Introduction to Bitcoin

Chapter · December 2015

DOI: 10.1016/B978-0-12-802117-0.00001-1

2 authors, including:

David Lee Kuo Chuen
Stanford University
221 PUBLICATIONS **1,570** CITATIONS

SEE PROFILE

CHAPTER 1

Introduction to Bitcoin

Lam Pak Nian, David LEE Kuo Chuen
Sim Kee Boon Institute for Financial Economics, Singapore Management University, Singapore

Contents

1.1 THE NEXT GENERATION OF MONEY AND PAYMENTS

There are various innovative money payment systems in the market today, many of which are built on platforms like the mobile phone, the Internet, and the digital storage card. These alternative payment systems have seen encouraging or even continued growth, from the likes of PayPal, Apple Pay, Google Wallet, Alipay, Tenpay, Venmo, M-Pesa, BitPay, Moven, BitPesa, PayLah!, Dash, FAST, Transferwise, and others.

Beyond payment systems that are based on fiat currency, the growing use of digital currency allows for faster, more flexible, and more innovative payments and ways in financing goods and services. One digital currency, however, stands out among the rest. Bitcoin is one of the most well-known digital currencies today. To be specific, Bitcoin is a *crypto*currency, which is a subset of what is generally known as a *digital* currency. Bitcoin is a unique cryptocurrency that is widely considered to be the first of its kind. Like many created after it, Bitcoin uses the power of the Internet to process its transactions. This chapter introduces the characteristics and features of Bitcoin and sets the stage for further discussion of cryptocurrencies in the rest of this book.

1.2 DIGITAL CURRENCY AS ALTERNATIVE CURRENCY

1.2.1 "Digital" versus "virtual"

Although *digital* and *virtual* are often used interchangeably when describing currencies based on an electronic medium, the term "virtual" has a negative connotation. "Virtual" signals something that is "seemingly real" but not exactly "real" when referring to a currency that is stored in a "digital" or electronic register. Indeed, in languages like Chinese, the word "virtual" is interpreted as "created from nothing" (虚拟的) in the sense that it is not "physical" but computer-generated or computer-simulated. However, the currencies often described as "virtual" are very "real," in the sense that they exist. Thus, the more neutral term *digital currency* is generally preferred over *virtual currency*.

1.2.2 Classifying alternative currencies

Alternative currencies refer to a medium of exchange other than fiat currency. Historically, there are various types of alternative currencies, as classified by Hileman (2014) broadly into two categories: tangible and digital. Tangible currencies, closely associated with "commodity money," derive their value from relative scarcity and nonmonetary utility:

(a) Currencies with intrinsic utility

This class of currency includes metals and cigarettes in post-WWII Berlin and more contemporary examples are prepaid phone cards and, to some extent, cash value smart cards. This class is not dependent upon governance as in the case of

monetary instruments, and more importantly, its intrinsic value is not an abstraction and it is not necessarily geographically bound.

(b) Token

Seventeenth- to nineteenth-century British tokens and the Great Depression scrip of the 1930s are historical examples. More contemporary examples are local or community currencies such as Brixton Pound and Bristol Pound that are used in England, BerkShares that is circulated in Berkshire region of Massachusetts, and Salt Spring Dollar in Canada. Token has less intrinsic value as its use is more specific and usually bounded by some social contracts or agreement such as honoring them for exchange for goods or to limit the supply of goods.

(c) Centralized digital currency

Examples are loyalty points from financial, telecom, or retail companies; air miles from airlines; Second Life's Linden Dollar and World of Warcraft Gold, which are closed system with transactions within specific entities; and Flooz and Beenz, which are open market system and can be transacted with other entities. Local currencies such as Brixton Pound, BerkShares, and Salt Spring Dollar also fall under this category besides being classified as tokens. The governance structure is centralized.

(d) Distributed and/or decentralized digital currency

This includes the cryptocurrencies such as Bitcoin, Litecoin, and Dogecoin. They can be transacted with any outside agents and the governance is decentralized mainly but not necessary due to open-source software. There is no legal entity responsible for the activities, and therefore, they fall outside traditional regulation.

1.2.3 Why alternative currencies

There are various socioeconomic forces that drive the demand for alternative currencies:

(a) Localism

By promoting community commerce or "save high street," localism retains consumption within a group of independent retailers or within a geographic area for job creation and improved business conditions.

(b) Technology

It has become much easier to use with improved software and low entry barriers contributing to network effects.

(c) Political economy

There is disillusionment about the high pay of CEOs and bankers and the notion of traditional banks being too big to fail. With high debt and quantitative easing, there is great discomfort with the economic uncertainty.

(d) Environmentalism

There are ecology concerns and the question of whether we have reached the point of maximum extraction of natural resources such as oil.

(e) Inefficiencies

Financial services are overpriced and whole financial system is too expensive.

(f) Financial freedom

Some digital currencies such as cryptocurrencies have the advantage of transferring value through the Internet where control is weak. Such digital currencies may allow users to bypass capital controls and may provide safe harbor during a fiat currency crisis.

(g) Speculation

Buyers of some digital currencies such as cryptocurrencies are anticipating a price appreciation due to subsequent wider acceptance.

It is very easy to create a cryptocurrency as an alternative currency for free today. However, most of these new creations will cease circulation within a relatively short time. With many alternative currencies in competition, only a few will be globally adopted, reach a sufficient scale, or find a suitable market. Unless the idea of national digital currencies takes off, it is likely that many of these alternative currencies will cease circulation because of superseding advancements in technology, tighter regulation, and insufficient demand.

1.3 CRYPTOCURRENCY

1.3.1 The nature of cryptocurrency

Cryptocurrency in its purest form is a peer-to-peer version of electronic cash. It allows online payments to be sent directly from one party to another without going through a financial institution. The network time-stamps transactions using cryptographic proof of work. The proof-of-work Bitcoin protocol is basically a contest for decoding and an incentive to reward those who participate. For Bitcoin, first participant to crack the code will be rewarded with the newly created coins. This contest will form a record of the transactions that cannot be changed without redoing the proof of work.

Cryptocurrency is a subset of digital currency. Examples of the many digital currencies are air miles issued by airlines, game tokens for computer games and online casinos, Brixton Pound to be spent only in the Brixton local community in the Greater London area, and many other forms that can be exchanged for virtual and physical objects in a closed system and, in the case of an open system, exchanged for fiat currency.

1.3.2 The beginning: eCash

Commercially, it all began with DigiCash, Inc.'s eCash system in 1990, based on two papers by its founder (Chaum, 1983; Chaum et al., 1992). Payments were transferred online and offline using cryptographic protocols to prevent double-spending. The cryptographic protocols also used blind signatures to protect the privacy of its users.

As the first cryptocurrency, the eCash system was available via various banks and smart cards in various countries like the United States and Finland. It slowly evolved into the current form of cryptocurrencies with many refinements by various software developers over the last 20 years.

eCash was a centralized system owned by DigiCash, Inc. and later eCash Technologies. However, after it was acquired by InfoSpace in 1999, eCash and cryptocurrency faded into the background.

