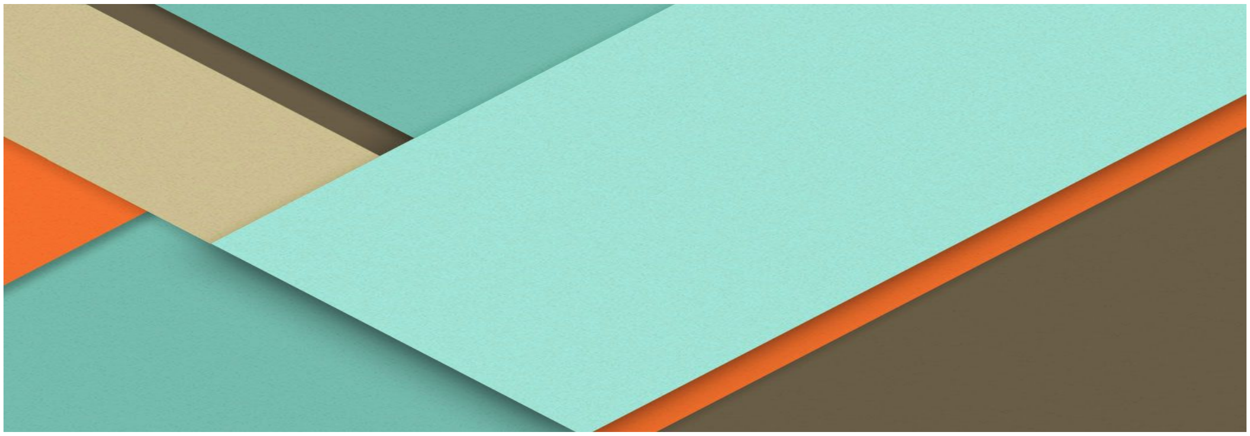

A History of Bitcoin

30th September, 2017[1]

Usman W. Chohan, MBA
School of Business and Economics

University of New South Wales, Canberra

Discussion Paper

Discussion Paper Series: *Notes on the 21st Century*

Abstract: The meteoric rise of Bitcoin has led to heightened investment, academic, commercial, numismatic, transactional, and practitioner interest in that cryptocurrency, as well as in the growing array of such instruments worldwide. This leads to an accentuated need for an examination of the historical evolution of Bitcoin as the seminal instrument in the development of cryptocurrencies, and this discussion paper seeks to address that gap.

[1] Originally prepared in November, 2016, and updated in February and September, 2017 to reflect regulatory changes

A History of Bitcoin

The meteoric rise of Bitcoin has led to heightened investment, academic, commercial, numismatic, transactional, and practitioner in the cryptocurrency, as well as in the growing array of such instruments worldwide (see multidisciplinary academic discussions and analyses in Ametrano 2016; Brenig et al. 2015; Cheung et al. 2015; Chohan 2017a, 2017b, 2017c, 2017d, 2017e; Cocco et al. 2017; Darlington 2014; Davis 2011; Farell 2015; Gjermundrod and Dionysiou 2014; Graeber 2011; Greenberg 2011; Harwick 2015; Houy 2014; Howden 2015; Hughes and Middlebrook 2015; Iwamura et al. 2014a, 2014b; Koning 2016; Narayanan 2016; Stapenhurst et al. 2015; Vigna et al. 2015). This leads to an accentuated need for a revisitation of the history of Bitcoin as the seminal instrument in the development of cryptocurrencies. This discussion paper aims to address that gap. It progresses chronologically, attempting to incorporate technological, regulatory, and economic events salient to the genesis and deployment of Bitcoin, as well as to the adoption and proliferation of the cryptocurrency.

Genesis of Bitcoin

Virtual money has come into vogue at different times during the history of sedentary human civilization, and has often stayed for extended periods of time before being replaced by 'tangible' money alternatives, only to be superseded by virtual money in what has been described as a series of long-cycles of money instruments and debt (Graeber 2011). Even within the specific category of digital cash instruments, some vehicles did exist before Bitcoin, but had not assumed the central or preeminent position that Bitcoin would eventually come to adopt. Despite Bitcoin's unique propositions, there were other digital monetary instruments in circulation in the online sphere that wielded traits similar to Bitcoin such as ***proof-of-work*** or ***digital scarcity***. The issuer-based ***ecash*** of Chaum and Brands is the earliest example, while Adam Back had created a proof-of-work scheme for spam control known as hashcash. The proof-of-work algorithm in hashcash was further developed into a ***reusable proof-of-work*** (RPOW) by Hal Finney. Proposals for cryptocurrencies that had distributed digital scacity included B-Money (Wei Dai) and Bit Gold (Nick Szabo). The problem of market-based collectible mechanisms for controlling currency inflation were part of Bit Gold's proposal, as were other enabling aspects such as a Byzantine fault-tolerant asset registry, which would store and transfer enchained proof-of-work solutions. With these innovators laying the groundwork, Bitcoin itself was "authored" by a pseudonymous person(s) or entity(-ies) known as Satoshi Nakamoto. Wei Dai and Hal Finney were suspected of being the agents behind the ***nom de plume*** Satoshi Nakamoto, but they issued denials to that effect.

