Technology Review of Bitcoin

Zhimin Sun
903520402
zhimin.sun@gatech.edu

Abstract. In this technology review, I will review the hot topic Bitcoin. Bitcoin is a peer-to-peer decentralized electronic cash system based on cryptography. It’s a product derived from the development of internet. I will introduce the motivation of Bitcoin, advantages of Bitcoin compared to the traditional electronic cash system, the technical components in Bitcoin and economics behind Bitcoin as well. The target audiences of this technology review are my peers or classmates who have univ education but non-cs major.

1. Introduction

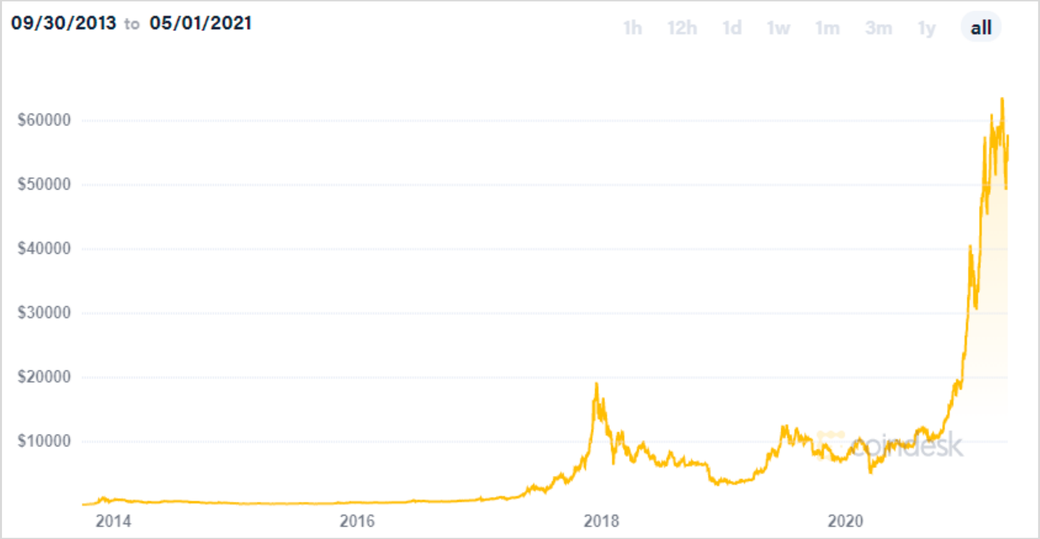
I choose Bitcoin as the topic to review because it is kind of hot topic recently and some friends around me have several questions about it. It is a little bit mysterious to them who are not CS major or not have related experience before.

To introduce Bitcoin, we must mention the person named Satoshi Nakamoto. Satoshi Nakamoto is the name used by the anonymous person who came up with Bitcoin and authored the Bitcoin white paper. We don’t know his real identity in the real world yet. There were some people claiming or be claimed to be Nakamoto, but no one could verify it. Bitcoin is invented in 2008 and firstly began to use in 2009. To describe Bitcoin shortly, we could describe it as a peer-to-peer, decentralized, cryptography based electronic cash system. I will firstly introduce the development history of Bitcoin, then the technology used in Bitcoin, and the current state of Bitcoin, so that we could have a whole comprehensive view and understanding of Bitcoin.

