CRYPTO-CURRENCIES
Intellectual Curiosity or the Future of Finance?
CRYPTO-CURRENCIES

Intellectual Curiosity or the Future of Finance?

What Are Crypto-Currencies?

Crypto-currencies are innovative virtual payments systems that do not rely on a central authority to generate currency supply, or to verify, track, and record transactions. They most closely resemble a fiat currency that is not backed by a Central Bank and that has a fixed, predefined rate of money supply growth. Crypto-currencies are so called because cryptographic techniques (the use of hash functions to create digital signatures) lie at the heart of their implementation.

Bitcoin is the best-known crypto-currency. Introduced in early 2009, it has since attracted a lot of public and regulatory attention. With a market capitalization of approximately $4.5 billion, Bitcoin dwarfs the 300 or so other crypto-currencies in existence, many of which are based on Bitcoin’s open-source code.

How Does Bitcoin Work?

The Bitcoin protocol comprises a widely distributed digital ledger (known as the blockchain, or more generally, crypto-ledger) of the transaction history of the entire bitcoin money supply. Unlike cash, the entire transactions history of each bitcoin\(^1\) can be traced to its initial release into the money supply. Cryptographic techniques combine with this distributed ledger to allow Bitcoin to satisfy two critical functions of any medium of exchange: proof of ownership and proof that the funds have not been double-spent. Proof of ownership is established by a digital signature based on a cryptographic combination of a public alphanumeric key, which can be thought of as an account number, and a private alphanumeric signing key, which can be thought of as a password\(^2\). This digital signature allows certain participants in the Bitcoin system, called miners or nodes\(^3\), to search for the transactions history of the user in the blockchain and verify that the payer does indeed own the funds being transferred.

To ensure funds are not being double-spent, transactions are not considered complete until they appear in the blockchain master ledger. Transactions are appended to the master ledger in blocks (hence blockchain) approximately every 10 minutes. Typically, six or more nodes must all confirm a given block of transactions before the ecosystem accepts verification and moves onto the next block of transactions\(^4\). The node that verified the block first is rewarded with newly created bitcoins, which is how bitcoins are added to the money supply. This node also collects any transaction fees volunteered by the two sides of each transaction. The reward to mining is halved approximately every four years so there is a predefined

---

\(^1\) The convention is to use upper-case Bitcoin when referring to the protocol itself, and lower-case bitcoin to refer to the currency unit.

\(^2\) The cryptographic elements in Bitcoin are hash functions, which convert any input into a fixed-length alphanumeric key. The public and private keys are entered into this hash function to produce the digital signature, which cannot be reverse-engineered due to the unidirectional nature of hash functions. It is important to note that there is no central record of the private key, so if it is lost or stolen users have no ability to retrieve the password and no recourse to reclaim stolen funds.

\(^3\) Any user can be a miner; the only hurdle is the willingness of the user to devote computing resources to the task.

\(^4\) An alternative view is that bitcoins are like land in that they do not circulate but merely change ownership. Bitcoin mining is then simply verification of the true owner of any given parcel of land and the processing of any change of ownership.
limit to the creation of bitcoins with no more than 21 million bitcoins ever to be created. The final bitcoin is expected to be created around the year 2140.

The process of updating the ledger and receiving the reward of new bitcoins is made purposefully challenging and is known as “proof-of-work”. This difficulty serves two purposes: it limits the extent of bitcoin creation (controlling the money supply), and it supports the integrity of the currency (minimizing fraud and misconduct) by making it difficult, if not impossible, for a node to append and maintain fraudulent transactions in the blockchain.

The oft-quoted “cryptographic puzzle” underlying block verification distils into a trial-and-error exercise of brute computing power. Specifically, successive prime numbers are input into a hash function until a specified, desired output is obtained. The difficulty of the problem is calibrated by the Bitcoin protocol to make the rate of block updating, and hence money supply creation, relatively constant (one update every 10 minutes) in the face of growing computing power. By construction it is almost impossible for one fraudulent node to corrupt the blockchain since it would need more computing power than a combination of the majority of the other nodes (known as the 51% attack), which is considered impossible for all practical purposes.