Nakamoto posted a paper to a cryptography mailling list in 2008 with the title "Bitcoin: A Peer-to-Peer Electronic Cash System," (Nakamoto 2008). This paper laid out the schema for a peer-to-peer network that would foster a "system for electronic transactions without relying on trust," (Nakamoto 2008). The underlying message was the elements of trust, accountability, or oversight, that had characterised commerce and exchange throughout history would be replaced by a system that would simply have no ***need*** for transacting agents to know one another (Chohan 2017a, 2017b, 2017c, 2017d, 2017e).

Launching Bitcoin

After the dissemination of the paper (Nakamoto 2008), the actual platform for bitcoin transactions came into being through the release of the first open-source ***Bitcoin-Client*** and the concommittant issuing of Bitcoins. Nakamoto mined the first block of bitcoins with a reward of 50 bitcoins. This block is commonly referred to as the "genesis block." Hal Finney downloaded the bitcoin client and received the first 10 bitcoins from Nakamoto, which represented the first Bitcoin transaction in history. Nick Szabo and Wei Dai were also expressed strong support for Bitcoin after its release. Nakamoto himself mined an amount approximating 1 million bitcoins, before disappearing and severing involvement with the bitcoin movement. Gavin Andresen became the lead developer at the Bitcoin Foundation, and thereafter became the equivalent of the 'public face' of Bitcoin.

In the initial phases of release, the monetary value of bitcoin was arrived at through a proto-market bargaining process, as for example when 10,000 bitcoins were used to purchase (indirectly) two pizzas from Papa Johns. At this early juncture, despite the seeming vulnerability of the system, only one significant vulnerability was discovered, which led to the exploited overproduction of 180 billion bitcoins. However, those coins were removed from the blockchain, and an updated security protocol countered the extant flow.

Growth-Era

The open source code of Bitcoin helped other cryptocurrency developers to create alternative coins based on its code (Chohan 2017e). Early adopters of Bitcoin for transactional purposes included Wikileaks (donations) and the Electronic Frontier Foundation (doing so intermittently). In 2011, a bitcoin-related public magazine ***Bitcoin Magazine*** was released. Bitcoin also appeared in entertainment, as in the CBS Drama ***The Good Wife.*** The show insinuated that Bitcoin was not a 'true currency.' In 2012, the Bitcoin Foundation was launched to focus on the standardization, protection, and promotion of Bitcoin. By 2012, the global bitcoin payment service BitPay reported that 1000+ merchants were accepting Bitcoin under its payment processing service. In 2013, Coinbase, another payment processor, announced that it had sold $1 million (USD) worth of bitcoins in one month, at per unit equivalent above $22 per bitcoin.

By 2013, bitcoin was under the radar of regulatory bodies worldwide, and had grown in volume to the point of causing encumbrances to clearinghouses. That year, several exchange- and clearinghouse-related incidents occurred, including the splitting of the chain into two bitcoin networks, and processing delays due to insufficient capacity, which led to precipitous drops in price and even temporary halting of trade. The American Financial Crimes Enforcement Network (FinCEN) established regulatory guidelines for decentralized virtual currencies (including Bitcoin). They classified those American bitcoin miners who would sell generated bitcoins as ***Money Service Businesses*** (MSBs), as subject to legal obligations including registration. The violation of these rulings, specifically the failure to register as a money transmitter, by bitcoin exchange Mt. Gox resulted in US authorities seizing accounts associated with the exchange. New businesses such as dating site ***OkCupid*** and food-ordering service ***Foodler*** began to accept Bitcoins at this time. A slight trend towards monopolization of bitcoin processing began to be observed when it was noted that BitInstant processed roughly 30% of in-bound and out-bound transactions from traditional money into bitcoin, and that BitInstant would do in excess of 30,000 transactions in a month. US enforcement agencies found bitcoins in various incidents and investigations, as when the Drug

Enforcement Agency (DEA) had reported 11.02 bitcoins as a seized asset in a United States Department of Justice seizure notice pursuant to 21 U.S.C. § 881. In Kenya, a project was initiated to link bitcoin payments to the robust infrastructure of M-Pesa, with a view to spurring financial development in the developing world. Meanwhile, Robocoin and Bitcoiniacs together launched the world's first bitcoin Automated Teller Machine (ATM) on 29 October, 2013 in Vancouver, BC, Canada, which allowed clients to sell or purchase bitcoin currency at a downtown coffee shop.