2. Development history of Bitcoin

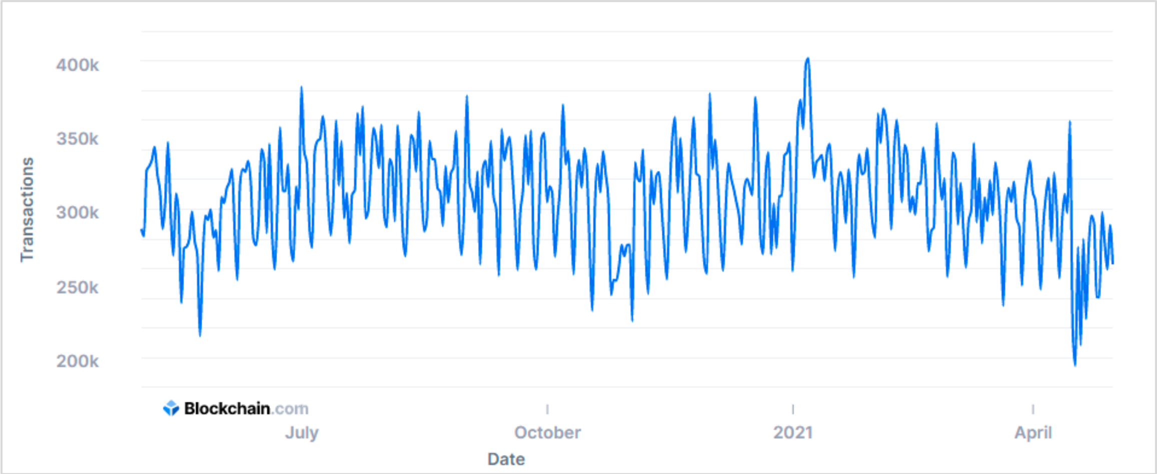
The domain name bitcoin.org was registered in 2008 and later on Satoshi Nakamoto released the bitcoin white paper. Satoshi integrated several existing ideas in the cryptography field into Bitcoin and take Bitcoin as a new kind of electronic transaction system based on cryptography instead of trust-based model. Bitcoin network came into existence in 2009. And Hal Fenney and Wei Dai are two of the early supporters of Bitcoin. Bitcoin has limitations of

The unit of account of Bitcoin is one bitcoin, typically represented by BTC. The price change of bitcoin over these years are in the chart below. As we can see, price of bitcoin has a huge leap in recent two or three years.



Data source: coindesk.com

Number of confirmed transactions per day are in the chart below. In the past half year, the number of transactions does not have much variations. It's about 30 transactions per minute.



Data source: Blockchain.com

You may ask that how can you own a bitcoin or make transactions of bitcoin? There are several ways to own a bitcoin. Firstly, we can buy bitcoin from other people or take bitcoin as payment method. Secondly, we could do bitcoin mining. We can send, receive and store bitcoin using digital wallet application which are free to download and use. I will introduce the math and theory behind the bitcoin transactions and mining shortly.

3. Technology used in Bitcoin

In the traditional transaction electronic system, there is a third trusted party, normally is the financial institutions who take charge of reviewing and processing our transactions. The existence of the third party brings some problems: 1) firstly, the financial instructions' work increases the transaction cost; 2) the transaction cannot be flexible as it should be, because the existence of the third party's mediation; 3) Since the traditional transaction system allows for the reversible payment, the merchants have to collect more information from their customers to avoid unnecessary loss.

To eliminate the weakness of the trusted based transaction system, Bitcoin was proposed as a peer-to-peer transaction system where those financial institutions do not exist. Digital signature is the technology used in Bitcoin to avoid using the third party. Besides, Bitcoin solves the double-spending problem using the peer-to-peer network. I will describe how the digital signature used here firstly, and then talk about the double-spending problem.

a. Digital signature

Bitcoin is based on the Elliptic Curve Digital Signature Algorithm (ECDSA). The formula of Elliptic curve is $y^2 = x^3 + ax + b\ (a = 0, b = 7, in\ Bitcoin\ version)$. There are two important properties we need to know existed in the elliptic curve: ① A non-vertical line intersecting two non-tangent points will always intersect with third point; ② A non-vertical line intersecting one tangent point will always intersect with the second point.

Based on those two properties in elliptic curve, we also need to know two operations:
① point addition: $P + Q = R$,
R is the reflection point through xaxis of the third intersection point R$'$.
Using point addition to find r is defined as:

$$c = \frac{q_y - p_y}{q_x - p_x}, r_x = c^2 - p_x - q_x, r_y = c(p_x - r_x) - p_y$$

② point doubling: $P + P = R$,
R is the reflection point through xaxis of the second intersection point R$'$.
Using point doubling to find r is defined as:

$$c = \frac{3{p_x}^2 + a}{2p_y}, r_x = c^2 - 2p_x, r_y = c(p_x - r_x) - p_y$$

With those two operations, we could do the scalar multiplication using the combination of point addition and point doubling.

b. Finite Field

Another terminology we need know is finite field. The results of each calculation must fall within the finite field. For example, finite field modulo 13, then all mod operation results will fall within range 0-12. In the context of finite field, the shape of the elliptic curve may change, but the two properties existed in elliptic curve we talked through above still work in the finite field.