Once all bitcoins have been created, transactions fees will likely rise since they will be the only incentive for block verification. The issue of a suitable return for miners to continue participating is critical. Already, mining is not profitable for all but the largest mining conglomerates with estimates suggesting upwards of $1 billion has been invested in specialised mining computers.

Specifically, miners must take the existing blockchain and the proposed block of transactions and input them into a hash function to yield an alphanumeric expression. They must then add an unknown number, known as the nonce, and input the concatenation into the hash function again. The output of this hash must have a predetermined number of leading zeroes. By the unidirectional nature of the hash function, the only known solution is to try successive prime numbers as the nonce. The difficulty of this problem is calibrated by requiring fewer or greater leading zeroes in the output of the hash function.

The computing power arms race has gone through several steps with the latest being the transition to so-called Application Specific Integrated Circuits (ASICs), which are extremely capital intensive. Their use is expected to cause the protocol to dramatically increase the difficulty of the hash challenge to maintain the 10-minute update time and therefore drive smaller miners out of business since their equipment will be too slow to mine enough bitcoins to cover electricity costs. The issue of electricity costs has driven other groups to develop alternative crypto-currencies where the creation of the money supply is detached from the verification of transactions in order to have a more energy-efficient crypto-currency.

Clearly, if mining nodes representing 51% of the computing power collude they could mount a 51% attack. Due to significant and increasing capital costs of bitcoin mining, mining pools currently make up the majority of successful block updates. The largest are Discus Fish and GHash.io with approximately 26% and 23% of the hash rate respectively, with GHash.io having peaked at more than 50%. However, mining pools have so far cooperated quite openly to avoid the 51% attack problem.
Altcoins: Variations on Bitcoin

There are a number of other crypto-currencies, collectively referred to as altcoins (alternative coins), many of which are derivatives of the Bitcoin protocol. Variations include the use of different hash functions and different block-updating times, as well as conceptual differences such as an unlimited money supply and alternatives to the proof-of-work protocol. To put these altcoins into perspective, the second-largest crypto-currency, Ripple, has a market capitalization of approximately $140 million followed by Litecoin with a market capitalization of approximately $125 million.

Using Bitcoins: e-Wallets and Exchanges

Two services necessary for accessing the Bitcoin ecosystem are the e-wallet and bitcoin exchanges. An e-wallet does not actually contain or record bitcoins themselves, which only exist on the master blockchain; rather an e-wallet is a mechanism for storing the public and private keys. Several kinds of e-wallets exist: software wallets, Web wallets (allowing access from any device connected to the Internet), cold wallets (e.g. paper record, USB drive), brain wallet (software converts the keys into easily remembered pass phrases that the user commits to memory) and hardware wallets (e.g., Quick Response, or QR, codes recorded on paper).

In turn, a bitcoin exchange facilitates conversion of bitcoins into fiat currencies or other crypto-currencies and vice versa. Popular examples include Kraken, HitBTC, Bitstamp and BTC China, as well as the infamous Mt. Gox. A bitcoin exchange account requires a linked bank account and typically allows unrestricted trading (i.e. no daily limits) only once proof of address and ID documents are provided. Bitcoin exchanges charge trading, deposit and withdrawal fees to earn revenue. As of September 2014, Bitstamp is the largest exchange by volume with 34% market share and a volume of $142 million per day.