Regulatory responses to bitcoin (see also Chohan 2017e) began to significantly diverge in 2013. In Thailand, Foreign Exchange Administration and Policy Department de-legitimized bitcoin by stating that would be illegal given that it lacked any legal framework. Meanwhile, Federal Judge Amos Mazzant of the Eastern District of Texas of the Fifth Circuit ruled that bitcoins are "a currency or a form of money" as defined by Federal Securities Laws, and as such were subject to the court's jurisdiction. At the same time, Germany's Finance Ministry subsumed bitcoins under the term "unit of account"—a financial instrument—though not as e-money or a functional currency, a classification nonetheless having legal and tax implications. In October 2013, the FBI seized roughly 26,000 bitcoins during the arrest of Ross William Ulbricht, owner of the website ***Silk Road***.

China became the largest point of exchange for bitcoins in 2013, when BTC China overtook the Japanese Mt. Gox and the European Bitstamp to become the largest exchange by volume. However, the monetary authority People’s Bank of China prohibited Chinese financial institutions from using bitcoins in December 2013, leading to a drop in the instrument’s value.

An even larger assortment of businesses began to accept bitcoin in 2014, including Zynga, D Las Vegas Casinos, Golden Gate Hotel & Casino, TigerDirect, Overstock.com, Newegg, Dell, and

Microsoft. Furthermore, Bitcoin based derivative products emerged in 2014, when TeraExchange received approval from the U.S.Commodity Futures Trading Commission to begin listing an over-the-counter swap product whose underlying asset was the price of a bitcoin.A clearinghouse crisis emerged when Japanese Mt. Gox reported the theft of 744,000 bitcoins and filed for bankruptcy, following months of reported user-difficulties. Another hack occurred the following year at the British exchange Bitstamp, which reported 19,000 bitcoins stolen from their hot wallet ($5 million USD at the time). Unlike Mt Gox, Bitstamp continued trading after a minor interval.

By 2015, the number of merchants worldwide had swollen to an estimated 160,000 merchants. Digital currency-related companies continued to draw funder attention from mainstream markets, as when ***21 Inc*** raised $116 million (USD) in venture-capital funding.

Global expansion of bitcoin-related transactions continued an inexorable rise in 2016. By September, 2016 there were 771 ATMs worldwide servicing bitcoins. In March 2016, the Cabinet of Japan recognized virtual currencies like bitcoin as having a function similar to real money. The largest South African online marketplace, Bidorbuy launched bitcoin payments for both buyers and sellers. In Argentina, Uber switched to bitcoin after the government preempted credit card companies from transacting with Uber. In terms of hacks, major clearinghouse Bitfinex reported 120,000 bitcoins stolen, equivalent to $60 million (USD) at the time. Typical of the lag-time of academia in responding to practitioner phenomena, it was only in 2016 that the first cryptocurrency-related journal, ***Ledger,*** was launched.

In 2017, the momentum of the bitcoin has remained sustained, and now occupies niches heretofore unexplored, including business-to-business (B2B) supply chains, ticketing and transport services, consumer services, value storage, derivative products, hedging mechanisms, and more.

More countries are also legalizing bitcoin as a form of payment (see also discussion in Chohan 2017e). Japan passed a law in 2017 to accept bitcoin as a legal payment method. Russia announced that it would legalize the use of cryptocurrencies such as bitcoin. Norway's largest online bank, Skandiabanken, is integrating bitcoin accounts.

The value of bitcoin, meanwhile has continued to soar, albeit with sharp volatility (see also Chohan 2017d, 2017e). On 20 May 2017, the price of one bitcoin passed US$2,000 for the first time, rising to $3000 on 5 August, and then to $4000 on 12 August. Bitcoin has split into two trading instruments as well: bitcoin classic (BTC) and bitcoin cash (BCH).