Overall, bitcoin can be seen as a protocol with a set of specific parameters for the elliptic curve in the context of finite field. The set of specific parameters of bitcoin protocol are: elliptic curve: $y^2 = x^3 + y, (where\ a = 0, b = 7)$; prime modulo = $2^{256} - 2^{32} - 977$; Based point and Order. The elliptic curve with those specific parameters is called secp256k1 algorithm.

c. Public Key and Private Key

Next important thing we need to know is the public keys and the private keys. Owner signs data with the private key and payee verify the signature the public key. We can deduce the public key from the public key: $public\ key = private\ key * base\ point$. For example, the private key is 2. Then we can calculate the public key using point doubling.

Take some small numbers for a simple example, equation: $y^2 = x^3 + 7$, prime modulo: 67, base point: (2, 22), order: 79, private key: 2.
Then $Public\ key = 2 * (2,22) = (2, 22) + (2, 22)$, to calculate using point doubling:

$$c = \frac{3{p_x}^2 + a}{2p_y} = \frac{3*2^2+0}{2*22} mod\ 67 = \frac{12}{44} mod\ 67.$$

Here we need to introduce another definition: the number b is inverse of a mod N
if a•b ≡ 1(mod N). Notation: b will be represented as a^{-1}. The inverse of a modulo can be calculated with the Extended Euclidean algorithm. I won’t expand the details about this algorithm here.
Here, in this situation, the result of $44^{-1} mod\ 67\ is\ 32$.
Thus, through point doubling, we can get,

$$c = \frac{12}{44} mod\ 67 = 12 * 32\ mod\ 67 = 49.$$

$$r_x = c^2 - 2p_x = (49^2 - 2 * 2) mod\ 67 = 52$$

$$r_y = c(p_x - r_x) - p_y = (49(2 - 52) - 22) mod\ 67 = 7$$

Thus, we can get the public key is (52, 7), given the private key 2.

However, deducing private key from public key is computationally impossible in the actual cryptography environments with enormous parameters. Thus, it’s a one-way calculation, which protects our data efficiently without the third parties.

Owner signs data with private key. The way to calculate the signature using private key is shown as below. Given raw data z, base point G, the order n, the private d, the signature can be calculated through follow steps.

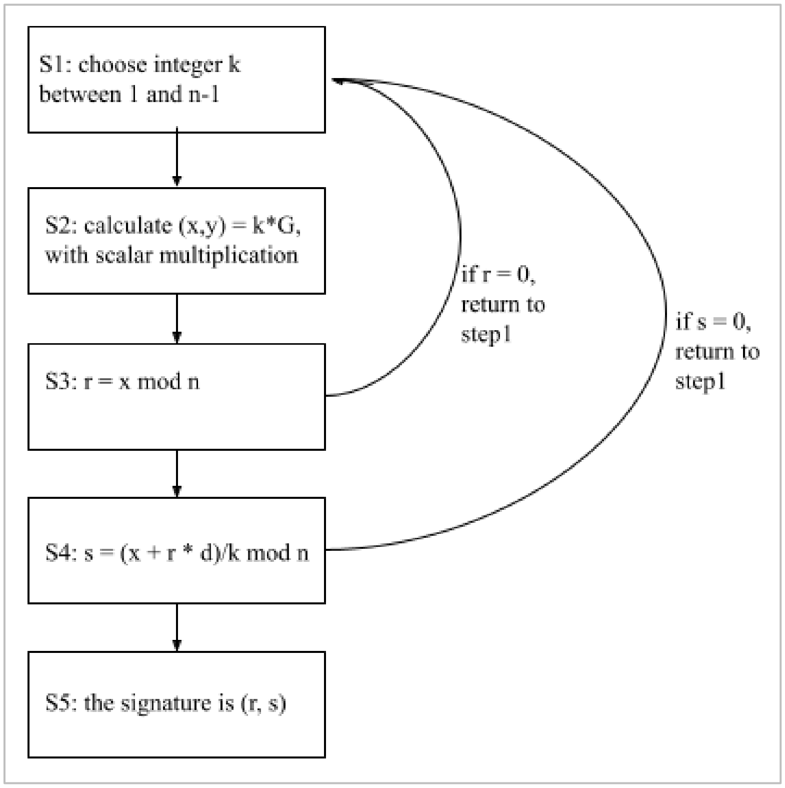

S1: choose integer k between 1 and n-1
S2: calculate (x,y) = k*G, with scalar multiplication
S3: r = x mod n
S4: s = (x + r * d)/k mod n
S5: the signature is (r, s)
if r = 0, return to step1
if s = 0, return to step1

Figure: calculation of signature

Payee verifies data with public key. The way to verify the sender valid is shown as below. Given the public key Q and other parameters as above, the steps to verify data using public key are shown below.

