Bitcoin

PREPARED BY

Rayan ELHAMOUD

SUPERVISOR

Dr.Farah ANKOUD

Summary:

- Bitcoin is an open-source solution run on a peer-to-peer network, so no one ‘owns’ it. Transactions are recorded on a public ledger distributed over the network. That ledger is called the 'blockchain', and all the peers in the network work towards its ‘protection’. It is constantly being tested and verified by the community to ensure that all transactions are in order. Peers contribute computer processor power in exchange for bitcoins. This ‘protection of the ledger’ process is called ‘mining’. A user needs a pair of keys, which are included in a 'wallet' application. A wallet is unlike a bank account; it’s more like one’s own bank, out of which one can assign unlimited number of accounts or ‘addresses’ to send /receive digital currencies. It is useful in tracking incomes. All accounts are maintained for free, while transaction fees are significantly small. People are already contributing bitcoins to Open Science, a crowdfunding project to fund scientific research. It can also be used as a second national currency, for e-voting, and to make remittances, to take a few examples.

- Bitcoin est une solution open-source fonctionnant sur un réseau peer-to-peer, de sorte que personne ne le "possède". Les transactions sont enregistrées sur un grand livre public distribué sur le réseau. Ce registre est appelé "blockchain", et tous les pairs du réseau travaillent à sa "protection". Il est constamment testé et vérifié par la communauté pour s'assurer que toutes les transactions sont en règle. Les pairs fournissent de la puissance de traitement informatique en échange de bitcoins. Ce processus de "protection du grand livre" est appelé "minage". Un utilisateur a besoin d'une paire de clés, qui sont incluses dans une application "portefeuille". Un portefeuille n'est pas comme un compte banquaire ; il s'agit plutôt de sa propre banque, à partir de laquelle on peut attribuer un nombre illimité de comptes ou d'"adresses" pour envoyer/recevoir des devises numériques. Il est utile pour suivre les revenus. Tous les comptes sont gérés gratuitement, tandis que les frais de transaction sont très faibles. Des personnes contribuent déjà en bitcoins à Open Science, un projet de crowdfunding pour financer la recherche scientifique.

Table of Contents

Table of Figures

Table of tables:

Chapter 1: Design

1. Units and divisibility:

The unit of account of the bitcoin system is the *bitcoin*. *Currency codes* for representing bitcoin are BTC and XBT. Its character is ₿.[1] One bitcoin is divisible to eight decimal places. Units for smaller amounts of bitcoin are the milli bitcoin (mBTC), equal to $^{1}/_{1000}$ bitcoin, and the Satoshi (sat), which is the smallest possible division, and named in homage to bitcoin's creator, representing $^{1}/_{100000000}$ (one hundred millionth) bitcoin. 100,000 Satoshis are one mBTC.

2. Blockchain:

The bitcoin blockchain is a public ledger that records bitcoin transactions. It is implemented as a chain of blocks, each block containing a hash of the previous block up to the genesis block in the chain.

Network nodes can validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes. To achieve independent verification of the chain of ownership each network node stores its own copy of the blockchain. At varying intervals of time averaging to every 10 minutes, a new group of accepted transactions, called a block, is created, added to the blockchain, and quickly published to all nodes, without requiring central oversight. This allows bitcoin software to determine when a particular bitcoin was spent, which is needed to prevent double-spending.

Figure 1

3. Transactions:

Transactions are defined using a Forth-like scripting language. Transactions consist of one or more inputs and one or more outputs. When a user sends bitcoins, the user designates each address and the amount of bitcoin being sent to that address in an output. To prevent double spending, each input must refer to a previous unspent output in the blockchain. The use of multiple inputs corresponds to the use of multiple coins in a cash transaction. Since transactions can have multiple outputs, users can send bitcoins to multiple recipients in one transaction. As in a cash transaction, the sum of inputs (coins used to pay) can exceed the intended sum of payments. In such a case, an additional output is used, returning the change back to the payer. Any input Satoshis not accounted for in the transaction outputs become the transaction fee.

Though transaction fees are optional, miners can choose which transactions to process and prioritize those that pay higher fees. Miners may choose transactions based on the fee paid relative to their storage size, not the absolute amount of money paid as a fee. These fees are generally measured in Satoshis per byte (sat/b). The size of transactions is dependent on the number of inputs used to create the transaction, and the number of outputs.

The blocks in the blockchain were originally limited to 32 megabytes in size. The block size limit of one megabyte was introduced by Satoshi Nakamoto in 2010. Eventually the block size limit of one megabyte created problems for transaction processing, such as increasing transaction fees and delayed processing of transactions. Andreas Antonopoulos has stated Lightning Network is a potential scaling solution and referred to lightning as a second layer routing network.

4. Ownership:

In the blockchain, bitcoins are registered to bitcoin addresses. Creating a bitcoin address requires nothing more than picking a random valid private key and computing the corresponding bitcoin address. This computation can be done in a split second. But the reverse, computing the private key of a given bitcoin address, is practically unfeasible. Users can tell others or make public a bitcoin address without compromising its corresponding private key. Moreover, the number of valid private keys is so vast that it is extremely unlikely someone will compute a key-pair that is already in use and has funds. The vast number of valid private keys makes it unfeasible that brute force could be used to compromise a private key. To be able to spend their bitcoins, the owner must know the corresponding private key and digitally sign the transaction. The network verifies the signature using the public key; the private key is never revealed.

If the private key is lost, the bitcoin network will not recognize any other evidence of ownership; the coins are then unusable, and effectively lost. For example, in 2013 one user claimed to have lost 7,500 bitcoins, worth $7.5 million at the time, when he accidentally discarded a hard drive containing his private key. About 20% of all bitcoins are believed to be lost - they would have had a market value of about $20 billion at July 2018 prices.

To ensure the security of bitcoins, the private key must be kept secret. If the private key is revealed to a third party, e.g. through a data breach, the third party can use it to steal any associated bitcoins. As of December 2017, around 980,000 bitcoins have been stolen from cryptocurrency exchanges.

Regarding ownership distribution, as of 16 March 2018, 0.5% of bitcoin wallets own 87% of all bitcoins ever mined.

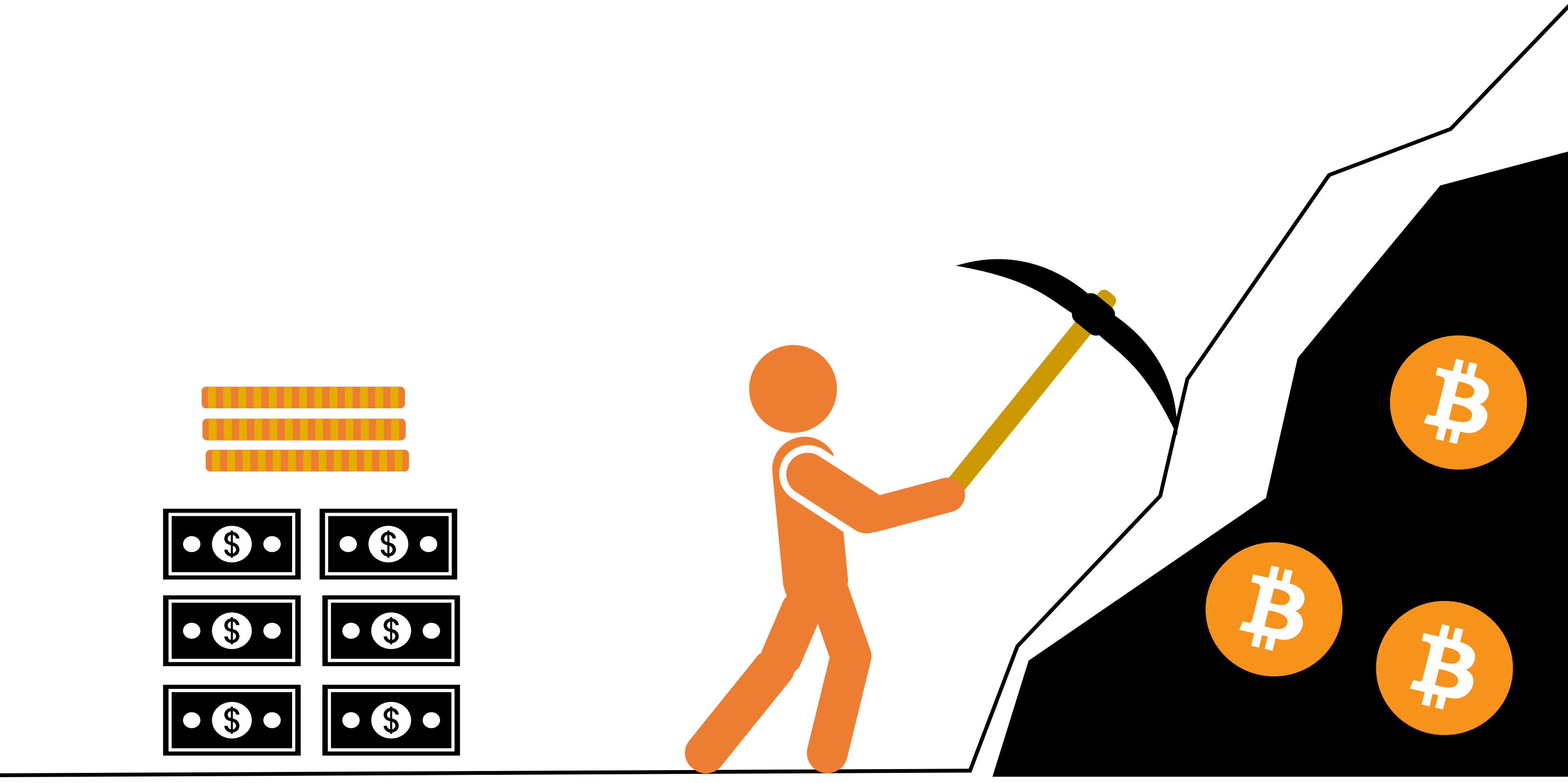
Chapter 2: Mining

Mining is a record-keeping service done through the use of computer processing power. Miners keep the blockchain consistent, complete, and unalterable by repeatedly grouping newly broadcast transactions into a block, which is then broadcast to the network and verified by recipient nodes. Each block contains a SHA-256 cryptographic hash of the previous block, thus linking it to the previous block and giving the blockchain its name.