1.3.3 Pioneering Internet payments with digital gold

Digital gold currency came into the limelight between 1999 and the early 2000s. Most of these new forms of electronic money based on ounces of gold are stored at the bullion and storage fees are charged. We have seen the growth of e-dinar, Pecunix, iGolder, Liberty Reserve, gBullion, e-gold, and eCache. With a couple of exceptions, most have ended up in the graveyard due to either compliance issues or regulatory breaches.

e-Gold was a pioneer for Internet payments. As the first successful online micropayment system, it pioneered many new techniques and methods for e-commerce, which later became widely used in other online aspects. These techniques and methods include making payments over a Secure Sockets Layer-encrypted connection and offering an application programming interface to enable other websites to build services using e-gold's transaction system. However, its Achilles heel was its failure to fulfill know-your-customer (KYC) and suspicious transaction reporting requirements. With the introduction of the US Patriot Act, compliance has been a major issue for money transmitters. Furthermore, it has to contend with hackers and Internet fraud. Before the motion to seize and liquidate the entire gold reserve of e-gold under asset forfeiture law in 2008, e-gold was processing more than USD2 billion worth of precious metal transactions per year. There are clear lessons to be learned by the cryptocurrency community.

1.3.4 Revival of cryptocurrency

At the onset of the global financial crisis in 2008, interest on cryptocurrency was revived. Cryptocurrency had the potential to counter a few problems associated with the fiat currency system, argued Szabo (2008) in a blog post just at the beginning of the global financial crisis. Given that it is cumbersome to transact using commodities, the concept of bit gold was mooted. As the name suggests, there is gold to be mined and bit recorded on a digital register. The digital record would resolve the issues of a trusted third party, and in his own words,

> Thus, it would be very nice if there were a protocol whereby unforgeably costly bits could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust. Bit gold.

> My proposal for bit gold is based on computing a string of bits from a string of challenge bits, using functions called variously "client puzzle function," "proof of work function," or "secure benchmark function." The resulting string of bits is the proof of work. Where a one-way function is prohibitively difficult to compute backwards, a secure benchmark function ideally comes with a specific cost, measured in compute cycles, to compute backwards."

Despite sounding technical, what Szabo described was a simple protocol that requires participants to spend resources to mine the digital gold or bit gold, be rewarded, and in the process validate the public digital register. What differentiated his approach from failed digital currencies of the past were the timing of the financial crisis and the distributed nature of the protocol. The reward to the miners was one innovation and the free access to digital record for the users was another. One of the reasons is that the nature of the Internet makes collecting mandatory fees much harder, while voluntary subsidy is much easier. Therefore, there must be no barrier to access content or digital record, and there must be ease of use and voluntary payments.

Ideas were discussed in the literature, and technology was developed over time by a group of cryptographers, old and new, such as Chaum (1983) on DigiCash, Back (1997) on Hashcash, Dai (1998) on b-money, Szabo (1999, 2002, 2008) on the concept of money, and Shirky (2000) on micropayments. Cypherpunk is an activist group since the early 1980s that advocates the widespread use of strong cryptography as a route to social and political changes. Finney (2004), who ran two anonymous remailers as a cypherpunk member, created the first reusable proof of work (RPOW), which is an economic measure to deter denial-of-service attacks and other service abuses such as spam on a network by requiring some work from the service requester. It means that whoever requests for the information has to incur more processing time on a computer than the provider. Hashcash, used by Bitcoin, is a proof-of-work system designed to limit e-mail spam and denial-of-service attacks (Back, 2002).

At the same time, sociopolitical interest in cryptocurrency grew. Since we abandoned the gold standard in 1971 and adopted the fiat currency system, central banks have used their discretion to print as much as they desired during a crisis. This has created an asset inflation environment and worsened income equality. The supply of cryptocurrency or coins may or may not be limited but the new coins are usually created by a predetermined rule. The loss of trust in the fiat currency system, caused mainly by quantitative easing and huge government debts, has brought attention to cryptocurrency for those who wanted to hedge their positions with a currency that has a finite supply.

Cryptocurrency was thought to possess the characteristics of a currency that can impose fiscal discipline on the government and it is perceived to be a debt-free currency with a constant growth rate with finite supply. For asset managers who were constantly seeking for negative correlation with their core portfolio, cryptocurrency provided a glimpse of hope for a high-risk and complex asset class that enhances the returns of a portfolio with bitcoins acting as a negatively correlated alternative asset

class. But the origins of Bitcoin have their roots in cryptoanarchy that started as a movement in 1992:

> Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property. (May1992)

The use of cryptocurrency as a safe haven and an alternative asset class was demonstrated in the 2013 Cypriot property-related banking crisis where a 6.75% levy was imposed on bank deposits up to EUR100k and 9.9% for larger deposits. With confidence in traditional banking shaken, investors were betting heavily on the most well-known cryptocurrency, bitcoins, to offer a more stable alternative. Many investors converted their fiat money into cryptocurrency, sending the price and volume to spike. The price of bitcoins spiked 57% within a week to USD74. Like gold and other commodities, Bitcoin's price spikes in moments of uncertainty. Both assets are increasingly favored by a small group of managers in alternative investment and critics of contemporary monetary policy. The most common arguments against Bitcoin are (i) the lack of a central issuing authority like that of a central bank, (ii) its fixed supply and deflationary nature by design, (iii) doubts that the price is stable enough to function as a currency, and (iv) the risk associated with it.

1.3.5 The rise of Bitcoin

An example of a cryptocurrency is bitcoins. Satoshi Nakamoto published a paper on the Web in 2008 for a peer-to-peer electronic cash system. Despite many efforts, the identity of Satoshi remains unknown to the public and it is not known whether Satoshi is a group or a person.[1]

The cryptocurrency invented by Satoshi Nakamoto, called bitcoins, is run using open-source software. It can be downloaded by anyone, and the system runs on a decentralized peer-to-peer network. It is not only decentralized but also supposedly fully

[1]Satoshi in Japanese means "wise" and someone has suggested that the name might be a portmanteau of four technology companies: SAmsung, TOSHIba, NAKAmichi, and MOTOrola. Others have noted that it could be a team from the National Security Agency (NSA) or an e-commerce firm (Wallace, 2011). Other suggestions are David Chaum, the late Hal Finney, Nick Szabo, Wei Dai, Gavin Andresen, and the Japanese living in the neighborhood of Finney by the same surname Dorian Nakamoto. There are other suggestions such as Vili Lehdonvirta, Michael Clear, Neal King, Vladimir Oksman, Charles Bry, Shinichi Mochizuki, Jed McCaleb, and Dustin Trammell, but most have publicly denied that they are Satoshi.

distributed. That means that every node or computer terminal is connected to each other. Every node can leave and rejoin the network at will and will later accept the longest proof of work known as the blockchain as the authoritative record.

This longest blockchain is proof of what has happened while these nodes were gone. Cryptocurrency is mysterious and misunderstood for a few reasons.

First, no one knows who is really behind some of these cryptocurrency systems. It was designed so that third-party trust is not needed and sometimes there is no legal entity behind it but open-source software.

Second, many have jokingly remarked that Bitcoin sounded more like "big con" especially after the collapse of Mt. Gox. But it is important to note that Mt. Gox was merely a financial intermediary, being just one of many unregulated exchanges that trade in Bitcoins. Mt. Gox was not part the Bitcoin system itself. It is a complex currency system to the men in the street and therein lies the confusion.

Third, cryptocurrency involves mining or proof of work. There are rewards for mining and the reward is given to the first who can solve a cryptography problem. The degree of difficulty of the problem will ensure that the timing to solve the problem is approximately 10 min for Bitcoin. Cryptocurrency cleverly solves the double-spending problem so that every cryptocurrency can be spent only once. It is a financial technology and it involves financial regulation but therein lies the difficulty in execution and understanding even for the professionals. That is why it is an area of great interest to researchers, regulators, investors, and merchants and it is hitting the headlines regularly.