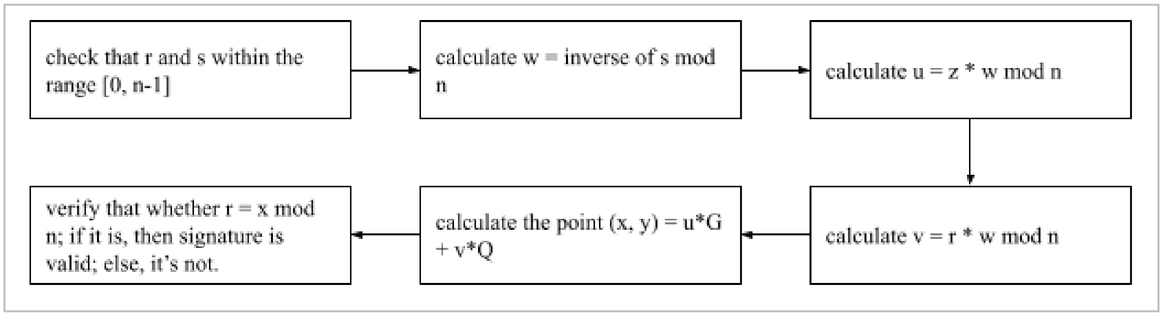

check that r and s within the range [0, n-1]
calculate w = inverse of s mod n
calculate u = z * w mod n
calculate v = r * w mod n
calculate the point (x, y) = u*G + v*Q
verify that whether r = x mod n; if it is, then signature is valid; else, it's not.

Figure: verification of signature

Bitcoin is seen as a chain of digital signatures. As we talked above, owner can sign the signature with private key and payee can verify the owner's identify using public key.

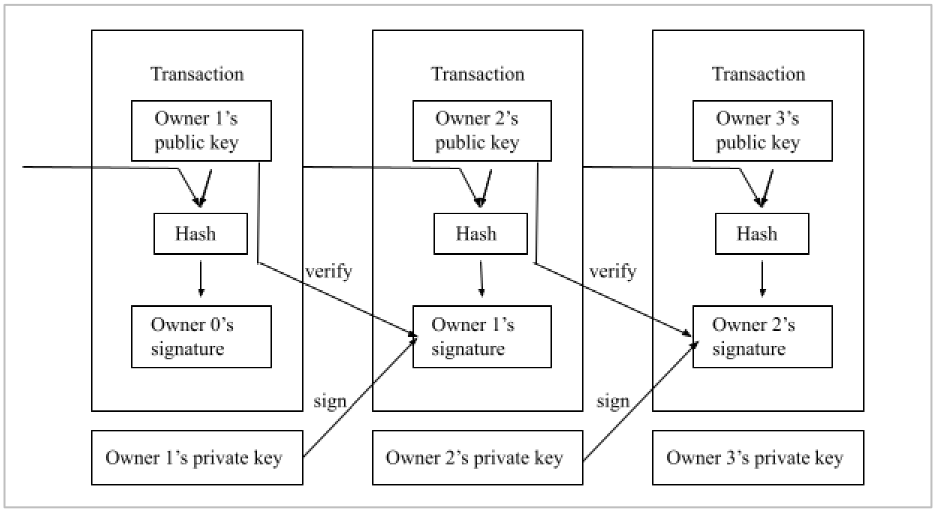


Figure: Diagram of Transaction

The problem here is payee cannot know whether the coin has been spent by the owner before, which introduces us the double-spending problem. To solve the double-spending problem without using the help of the third party, we need to make all transactions publicly, which means all people can see all the transactions. The earliest transaction will be valid and the later transaction will be seen as invalid. In this way, the double-spending problem could be solved. Bitcoin uses timestamp server to serve the solution. Timestamp proves that the block has existed at the time and timestamp server takes a hash of block to be timestamped.