To be accepted by the rest of the network, a new block must contain a proof-of-work (PoW). The PoW requires miners to find a number called a nonce (number used once), such that when the block content is hashed along with the nonce, the result is numerically smaller than the network's difficulty target. This proof is easy for any node in the network to verify, but extremely time-consuming to generate, as for a secure cryptographic hash, miners must try many different nonce values (usually the sequence of tested values is the ascending natural numbers: 0, 1, 2, 3, ...) before a result happens to be less than the difficulty target. Because the difficulty target is extremely small compared to a typical SHA-256 hash, block hashes have many leading zeros as can be seen in this example block hash:

0000000000000000000590fc0f3eba193a278534220b2b37e9849e1a770ca959

By adjusting this difficulty target, the amount of work needed to generate a block can be changed. Every 2,016 blocks (approximately 14 days given roughly 10 minutes per block)



Chapter 3: Supply

The successful miner finding the new block is allowed by the rest of the network to collect for themselves all transaction fees from transactions they included in the block, as well as a pre-determined reward of newly created bitcoins. As of 11 May 2020, this reward is currently 6.25 newly created bitcoins per block. To claim this reward, a special transaction called a Coinbase is included in the block, with the miner as the payee. All bitcoins in existence have been created through this type of transaction. The bitcoin protocol specifies that the reward for adding a block will be reduced by half every 210,000 blocks (approximately every four years). Eventually, the reward will round down to zero, and the limit of 21 million bitcoins[h] will be reached c. 2140; the record keeping will then be rewarded by transaction fees only.

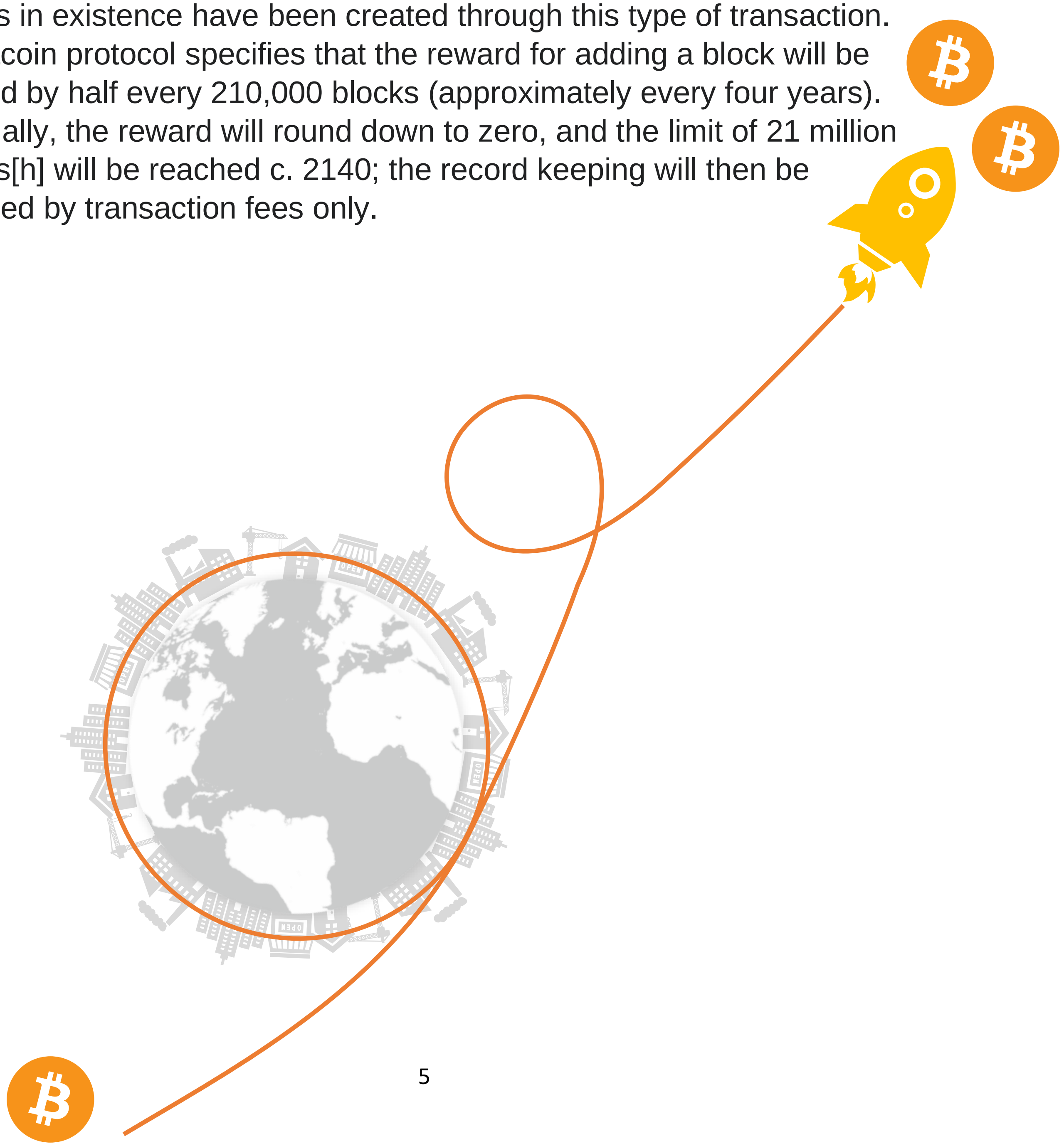


Figure 3

Chapter 4: Privacy and Fungibility

Bitcoin is pseudonymous, meaning that funds are not tied to real-world entities but rather bitcoin addresses. Owners of bitcoin addresses are not explicitly identified, but all transactions on the blockchain are public. In addition, transactions can be linked to individuals and companies through "idioms of use" (e.g., transactions that spend coins from multiple inputs indicate that the inputs may have a common owner) and corroborating public transaction data with known information on owners of certain addresses. Additionally, bitcoin exchanges, where bitcoins are traded for traditional currencies, may be required by law to collect personal information. To heighten financial privacy, a new bitcoin address can be generated for each transaction.

Wallets and similar software technically handle all bitcoins as equivalent, establishing the basic level of fungibility. Researchers have pointed out that the history of each bitcoin is registered and publicly available in the blockchain ledger, and that some users may refuse to accept bitcoins coming from controversial transactions, which would harm bitcoin's fungibility. For example, in 2012, Mt. Gox froze accounts of users who deposited bitcoins that were known to have just been stolen.

Figure 4

Chapter 5: Wallets

1. Software Wallets:

The first wallet program, simply named Bitcoin, and sometimes referred to as the Satoshi client, was released in 2009 by Satoshi Nakamoto as open-source software. In version 0.5 the client moved from the wx Widgets user interface toolkit to Qt, and the whole bundle was referred to as Bitcoin-Qt. After the release of version 0.9, the software bundle was renamed Bitcoin Core to distinguish itself from the underlying network. Bitcoin Core is, perhaps, the best-known implementation or client. Alternative clients exist, such as Parity Bitcoin.

There are several modes which wallets can operate in. They have an inverse relationship with regards to trust lessness and computational requirements.

Full clients verify transactions directly by downloading a full copy of the blockchain (over 150 GB as of January 2018). They are the most secure and reliable way of using the network, as trust in external parties is not required. Full clients check the validity of mined blocks, preventing them from transacting on a chain that breaks or alters network rules. Because of its size and complexity, downloading and verifying the entire blockchain is not suitable for all computing devices.

Lightweight clients consult full nodes to send and receive transactions without requiring a local copy of the entire blockchain. This makes lightweight clients much faster to set up and allows them to be used on low-power, low-bandwidth devices such as smartphones. When using a lightweight wallet, however, the user must trust full nodes, as it can report faulty values back to the user. Lightweight clients follow the longest blockchain and do not ensure it is valid, requiring trust in full nodes.

