Democratizing Value through Digital Currencies

Theo Prineas

Tufts University

Mentored by Ming Chow

Abstract

The evolution of computers has advanced the reach of information, increased global production, and expanded collective intelligence. The cascading effect of this liberation has led the revolution in what is created, and how it is disseminated and controlled. The underlying theme is web technology creates value, removes intermediaries and reshapes established traditions. Developments in the evolution of finance are no exception, and the advent of digital currencies is one of the most significant changes facing established, government-backed, and controlled, currencies. Digital currencies were created to decentralize the creation and transfer of money but more importantly, they are medium of exchange. This paper looks into the confluence of existing technologies to create digital currencies that are poised to revolutionize how value is exchanged.

Keywords: digital currency, democratization, value exchange

Democratizing Value through Digital Currencies

The egalitarian principles that were built into the World Wide Web and the Internet have helped to revolutionize the world. Anyone with a computer and an internet connection can create content for the world to see (democratization of publishing); creators can affordably turn digital designs into tangible prototypes through 3D printing (democratization of manufacturing and production); recording artists can choose to become their own record label without ceding creative control or revenue to major labels with products like TuneCore (democratization of music). In the finance industry, the Internet allows for faster access to money through the established, heavily mediated system. However, developments in Peer-to-Peer (P2P) communication, cryptography and data storage have the potential to revolutionize finance through the creation of digital currencies like Bitcoin (the first and leading crypto-currency), Ripple and a slew of imitations and variations. At the core of this revolution is the block-chain protocol, the distributed, open source processing engine that records and verifies transactions, powering digital and cryptographic currencies (referred to hereafter as "crypto-currency"). Block-chain technology is "a protocol through which any titled asset can be transferred," (Macheel, 2014).

To the Community

The importance of the development of crypto-currencies and block-chain technology cannot be ignored. Using Bitcoin offers powerful protection and control over the privacy of financial transactions. Bitcoin does not attach identity to transactions (e.g. login details, name, banking details, etc.) instead it withholds sensitive account identifiers that are found in typical banking transactions. Bitcoin financial services are not vulnerable to central points of failure unlike existing banking models (think the loss of credit card information by Target, Sony PSN,

and eBay), and as such, centralized oversight and regulation is not yet required. This may change once the technology matures and is adopted by more people and industries. Powering Bitcoin is the block-chain, which uses mathematical algorithms to execute transactions. The block-chain is "the only workable, distributed key value store in existence," (Reverend, 2015). Bitcoin is built on the block-chain protocol, and it is regarded as the Internet for money. It is drawing the attention of Wall Street and almost every bank in the world, for the risk it poses to their existing intermediary model, and the potential is offers to improve their model. By way of example, Bank of America has already filed 10 patent applications related to the block-chain.

Democratization of Money

The current, established global banking system relies on centralized, trusted intermediaries to keep an accurate ledger of the movement of assets, typically imposing restrictions and charging fees along the way. Structurally different to traditional banking, crypto-currencies do not depend on existing payment systems or interactions with intermediaries and central banks. Investopedia.com describes crypto-currency as,

> *transferred directly from person to person, without going through an intermediary or clearing house, meaning the fees are much lower, they can be used almost in every country (where governments allow), a user's account cannot be frozen (e.g. PayPal), and there are no prerequisites or arbitrary limits.*

The innovation with crypto-currencies lies with decentralizing the ledger. To ensure accuracy, crypto-currencies distribute copies of the ledger to every user across the computer network. The trust in the accuracy of the ledger lies not with one central entity but with every node in the network. Providing the encryption is robust, the network and the transactions are secure and partially anonymous. The key motivation for the creation of crypto-currencies is financial

freedom. Considering "money" no longer refers solely to paper and coins but rather as database entries stored on a bank's central computer, crypto-currencies are decentralized, low-cost, low latency mediums of exchange to which value is stored and regulated by the users of the medium through P2P networks.

Since modern day financial assets, like money, are merely digital records, there are numerous other applications to which that this technology can be applied across all industries, highlighting its great potential. This concept is rousing interest in numerous industry leaders. Recently, the Linux Foundation announced it is working to develop block-chain technology with a number of technology and finance companies such as IBM, Intel, J.P. Morgan, London Stock Exchange Group and Wells Fargo to name a few. Microsoft announced it will add block-chain software services to its Azure platform, all of ING's businesses are exploring the integration of block-chain, the Philippine Government is seeking to create a government-backed digital currency based on Bitcoin technology (although Canada tried this with their MintChip offering and failed), Andreesen Horowitz, Google Ventures and a stream of other Silicon Valley investors are actively building stakes in virtual currency start-ups. In summary, crypto-currencies and the underlying block-chain technologies are big news.