d. Proof-of-work Mechanism

Back to the mining we said before, bitcoin has proof-of-work mechanism to support the timestamp mechanism. What is the proof-of-work used for? The idea of proof-of-work was firstly being extended to secure digital money by Hal Finney in 2004 and Bitcoin was the first widely adaptation of his idea. In Bitcoin, basically, proof-of-work is a mechanism which could provide evidence that they have expended CPU power on it to achieve consensus in the peer-to-peer system. The content of proof of work is to expend CPU effort to find a value that could give the block's hash the required zero bits. It uses a nonce to implement proof-of-work. People who can find the value to make the block being accepted in the system will get the bitcoin reward.

For now, we have reviewed the most significant technical parts of Bitcoin. With the knowledge of digital signature and proof-of-work. The map of the whole network of Bitcoin looks like below. Vertices are nodes in the peer-to-peer network and edges are their P2P connections.

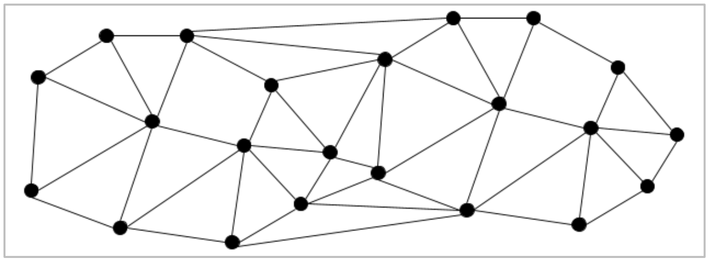


Figure: Peer to peer network example

e. Incentive Mechanism

We have reviewed what is bitcoin, how to make transactions of bitcoin, what is digital signature, and how to solve the double-spending problem. You may wonder how the Bitcoin network could work in such a success in the past ten years without a third party to manage or monitor. The answer is the incentive mechanism existed in the design of Bitcoin. It was also introduced in the white paper of Bitcoin.

As we've already known, those miners in the system spend CPU time and electricity to solve the proof-of-work puzzle. The miners could get bitcoin as payback once they are the first to be validated. Thus, coins are added to the circulation steadily by the miners' work. Besides, transaction fee is also another incentive mechanism in the system. Normally, output value of the transaction is smaller than the input value of the transaction. The difference between the output value and the input value is the transaction fee, and will be given to those miners. As we can imagine, if the sender who send the transaction does not pay the transaction fee, then the transaction could be failed because no one of miners would like to work for this if there is no pay.

You may also wonder if some bad person has the more CPU and electricity resource, will they do bad things, for example, defrauding? The important and magic part of the incentive mechanism of Bitcoin is that people would choose to generate new coins instead of doing bad things in the system even if they have more resources. Because in this incentive mechanism, they will get higher income through generating new coins instead of doing bad things.

Overall, as we can see, with the incentive mechanism, miners could get incentive in the format of new coins and transaction fees; also, this mechanism will avoid the defraud things happening even without the third party managing or monitoring. This incentive mechanism is kind of the answer why Bitcoin could work itself without any back companies or organizations intervening.

f. Storage – Merkle Tree

Next thing I want to mention is about the storage. To minimize the storage size of transactions, once the latest transaction has been saved in the block the header, the previous transactions could be discarded. This is implemented using data structure called Merkle Tree without breaking the block's hash.

To introduce Merkle Tree, first thing we should know is hashing. Using hash function, it can convert data into a hash value. Hash function can verify the validation of the whole data file. Next definition extended from hashing is hash list. In P2P network, data file is split into several small blocks. For each small block, using hashing function to get the hash value.