Third-party internet services called online wallets or web wallets offer similar functionality but may be easier to use. In this case, credentials to access funds are stored with the online wallet provider rather than on the user's hardware. As a result, the user must have complete trust in the online wallet provider. A malicious provider or a breach in server security may cause entrusted bitcoins to be stolen. An example of such a security breach occurred with Mt. Gox in 2011.

2. Cold storage:

Wallet software is targeted by hackers because of the lucrative potential for stealing bitcoins.[36] A technique called "cold storage" keeps private keys out of reach of hackers; this is accomplished by keeping private keys offline at all times by generating them on a device that is not connected to the internet. The credentials necessary to spend bitcoins can be stored offline in a number of different ways, from specialized hardware wallets to simple paper printouts of the private key.

3. Hardware Wallets:

A hardware wallet is a computer peripheral that signs transactions as requested by the user. These devices store private keys and carry out signing and encryption internally, and do not share any sensitive information with the host computer except already signed (and thus unalterable) transactions. Because hardware wallets never expose their private keys, even computers that may be compromised by malware do not have a vector to access or steal them. The user sets a passcode when setting up a hardware wallet. As hardware wallets are tamper-resistant, the passcode will be needed to extract any money.

4. Paper Wallets:

A paper wallet is created with a keypair generated on a computer with no internet connection; the private key is written or printed onto the paper and then erased from the computer. The paper wallet can then be stored in a safe physical location for later retrieval.

Physical wallets can also take the form of metal token coins with a private key accessible under a security hologram in a recess struck on the reverse side. The security hologram self-destructs when removed from the token, showing that the private key has been accessed. Originally, these tokens were struck in brass and other base metals, but later used precious metals as bitcoin grew in value and popularity. Coins with stored face value as high as ฿1000 have been struck in gold. The British Museum's coin collection includes four specimens from the earliest series of funded bitcoin tokens; one is currently on display in the museum's money gallery. In 2013, a Utahn manufacturer of these tokens was ordered by the Financial Crimes Enforcement Network (FinCEN) to register as a money services business before producing any more funded bitcoin tokens.

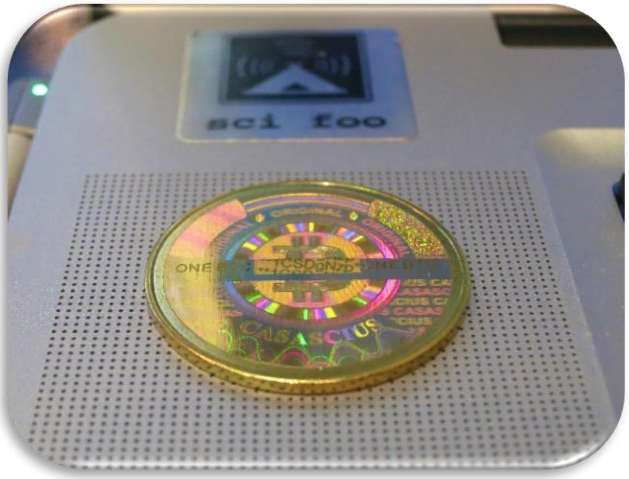


Figure 7

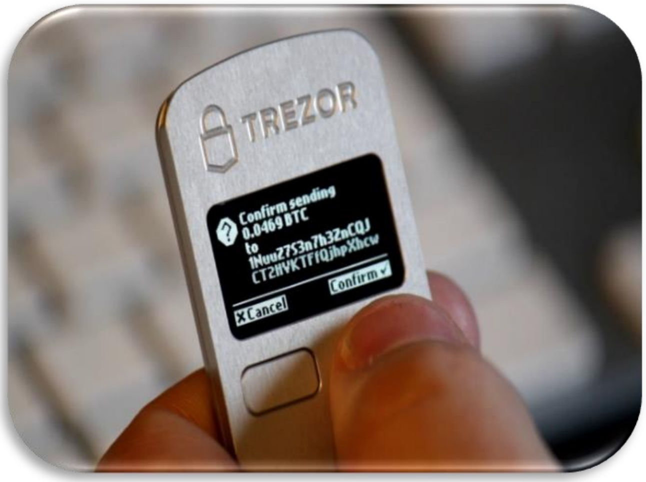


Figure 6

Figure 5

Chapter 6: History

1. 2011-2012:

After early transactions, the first major users of bitcoin were black market, such as Silk Road. During its 30 months of existence, beginning in February 2011, Silk Road exclusively accepted bitcoins as payment, transacting 9.9 million in bitcoins, worth about $214 million.

In 2011, the price started at $0.30 per bitcoin, growing to $5.27 for the year. The price rose to $31.50 on 8 June. Within a month, the price fell to $11.00. The next month it fell to $7.80, and in another month to $4.77.

In 2012, bitcoin prices started at $5.27, growing to $13.30 for the year. By 9 January the price had risen to $7.38, but then crashed by 49% to $3.80 over the next 16 days. The price then rose to $16.41 on 17 August, but fell by 57% to $7.10 over the next three days.

The Bitcoin Foundation was founded in September 2012 to promote bitcoin's development and uptake.

On 1 November 2011, the reference implementation Bitcoin-Qt version 0.5.0 was released. The software previously used for database management. Developers switched to LevelDB in release 0.8 in order to reduce blockchain sychronizartion time. The update to this release resulted in a minor blockchain fork on 11 March 2013. The fork was resolved shortly afterwards.[Seeding nodes through IRC was discontinued in version 0.8.2. From version 0.9.0 the software was renamed to Bitcoin Core. Transaction fees were reduced again by a factor of ten as a means to encourage microtransactions. Although Bitcoin Core does not use OpenSSL for the operation of the network, the software did use OpenSSL for remote procedure calls. Version 0.9.1 was released to remove the network's vulnerability to the heartblead bug .

2. 2013-2016:

In 2013, prices started at $13.30 rising to $770 by 1 January 2014

In March 2013 the blockchain temporarily split into two independent chains with different rules due to a bug in version 0.8 of the bitcoin software. The two blockchains operated simultaneously for six hours, each with its own version of the transaction history from the moment of the split. Normal operation was restored when the majority of the network downgraded to version 0.7 of the bitcoin software, selecting the backwards-compatible version of the blockchain. As a result, this blockchain became the longest chain and could be accepted by all participants, regardless of their bitcoin software version. During the split, briefly halted bitcoin deposits and the price dropped by 23% to $37 before recovering to the previous level of approximately $48 in the following hours.

The US Fiancial Crime (FinCEN) established regulatory guidelines for "decentralized virtual currencies" such as bitcoin, classifying American bitcoin miners who sell their generated bitcoins as Money Service Businesses (MSBs), that are subject to registration or other legal obligations.

In April, exchanges BitInstant and Mt. Gox experienced processing delays due to insufficient capacity resulting in the bitcoin price dropping from $266 to $76 before returning to $160 within six hours. The bitcoin price rose to $259 on 10 April, but then crashed by 83% to $45 over the next three days.

On 15 May 2013, US authorities seized accounts associated with Mt. Gox after discovering it had not registered as a money transmitter with FinCEN in the US. On 23 June 2013, the US Drug Enforcement Administration listed ₿11.02 as a seized asset in a United States Department of Justice seizure notice pursuant to 21 U.S.C. § 881. This marked the first time a government agency had seized bitcoin. The FBI seized about ₿30,000[113] in October 2013 from the dark web website Silk Road, following the arrest of Ross William Ulbricht. These bitcoins were sold at blind auction by the United States Marshals Service to venture capital investor Tim Draper. Bitcoin's price rose to $755 on 19 November and crashed by 50% to $378 the same day. On 30 November 2013, the price reached $1,163 before starting a long-term crash, declining by 87% to $152 in January 2015.

On 5 December 2013, the People's Bank of China prohibited Chinese financial institutions from using bitcoins. After the announcement, the value of bitcoins dropped, and Baidu no longer accepted bitcoins for certain services. Buying real-world goods with any virtual currency had been illegal in China since at least 2009.

In 2014, prices started at $770 and fell to $314 for the year. On 30 July 2014, the Wikimedia Foundation started accepting donations of bitcoin.[121]

In 2015, prices started at $314 and rose to $434 for the year. In 2016, prices rose and climbed up to $998 by 1 January 2017.

Release 0.10 of the software was made public on 16 February 2015. It introduced a consensus library which gave programmers easy access to the rules governing consensus on the network. In version 0.11.2 developers added a new feature which allowed transactions to be made unspendable until a specific time in the future. Bitcoin Core 0.12.1 was released on 15 April 2016, and enabled multiple soft forks to occur concurrently. Around 100 contributors worked on Bitcoin Core 0.13.0 which was released on 23 August 2016.

In July 2016, the CheckSequenceVerify soft fork activated.

In October 2016, Bitcoin Core's 0.13.1 release featured the "Segwit" soft fork that included a scaling improvement aiming to optimize the bitcoin blocksize. The patch which was originally finalised in April, and 35 developers were engaged to deploy it.] This release featured Segregated Witness (SegWit) which aimed to place downward pressure on transaction fees as well as increase the maximum transaction capacity of the network. The 0.13.1 release endured extensive testing and research leading to some delays in its release date. SegWit prevents various forms of transaction malleability.