However, other than reducing cost and latency in financial transactions in the developed world, it also has the potential to grant banking capabilities to every person with a mobile telephone anywhere in the world. For the majority of the "unbanked" and "under-banked" global population, those that do not have a bank account or limited access to banking facilities respectively, digital crypto-currencies can instantaneously provide them with the means to join the global marketplace. Essentially, they can become their own bank. The impact that block-chain technology has on every asset class is immensely disruptive. A Wired.com article

described block-chain as the "like watching the birth of the internet all over again," (Bheemaiah, 2015).

The Problems Facing Crypto-Currencies

Security vulnerabilities are the main concerns hindering the adoption of Bitcoin. Principle among these is the theft of the virtual wallet that contains Bitcoins. For the last few years, news headlines have reported the theft of millions of dollars' worth of Bitcoins. The majority of the thefts were at the hands of cyber criminals who executed a Distributed Denial of Service, cracking their way through the security protocols of online commercial Bitcoin wallet providers and payment processors. Others were through user error; one unlucky Bitcoin holder threw away a hard drive containing USD 7.5 Million of Bitcoin. Despite these headlines appearing infrequently, and the impacts affecting a small minority of early Bitcoin adopters, it is still enough to instill distrust in the unproven technology.

It is possible to trace a coin's history, and in turn a user's identity, if any identifiable information is attached to an address (a destination for a Bitcoin payment). According to bitcoin.it, a public resource for the Bitcoin community, any past or future address can be tied to an actual identity, making it might be possible to guess who may own all of the other addresses. The identity might come from network analysis, surveillance, Sybil attack, packet sniffing, Denial-of-Service attack, or even from a search engine. To reduce the risk of exposure, Bitcoin encourages using a new address for every transaction e.g. creating new virtual wallets to store and trade Bitcoins.

The Bitcoin market is volatile. Yet despite its increasing acceptance by merchants on/off line around the world, it suffers from short-term price fluctuations, due to the illiquid and immature market. Due to the instability of the currency, the current Bitcoin market is a high-risk

investment, and the currency cannot be used as a stable unit of account like other, legal currencies can, like the US dollar. Retaining savings in the currency, especially in a virtual wallet is not recommended. At its peak in Q4 2013, the value of one Bitcoin was trading at around USD 1,147.25, falling to around USD 177.28 in Q1 2014. At time of writing, they are now at USD 435.34, so speculators that wish to profit from arbitrage are faced with limited opportunities and they will have to wait sometime before prices rise. However, this may happen sooner than the last few years, as the currency grows in popularity. In the meantime, Bitcoins are still highly-speculative and should be converted to local currency to minimize loss in value, or saved in cold storage (offline) to minimize theft of the Bitcoins from insecure wallets. In essence, Bitcoin should be treated like any other wallet and currency in that it should be protected. In addition, Bitcoin payments are irreversible, so should a fraudulent transaction occur, there is no recourse for the victim unless the network can prove that fraud has occurred. In that case, the network cancels the transaction and removes it from the block-chain as if it never existed.

Lastly, government taxes and regulations will impact upon Bitcoin and other crypto-currencies as they try to regulate the technology. Unlike fiat currencies, crypto-currencies are not backed by regulation or law. Therefore, there is no recourse for Bitcoins stolen through security cracking or loss of any other kind. There is no insurance against fraud, and once the Bitcoins are stolen, because of their anonymity, they cannot be traced. Despite Bitcoin not (yet) being recognized as an official currency, there is interest in, and perhaps fear of, its development, by international governments. Bitcoin uses SHA256 to encrypt its Proof-of-Work (PoW) system and for transaction verification. So far this has remained un-cracked, but international governments fear terrorists will migrate to crypto-currencies to hide their nefarious activities,

ergo policy makers may be threatened by the technology and they will no doubt seek ways to control it, in the interest of currency stability, taxation, fraud prevention, and money laundering – the closure of Silk Road and Mt. Gox highlight this, drawing the ire of the Senate Committee on Homeland Security and Governmental Affairs, the Senate banking committee, along with policy makers and governors from reserve banks across the world. For example, the Bank of England's Chief Economist admits that "block-chain-based crypto-currencies issued by Central Banks could replace cash." However, this flies in the face of the decentralized model.

Summary

At its current pace of development, Bitcoin is expected to hit mainstream acceptance in approximately five to ten years. As evidenced by the Open Ledger Project, the growth of crypto-currencies and variations of block-chains is drawing the attention of large technology providers, and they start to formulate and incorporate the new technology into their frameworks. The block-chain consortium, R3 CEV, already has 42 banks interested in experimenting and developing block-chain standards, with the aim of building new financial technology platforms. Once corporations and consumers join en masse, the leading crypto-currencies will have refined their products, addressing any shortcomings and creating more opportunities. These new transaction technologies will evolve in parallel with the online and offline world, and businesses and governments will adopt each one to suit their needs.