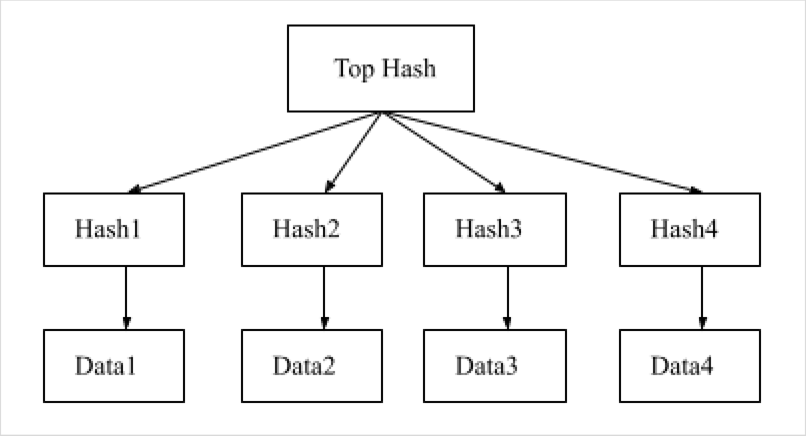


Figure: Hash List

Merkle tree is a kind of Tree data structure and an extension from hash list. Each hash list is a sub-tree of Merkle tree. Advantage of Merkle tree over hash list is that using Merkle tree can verify a sub-tree of whole tree at each time.

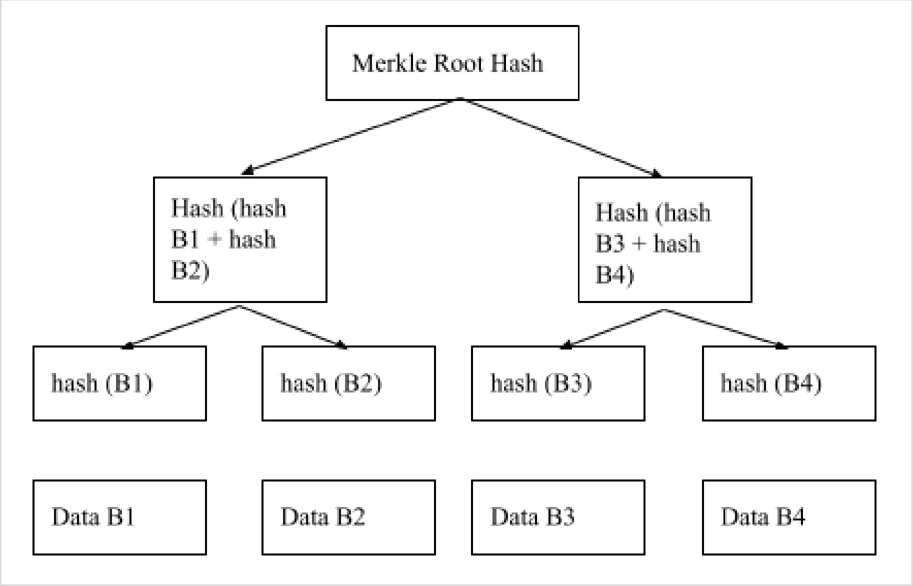


Figure: Merkle Tree

With the useful data structure, storage would not be a problem in Bitcoin. Assume that a blocker header with no transaction would be 80 bytes and block is generated every 10 minutes, we can calculate that each year we need 80 * 6 * 24 * 365 = 4.2 Megabytes, which is relatively a small size compared to the development of the hardware. Thus, storage would not be a problem to Bitcoin system with the growth of hardware year by year.

g. Privacy

For the privacy part, in the previous traditional electricity transaction system, with the third trusted party, privacy is being protected at a certain level. In Bitcoin, though there is no trusted third party involved and all transactions are being announced publicly, there is still privacy existed because all the transactions are anonymous.