3. 2017-2019:

Research produced by the University of Cambridge estimated that in 2017, there were 2.9 to 5.8 million unique users using a cryptocurrency wallet, most of them using bitcoin. On 15 July 2017, the controversial Segregated Witness [SegWit] software upgrade was approved ("locked-in"). Segwit was intended to support the Lightning Network as well as improve scalability.[128] SegWit was subsequently activated on the network on 24 August 2017. The bitcoin price rose almost 50% in the week following SegWit's approval. On 21 July 2017, bitcoin was trading at $2,748, up 52% from 14 July 2017's $1,835. Supporters of large blocks who were dissatisfied with the activation of SegWit forked the software on 1 August 2017 to create Bitcoin Cash, becoming one of many forks of bitcoin such as Bitcoin Gold. Prices started at $998 in 2017 and rose to $13,412.44 on 1 January 2018, after reaching its all-time high of $19,783.06 on 17 December 2017.

China banned trading in bitcoin, with first steps taken in September 2017, and a complete ban that started on 1 February 2018. Bitcoin prices then fell from $9,052 to $6,914 on 5 February 2018. The percentage of bitcoin trading in the Chinese renminbi fell from over 90% in September 2017 to less than 1% in June 2018.

Throughout the rest of the first half of 2018, bitcoin's price fluctuated between $11,480 and $5,848. On 1 July 2018, bitcoin's price was $6,343. The price on 1 January 2019 was $3,747, down 72% for 2018 and down 81% since the all-time high.

Tn September 2018, an anonymous party discovered and reported an invalid-block denial-of-server vulnerability to developers of Bitcoin Core, Bitcoin ABC and Bitcoin Unlimited. Further analysis by bitcoin developers showed the issue could also allow the creation of blocks violating the 21 million coin limit and CVE-2018-17144 was assigned Ind the issue resolved.

Bitcoin prices were negatively affected by several hacks or thefts from cryptocurrency exchanges, including thefts from Coincheck in January 2018, Bithumb in June, and Bancor in July. For the first six months of 2018, $761 million worth of cryptocurrencies was reported stolen from exchanges. Bitcoin's price was affected even though other cryptocurrencies were stolen at Coinrail and Bancor as investors worried about the security of cryptocurrency exchanges. In September 2019 the Intercontinental Exchange (the owner of the NYSE) began trading of bitcoin futures on its exchange called Bakkt. also announced that it would launch options on bitcoin in December 2019. In December 2019, YouTube removed bitcoin and cryptocurrency videos, but later restored the content after judging they had "made the wrong call."

In February 2019, Canadian cryptocurrency exchange Quadriga Fintech Solutions failed with approximately $200 million missing.[143] By June 2019 the price had recovered to $13,000.

4. Present:

On 13 March 2020, bitcoin fell below $4,000 during a broad market selloff, after trading above $10,000 in February 2020. On 11 March 2020, 281,000 bitcoins were sold, held by owners for only thirty days. This compared to ₿4,131 that had laid dormant for a year or more, indicating that the vast majority of the bitcoin volatility on that day was from recent buyers. During the week of 11 March 2020, cryptocurrency exchange Kraken experienced an 83% increase in the number of account signups over the week of bitcoin's price collapse, a result of buyers looking to capitalize on the low price. These events were attributed to the onset of the COVID-19 pandemic.

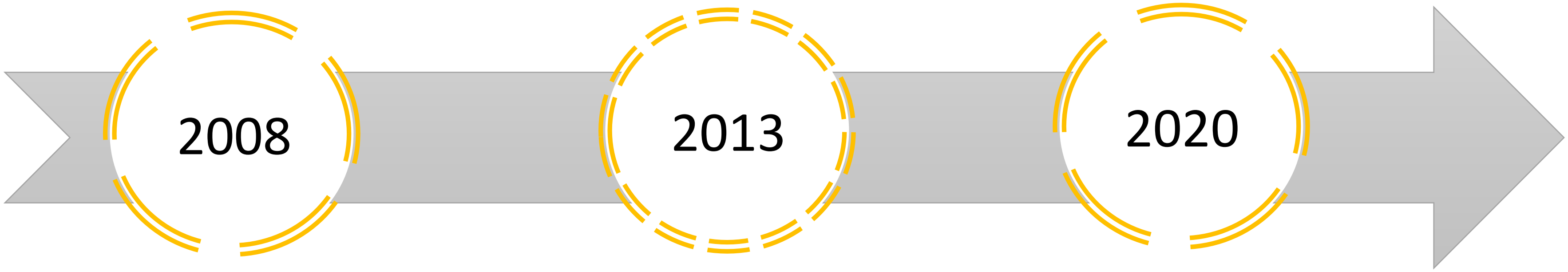
In August 2020, MicroStrategy invested $250 million in bitcoin as a treasury reserve asset. In October 2020, Square, Inc. placed approximately 1% of total assets ($50 million) in bitcoin. In November 2020, PayPal announced that US users could buy, hold, or sell bitcoin. On 30 November 2020, the bitcoin value reached a new all-time high of $19,860, topping the previous high of December 2017.Alexander Vinnik, founder of BTC-e, was convicted and sentenced to five years in prison for money laundering in France while refusing to testify during his trial. In December 2020 Massachusetts Mutual Life Insurance Company announced a bitcoin purchase of US$100 million, or roughly 0.04% of its general investment account.

On 19 January 2021, Elon Musk placed the handle *#Bitcoin* in his Twitter profile, tweeting "In retrospect, it was inevitable", which caused the price to briefly rise about $5000 in an hour to $37,299. On 25 January 2021, Microstrategy announced that it continued to buy bitcoin and as of the same date it had holdings of ₿70,784 worth $2.38 billion. On 8 February 2021 Tesla's announcement of a bitcoin purchase of US$1.5

billion and the plan to start accepting bitcoin as payment for vehicles, pushed the bitcoin price to $44,141. On 18 February 2021, Elon Musk stated that "owning bitcoin was only a little better than holding conventional cash, but that the slight difference made it a better asset to hold". After 49 days of accepting the digital currency, Tesla reversed course on 12 May 2021, saying they would no longer take Bitcoin due to concerns that "mining" the cryptocurrency was contributing to the consumption of fossil fuels and climate change. The decision resulted in the price of Bitcoin dropping around 12% on 13 May. During a July Bitcoin conference, Musk suggested Tesla could possibly help Bitcoin miners switch to renewable energy in the future and also stated at the same conference that if Bitcoin mining reaches, and trends above 50 percent renewable energy usage, that "Tesla would resume accepting bitcoin." The price for bitcoin rose after this announcement.

In September 2020, the Canton of Zug, Switzerland, announced to start to accepting tax payments in bitcoin by February 2021.

In June 2021, the Legislative Assembly of El Salvador voted legislation to make Bitcoin legal tender in El Salvador. The law took effect on 7 September. The implementation of the law has been met with protests and calls to make the currency optional, not compulsory. According to a survey by the Central American University, the majority of Salvadorans disagreed with using cryptocurrency as a legal tender, and a survey by the Center for Citizen Studies (CEC) showed that 91% of the country prefers the dollar over Bitcoin. As of October 2021, the country's government was exploring mining bitcoin with geothermal power and issuing bonds tied to bitcoin. According to a survey done by the Central American University 100 days after the Bitcoin Law came into force: 34.8% of the population has no confidence in Bitcoin, 35.3% has little confidence, 13.2% has some confidence, and 14.1% has a lot of confidence. 56.6% of respondents have downloaded the government Bitcoin wallet; among them 62.9% has never used it or only once whereas 36.3% uses Bitcoin at least once a month. In 2022, the International Monetary Fund (IMF) urged El Salvador to reverse its decision after Bitcoin lost half its value in two months. The IMF also warned that it would be difficult to get a loan from the institution.



CREATION

2008

The domain name bitcoin.org was registered

Started at 13$ until it increases to 770$

2013

MARKET

GOLDEN AGE

2020

Reached the top with a price of ~50,000$

Figure 8

Chapter 7: Economics

1. Acceptance by merchants:

- Bitcoins can be bought on digital currency exchanges.
- Per researchers, "there is little sign of bitcoin use" in international remittances despite high fees charged by banks and Western Union who compete in this market. The South China Morning Post, however, mentions the use of bitcoin by Hong Kong workers to transfer money home.
- In 2014, the National Australia Bank closed accounts of businesses with ties to bitcoin, and HSBC refused to serve a hedge fund with links to bitcoin. Australian banks in general have been reported as closing down bank accounts of operators of businesses involving the currency.
- On 10 December 2017, the Chicago Board Options Exchange started trading bitcoin futures,[204] followed by the Chicago Mercantile Exchange, which started trading bitcoin futures on 17 December 2017.
- In September 2019 the Central Bank of Venezuela, at the request of PDVSA, ran tests to determine if bitcoin and ether could be held in central bank's reserves. The request was motivated by oil company's goal to pay its suppliers.

2. As an investment:

The Winklevoss twins have purchased bitcoin. In 2013, The Washington Post reported a claim that they owned 1% of all the bitcoins in existence at the time.

Other methods of investment are bitcoin funds. The first regulated bitcoin fund was established in Jersey in July 2014 and approved by the Jersey Financial Services Commission.