The general arguments for a successful distributed cryptocurrency are as follows:

1. *Open-source software*: A core and trusted group of developers is essential to verify the code and possible changes for adoption by the network.
2. *Decentralized*: Even if it is not fully distributed, it is essential that it is not controlled by a single group of person or entity.
3. *Peer-to-peer*: While the idea is not to have intermediaries, there is a possibility of pools of subnetworks forming.
4. *Global*: The currency is global and this is a very positive point and workable for financial integration with or without smart contracts among the parties.
5. *Fast*: The speed of transaction can be faster and confirmation time can be shortened.
6. *Reliability*: The advantage is that there is no settlement risk and it is nonrepudiable. The savings in cost of a large settlement team for financial activities can be potentially huge.
7. *Secure*: Privacy architecture can be better designed incorporating proof of identity with encryption. If that is done, the issues surrounding Know Your Customer/Client (KYC) and anti-money laundering and terrorist financing (AML/TF) will be resolved.
8. *Sophisticated and flexible*: The system will be able to cater to and support all types of assets, financial instruments, and markets.

9. *Automated*: Algorithm execution for payments and contracts can be easily incorporated.
10. *Scalable*: The system can be used by millions of users.
11. *Platform for integration*: It can be designed to integrate digital finance and digital law with an ecosystem to support smart contracts with financial transactions. Customized agreements can be between multiple parties, containing user-defined scripted clauses, hooks, and variables.

The possible applications will be wide-ranging and include global payment and remittance systems, decentralized exchanges, merchant solutions, online gaming, and digital contracting systems. Each cryptocurrency is a great and an interesting experiment. No one knows where these cryptocurrency experiments are heading but the experiments are interesting because of the technology that is developed along with them.

The technology disrupts the payment system as we know it because it costs almost nothing to transfer payments. Cryptocurrency technology will allow us to reach out to the unbanked and underbanked. It presents the opportunity to function as a conduit for payments and funds. It will transform the way business is being done by diminishing the role of the middleman, whether it is smart accounting or smart contract.

It will also change the way financial world operates especially in fund raising and lending. Basically, it is possible to do an Initial Crowd Offering or crowd lending, all in the peer-to-peer framework, eliminating the middleman.

However, there are downsides or potential risks for cryptocurrency too. Cryptocurrency like Bitcoin depends on mining, and once the incentives for mining disappear, no one knows if the cryptocurrency in question will continue to have consensus on the digital register. They are over 400 cryptocurrencies and the number is increasing on a daily basis. But many of them are in the graveyard.

So, as they say, "let the buyer beware," because what you own may just be worthless once there are doubts about the blockchain. It seems that if the cryptocurrency exhausts most of their coin supply too fast and too early, the probability of the coins dying is higher. For some coins, it is difficult to know who is behind them and whether there could be a backdoor that allows someone to control the system. Cryptocurrency with unknown developers has a higher probability of being buried in the graveyard.

The blockchain may come under attack as well. The blockchain serves as a proof of the sequence of events as well as proof that it came from the largest pool of computing power. As soon as the computing power is controlled by nodes that are cooperating to attack the network, they may produce the longest chain of their choice creating doubts about the validity of the blockchain. This can easily happen once the interest on a particular currency wanes and the number of miners shrinks, which opens up the possibility of having a few blockchains in concurrent existence. Once there is any doubt of the accuracy of the blockchain, even if it was subsequently corrected, the coin will be heading for the graveyard.

When there are no new coins to reward the miners, the system is unlikely to continue. Once no new coins are issued as the mining reward, then the miners are expected to be rewarded purely by transaction fees. This can be a problem. On the other hand, if the fees are increased too quickly or to an unreasonable level, interest on the coins will wane as well. With higher mining cost due to expensive equipment, mining pools will be formed. This is because miners prefer higher probability of success in cracking the code. However, this will lead to an undesirable outcome of mining pools exceeding 30% or even 50% of the network, thus exposing the cryptocurrency to attack. This was indeed the case for Bitcoin when the mining pool accounted for over 50% in the middle of 2014. This is one serious problem that needs to be solved sooner rather than later and consensus ledger or digital register without mining may be one solution.

1.4 GENERAL FEATURES OF BITCOIN

1.4.1 Network and digital currency

Bitcoin is a decentralized network and a digital currency that uses a peer-to-peer system to verify and process transactions. Instead of relying on trusted third parties, like banks and card processors, to process payments, the Bitcoin technology uses cryptographic proof in its computer software to process transactions and to verify the legitimacy of Bitcoins (Nakamoto, 2008) and spreads the processing work among the network. We make a clear distinction between the Bitcoin system where a capital B is used for the word Bitcoin and that of a Bitcoin, which is a unit of the currency or a digital address created by the Bitcoin system.

With the invention of Bitcoin, payments can be made over the Internet without the control and costs of a central authority (Bitcoin Project) for the first time. Prior to the invention, transactions carried out online always required a third party as a trusted intermediary to verify transactions (Brito and Castillo, 2013). For example, when Alice wants to send $10 to Bob, she would have to use a third-party service like a credit card network or PayPal. The function of the third-party service is to provide an assurance that the sender, Alice, has the funds to transfer and that the recipient, Bob, has successfully received the funds. This is possible because these intermediaries help maintain a record, or ledger, of balances for their account holders. Here, when Alice sends Bob the $10, an intermediary like PayPal would deduct the amount from her account and accordingly add it to Bob's account, subject to a transaction fee.

However, the currency unit used in payments on the Bitcoin network is Bitcoins, not a fiat currency. Therefore, bitcoins in itself is also a digital currency, in the sense that it exists "digitally" and, for most intents and purposes, satisfies the economic definition of money: it is a medium of exchange, unit of account, and store of value. Conventionally, the uppercase "Bitcoin" refers to the network and technology, while the lowercase "bitcoin(s)" refers to units of the currency. The currency is also commonly abbreviated to "BTC," although some exchanges use "XBT," a proposed currency code that is compatible with ISO 4217 (Matonis, 2013).

1.4.2 Genesis and decentralized control

The first bitcoin was mined, or created, in 2009, following the online publication of a paper by a Satoshi Nakamoto describing the proof of concept for a currency that uses cryptography, rather than trust in a central authority (Nakamoto, 2008), to manage its creation and transactions. Nakamoto left the project in 2010 and his identity largely remains unknown. However, with the open-source nature of the Bitcoin software protocol, other developers have continued working on it and the Bitcoin community flourishes today.

At the same time, although Nakamoto remains anonymous, users need not be concerned that he, or anyone, secretly has full control of Bitcoin. The open-source nature of Bitcoin means that the source code is fully disclosed. This disclosure allows any software developer to examine the protocol and create their own versions of the software for testing or further development, and so far, no red flag has been raised as to the presence of Nakamoto or any other party with secret control. Furthermore, Bitcoin is designed to operate only with full consensus of all network users. This ensures that software developers who modify the Bitcoin source code in their own versions of the software cannot force a nefarious change in the Bitcoin protocol without breaking compatibility with the rest of the network. The power to change the Bitcoin protocol requires full agreement among Bitcoin users and developers.

1.4.3 How Bitcoin works

To a layperson, bitcoin is a digital currency that is created and held electronically. These bitcoins are sent and received using a mobile app, computer software, or service provider that provides a bitcoin wallet. The wallet generates an address, akin to a bank account number, except that a Bitcoin address is a unique alphanumeric sequence of characters where the user can start to receive payments. Usually, bitcoins may be obtained by buying them at a Bitcoin exchange or vending machine or as payment for goods and services.