4. Summary

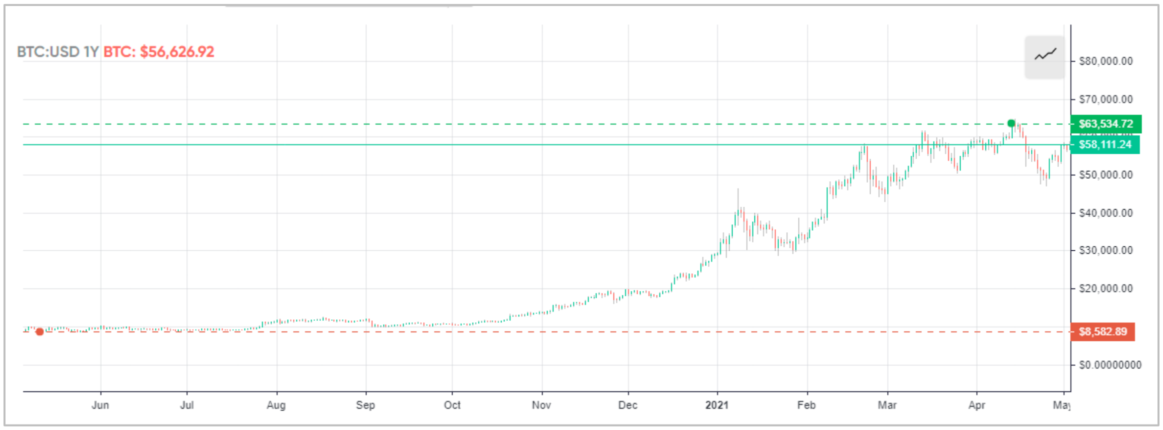
Bitcoin is a new kind of electricity transaction system invented based on cryptography, blockchain and P2P network. This new kind electricity transaction system avoids the intervene of the third trusted party to eliminate the weakness of trust-based model and solves the double-spending problem.

Because this new format of "money" challenges the traditional definition of money and avoids the trusted third party's processing and monitoring, there are lots of different views of this new internet product. With decentralized characteristic and trading online in different countries, regulation of Bitcoin is much hard. Also, though the transactions are announced in network publicly, the transactions are anonymous which means there is no easy way to monitor the transactions in Bitcoin. A few countries have "absolute ban" of Bitcoin; some countries have "implicit ban" of Bitcoin; while other countries are waiting to observe the reaction of market. Many experts question the legality of Bitcoin. In the introduction website of bitcoin, they also said Bitcoin may be used in illegal activities because they treated bitcoin as real money and money can be used both in legal and illegal activities.

Though there are lots of different views of Bitcoin existing, Bitcoin is used in a growing number of business and individuals, such as apartments, restaurants, online services, etc. For example, Distributor of Coca Cola allows Bitcoin as a payment option. Whole Foods also partnered with digital application to accept Bitcoin as a payment method.

Current development and application state of Bitcoin (Trading platform and current price)
In recent few years, the whole world is inching towards a digitalized version of currencies. People do not need to use traditional currency to make a payment or transaction. With digitalized version of currencies truly make our life more convenient. However, this is

based on the prerequisite that there are trusted third parties managing the whole system. Compared to the traditional centralized system, Bitcoin is decentralized P2P network which has more flexibility and uncertainty. From the price the bitcoin recently, we can see the huge variation of Bitcoin. In May 10, 2020, price of 1 bitcoin is $8582.89, while in April 12, 2021, price of 1 bitcoin is $63534.72. We can feel the huge variation in the past one year. Especially in the first half year of 2021, price of bitcoin has a substantial increase.



Data source: bitcoin.com

Also, we must aware that Bitcoin has very high risk, just imagine like other high-risk investments. Especially at this time period, there are already lots of miners around the world. You may want to think the tradeoffs thoroughly before mining or diving much deep into it. It is meaningful to know the theory related to Bitcoin though.

Reference

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] Nakamoto, S. (2019). *Bitcoin: A peer-to-peer electronic cash system*. Manubot.

[3] Catalini, C., & Gans, J. S. (2016). *Some simple economics of the blockchain* (No. w22952). National Bureau of Economic Research.

[4] *Bitcoin - Open source P2P money*. (2008). Bitcoin. https://bitcoin.org/en/

[5] Wikipedia contributors. (2021). *Bitcoin*. Wikipedia. https://en.wikipedia.org/wiki/Bitcoin

[6] Wikipedia contributors. (2021b, April 21). *Elliptic curve*. Wikipedia. https://en.wikipedia.org/wiki/Elliptic_curve

[7] Finney, H. (2004). Rpow-reusable proofs of work. *Internet: https://cryptome. org/rpow. htm*.

[8] *Bitcoin Price Index — CoinDesk 20*. (2021). CoinDesk. https://www.coindesk.com/price/bitcoin

[9] Merkle, R. C. (1987, August). A digital signature based on a conventional encryption function. In *Conference on the theory and application of cryptographic techniques* (pp. 369-378). Springer, Berlin, Heidelberg.

[10] Rykwalder, E. (2020, December 17). *The Math Behind the Bitcoin Protocol*. CoinDesk. https://www.coindesk.com/math-behind-bitcoin