Forbes named bitcoin the best investment of 2013. In 2014, Bloomberg named bitcoin one of its worst investments of the year. In 2015, bitcoin topped Bloomberg's currency tables.

According to bitinfocharts.com, in 2017, there were 9,272 bitcoin wallets with more than $1 million worth of bitcoins. The exact number of bitcoin millionaires is uncertain as a single person can have more than one bitcoin wallet.

In August 2020, MicroStrategy invested in Bitcoin. In May 2021, the Bitcoin's market share on exchanges dropped from 70% to 45% as investors pursued altcoins.

Chapter 8: Criticisms

1. Economics concern:

Bitcoin, along with other cryptocurrencies, has been described as an economic bubble by at least eight Nobel Memorial Prize in Economic Sciences laureates at various times, including Robert Shiller on 1 March 2014, Joseph Stiglitz on 29 November 2017, and Richard Thaler on 21 December 2017. On 29 January 2018, a noted Keynesian economist Paul Krugman has described bitcoin as "a bubble wrapped in techno-mysticism inside a cocoon of libertarian ideology, on 2 February 2018, professor Nouriel Roubini of New York University has called bitcoin the "mother of all bubbles", and on 27 April 2018, a University of Chicago economist James Heckman has compared it to the 17th-century tulip mania.

Journalists, economists, investors, and the central bank of Estonia have voiced concerns that bitcoin is a Ponzi scheme. In April 2013, Eric Posner, a law professor at the University of Chicago, stated that "a real Ponzi scheme takes fraud; bitcoin, by contrast, seems more like a collective delusion." A July 2014 report by the World Bank concluded that bitcoin was not a deliberate Ponzi scheme. In June 2014, the Swiss Federal Council examined concerns that bitcoin might be a pyramid scheme, and concluded that "since in the case of bitcoin the typical promises of profits are lacking, it cannot be assumed that bitcoin is a pyramid scheme."

2. Energy consumption:

Bitcoin has been criticized for the amount of electricity consumed by mining.

As of 2015, estimated combined electricity consumption attributed to mining was 166.7 megawatts and by 2017, was estimated to be between one and four gigawatts of electricity. In 2018, bitcoin was estimated to use 2.55 to 3.572 GW, or around 6% of the total power consumed by the global banking sector. In July 2019 BBC reported bitcoin consumes about 7 gigawatts, 0.2% of the global total, or equivalent to that of Switzerland.[275] A 2021 estimate from the University of Cambridge suggests bitcoin consumes more than 178 (TWh) annually, ranking it in the top 30 energy consumers if it were a country.

Bitcoin is mined in places like Iceland where geothermal energy is cheap and cooling Arctic air is free. Bitcoin miners are known to use hydroelectric power in Tibet, Quebec, Washington (state), and Austria to reduce electricity costs. Miners are attracted to suppliers such as Hydro Quebec that have energy surpluses.

According to a University of Cambridge study, much of bitcoin mining is done in China, where electricity is subsidized by the government. A significant part of Bitcoin mining is powered by cheap electricity in Xinjiang, which mostly comes from coal power. In April 2021 a coal mine explosion in the province coincided with a 35% drop in hashing power and a flash crash in price. In other provinces, such as Hunan and Sichuan, mining farms use more hydropower, however these account for at most 4% of hash power. According to Alex de Vries, renewable energy is not a good match for Bitcoin mining as 24/7 operations are best for ROI on mining devices. In 2021, a US company purchased the Greenridge coal power plant and converted it to burn natural gas for the sole purpose of mining bitcoin, which has proven to be highly profitable, in spite of protests of local residents against air pollution and thermal pollution in the nearby Seneca lake.

Concerns about bitcoin's environmental impact relate bitcoin's energy consumption to carbon emissions. The difficulty of translating the energy consumption into carbon emissions lies in the decentralized nature of bitcoin impeding the localization of miners to examine the electricity mix used. The results of recent studies analyzing bitcoin's carbon footprint vary. A study published in Nature Climate Change in

2018 claims that bitcoin "could alone produce enough CO2 emissions to push warming above 2 °C within less than three decades." However, other researchers criticized this analysis, arguing the underlying scenarios were inadequate, leading to overestimations. According to studies published in Joule and American Chemical Society in 2019, bitcoin's annual energy consumption results in annual carbon emission ranging from 17to 22.9 MtCO2 which is comparable to the level of emissions of countries as Jordan and Sri Lanka or Kansas City. George Kamiya, writing for the International Energy Agency, says that "predictions about bitcoin consuming the entire world's electricity" are sensational, but that the area "requires careful monitoring and rigorous analysis".

3. Use in illegal transactions:

Bitcoin held at exchanges are vulnerable scamming, and hacking. As of December 2017, around 980,000 bitcoins have been stolen from cryptocurrency exchanges. The use of bitcoin by criminals has attracted the attention of financial regulators, legislative bodies, law enforcement, and the media. Bitcoin gained early notoriety for its use on the Silk Road. The U.S. Senate held a hearing on virtual currencies in November 2013. The U.S. government claimed that bitcoin was used to facilitate payments related to Russian interference in the 2016 United States elections. Several news outlets have asserted that the popularity of bitcoins hinges on the ability to use them to purchase illegal goods. Nobel-prize winning economist Joseph Stiglitz says that bitcoin's anonymity encourages money laundering and other crimes. In 2014, researchers at the University of Kentucky found "robust evidence that computer programming enthusiasts and illegal activity drive interest in bitcoin, and find limited or no support for political and investment motives”. Australian researchers have estimated that 25% of all bitcoin users and 44% of all bitcoin transactions are associated with illegal activity as of April 2017.

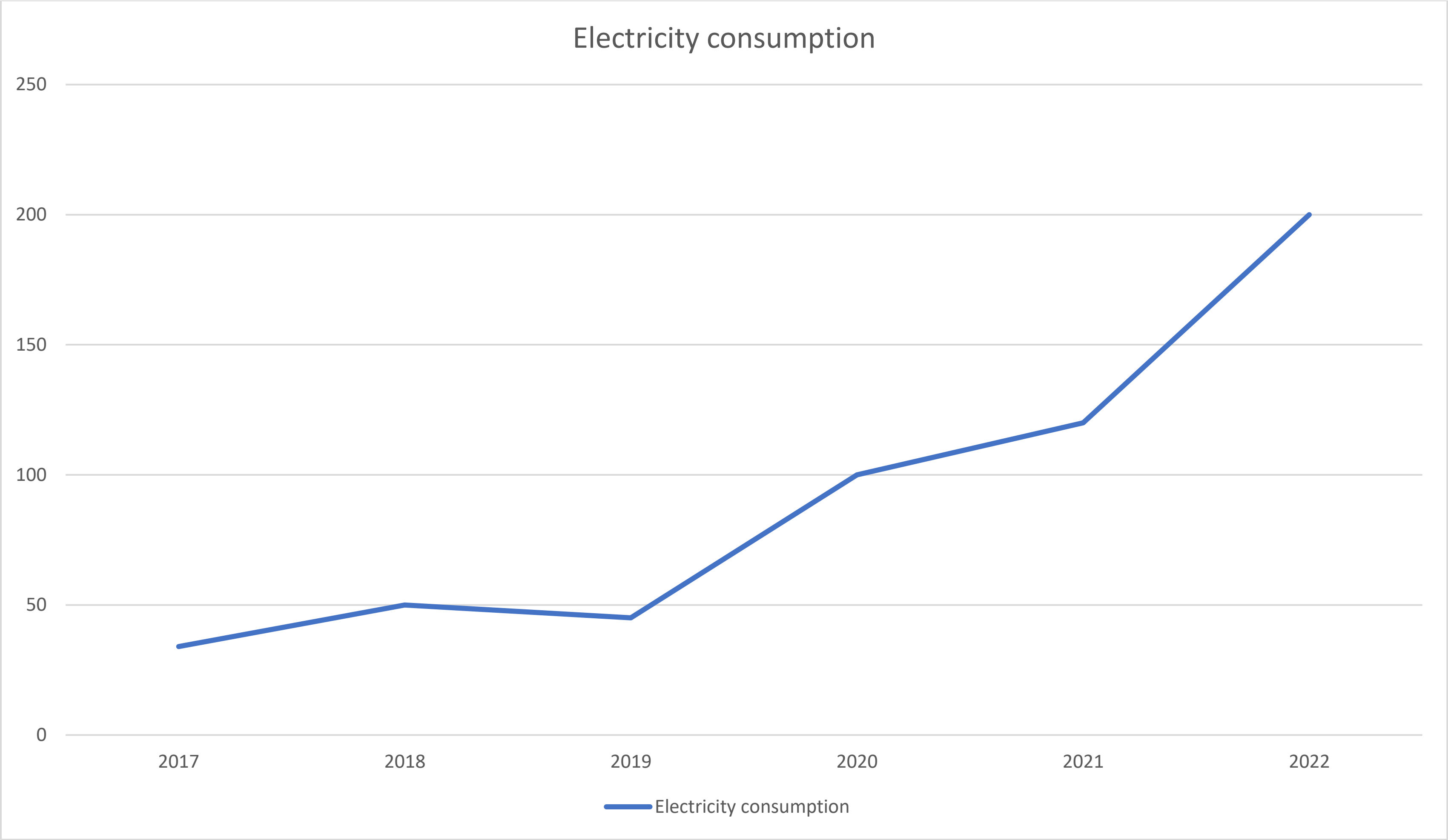


Figure 9

Electricity consumption (TWh)

Chapter 9: Decentralization

Bitcoin is decentralized thus:

- Bitcoin does not have a central authority.
- The bitcoin network is peer-to-peer, without central servers.
- The network also has no central storage; the bitcoin ledger is distributed.
- The ledger is public; anybody can store it on a computer
- There is no single administrator; the ledger is maintained by a network of equally privileged miners.
- Anyone can become a miner.
- The additions to the ledger are maintained through competition. Until a new block is added to the ledger, it is not known which miner will create the block
- The issuance of bitcoins is decentralized. They are issued as a reward for the creation of a new block.
- Anybody can create a new bitcoin address (a bitcoin counterpart of a bank account) without needing any approval.
- Anybody can send a transaction to the network without needing any approval; the network merely confirms that the transaction is legitimate.

