Blockchain and Cryptocurrency

A Blockchain and Cryptocurrency Guidebook for Everyone

By Dr. Liew

About the Author

Dr. Liew Voon Kiong holds a bachelor's degree in Mathematics, a master's degree in Management and a doctorate in Business Administration.

Dr. Liew is a sought-after **Blockchain Architect** by companies in the blockchain industry. He has played a lead role in designing and developing the native cryptocurrency of an incubation hub in Southeast Asia, as well as successfully getting it listed on a renowned exchange via an IEO campaign. He is also the Chief Strategy Officer of an Australian blockchain company that manages a crypto fund.

Dr. Liew is also a blockchain researcher and has developed several use cases such as blockchain-powered supply chain management for the automotive and textile industries, building a blockchain-powered digital government, event and ticketing DApps, and more. He is skilled in setting up blockchain networks such as private Ethereum networks, as well as writing smart contracts using Solidity and creating DApps. He has also created a blockchain blog titled Blockchain Guide for Everyone (http://www.blockchainguide.biz/).

He is the head of the education subcommittee of the Access Blockchain Association of Malaysia, as well as a regular speaker in regional blockchain events and workshops.

Preface

Blockchain has been the most hyped technology in the last decade. Though blockchain technology is being overhyped somewhat, it has the potential to disrupt many existing industries. Many start-ups, MNCs, governments, non-profit organizations and individuals have developed and implemented blockchain-based applications.

Blockchain has crept into our daily life as we are bombarded with news from social media, web portals and advertisements. As a result, nearly everyone is talking about cryptocurrency today. However, most people still do not understand blockchain, the technology that powers cryptocurrencies. Therefore, I have written this book with the hope to help everyone understand blockchain technology and cryptocurrencies better.

This book is a comprehensive guide covering fundamental and advanced topics such as:

- Storing your cryptocurrencies securely in crypto wallets
- Smart contracts
- dApps
- Enterprise blockchain frameworks like Hyperledger and Corda
- How to conduct ICO and IEO
- DeFi
- Blockchain for financial services
- Blockchain for supply chain management
- Building a digital government with blockchain
- HR transformation powered by blockchain

The book also covers technical topics such as:

- Improving scalability with Plasma
- Storing blockchain data on IPFS
- Writing smart contracts with Solidity
- Developing DApps
- Developing ERC-20 tokens
- Setting up a private Ethereum blockchain
- Creating a multisig wallet
- Creating an automotive supply chain management blockchain platform with Hyperledger Fabric

Table of Contents

Chapter 1

Introduction to Blockchain

Blockchain has been the most hyped technology in the last decade. A recent World Economic Forum report predicts that by 2025, 10% of GDP will be generated by blockchain. Though blockchain technology is being overhyped somewhat, it has the potential to disrupt many existing industries. Start-ups, MNCs, governments, non-profit organizations and even individuals have already developed and implemented blockchain-based applications. For example, Walmart has collaborated with IBM to implement blockchain for food traceability as part of its food safety initiative. Therefore everyone, particularly business owners and enterprises, should take notice of this trend.

Blockchain has slowly crept into our daily life as we are bombarded with news from social media, web portals and advertisements. As a result, nearly everyone is talking about cryptocurrency today. In fact, many have invested in cryptocurrencies such as Bitcoin, Ethereum and other altcoins. While many people have made lots of money, many others have experienced substantial losses too. However, most people still do not understand blockchain, the technology that powers cryptocurrency. Therefore, I have written this book with the aim to help everyone understand blockchain technology and cryptocurrency better.

1.1 A Short History of Blockchain

To begin with, the first blockchain was invented by Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency Bitcoin. That year, he or she posted a paper called Bitcoin – A Peer to Peer Electronic Cash System to a mailing list discussion on cryptography. Therefore, we can say that Satoshi Nakamoto invented Blockchain and Bitcoin as its application. However, Satoshi Nakamoto's real identity remains a mystery to this day. In fact, Satoshi Nakamoto may not be a person, but a group of people.

On the other hand, Satoshi Nakamoto might not be the first person to come up with the idea of blockchain technology. The idea behind blockchain technology can be traced back to 1991, when Stuart Haber and W. Scott Stornetta (Scott-Briggs, 2018) conceived the idea of a cryptographically secured chain of blocks. In 1992, they incorporated Merkle trees into the design, allowing several documents to be collected into a block.

In addition, there were also previous attempts at creating online currencies with ledgers secured by encryption, such as B-Money and Bit Gold. B-money was an early proposal created by Wei Dai for an "anonymous, distributed electronic cash system". His essay was published on the Cypherpunks mailing list in November 1998. Even Satoshi Nakamoto referenced B-Money when he invented Bitcoin. Another precursor of Bitcoin is Bit Gold,

invented by Nick Szabo in 1998. Bit Gold is a decentralized digital currency but was never implemented.