Conclusion

Bitcoin has thus far exemplified the ***rise-and-rise*** archetype of inexorable growth, and this leads to the consideration of several thematic points. First, the monetary value of bitcoin continues to rise, as it serves an increasing array of purposes and is recognized by an increasing number of businesses and services. Second, legislation and legality is trending more favorable towards the legitimization of bitcoin (see also 2017e). Third, despite hacks of theft, the general amount of bitcoins has been able to grow without significant disruption. Third, bitcoin is enetering a phase of higher substitutability with traditional currencies, as remarked by the increasing number of bitcoin related products (direct or derivative), and the volume of exchange that is occurring. Fourth, there is a growth in the number of alternative currencies, as well as in blockchain based solutions for other technical and social problems, bolstered by the preeminence of bitcoin. In sum, the prognostications of bitcoin point towards the favorable, and future academic research (see also discussion sin Chohan 2017d, 2017e) can pave the way for a much richer exploration of the issues surrounding bitcoin as it edges closer to a phase of maturation.

References

1. Ametrano, F. M. (2016). Hayek money: The cryptocurrency price stability solution.
2. Brenig, C., Accorsi, R., & Müller, G. (2015, May). Economic Analysis of Cryptocurrency Backed Money Laundering. In ***ECIS***.
3. Cheung, A., Roca, E., & Su, J. J. (2015). Crypto-currency bubbles: an application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices. ***Applied Economics***, ***47***(23), 2348-2358.
4. Chohan, U.W. (2017a). Independent Budget Offices and the Politics-Administration Dichotomy. ***International Journal of Public Administration***. http://dx.doi.org/10.1080/01900692.2017.1317801
5. Chohan, U.W. (2017b). "Legislative Oversight of the Bureaucracy". In Farazmand, A. (ed.). ***Global Encyclopedia of Public Administration, Public Policy, and Governance.*** https://link.springer.com/referenceworkentry/10.1007/978-3-319-31816-5_698-1
6. Chohan, U.W. (2017c). "Budget Offices". In Farazmand, A. (ed.). ***Global Encyclopedia of Public Administration, Public Policy, and Governance.***
7. https://link.springer.com/referenceworkentry/10.1007/978-3-319-31816-5_338-1
8. Chohan, U.W. (2017d). Cryptocurrencies: A Brief Thematic Review. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3024330
9. Chohan, U.W. (2017e).Assessing the Differences in Bitcoin & Other Cryptocurrency Legality Across National Jurisdictions. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3042248
10. Cocco, L., Concas, G., & Marchesi, M. (2017). Using an artificial financial market for studying a cryptocurrency market. ***Journal of Economic Interaction and Coordination***, 1-21.
11. Darlington III, J. K. (2014). The Future of Bitcoin: Mapping the Global Adoption of World's Largest Cryptocurrency Through Benefit Analysis.
12. Davis, J. (2011). The crypto-currency. ***New Yorker***, ***87***(31), 62-70.
13. Farell, R. (2015). An analysis of the cryptocurrency industry.
14. Gjermundrød, H., & Dionysiou, I. (2014, May). Recirculating Lost Coins in Cryptocurrency Systems. In ***International Conference on Business Information Systems*** (pp. 229-240). Springer, Cham.
15. Graeber, D. (2011). ***Debt: The First 5000 Years.*** Melville House: London.;

16. Greenberg, A. (2011). Cryptocurrency: Money you can't trace. ***Forbes***, 40.

17. Harwick, C. (2015). Cryptocurrency and the Problem of Intermediation. SSRN.

18. Houy, N. (2014). It Will Cost You Nothing to'Kill'a Proof-of-Stake Crypto-Currency. SSRN.

19. Howden, E. (2015). The crypto-currency conundrum: Regulating an uncertain future.

20. Hughes, S. J., & Middlebrook, S. T. (2015). Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries. ***Yale J. on Reg.***, ***32***, 495.

21. Iwamura, M., Kitamura, Y., Matsumoto, T., & Saito, K. (2014a). Can we stabilize the price of a Cryptocurrency?: Understanding the design of Bitcoin and its potential to compete with Central Bank money. SSRN.

22. Iwamura, M., Kitamura, Y., & Matsumoto, T. (2014b). Is Bitcoin the Only Cryptocurrency in the Town? Economics of Cryptocurrency and Friedrich A. Hayek. SSRN.

23. Koning, J. P. (2016). Fedcoin: A Central Bank-issued Cryptocurrency. ***November***, ***15***, 2016.

24. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

25. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). ***Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction***. Princeton University Press.

26. Stapenhurst, Frederick Rick C; Pelizzo, R.; O'Brien, M.; and Chohan, U.W. (2015). ***Public Accounts Committees and Parliamentary Budget Offices.***

27. Vigna, P., & Casey, M. J. (2015). ***Cryptocurrency: How Bitcoin and Cybermoney Are Overturning the World Economic Order.*** Random House.