However, Bitcoin is revolutionary because the double-spending problem can be solved without needing a third party. In computer science, the double-spending problem refers to the problem that digital money could be easily spent more than once. Consider the situation where digital money is merely a computer file, just like a digital document. Alice could send $10 to Bob by sending a money file to him and can easily do so by e-mail. However, remember that sending a file actually sends a copy of the file and does not delete the original file from the computer. When Alice attaches a money file in an e-mail to Bob, she still retains a copy of the money file even after she has sent and therefore spent it. Without a trusted third-party intermediary to ensure otherwise, Alice could easily send the same $10 to another person, Charlie.

Bitcoin solves the double-spending problem by maintaining a ledger of balances, but instead of relying on a single trusted third party to manage this ledger, Bitcoin

decentralizes this responsibility to the entire network. Behind the scenes, the Bitcoin network constantly keeps track of bitcoin balances in a public ledger called the blockchain. The blockchain is a publicly accessible authoritative record of all transactions ever processed, allowing anyone to use Bitcoin software to verify the validity of a transaction. Transfers of bitcoins, or transactions, are broadcast to the entire network and are included onto the blockchain upon successful verification, so that spent bitcoins cannot be spent again. New transactions are checked against the blockchain to make sure that the bitcoins have not been already spent, thus solving the double-spending problem.