Conversely, researchers have pointed out at a "trend towards centralization". Although bitcoin can be sent directly from user to user, in practice intermediaries are widely used. Bitcoin miners join large mining pools to minimize the variance of their income. Because transactions on the network are confirmed by miners, decentralization of the network requires that no single miner or mining pool obtains 51% of the hashing power, which would allow them to double-spend coins, prevent certain transactions from being verified and prevent other miners from earning income. As of 2013 just six mining pools controlled 75% of overall bitcoin hashing power. In 2014 mining pool Ghash.io obtained 51% hashing power which raised significant controversies about the safety of the network. The pool has voluntarily capped their hashing power at 39.99% and requested other pools to act responsibly for the benefit of the whole network. Around the year 2017, over 70% of the hashing power and 90% of transactions were operating from China.

Chapter 10: Software implementation

Bitcoin Core is free and open-source software that serves as a bitcoin node (the set of which form the bitcoin network) and provides a bitcoin wallet which fully verifies payments. It is considered to be bitcoin's reference implementation. Initially, the software was published by Satoshi Nakamoto under the name "Bitcoin", and later renamed to "Bitcoin Core" to distinguish it from the network. It is also known as the *Satoshi client*.

The MIT Digital Currency Initiative funds some of the development of Bitcoin Core.] The project also maintains the cryptography library libsecp256k1.

Bitcoin Core includes a transaction verification engine and connects to the bitcoin network as a full node. Moreover, a cryptocurrency wallet, which can be used to transfer funds, is included by default. The wallet allows for the sending and receiving of bitcoins. It does not facilitate the buying or selling of bitcoin. It allows users to generate QR codes to receive payment.

The software validates the entire blockchain, which includes all bitcoin transactions ever. This distributed ledger which has reached more than 235 gigabytes in size as of Jan 2019, must be downloaded or synchronized before full participation of the client may occur. Although the complete blockchain is not needed all at once since it is possible to run in pruning mode. A command line-based daemon with a JSON-RPC interface, bitcoin, is bundled with Bitcoin Core. It also provides access to testnet, a global testing environment that imitates the bitcoin main network using an alternative blockchain where valueless "test bitcoins" are used. Regtest or Regression Test Mode creates a private blockchain which is used as a local testing environment. Finally, bitcoin-cli, a simple program which allows users to send RPC commands to bitcoind, is also included.

Checkpoints which have been hard coded into the client are used only to prevent Denial of Service attacks against nodes which are initially syncing the chain. For this reason the checkpoints included are only as of several years ago. A one megabyte block size limit was added in 2010 by Satoshi Nakamoto. This limited the maximum network capacity to about three transactions per second. Since then, network capacity has been improved incrementally both through block size increases and improved wallet behavior. A network alert system was included by Satoshi Nakamoto as a way of informing users of important news regarding bitcoin. In November 2016 it was retired. It had become obsolete as news on bitcoin is now widely disseminated.

Bitcoin Core includes a scripting language inspired by Forth that can define transactions and specify parameters. Script Pub Key is used to "lock" transactions based on a set of future conditions. Script Sig is used to meet these conditions or "unlock" a transaction. Operations on the data are performed by various Codes. Two stacks are used - main and alt. Looping is forbidden.

Bitcoin Core uses Open Timestamps to timestamp merge commits.

Table 1

The original creator of the bitcoin client has described their approach to the software's authorship as it being written first to prove to themselves that the concept of purely peer-to-peer electronic cash was valid and that a paper with solutions could be written. The lead developer is Wladimir J. van der Laan, who took over the role on 8 April 2014. Gavin Andresen was the former lead maintainer for the software client.

Construct	Composite reliability	Cronbach's alpha	Av
Intention to use	0.898	0.897	0.814
Social Influence	0.96	0.97	0.955
Facilitating condition	0.962	0.978	0.95
Financial literacy	0.852	0.876	0.87

Chapter 11: Legal Status

Because of bitcoin's decentralized nature and its trading on online exchanges located in many countries, regulation of bitcoin has been difficult. However, the use of bitcoin can be criminalized, and shutting down exchanges and the peer-to-peer economy in a given country would constitute a de facto ban. The legal status of bitcoin varies substantially from country to country and is still undefined or changing in many of them. Regulations and bans that apply to bitcoin probably extend to similar cryptocurrency systems.

According to the Library of Congress, an "absolute ban" on trading or using cryptocurrencies applies in nine countries: Algeria, Bolivia, Egypt, Iraq, Morocco, Nepal, Pakistan, Vietnam, and the United Arab Emirates. An "implicit ban" applies in another 15 countries, which include Bahrain, Bangladesh, China, Colombia, the Dominican Republic, Indonesia, Kuwait, Lesotho, Lithuania, Macau, Oman, Qatar, Saudi Arabia and Taiwan.

In October 2020, the Islamic Republic News Agency announced pending regulations that would require bitcoin miners in Iran to sell bitcoin to the Central Bank of Iran, and the central bank would use it for imports. Iran, as of October 2020, had issued over 1,000 bitcoin mining licenses. The Iranian government initially took a stance against cryptocurrency, but later changed it after seeing that digital currency could be used to circumvent sanctions. The US Office of Foreign Assets Control listed two Iranians and their bitcoin addresses as part of its Specially Designated Nationals and Blocked Persons List for their role in the 2018 Atlanta cyberattack whose ransom was paid in bitcoin.

The U.S. Commodity Futures Trading Commission has issued four "Customer Advisories" for bitcoin and related investments. A July 2018 warning emphasized that trading in any cryptocurrency is often speculative, and there is a risk of theft from hacking, and fraud. In May 2014 the U.S. Securities and Exchange Commission warned that investments involving bitcoin might have high rates of fraud, and that investors might be solicited on social media sites. An earlier "Investor Alert" warned about the use of bitcoin in Ponzi schemes.

The European Banking Authority issued a warning in 2013 focusing on the lack of regulation of bitcoin, the chance that exchanges would be hacked, the volatility of bitcoin's price, and general fraud. FINRA and the North American Securities Administrators Association have both issued investor alerts about bitcoin

U.S. Commodity Futures Trading Commission has issued four "Customer Advisories" for bitcoin and related investments. A July 2018 warning emphasized that trading in any cryptocurrency is often speculative, and there is a risk of theft from hacking, and fraud. In May 2014 the U.S. Securities and Exchange Commission warned that investments involving bitcoin might have high rates of fraud, and that investors might be solicited on social media sites. An earlier "Investor Alert" warned about the use of bitcoin in Ponzi schemes. The European Banking Authority issued a warning in 2013 focusing on the lack of regulation of bitcoin, the chance that exchanges would be hacked, the volatility of bitcoin's price, and general fraud.

Figure 10

Chapter 12: Associated Ideologies

Satoshi Nakamoto stated in his white paper that: "The root problem with conventional currencies is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.

1. Austrian economics roots

According to the European Central Bank, the decentralization of money offered by bitcoin has its theoretical roots in the Austrian school of economics, especially with Friedrich von Hayek in his book *Denationalization of Money: The Argument Refined*, in which Hayek advocates a complete free market in the production, distribution and management of money to end the monopoly of central banks.

2. Anarchism and libertarianism

According to *The New York Times*, libertarians and anarchists were attracted to the philosophical idea behind bitcoin. Early bitcoin supporter Roger Ver said: "At first, almost everyone who got involved did so for philosophical reasons. We saw bitcoin as a great idea, as a way to separate money from the state." *The Economist* describes bitcoin as "a techno-anarchist project to create an online version of cash, a way for people to transact without the possibility of interference from malicious governments or banks". Economist Paul Krugman argues that cryptocurrencies like bitcoin are "something of a cult" based in "paranoid fantasies" of government power.