Security Issues: Silk Road Collapse and Mt. Gox Theft

While the Bitcoin protocol itself is considered to be very secure by design, the exchanges and e-wallets give greater scope for fraud. The most recent and serious case occurred on a Japanese bitcoin exchange, Mt. Gox, which was at the time the dominant trading venue for bitcoins, accounting for up to 80% of all bitcoin trades. On 7 February 2014, after a year-long period of seemingly unrelated legal disputes and operational problems, Mt. Gox ceased bitcoin withdrawals. On 24 February 2014, Mt. Gox ceased trading entirely after rumors from a leaked internal document suggested that 850,000 bitcoins, worth more than $470 million and amounting to 7% of the bitcoin money supply at the time, had been stolen or lost from active and cold storage accounts. On 28 February 2014, Mt. Gox filed for bankruptcy protection in Tokyo, confirming the loss of approximately 750,000 customer bitcoins along with 100,000 of Mt. Gox reserves. To date, 200,000 bitcoins have been rediscovered.

---

9 Litecoin, for example, focuses on reducing the time taken to update blocks. Having unconfirmed transactions for 10 minutes or so is problematic for retailers and may limit the attractiveness of bitcoins in retail applications. Litecoin also uses a verification puzzle that cannot be solved using custom mining chips like ASICs, which should allow a much wider base of mining nodes to exist relative to Bitcoin making the Litecoin system theoretically more robust.

10 The Mt. Gox incident has resulted in the creation of a new verb: to be “Goxxed”.
It is believed that the vulnerability that made this theft possible was due to the interaction between the Mt. Gox e-wallet software and the Bitcoin protocol. Specifically, it was possible for a user to use the Bitcoin network to make it appear that a transfer to a bitcoin wallet did not occur when in fact it did. The failed transaction could then result in the bitcoins being sent again. On 16 April 2014, Mt. Gox filed for liquidation in a Tokyo court and as of July 2014 proceedings and negotiations with creditors were continuing. Since Mt. Gox, there have been several thefts from e-wallets and exchanges meaning security concerns are still a hurdle for mainstream users.

Early adopters of Bitcoin gained notoriety in the public consciousness for two reasons. First, the anonymity afforded by using bitcoins as a medium of exchange facilitated completely untraceable transactions on websites such as Silk Road, which was a popular early marketplace for Bitcoin users that offered for sale (amongst other things) illicit substances and services and was shut down by US authorities in October 2013\(^\text{11}\). Second, Bitcoin’s lack of a centralized authority, its fixed rate of money growth as well as the upper limit on the total number of bitcoins in circulation attracted users with a fear of governments debasing fiat currencies (money printing or seignorage). In summary, the early adopters tended to have political persuasions deriving from some combination of anarcho-capitalism and libertarianism\(^\text{12}\). As Bitcoin becomes better known, ancillary services are being created to cater to and attract mainstream users that are more interested in bitcoins for retail purchases or as an investment class. Already, several major corporations such as Dell, eBay, Expedia.com and Tesla Motors accept payment in bitcoins. Payment platforms, such as BitPay and Coinbase have been developed to make it easier for merchants to accept bitcoins as payment.

**Bitcoin and Banks: Friend or Foe?**

The financial services industry is potentially threatened by Bitcoin since it could make money transfers cheaper with far lower cross-border fees. In early 2014, Goldman Sachs estimated that using the Bitcoin system for all electronic payments could save around $150 billion in point-of-sale fees and $12 billion in e-commerce fees per annum. Remittances could also be a large market with current fees averaging around 9% and making Bitcoin an attractive alternative. Goldman Sachs also suggested that payment services providers will need to adapt or co-opt the Bitcoin system to compete. The major player in this market, Western Union, has so far been unwilling to use Bitcoin since it is not typically considered a currency. In contrast, PayPal announced in September 2014 that it would embrace Bitcoin as part of its payments systems.

A major challenge facing Bitcoin is that even when merchants choose to accept payments, it is difficult for them to convert bitcoins into fiat currencies or store them in deposit accounts. This is due to the reluctance of banks to create bitcoin-denominated products. However, Coinbase has recently announced

\(^\text{11}\) The Silk Road is one of the more well-known examples of the “Deep Web,” an area of the Internet accessed via software such as The Onion Router (TOR) that enables the anonymisation of user IP addresses.