Bitcoin extensively uses public-key cryptography to solve the double-spending problem. In public-key cryptography, each transaction has a digital signature and contains a hash that allows for easy tamper detection (see Figures 1.1 and 1.2 for an example of a Bitcoin transaction).


```
{

"hash":"e9a66845e05d5abc0ad04ec80f774a7e585c6e8db975962d069a522137b8
0c1d",
  "ver":1,
  "vin_sz":1,
  "vout_sz":1,
  "lock_time":0,
  "size":225,
  "in":[
    {
      "prev_out":{

"hash":"f4515fed3dc4a19b90a317b9840c243bac26114cf637522373a7d486b372
600b",
        "n":0
      },

"scriptSig":"3046022100bb1ad26df930a51cce110cf44f7a48c3c561fd977500b
1ae5d6b6fd13d0b3f4a022100c5b42951acedff14abba2736fd574bdb465f3e6f8da
12e2c5303954aca7f78f301
04a7135bfe824c97ecc01ec7d7e336185c81e2aa2c41ab175407c09484ce9694b449
53fcb751206564a9c24dd094d42fdbfdd5aad3e063ce6af4cfaaea4ea14fbb"
    }
  ],
  "out":[
    {
      "value":"0.01000000",
      "scriptPubKey":"OP_DUP                                OP_HASH160
39aa3d569e06a1d7926dc4be1193c99bf2eb9ee0 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```


Figure 1.1 Example of a raw transaction data.

General information about this transaction		
Hash	e9a66845e05d5abc0ad04ec80f774a7e585c6e8db975962d069a522137b80c1d	The hash for this transaction
Block	100000 (2010-12-29 11:57:43)	Obtained from examining the block on the blockchain where this transaction was found
Version	1	Bitcoin software version
Size	225	The filesize in bytes of the transaction is recorded in the transaction data itself
Input from		
Previous output	f4515fed3dc4a19b90a317b9840c243bac26114cf637522373a7d486b372600b	The truncated hash of the previous transaction which provides the bitcoins to be sent for this transaction
Previous amount	0.01	The amount in the previous transaction which provides the bitcoins to be sent for this transaction
Public address	1JxDJCyWNakZ5kECKdCU9Zka6mh34mZ7B2	The public address of the sender, obtained from examining the blockchain
Signature	3046022100bb1ad26df930a51cce110cf44f7a48c3c561fd977500b1ae5d6b6fd13d0b3f4a022100c5b42951acedff14abba2736fd574bdb465f3e6f8da12e2c5303954aca7f78f30104a7135bfe824c97ecc01ec7d7e336185c81e2aa2c41ab175407c09484ce9694b44953fcb751206564a9c24dd094d42fdbfdd5aad3e063ce6af4cfaaea4ea14fbb	The digital signature of the transaction, signed by the sender
Output to		
Index	0	"0" indicates the first recipient in the transaction; here this transaction only has one recipient
Amount	0.01	Amount sent to this user in this transaction
Public address	16FuTPaeRSPVxxCnwQmdyx2PQWxX6HWzhQ	The public address of the recipient, obtained from the scriptPubKey
Bitcoin address (scriptPubKey)	39aa3d569e06a1d7926dc4be1193c99bf2eb9ee0	A hash160 of the public address
Conditions	OP_DUP OP_HASH160 OP_EQUALVERIFY OP_CHECKSIG	Conditions to be met together with the scriptPubKey for the output bitcoins to be redeemed by the recipient

Figure 1.2 Explanation for the transaction.

1.4.4 Buying and storing bitcoins

Against this technical backdrop, bitcoins are often used simply as payment in exchange for goods and services (Kaplanov, 2012). While the numbers of brick-and-mortar merchants who accept payments in bitcoins remain low, there are many more online

merchants who accept bitcoins for both digital and physical goods and services. The price of these goods and services is usually based on the exchange rate between Bitcoin and a real-world currency, which can be found easily online (XE).

Typically, a user who wishes to spend bitcoins obtains it by exchanging real-world currency for bitcoins. This can be achieved by purchasing bitcoins from a vending machine, from an exchange, or simply from another person. Bitcoin vending machines, often called "ATMs," are the most convenient way to buy bitcoins, because one can easily insert cash into a machine to obtain bitcoins instantly (Ulm, 2014). Bitcoin exchanges are also a popular means to obtain bitcoins, but users often face a time delay while waiting for bank transfers to clear (Ulm, 2014). Trading real-world cash for bitcoins is also a possibility but it is inconvenient if bitcoins are needed on the spot. However, marketplace websites like LocalBitcoins have sprouted up to connect people interested in buying and selling bitcoins to enable them to do so privately, whether in person or online (LocalBitcoins). This option is more likely to be used in countries with restricted or no access to Bitcoin vending machines or exchanges.

Bitcoins are typically stored in a wallet, so a user needs to have a wallet available to buy and sell bitcoins. Specifically, it is the private keys that are stored in a wallet (CoinDesk, 2014). These keys are used to access the Bitcoin addresses and sign transactions and therefore must be kept securely. There are various types of Bitcoin wallets, including desktop, mobile, webs, and hardware wallets.

Users who choose to install a desktop wallet on their computer can create and keep wallets on their computer. The original Bitcoin client software, known as Bitcoin Core, which is still in use today, includes the functionality of creating a bitcoin address to send and receive bitcoins and to store the corresponding private key for that address. There are various other wallet software in which users may elect to install on their computer, like the cross-platform MultiBit and the security-conscious Armory (Bitcoin.org). The different wallet software have varying additional features, although the most basic function of a wallet in storing the private keys for corresponding bitcoin addresses remains the same. While the user maintains control of his desktop wallet at all times, such wallets, like any other computer file, are vulnerable to theft by malicious users or software.

Desktop wallets are not the be-all and end-all of wallets, even if they were the first. When transacting at a physical store, a mobile wallet is often the most convenient way to spend some bitcoins. Mobile wallets are simply an application that provides for Bitcoin wallet functionality in a mobile phone. There are apps like Bitcoin Wallet and Mycelium that only exist on the mobile platform, while some desktop wallets like Blockchain.info also have mobile versions (Bitcoin.org). However, in the early 2014, Apple removed Bitcoin Wallet apps like Blockchain.info from its App Store (Southurst, 2014), although unofficial versions and mobile browser-based wallets continue to exist.

Another convenient type of wallet is the online wallet, which is generally accessible from anywhere through a browser with an Internet connection, regardless of the device

used (CoinDesk, 2014). The private keys for a user's Bitcoin addresses are kept and stored by the service provider of the online wallet, which may present a risk of the service provider or a third party absconding with the bitcoins, if security was not implemented properly. Blockchain.info also has a popular web-based online wallet and some online wallets offer extra encryption and two-factor authentication for additional security.

Finally, there is small but growing interest in hardware wallets, which are specialized devices that can hold keys electronically and are also able to send and receive bitcoins. An example of a dedicated Bitcoin device is the Trezor, a single-purpose token-sized device for making secure Bitcoin transactions (SatoshiLabs).

1.4.5 Mining to create new bitcoins and process transactions

Bitcoin is designed with a hard limit of 21 million bitcoins, which are expected to be created by 2040 (Figure 1.3). For now, these bitcoins are generated through mining, during which miners, who are Bitcoin users running software on specialized hardware, process transactions and are rewarded with new bitcoins for contributing their computer power to maintain the network. Mining is important not only for new bitcoins to be issued but also because it is a necessary process for transactions to be added onto the blockchain and be subsequently confirmed. The verification process is a computationally intensive process that ensures that only legitimate transactions are verified and recorded onto the blockchain. It is the network that provides the computing power for the transactions to take place and for the transactions to be recorded.

What happens during mining is actually a mathematical process. A real-life analogy to bitcoin mining would be the search for prime numbers: while it was easy to find the small ones, it became increasingly more difficult to find the larger numbers, leading researchers to use special high-performance computers to find them (Tindell, 2013).

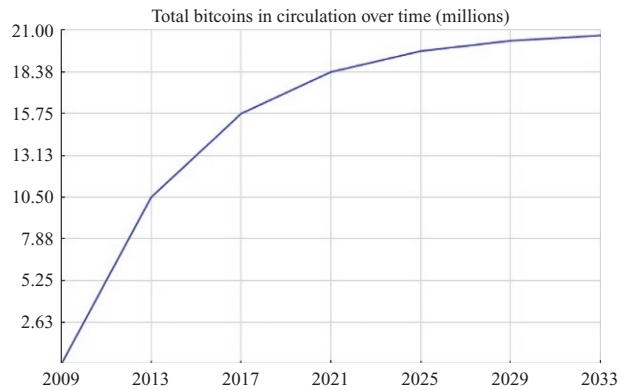

Figure 1.3 Bitcoin supply.

Mining is a computationally intensive task that requires miners to find the solution to a predetermined mathematical problem in order to create a new block. This is the mathematical proof of work. Mining is difficult because besides ensuring that the transactions are valid, miners have to fit the data in a particular manner in order to add it to the blockchain. Miners have to guess and search for a sequence of data that produces a required pattern.

The difficulty of the problem is automatically adjusted so that a new block can only be created every 10 min on average. The Bitcoin protocol is designed to generate new bitcoins progressively, at a predictable but decreasing rate. To ensure a progressive growth in new bitcoins, the reward for solving a block is halved automatically every 4 years, and the difficulty of solving increases over time. These two effects work together to produce an effect that over time, the rate at which bitcoins are produced will be similar to the production rate of a commodity like gold (see Figure 1.3). There will be a point in the future when the hard limit of bitcoins will be reached and the incentive for miners will instead be transaction fees. The arbitrary number chosen to be the limit in number of bitcoins is 21 million. Once the very last bitcoin, or to be specific, the very last satoshi—0.00000001 of a bitcoin—is produced through mining, miners who continue to contribute their computing power to verify transactions will instead be rewarded with transaction fees. This may be a less desirable situation for people and businesses relying on bitcoin payments, which will have to pay a transaction fee, but it ensures that miners will still have an incentive to keep the network up and running even after the last bitcoin is mined.