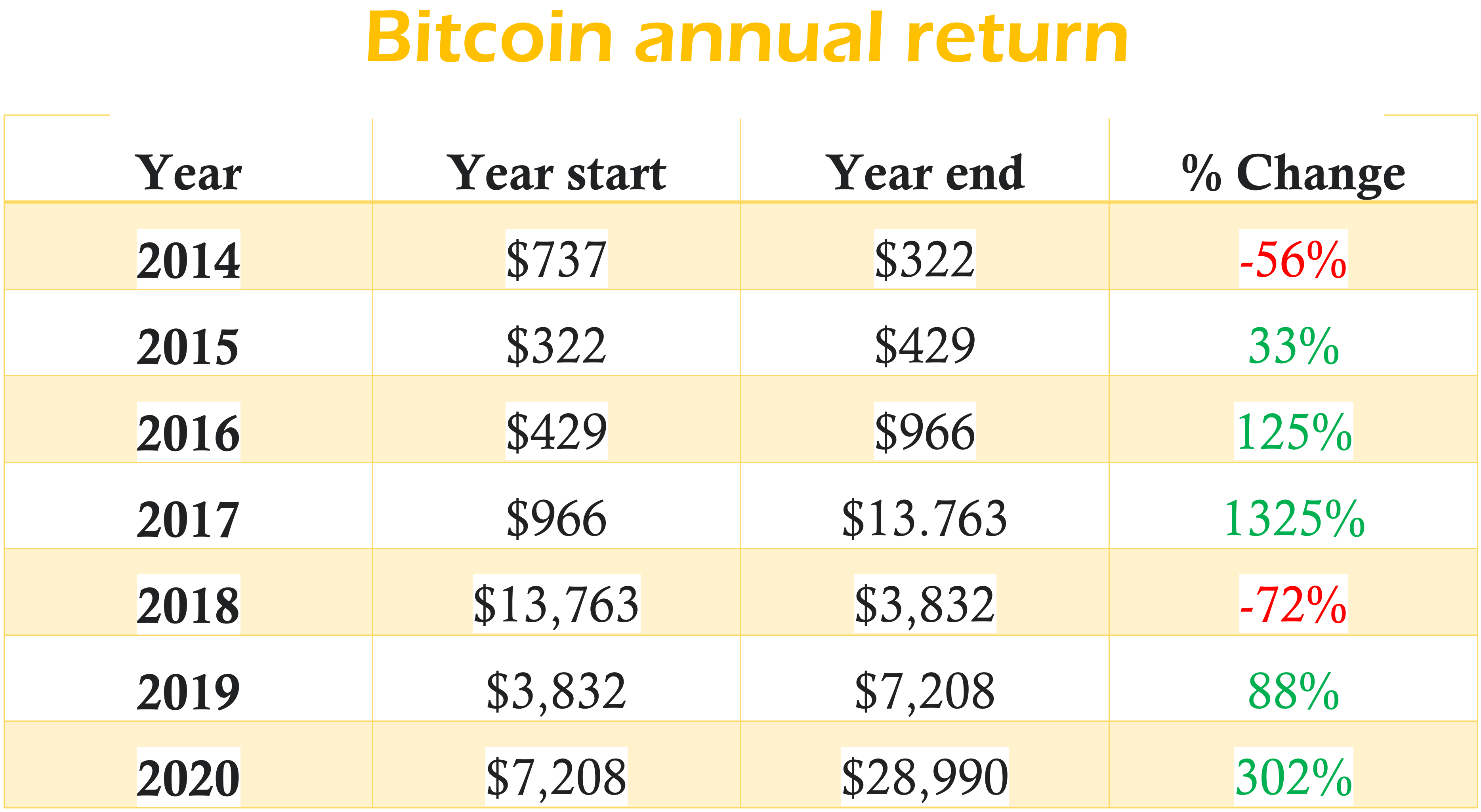
Nigel Dodd argues in *The Social Life of Bitcoin* that the essence of the bitcoin ideology is to remove money from social, as well as governmental, control.[191] Dodd quotes a YouTube video, with Roger Ver, Jeff Berwick, Charlie Shrem, Andreas Antonopoulos, Gavin Wood, Trace Meyer and other proponents of bitcoin reading *The Declaration of Bitcoin's Independence.* The declaration includes a message of crypto-anarchism with the words: "Bitcoin is inherently anti-establishment, anti-system, and anti-state. Bitcoin undermines governments and disrupts institutions because bitcoin is fundamentally humanitarian.

David Golumbia says that the ideas influencing bitcoin advocates emerge from right-wing extremist movements such as the Liberty Lobby and the John Birch Society and their anti-Central Bank rhetoric, or, more recently, Ron Paul and Tea Party-style libertarianism. Steve Bannon, who owns a "good stake" in bitcoin, considers it to be "disruptive populism. It takes control back from central authorities. It's revolutionary.

Figure 11

Chapter 13: Returns

The return obtained from bitcoin cryptocurrency is compared to other investment instruments, namely stock returns, gold and the rupiah exchange rate. The research period was carried out based on research data from 2011 to 2020. This study employee compares means test and analysis of variance on rate of return of bitcoin investment. The bitcoin return compare to the rate of return form the others investments instruments namely exchange rate, gold and stock. The study collected 120 data of each investments instruments: bitcoin, exchange rate, gold and stock from various of sources during 2011–2020. Then, we calculate the return and risk of individual investment instruments. The results showed that the bitcoin currency had the highest rate of return 18% with a standard deviation of 61% compared to exchange rate, gold and stock returns. While the rate of return for the others investment instruments showed less than 0.5% with standard deviation less than 5%.



Bitcoin annual return

Year	Year start	Year end	% Change
2014	$737	$322	-56%
2015	$322	$429	33%
2016	$429	$966	125%
2017	$966	$13.763	1325%
2018	$13,763	$3,832	-72%
2019	$3,832	$7,208	88%
2020	$7,208	$28,990	302%

Table 2

Conclusion

Bitcoin's value has on balance risen substantially in recent months, despite large fluctuations. These fluctuations have attracted much attention from various sides. It appears that opinions on the future of this cryptocurrency are strongly divided. Most economists often take a different view on Bitcoin than people in the crypto world. The latter group emphasize the innovation that Bitcoin (more specifically the blockchain) brings, while economists often see Bitcoin as a bubble, with characteristics of a Ponzi scheme and underpinned by spectacular, but poorly founded economic claims. Most people have above all successful. So far, despite its success, the fluctuations of the Bitcoin price have no economic effect many questions. Bitcoin is not the money of the future and certainly not a future 'world money'. Because as we saw in this report there is no such a way to keep your money, to guarantee them if you take the risk, you may win you might lose and because of its uncertainty bitcoin might have a huge value but never used as a worldwide stable currency. If it survives, which it may, it will probably be as a high-risk asset class. As such, it may strongly increase in value in the future, but it could just as easily go the other way and end up valueless. Finally, Bitcoin faces a slightly contradictory threat, namely, that it could become too at all. Neither its increase by a staggering 500% in less than a half year nor its following fall by 30% has left any traces in the real economy. So-called wealth-effects were not visible. From a stability point of view, Bitcoin is not very relevant. But this may change if more and more people would invest substantial parts of their wealth in an ever more expensive Bitcoin.

References

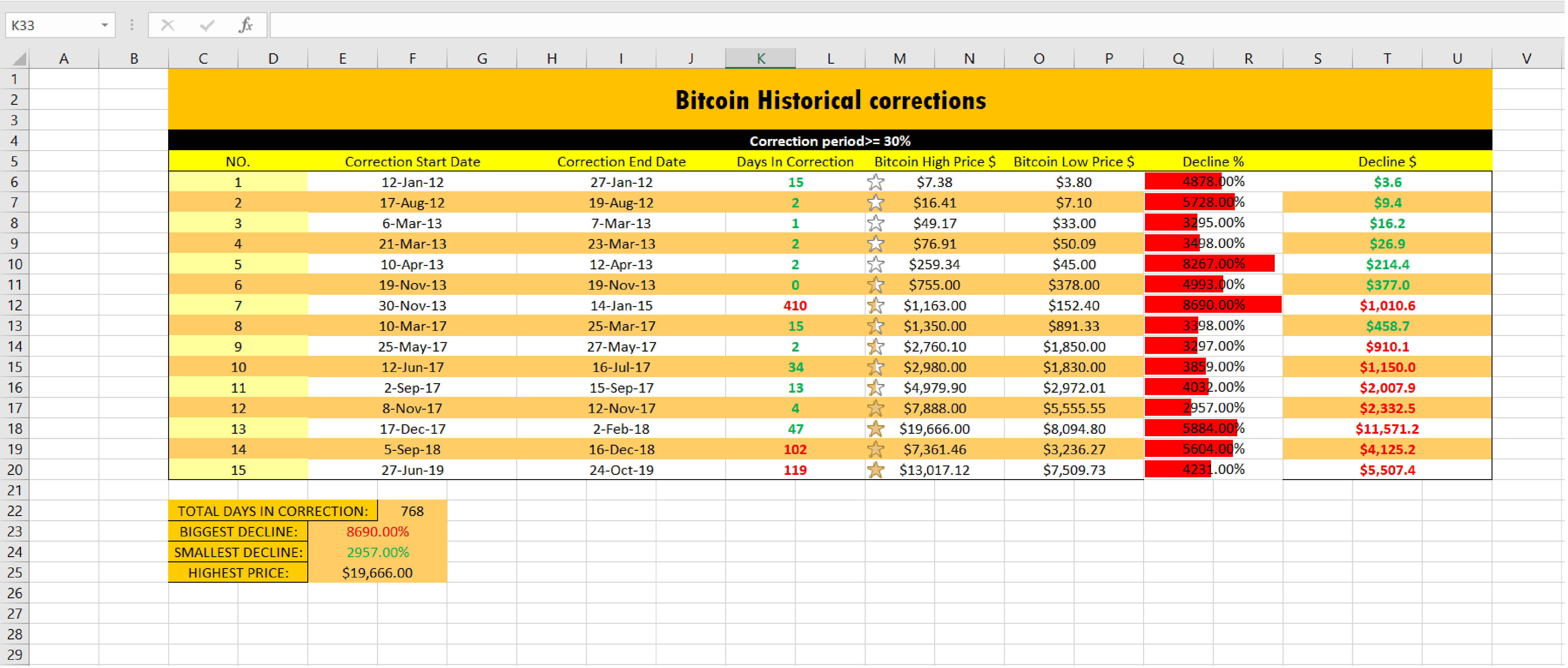
Anon., n.d. *BBC.* [Online]
Available at: https://www.bbc.co.uk/newsround/25622442