\(^\text{12}\) There is some informal empirical evidence to this effect with some voluntary and anonymous user surveys reinforcing a priori stereotypes. Specifically, 95% of users identified as males in their late 20s with 44% describing themselves as anarcho-capitalists while 38% were liberals or environmentalists. However, in contrast to the perception created by Silk Road, only 10% of responders to the anonymous survey had used bitcoins to purchase illegal substances.
an alliance with an unnamed European bank\textsuperscript{13} connected to SEPA\textsuperscript{14}, the euro payments clearing system, to link its Bitcoin wallet to mainstream financial infrastructure. This is considered a key step in bringing Bitcoin into the commercial mainstream.

Banks are also working on creating their own virtual currencies and payments systems. While the currency aspect of distributed ledgers is not yet obviously attractive to banks, the settlement possibilities are more valuable. JPMorgan has been attempting to patent its own crypto-currency payments system for low-dollar, high-volume transactions. In Russia, Sberbank has announced the development of its own virtual currency in association with the Internet company Yandex. Since the original announcement, it has also been promoted as a potential way for Russia to lessen its exposure to any future sanctions on its financial sector, in particular possible restrictions on its access to the SWIFT network. In September 2014 this process took a step forward when two American banks — CBW Bank and Cross River Bank — joined the German-based Fidor Bank in adopting the distributed transaction infrastructure from Ripple Labs to facilitate international transactions.

One recurring question is whether crypto-currencies should be considered as currency or assets for regulatory and taxation purposes. In most instances where such a conversation has happened, the taxation authorities have decided to treat crypto-currencies as assets for capital gains tax purposes. David Yermack from New York University outlines three arguments against considering crypto-currencies as currency, which refer to the three traditional uses of money. First, the high price volatility of crypto-currencies means they do not represent a good store of value. Second, they are not useful as a medium of exchange since the number of merchants accepting bitcoins is still very small and almost zero for other coins. Finally, a bitcoin is not ideal as a unit of account since the price of one unit is very high at around $400, so day-to-day transactions involve decimal figures. However, the crypto-currency community is lobbying for recognition as a currency with bills promoting this change having been sponsored in Texas and California at the time of writing.

A development that may alleviate the issue around price volatility and further bring Bitcoin into the mainstream is the mooted creation of Bitcoin Exchange Traded Funds (ETFs). To date, Bitcoin Investment Trust (BIT) is one of the few ETFs in existence, although it is an exclusive fund open only to accredited investors to avoid SEC scrutiny. The more inclusive Winklevoss Bitcoin Trust, to be listed on NASDAQ, is currently being examined by the SEC, although this too will only be open to relatively wealthy investors. However, the owners of BIT, SecondMarket, are attempting to convert BIT into a publicly traded Bitcoin fund.

Ban, Tax, Regulate, Wait: Bitcoin Regulatory Developments

The increasing popularity of Bitcoin with retail users and the collapse of Mt. Gox brought worldwide attention to Bitcoin, including from regulators. To date, most countries have taken a policy stance only in respect to the taxation of Bitcoin-related activity. The US, UK, Bulgaria, Brazil, Finland and Norway treat Bitcoin as property and levy capital gains taxes on Bitcoin transactions. Germany classifies Bitcoin as a

\textsuperscript{13} The bank has not been identified to keep Coinbase competitors in the dark on which bank is willing to work with Bitcoin transactions.

\textsuperscript{14} Single Euro Payments Area
unit of account for the purposes of taxation, similar to private money. Canada and Singapore treat Bitcoin transactions in a similar manner to barter transactions. Some countries have banned the use of bitcoins, including Bolivia, Ecuador and Iceland. The use of Bitcoin is restricted, if not explicitly banned, in mainland China, Taiwan, India, Indonesia, Jordan and Lebanon.