Every new block that is successfully added onto the blockchain references the previous block, making it exponentially difficult to reverse previous transactions in previous blocks. Because changing a block on the blockchain will require recalculation of the proofs of work of all subsequent blocks (Bitcoin Project), it becomes more and more infeasible for an adversary to manipulate a block after more blocks have been added after it, and the Bitcoin protocol is accordingly designed to prefer longer chains. Miners therefore perform a vital task as they verify transactions and ensure that the blockchain cannot be tampered with.

While bitcoin transfers are broadcast instantaneously over the network, there is, in practice, a 10 min delay for a transaction to be confirmed. This is the result of the 10 min delay for a block to be created and added onto the blockchain. Having a confirmation ensures that the network (of miners) has verified that the bitcoins are valid and have not been already spent. Typically, most users wait for six confirmations, that is, an hour, before considering a transaction to be "confirmed," but each user has the freedom to decide how long they wish to wait before they consider their transaction confirmed.

1.4.6 Security and cryptography

The security of the technology used is supported using secure hash algorithms and has a good track record. The Bitcoin protocol is an open-source and is continuously improved by the developer community subject to consensus among all network users. The hash

function mainly used in Bitcoin is SHA-256 (Pacia, 2013), which was incidentally originally designed by the NSA in the United States. There is no need for suspicion against the NSA because the SHA algorithm is part of the public domain and has been extensively analyzed to be secure (Pacia, 2013). SHA-256 is an upgrade from the SHA-1 series and is presently used in Bitcoin for the digital signatures that secure the transactions and blockchain and it forms the basis of the proof-of-work mathematical problem.

Central to Bitcoin technology is public-key cryptography, which with the SHA-256 hash function is used to generate Bitcoin addresses, sign transactions, and verify payments. Public-key cryptography is a technique of reliably determining the authenticity of Bitcoin transactions using digital signatures. It uses an asymmetrical algorithm that generates two separate but asymmetrically linked keys: a public key and a private key. The keys are asymmetrical in the sense that the public key is derived from the private key but it is computationally impossible to obtain a private key from a public key. In such a system, the public key is used to verify digital signatures in transactions while the private key is used to sign transactions to produce those very digital signatures. The public key is publicly accessible; in Bitcoin, it is used as the Bitcoin address to and from which payments are sent. The private key, on the other hand, must be kept secret and safely. The beauty of such a system is that transactions can be easily verified using the public key without sharing the private key used to sign the transactions.

1.4.7 Pseudoanonymity

As seen from Figures 1.1 and 1.2, a Bitcoin address is an alphanumeric sequence of characters. There is no other information that can identify the sender and recipient of the bitcoins. However, it is a common misconception to say that bitcoin is an anonymous currency. This misconception often arises from a lack of understanding of the technology (Brito and Castillo, 2013).

Prior to Bitcoin, online transactions have not been anywhere close to anonymous because they have to go through third-party intermediaries, who have interests in knowing who their customers are, for risk assessment purposes and compliance with the relevant laws and regulations. For example, when Alice makes a transfer of $10 using PayPal to Bob, PayPal will have a record of the transfer. In addition, their PayPal accounts are likely to be linked to their respective credit cards or bank accounts, which will provide information as to their identities. On the other hand, if Alice gives Bob $10 in cash in person, there is neither an intermediary nor a record of the transaction. If the two of them do not know each other, then the transaction can be said to be completely anonymous.

Bitcoin is somewhere in between these two extremes. Bitcoins can be said to be like cash in the sense that when Alice gives bitcoins to Bob, she no longer has them, while Bob does. Since there is no third-party intermediary, nobody knows their identities as well. However, unlike cash, the transaction is recorded on the blockchain. Some of

the information recorded includes the public keys of the sender and recipient, the amount, and a time stamp. Every transaction in the history of bitcoin has been recorded and will be recorded on the blockchain and is publicly viewable.

While there is some privacy, the blockchain is a public record of all transactions and it may be possible for anyone to identify the parties behind them, especially if a person's identity is linked to a public key. While bitcoins may be anonymous like cash in the sense that parties can transact without disclosing their identities, it is also unlike cash because transactions to and from any Bitcoin address can be traced. Therefore, Bitcoin is pseudonymous, not anonymous.

It is not particularly difficult for anyone with the right tools and access to join the dots between a pseudonymous Bitcoin address and a real-world identity. Some personally identifiable information is often captured during a transaction on a website, like an IP address. To make it more difficult to connect an identity to a Bitcoin address, one would have to use software methods that obfuscate or shield such personally identifiable information from being tied to Bitcoin addresses.

Early studies have already shown some potential analyses that could erode the pseudonymity of Bitcoin. For those who are persistent in connecting Bitcoin addresses to real-world identities, their work should begin with the blockchain. In a simulated experiment, a study found that up to 40% of Bitcoin users within the experiment could be personally identified using behavior-based clustering methods (Androulaki et al., 2012). The statistical properties of the transaction graph could also, with the relevant analysis, reveal the activity and identity of Bitcoin users (Reid and Harrigan, 2013). Even the use of multiple public keys may not defend against such transaction graph analysis (Ober et al., 2013), as an observer may gradually be able discern patterns in user behavior to link the public keys together, using a process called entity merging (Brito and Castillo, 2013).

Besides the technical aspects of Bitcoin, it is important to also consider the pressures faced by Bitcoin intermediaries from regulators. Bitcoin regulation is evolving, and should Bitcoin intermediaries become regulated, it is expected that anonymity will become less guaranteed (Brito and Castillo, 2013), often with KYC and reporting requirements requiring these intermediaries to collect personally identifiable information from their customers.

1.5 BENEFITS AND RISKS

Bitcoin as a novel technology brings a range of benefits and risks to the table. This section outlines some of the most well-known benefits and risks.

1.5.1 Freedom of payments

Bitcoin was specifically designed for fast transactions at low costs (Nakamoto, 2008). Payments can be processed with little or no fees, with the sender having the option to include

a transaction fee for faster confirmations. A low transaction cost is possible because there is no single third-party intermediary. In addition to the lack of restrictions on transactions, users have full control of their bitcoins and the freedom to send and receive bitcoins anytime, anywhere, and to and from anyone.

Users may also choose to use Bitcoin to make fast cross-border transfers easily without paying expensive fees for remittances. There is great potential for remittances because the value of remittances, especially from people in developed countries to those in developing countries, is expected to increase to USD515 billion in 2015 (World Bank Payment Systems Development Group, 2013). The reduced costs of remittances could be substantial if remitted using bitcoins.

1.5.2 Merchant benefits

Bitcoin presents an alternative to the other methods of electronic payments accepted by businesses. Traditional credit card acceptance is expensive for merchants, with customers often having to pay for a merchant account and various fees for transactions, including but not limited to transaction fees, interchange fees, and statement fees. These fees add up and increase the costs of accepting credit cards for payments. Yet, merchants who forgo credit card payments may lose business from customers used to the ease of paying with credit cards. Not having to pay these expensive fees may allow businesses to pass on the cost savings to consumers, benefiting everyone.

Bitcoin transactions are also secure, unlike credit card payments, which may use insecure magnetic stripes and signatures, and are irreversible, unlike credit card payments, which are subject to the possibility of fraudulent charge-backs. The low cost of transactions also allows merchants to accept micropayments, paving the way for Bitcoin to be widely accepted without a minimum transaction level.

1.5.3 User control

Each Bitcoin transaction can only be effected by the user who has the private key, putting the user in full control of his bitcoins. Merchants cannot slip in unwanted charges later, unlike credit cards that offer limited protection against such charges once an unethical merchant has the card details. Transactions also do not contain substantial personal information, which is at risk of leakage and theft.

However, the converse effect of full user control is the point that the private key controls the access to one's bitcoins. Bitcoin, being a digital currency, brings specific security challenges (Kaminsky, 2013). Perhaps the most important risk to end users is that if the private key is lost, access to the bitcoins is irrecoverable. Poor wallet protection may leave users vulnerable to thefts, especially by specially crafted malicious software designed to steal bitcoins (Doherty, 2011). Bitcoin users should therefore be security conscious with Bitcoin, just as they do for other financial activities (Brito and Castillo, 2013).