Anon., n.d. buisness insiders. [Online]
Available at: https://markets.businessinsider.com/news/currencies/bitcoin-limited-real-use-volatility-speculative-bubble-ubs-wealth-management-2021-3

Anon., n.d. Investopedia. [Online]
Available at: https://www.investopedia.com/terms/b/bitcoin.asp

Anon., n.d. Wikipedia. [Online]
Available at: https://en.wikipedia.org/wiki/Bitcoin

Excel Information:



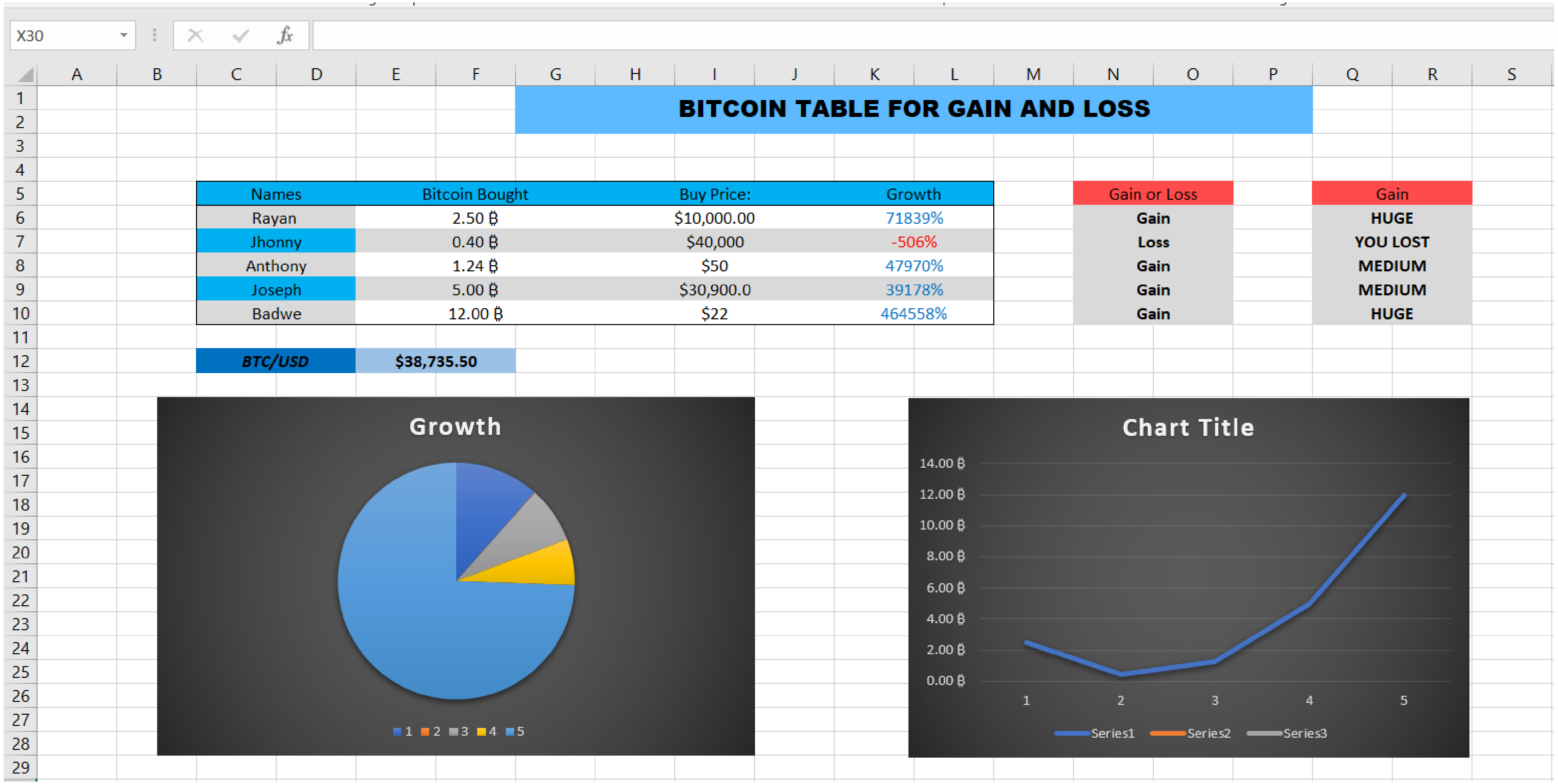
Bitcoin Historical corrections

Correction period>= 30%

NO.	Correction Start Date	Correction End Date	Days In Correction		Bitcoin High Price $	Bitcoin Low Price $	Decline %	Decline $
1	12-Jan-12	27-Jan-12	15	☆	$7.38	$3.80	4878.00%	$3.6
2	17-Aug-12	19-Aug-12	2	☆	$16.41	$7.10	5728.00%	$9.4
3	6-Mar-13	7-Mar-13	1	☆	$49.17	$33.00	3295.00%	$16.2
4	21-Mar-13	23-Mar-13	2	☆	$76.91	$50.09	3498.00%	$26.9
5	10-Apr-13	12-Apr-13	2	☆	$259.34	$45.00	8267.00%	$214.4
6	19-Nov-13	19-Nov-13	0	☆	$755.00	$378.00	4993.00%	$377.0
7	30-Nov-13	14-Jan-15	410	☆	$1,163.00	$152.40	8690.00%	$1,010.6
8	10-Mar-17	25-Mar-17	15	☆	$1,350.00	$891.33	3398.00%	$458.7
9	25-May-17	27-May-17	2	☆	$2,760.10	$1,850.00	3297.00%	$910.1
10	12-Jun-17	16-Jul-17	34	☆	$2,980.00	$1,830.00	3859.00%	$1,150.0
11	2-Sep-17	15-Sep-17	13	☆	$4,979.90	$2,972.01	4032.00%	$2,007.9
12	8-Nov-17	12-Nov-17	4	☆	$7,888.00	$5,555.55	2957.00%	$2,332.5
13	17-Dec-17	2-Feb-18	47	★	$19,666.00	$8,094.80	5884.00%	$11,571.2
14	5-Sep-18	16-Dec-18	102	★	$7,361.46	$3,236.27	5604.00%	$4,125.2
15	27-Jun-19	24-Oct-19	119	★	$13,017.12	$7,509.73	4231.00%	$5,507.4

TOTAL DAYS IN CORRECTION:	768
BIGGEST DECLINE:	8690.00%
SMALLEST DECLINE:	2957.00%
HIGHEST PRICE:	$19,666.00

Figure 12



BITCOIN TABLE FOR GAIN AND LOSS

Names	Bitcoin Bought	Buy Price:	Growth	Gain or Loss	Gain
Rayan	2.50 ฿	$10,000.00	71839%	**Gain**	**HUGE**
Jhonny	0.40 ฿	$40,000	-506%	**Loss**	**YOU LOST**
Anthony	1.24 ฿	$50	47970%	**Gain**	**MEDIUM**
Joseph	5.00 ฿	$30,900.0	39178%	**Gain**	**MEDIUM**
Badwe	12.00 ฿	$22	464558%	**Gain**	**HUGE**

BTC/USD **$38,735.50**

Figure 13

Appendix:

Sheet1:

- = ROUNDDOWN(S6/M6*100,2)
- =ROUNDUP(M6-O6,1)
- =MAX(Q6:R20)
- =SUM(K6:K20)
- =MIN(Q6:R20)
- =MAX(M6:N20)
- CONDITIONAL FORMATTING (Stars, Bars, Color Change)

Sheet2:

- =(E6*$E$12-H6*E6)/100 (Simple calculation)
- =IF(K6>0,"Gain","Loss") (For Gain and Loss)
- =IF(K6>=50000%,"HUGE",IF(K6>=10000%,"MEDIUM",IF(K6>=0%,"SMALL","YOU LOST"))) (Nested if)