Other regulations of the crypto-currency economy have not been finalized but are projected to focus on restricting its ability to be used by money launderers. For example, in July 2014, the European Banking Authority (EBA) published its opinion on crypto-currencies, which advises financial institutions to avoid interacting with crypto-currencies until a body of regulation is developed. The report does not go into detail but argues for the creation of scheme governing authorities that would be accountable for each crypto-currency. In the United States, it is unclear which government agency has jurisdiction over crypto-currencies. Since the SEC has not recognized Bitcoin as a security, it does not appear to have any jurisdiction. Janet Yellen, Federal Reserve chair, has stated that the Federal Reserve does not have authority. Interestingly, the Commodities Futures Trading Commission (CFTC) has argued that Bitcoins could come under its jurisdiction as being a commodity for future delivery. Some commentators have argued that regulation will most likely come from state regulators.

The New York Department of Financial Services has been particularly proactive on Bitcoin regulation and put forward the World’s first, concrete regulatory proposals on 17 July 2014. These introduce the concept of a BitLicence that will be necessary to operate a crypto-currency business (a broad umbrella) in the state of New York or with any person or company related in some way to the state of New York. Each Licensee will have a responsibility to ensure the existence of effective cyber security programs to help prevent assaults on the infrastructure of the company and, most importantly, any customer funds held within this infrastructure. Emergency response plans to a crisis are also required to avoid the kind of chaos that accompanied the Mt. Gox bankruptcy. There will also be annual reporting requirements outlining these security policies and evaluating their success and fitness for purpose. Internal auditing in the form of penetration testing is also required at least once a year to help determine weak points in a firm’s security infrastructure. To this end, each crypto-currency firm will need to have a mandated Chief Information Security Officer on staff. Moreover, a BitLicence holder will also be required to maintain 10-year audit trails including the names and physical addresses of all parties to every transaction. Capital requirements are also proposed, although there is no indication yet as to their size.

Many in the bitcoin community are cautiously welcoming regulations as a sign that crypto-currencies are maturing, becoming respectable and attractive to mainstream users and therefore ripe for growth. However, the proposed regulations have been derived from those used to regulate existing payments industries, which is problematic for a crypto-currency business. Since the physical address and ID requirements will hold for both sides of a transaction, the privacy of the overall network will be diluted. As

---

15 Interestingly, the Internal Revenue Service (IRS) has stated it considers crypto-currencies as property, similar to stocks, which seemingly contradicts the position of the SEC.

16 Bitcoin derivatives markets are more likely to come under the remit of CFTC. The promotion of Bitcoin derivatives markets and their regulation is an important one for the Bitcoin ecosystem as it would help alleviate the volatility concerns by allowing users to hedge exposures. As of early 2014, the largest Bitcoin futures market is ICBIT.se, which was started by two Russians in 2011. The most liquid derivative is a futures contract on the dollar price of Bitcoin.
a result, it is likely that New York-based bitcoins will be increasingly shunned from the network by other users using techniques such as IP address-blocking. If this were to happen, then traders that continue to trade with New York bitcoins would likely only accept them at a discount. Already there are reports that traders are working on arbitrage strategies for these “New York” bitcoins. It is possible that the bitcoin market will experience a phenomenon similar to that of the Argentinian “blue-dollar” exchange rate, which sees the USD trade at a premium to the official Central Bank rate. In this way, the BitLicence-bitcoin exchange rate may end up resembling a quasi-official “New York” exchange rate for bitcoin.

Beyond Bitcoin: Crypto 2.0

The developers of Bitcoin are often criticized for being slow-moving and conservative, which is to be expected since the Bitcoin ecosystem is now too large and too important for experiments. Therefore, a lot of crypto-currency development is occurring outside Bitcoin. This creates another issue for regulators in that the crypto-ledger is rapidly developing into second-generation or “Crypto 2.0” technologies where the Bitcoin protocol is applied to applications other than crypto-currencies. The commonly used terms for these applications are “smart contracts” or “smart property.” A group of developers known as Ethereum calls these technologies the “LEGO building blocks of crypto-finance”. Their particular software would allow users to easily and cheaply create their own crypto-ledger assets. In fact, any application that involves property rights could be traded using the bitcoin crypto-ledger principle (hence “smart contracts”).