1.5.4 Platform for further innovation

The Bitcoin protocol may, in its original form, work as a payment network, but it has the potential for further innovation. What actually happens in the Bitcoin network is that data in the form of Bitcoin transactions are broadcasted and verified before being kept on the blockchain. Bitcoin technology may therefore be adapted for the transfer of other types of data, like stocks or bets (Brito, 2013). Feature layers are beginning to be built on top of Bitcoin, which include smart property and assurance contracts (Brito and Castillo, 2013). Being an open-source technology, alternative digital currencies like Litecoin and Dogecoin, among others, have also emerged to suit different objectives.

1.5.5 Internal change and volatility

As a community-driven project, Bitcoin continues to undergo changes as software developers improve and change the software with consensus of network users. At the same time, the price of bitcoins continues to fluctuate as current events affect the price. Some significant price changes are said to resemble a traditional speculative bubble, which may occur when optimistic media coverage attracts investors (Salmon, 2013). This may make it difficult to determine how good bitcoins are as a store of value, and merchants accepting bitcoins therefore often convert them out into fiat currency very quickly. It is also difficult to predict the Bitcoin economy in the future as it is the first widely accessible cryptocurrency, although researchers are already working on models that will attempt to explain behavior in the Bitcoin world. At the same time, it may be possible that the value of bitcoins may become less volatile as familiarity with Bitcoin increases with time.

1.5.6 Facilitation of criminal activity

With the pseudoanonymity and ease of payments offered by Bitcoin, it is no wonder that governments are concerned with the use of Bitcoin in facilitating criminal activity. Indeed, one of the most well-known criminal uses of Bitcoin was on the Silk Road website, a black market often used to trade illicit drugs and counterfeit passports. Silk Road used a combination of Bitcoin payments and the anonymizing network Tor to create a marketplace for such illicit goods and services (Chen, 2011). Another major concern regarding Bitcoin is its use to launder money and finance terrorist activity. These concerns were stoked especially after the Liberty Reserve, a private and centralized digital currency was shut down on money laundering concerns (BBC News, 2013). It is important to remember, however, that bitcoins are like money, and money can be used for both lawful and unlawful purposes. Other methods of transferring money have been used for financing crimes and money laundering even before Bitcoin existed. However, many Bitcoin exchanges are beginning to employ antimoney laundering features that include

keeping records of their customers, which will reduce the attractiveness of Bitcoin to criminals.

Bitcoin, however, also offers benefits over traditional money that protect against some forms of financial crime. For example, the mining process of verifying transactions, which solves the double-spending problem, makes it extremely difficult for bitcoins to be double-spent or counterfeited. An adversary needs to amass sufficient computing power to overcome the combined network computing power in order to be able to attempt to modify present and future transactions before the rest of the network catches up.

1.5.7 Legal regulatory attitude

As Bitcoin is novel, its regulation by governments run the gamut of being permissive to outright bans. The regulatory landscape continues to change as governments grapple with the risks and benefits of Bitcoin to their country. For a start, regulators in some jurisdictions are beginning to provide rules and guidance on the treatment of digital currencies in their country, especially in measures relating to antimoney laundering and the countering of terrorist financing, as well as taxes. The challenge for regulators is to encourage beneficial uses and future innovations while minimizing the risks posed and to do so without preventing such innovations from spawning.

1.5.8 Economic risk

Bitcoin is something that is very different from the existing financial system for which country regulators have experience regulating. The innovative use of Bitcoin may be disruptive to the financial and payment markets in that Bitcoin, for example, can scale up to replace money transmission and card payment services, or even stock exchanges, which renders the incumbent service providers obsolete. If these changes occur rapidly, there is a risk that this will destabilize the financial and payment markets and ultimately price stability in a market.

1.6 IMPACT OF THE DIGITAL CURRENCY REVOLUTION

The digital currency revolution will have a lot of impact on the digital and physical world. A lot of devices will be connected to each other via near-field communication (NFC). Devices that are carried by our side or are worn on our body will contain information about our preferences, possibly our current state of health and most likely all our personal records including how much money we have. We may not need to carry physical wallets and identity cards anymore.

These devices will monitor us and improve our experience in every aspect of our life including medical care, education, and financial services. The blockchain technology can play a major role in lowering the cost of financial services via cost sharing through mining, and therefore, financial institutions can reach out to the unbanked and underbanked,

as well as those that require lending and fund raising. All these can be done via the peer-to-peer network of cryptocurrency, either decentralized or distributed. Financial services especially banking will likely be disrupted and margin will be affected as what eCash was set out to do in the early 1990s.

A second example is the use of smart contract for a sharing economy. We will be able to share our assets such as cars, hard disks, and computer memory that we do not use and rent them out to others for a fee. Smart contracts via the distributed peer-to-peer network will make all these possible in the future. This will ensure that infrastructure need not increase but excess capacity is used efficiently.

The desire to own entire assets will be less as more peer-to-peer digital assets or digital trusts can be held by the crowd via blockchain technology. There is also the possibility of time banking so that the cryptocurrency is stored in hours of work. One can then trade with the time spent in, say, palliative care when one is young, and then, the same person will be entitled to such care when he or she gets older with the hours that have been deposited. While these can be done with a centralized system, a distributed or decentralized blockchain system has unique advantages especially in terms of distributed computing. Cryptocurrency may not replace the fiat currency, but its blockchain technology will certainly have an impact on the welfare of the people and perhaps even out the inequality.

1.7 CONDITIONS FOR A SUCCESSFUL CRYPTOCURRENCY

1.7.1 Ecosystem

There is always the first-mover advantage and Bitcoin has certainly emerged as the leading cryptocurrency with an estimated 6 million electronic wallets, 70,000 merchants, and a market capitalization of USD5 billion. For the 6 months leading to October 2014, there were 50-80k transactions daily, and approximately USD50 million (equivalent to over 110,000 bitcoins in 2014) are traded daily. The number of wallets is small given that we have more than 7 billion people in the world. Bitcoin has been successful so far and an ecosystem is up to support its existence. Even though the network effect is kicking in, there is still a long way to go.

A successful digital currency must be able to ride on its initial success and leverage on the network effect. The more people use the coin, the more valuable it will become. As it becomes more valuable, the reward for mining will increase, and more miners will join in the competitive accounting exercise. Bitcoin is subject to the same problems we mentioned earlier.

1.7.2 Incentives

As the mining costs go up because equipment becomes more expensive, mining pools will be formed as miners are usually risk averse and want better odds in winning the race. This increases the possibility of an attack or the emergence of a gold finger that

determines to cause problems. There are slightly over 13.4 million bitcoins in circulation as of October 2014. Twenty-five bitcoins are created approximately every 10 min from 2013 to 2016 and the number of new coins created will halve every 4 years.

As soon as the full supply of 21 million bitcoins are issued by the year 2040, which is still very distant, the risk of miners dropping out may increase. If the only reward is transaction fees and if fees become too high, the merchants are likely to drop out.

Of course, there are technical solutions to all these and some cryptocurrencies have come up with the idea of proof of stake reducing the probability that any single person can use a quantum computer to overwrite the whole system. There are also attempts to lower the cost of mining so as to reduce the so-called 51% attack or gold finger problem. However, there is still no fool proof solution to the gold finger issue that if anyone with enough financial strength wishes to mess up the record, he or she can theoretically do it.

1.7.3 Identification

There are also cryptocurrencies that are looking into proof of identity to reduce the possibility of using the currency for money laundering or terrorism activities. If that problem can be resolved, cryptocurrency has a very real potential to be very popular.

If a particular cryptocurrency is able to accept that the government is part of the ecosystem and its community engages with the government meaningfully in creating the ecosystem, that cryptocurrency is likely to become more widely accepted. Given that most of the welfare improvement comes from the bottom of the wealth pyramid, emerging markets have the upper hand in harnessing the low-hanging fruits of cryptocurrency via a decentralized but not necessary distributed system. A cryptocurrency that addresses those issues mentioned will have a bright future.

1.8 FUTURE PROSPECTS AND CONCLUSION