References

Ali, R. (2014). Digital currencies: how do they work and what makes them different? Retrieved from http://www.bankofengland.co.uk/banknotes/Pages/digitalcurrencies/default.aspx

Aziz, J. (2013). Bitcoin would benefit from being boring. Retrieved from https://theweek.com/articles/456710/bitcoin-benefit-from-being-boring

Bheemaiah, K. (2015). Block Chain 2.0: The Renaissance of Money. Grenoble Ecole De Management. Retrieved from http://www.wired.com/insights/2015/01/block-chain-2-0/

Bitcoin Wiki. (2015). Weaknesses. Retrieved from https://en.bitcoin.it/wiki/Weaknesses

Cheb, C. (2014). Philippines' "E-Peso" Digital Currency Will Try to Use Bitcoin Technology. Retrieved from https://www.cryptocoinsnews.com/philippines-e-peso-digital-currency-use-bitcoin-technology/

Cuomo, J. (2015). The Force <of Blockchain> Awakens. Retrieved from https://www.ibm.com/developerworks/community/blogs/gcuomo/entry/The_Force_of_Blockchain_Awakens?lang=en

De Filippi, P. (2014). Tomorrow's Apps Will Come from Brilliant (And Risky) Bitcoin Code. Retrieved from http://www.wired.com/2014/03/decentralized-applications-built-bitcoin-great-except-whos-responsible-outcomes/

dree12. (2012). List of Bitcoin Heists. Bitcoin Forum. Retrieved from https://bitcointalk.org/index.php?topic=83794.0

Higginbotham, S. (2015). IBM, J.P. Morgan, and Others Build a New Blockchain For Business. Retrieved from http://fortune.com/2015/12/17/ibm-blockchain-for-business/

Higgins, S. (2015). ING Exec: ‘All Our Business Lines’ Involved in Blockchain Exploration. Retrieved from http://www.coindesk.com/ing-all-our-business-lines-involved-in-blockchain-exploration/

Higgins, S. (2015). Microsoft Adds New Blockchain Services to Software Sandbox. Retrieved from http://www.coindesk.com/microsoft-azure-announces-new-offerings-for-blockchain-as-a-service-platform/

Investopedia. (2012). The Future Of Cryptocurrency. Retrieved from http://www.investopedia.com/articles/forex/091013/future-crypto-currency.asp

Macheel, T. (2014). Andreessen Horowitz Leads Bitcoin Startup TradeBlock's $2.8 Million Funding. Retrieved from http://www.coindesk.com/andreessen-horowitz-2-8-million-funding-tradeblock/

Mcmillan, R., Metz, C. (2013). The Rise and Fall of the World’s Largest Bitcoin Exchange. Retrieved from http://www.wired.com/2013/11/mtgox/all/

Metz, C. (2015). Tech and Banking Giants Ditch Bitcoin for Their Own Blockchain. Retrieved from http://www.wired.com/2015/12/big-tech-joins-big-banks-to-create-alternative-to-bitcoins-blockchain/

Patron, T. (2015). Bitcoin Violates the Principle of Fungibility (Op-Ed). Retrieved from http://cointelegraph.com/news/113897/bitcoin-violates-the-principle-of-fungibility

Popper, N. (2013). $25 Million in Financing for Coinbase. Retrieved from http://dealbook.nytimes.com/2013/12/12/venture-capital-bets-big-on-bitcoin/?_r=0

Price, J. (2008). The Democratization of the Music Industry. Retrieved from http://www.huffingtonpost.com/jeff-price/the-democratization-of-th_b_93065.html

Pyro-E. (2013). Democratizing Energy Generation. Retrieved from https://medium.com/@luey02/democratizing-energy-generation-75fca3ec1288#.1eb27j74t

Reverend, (2015). Block-chain: The Only Workable, Distributed Key Value Store in Existence. Retrieved December 7, 2015, from http://bavatuesdays.com/block-chain-the-only-workable-distributed-key-value-store-in-existence/

Rizzo, P. (2014). Philippine Government Bill Could Pave Way for Bitcoin-Backed Money. Retrieved from http://www.coindesk.com/philippines-government-consider-bitcoin-e-peso/

Rizzo, P. (2015). IBM Creates Open-Source Blockchain With Linux and Big Banks. Retrieved from http://www.coindesk.com/ibm-launches-open-source-blockchain-project-backed-by-linux-and-big-banks/

Robinson, A. (2014). The Democratization of Manufacturing and the Roles of Its Citizens. Retrieved from http://cerasis.com/2014/06/02/democratization-of-manufacturing/

The Economist. (2015). Bitcoin - Much more than digital cash. Retrieved from http://www.economist.com/news/business-books-quarterly/21638093-rise-and-fall-crypto-currency-good-news-authors-least-much

Warren, C. (2012). Bitcoin: How the Internet Created Its Own Currency. Retrieved from http://mashable.com/2012/11/05/bitcoin-currency/#_bBZWG04faq4

Weisser, W. (2013). Why Security Issues May Chronically Hinder Bitcoin Adoption. Retrieved from http://www.tripwire.com/state-of-security/security-data-protection/security-issues-may-chronically-hinder-bitcoin-adoption/