To date, the most progress has been made on making crypto-currency exchanges themselves become decentralized. The motivation for the creation of “trustless,” decentralized exchanges has largely been to avoid a repeat of the Mt. Gox crisis. A leading example of this second-generation feature is NXT, which is a crypto-currency ecosystem that has a decentralized exchange. It has been growing rapidly and recently became the sixth largest crypto-currency in circulation with a market cap of approximately $24 million. NXT exchange functionality is open to any type of crypto-currency, including bitcoins.

Moving away from the currency aspect of Bitcoin, “coloured coins” are being developed, which are digital coins that are issued to represent a specific asset such as real estate, art, commodities, shares, bonds, or derivatives. These coins can then be exchanged using the Bitcoin protocol. For example, a portfolio manager could issue coloured coins to represent ownership of a portion of a stock portfolio, which can then trade on a decentralized exchange. These coins would be backed (or “coloured”) by a real position in the same stock portfolio.

---

17 These sorts of price differentials already exist with newly mined “virgin” bitcoins often commanding a premium. During the Mt. Gox crisis, exchange coins traded at a discount.
18 Other innovations include democratizing the mining process by making it unfriendly to the kind of specialized hardware that is causing high capital costs to concentrate mining power in a few mining pool conglomerates.
19 NXT is an example of a crypto-currency that eschews the proof-of-work protocol found in Bitcoin and its derivatives with a proof-of-stake protocol. This works by rewarding users who already have coins in their possession in proportion to their “stake” in the network. It therefore rewards those that hold the most coins and renders the currency immune to 51% attacks. NXT is far less resource-intensive than Bitcoin and in principle could be deployed on smartphones enhancing network stability by further decentralizing the ecosystem.
Another example of the power of this technology is given by Blackcoin, a competitor of NXT. Blackcoin began by focusing on smart contracts that could be used to transact goods and services on a distributed-ledger. In Blackcoin, two parties can enter into a contract where the buyer deposits the funds into an escrow account to be released when both parties agree the contract is fulfilled. To avoid fraud and scams, both sides are required to post a deposit that is lost by both sides if either side considers the contract unfulfilled. This is designed to make contract phishing scams unprofitable.

Both NXT and Blackcoin are converging in terms of their feature set with all second-generation protocols broadly aiming for the creation of a decentralized market for currencies, assets, goods, services, and contracts. In turn, these features are giving rise to a new crop of Decentralized Autonomous Corporations (DACs). Regulating these corporations will likely pose significant challenges to regulators since there may not be an obvious owner that could take on legal responsibility. For example, if a company raises financing by issuing crypto-equity, it may be impossible to impose foreign-ownership limits.

Second-generation protocols and exchanges tend to be open to any crypto-currency so they do not by themselves foreshadow the end of Bitcoin, which can be successfully traded and used in most ecosystems by virtue of its dominant market position. The developers behind Bitcoin say they will wait to see what second-generation functionality succeeds in the market and then simply add it to the Bitcoin protocol.

If one takes the claims of developers and Bitcoin proponents at face value and extrapolates to their logical endpoint, it is possible that the Bitcoin protocol could ultimately lead to the complete decentralization and disintermediation of global property rights. This is certainly what the more idealistic proponents of the technology see in the future. An analogy they often give is the impact that file sharing had on the music industry in the late 1990s and early 2000s. However, as has been the case with the music industry, it is unlikely that the new technology will meet the lofty socio-political goals of its proponents. It is more likely that Bitcoin will force incumbents in the financial industry, including regulators, to adapt the way they do business. What the future will look like is unclear, but it is increasingly less likely to look like the present.