Many people see similarities between the growth of the Internet and the growth of cryptocurrency and postulate that cryptocurrency is going to see exponential growth like the Internet. However, from the business perspective, the growth of the Internet has more to do with e-commerce and less to do with finance. On the other hand, with cryptocurrency, for once in the history of mankind, technology is playing a leading role in finance. In future, one should expect a bank to be a digital or technologically savvy bank. The disruptive force has now arrived at the door step of finance and the blockchain technology is one of the solutions.

There are also similarities between hedge funds and cryptocurrency at the industry level. When the hedge fund industry was in its infant stage, it was perceived to be disruptive to the currency system because hedge fund managers were perceived as the bad guys who took big bets. They were seen to be the mavericks who attacked the currency system and caused the stock markets to collapse. Some banks did not want to deal with

them as it did not make business sense with the high compliance costs. Start-ups in cryptocurrency today face the same problems.

There is a lot of bad press and misunderstanding in the media regarding cryptocurrency and some banks are unwilling to open accounts with cryptocurrency start-ups because of various reasons. Regulators are also generally uncomfortable at the moment to deal with a financial innovation as complex as Bitcoin or indeed any other cryptocurrency. At the same time, there is a general resistance and reluctance by Main Street to learn about the intricacies of this financial innovation—it is a wait-and-see situation. That is human nature and it is always the universities and those who are interested in the technology who will see the opportunities first.

There are a lot of similarities between cryptocurrency and hedge fund strategies that were inherently quantitative and difficult to understand. It was no surprise to anyone that hedge fund strategies were initially embraced by the university endowment funds that were less constrained than the traditional managers. Again, universities and financial entrepreneurs will be the first to embrace the cryptocurrency technology before it spills over to the main street.

Cryptocurrency is here to stay and will evolve over time. If Bitcoin loses its popularity for whatever reason, a new cryptocurrency will emerge to replace it with better features. Countries with huge debts have the incentive to create their own cryptocurrency and those who wish to promote financial integration may also turn to cryptocurrency, simply because the cost is low in creating a decentralized partially distributed system. There will be welfare improvement in a cryptocurrency world, which is decentralized but not necessary fully distributed, with proof of identity, proof of stake, and the flexibility to incorporate smart contracts for a sharing economy.

Eventually, it is about reduction of business cost, and welfare improvement will follow for those at the bottom of the wealth pyramid. Eventually, all of this will lead to enhanced efficiency in a sharing economy. The outlook on the development of cryptocurrency is much more optimistic because of the blockchain technology. We are likely to see a great leap in its use, with NFC and related mobile technology being the driver behind its boom. At the same time, it is difficult to predict if cryptocurrency is the next big thing as there is still a lot of uncertainty in the cryptocurrency world. But it is a technology that financial institutions cannot ignore.

In conclusion, Bitcoin is a novel invention, which is a breakthrough in terms of the payments and decentralized networks we know today. It brings with it various benefits and risks that users should be cognizant and indeed conversant with should they wish to deal with and in bitcoins. This chapter has mainly discussed the main features of Bitcoin, but other cryptocurrencies are likely to have similar features and a clear understanding of Bitcoin will aid in understanding other cryptocurrencies. It is only with a good foundation in the knowledge of this amazing new technology that we will be able to use it to its fullest potential without fear.

ACKNOWLEDGMENTS

The ideas for this chapter originated from the expertise of David Lee, especially in his introductory lectures on Bitcoin, and from Lam Pak Nian's earlier research on Bitcoin during his undergraduate degree. The authors also wish to thank Nirupamadevi Bhaskar for clarifying some of the basic concepts and for her guidance on interpreting the raw transaction data.

REFERENCES

Androulaki, E., et al., 2012. Evaluating user privacy in bitcoin. IACR Cryptology ePrint Archive 596. Retrieved from http://fc13.ifca.ai/proc/1-3.pdf.

Back, A., 1997. A partial hash collision based postage scheme, s.l.: s.n. Retrieved from http://www.hashcash.org/papers/announce.txt (accessed 25.01.2015).

Back, A., 2002. Hashcash—a denial of service counter-measure, s.l.: s.n. Retrieved from http://www.hashcash.org/papers/hashcash.pdf (accessed 25.01.2015).

BBC News, 2013. Liberty Reserve digital money service forced offline. BBC News. Retrieved from http://www.bbc.co.uk/news/technology-22680297 (accessed 27.05.13).

Bitcoin.org, 2014. Choose your bitcoin wallet. Retrieved from https://bitcoin.org/en/choose-your-wallet.

Bitcoin Project, 2014. Frequently asked questions. Retrieved from Bitcoin.org: https://bitcoin.org/en/faq.

Brito, J., 2013. The top 3 things I learned at the bitcoin conference. Retrieved from Mercatus Center Expert Commentary: http://mercatus.org/expert_commentary/top-3-things-i-learned-bitcoin-conference.

Brito, K., Castillo, A., 2013. Bitcoin: a primer for policymakers. Retrieved from Mercatus Center: http://mercatus.org/publication/bitcoin-primer-policymakers.

Chaum, D., 1983. Blind signatures for untraceable payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (Eds.), Advances in Cryptology. In: Proceedings of Crypto, vol. 82. Springer, pp. 199–203. Retrieved from http://link.springer.com/chapter/10.1007%2F978-1-4757-0602-4_18.

Chaum, D., Fiat, A., Naor, M., 1990. Untraceable electronic cash. Adv. Cryptol CRYPTO' 88 (403), 319–327.

Chen, A., 2011. The underground website where you can buy any drug imaginable. Gizmodo. Retrieved from http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable (accessed 01.06.11).

CoinDesk, 2014. How to store your bitcoins. CoinDesk. Retrieved from http://www.coindesk.com/information/how-to-store-your-bitcoins/ (accessed 22.07.14).

Dai, W., 1998. b-money, s.l.: s.n.

Doherty, S., 2011. All your bitcoins are ours... Symantec Blog. Retrieved from http://www.symantec.com/connect/blogs/all-your-bitcoins-are-ours (accessed 16.6.11).

Finney, H., 2004. RPOW—Reusable Proofs of Work, s.l.: s.n. Retrieved from http://cryptome.org/rpow.htm (accessed 25.01.2015).

Hileman, G., 2014. From bitcoin to the Brixton pound: history and prospects for alternative currencies (poster abstract). In: Böhme, R., Brenner, M., Moore, T., Smith, M. (Eds.), Springer, Berlin pp. 163–165.

Kaminsky, D., 2013. I tried hacking bitcoin and I failed. Business Insider. Retrieved from http://www.businessinsider.com/dan-kaminsky-highlights-flaws-bitcoin-2013-4 (accessed 12.04.13).

Kaplanov, N.M., 2012. Nerdy money: bitcoin, the private digital currency, and the case against its regulation. Retrieved from http://ssrn.com/abstract=2115203.

LocalBitcoins, 2014. Buy and sell bitcoins near you. Retrieved from https://localbitcoins.com/.

Matonis, J., 2013. Bitcoin gaining market-based legitimacy as XBT. Retrieved from CoinDesk:http://www.coindesk.com/bitcoin-gaining-market-based-legitimacy-xbt/.

May, T., 1992. The Crypto Anarchist Manifesto. s.l.: s.n. Retrieved from http://www.activism.net/cypherpunk/crypto-anarchy.html (accessed 25.01.15).

Nakamoto, S., 2008. Bitcoin: a peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf.

Ober, M., Katzenbeisser, S., Hamacher, K., 2013. Structure and anonymity of the bitcoin transaction graph. Fut. Int. 5 (2), 237–250. Retrieved from http://www.mdpi.com/1999-5903/5/2/237.

Pacia, C., 2013. Bitcoin mining explained like you're five: part 2—mechanics. Escape Velocity. Retrieved from http://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-2-mechanics/ (accessed 02.09.13).

Reid, F., Harrigan, M., 2013. An analysis of anonymity in the bitcoin system. In: Altshuler, Y. et al., (Eds.), Security and Privacy in Social Networks. Springer, New York. Retrieved from http://arxiv.org/pdf/1107.4524v2.pdf.

Salmon, F., 2013. The bitcoin bubble and the future of currency. Medium. Retrieved from http://medium.com/money-banking/2b5ef79482cb, 3 April, 2013 (accessed 03.04.13).

SatoshiLabs, 2013. What is TREZOR? Retrieved from http://doc.satoshilabs.com/trezor-faq/overview.html.

Shirky, C., 2000. The Case Against Micropayments. O'Reilly Media, Inc. Retrieved from http://www.openp2p.com/pub/a/p2p/2000/12/19/micropayments.html (accessed 25.01.2015).

Southurst, J., 2014. Apple removes blockchain bitcoin wallet apps from its app stores. CoinDesk. Retrieved from http://www.coindesk.com/apple-removes-blockchain-bitcoin-wallet-from-app-stores/ (accessed 06.02.14).

Szabo, N., 1999. The God Protocols. IT Audit, 15 November.

Szabo, N., 2002. Shelling Out—The Origins of Money, s.l.: s.n. Retrieved from http://szabo.best.vwh.net/shell.html (accessed 25.01.2015).

Szabo, N., 2008. Bit gold, s.l.: s.n. Retrieved from http://unenumerated.blogspot.com/2005/12/bit-gold.html (accessed 25.01.2015).

Tindell, K., 2013. Geeks love the bitcoin phenomenon like they loved the internet in 1995. Business Insider. Retrieved from http://www.businessinsider.com/how-bitcoins-are-mined-and-used-2013-4 (accessed 05.04.13).

Ulm, B., 2014. Bitcoin ATMs boom: new locations. CoinTelegraph. Retrieved from http://cointelegraph.com/news/112163/bitcoin-atms-boom-new-locations (accessed 28.07.14).

Wallace, B., 2011. The Rise and Fall of Bitcoin. Wired. (23), November 2011.

World Bank Payment Systems Development Group, 2013. Remittance Prices Worldwide: An Analysis of Trends in the Average Total Cost of Migrant Remittance Services. The World Bank, Washington, DC. Retrieved from http://remittanceprices.worldbank.org/~/media/FPDKM/Remittances/Documents/RemittancePriceWorldwide-Analysis-Mar2013.pdf.

XE, 2014. XBT—bitcoin. Retrieved from http://www.xe.com/currency/xbt-bitcoin.