However, blockchain technology did not gain traction until the emergence of Bitcoin. Since its debut in 2009, the price of Bitcoin has skyrocketed, though it turned south in the year 2018. Many people are actively involved in mining activities in the hopes of getting rich quickly. From 2011 onwards, many alternative cryptocurrencies or altcoins have emerged, such as Ethereum, EOS, Ripple, Ethereum Classic (ETC), XRP, Litecoin and more. Currently, there are over 1,000 cryptocurrencies in circulation with new ones frequently appearing.

None of the cryptocurrencies came close to challenging Bitcoin until the invention of Ethereum by Vitalik Buterin in 2013. The Ethereum platform introduced the concept of smart contracts and the cryptocurrency Ether. It is also a platform for ICO, crypto crowdfunding. I shall elaborate on Ethereum and ICO in a later chapter.

1.2 Blockchain in a Nutshell

A blockchain is a distributed and decentralized digital ledger that can be used to record transactions and data across numerous computers in a decentralized peer-to-peer network. We can also define a blockchain as a distributed encrypted database, like a spreadsheet that is duplicated thousands of times across a network of computers. This network is designed to regularly update this spreadsheet. It is a subset of **distributed ledger technologies (DLT)**.

The main feature of blockchain is decentralization. To understand what decentralization is, first we need to understand the traditional centralized operation mode. For example, if you go to the supermarket to buy something, you pay with a credit card when you check out. This process requires the approval of a third party, the bank. The transaction is completed after the bank approves it. However, if you use the blockchain platform to perform a transaction, you do not need a third party. The buyer and the seller can trade directly and seamlessly in a transparent and secure blockchain ecosystem.

Another feature of the blockchain is that all participants in the network do not need to establish any trust relationships to perform transactions. It relies on cryptographic authentication technology, a decentralized network, and a consensus mechanism to ensure the security and integrity of funds and information. Therefore, information on the blockchain is highly transparent and not easily falsified. Thus, the blockchain system is particularly suitable for the financial industry. Indeed, blockchain is an incorruptible digital ledger of economic transactions that can record not only financial transactions but pretty much everything of value((Don Tapscott, 2017).

In short, blockchain has the following advantages:

- Transparent
- Secure
- Decentralized
- Democratic
- Efficient
- Auditable
- Immutable
- Consensus

1.3 The Blockchain Network

The blockchain network is a peer-to-peer decentralized network. The peers, also known as nodes, are connected to this network in a synchronous way. The nodes can be a desktop, a laptop, a mobile phone, a mining rig, servers, or any other electronic devices. These nodes form the foundation of the blockchain network. They provide computing resources like disk storage space to keep the network alive and to maintain its integrity and security, and they do it voluntarily.

The decentralized peer-to-peer network is different from the traditional centralized client-server network, as shown in Figure 1.1 and Figure 1.2.

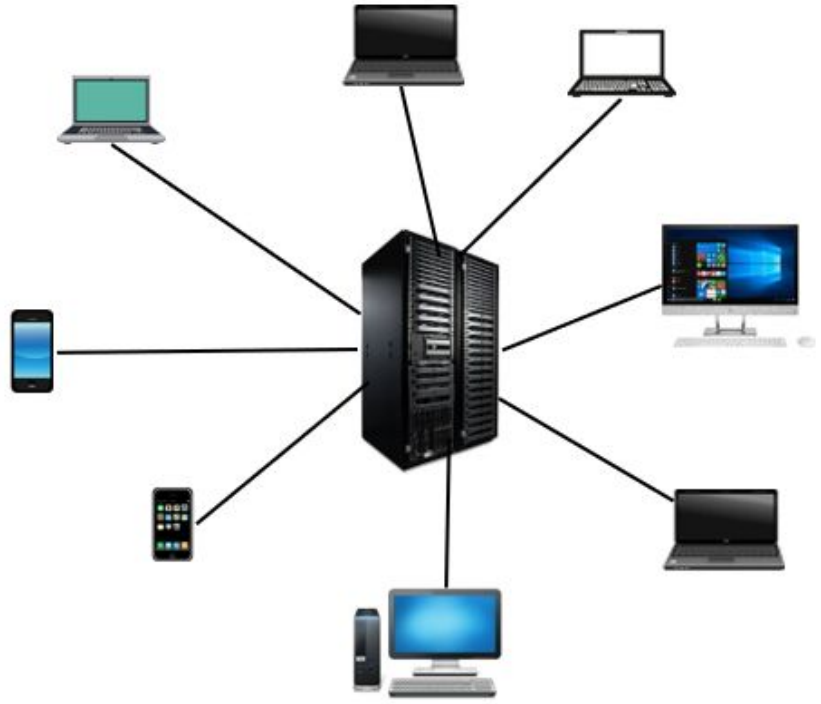

Figure 1.1 Centralized Client-Server Network

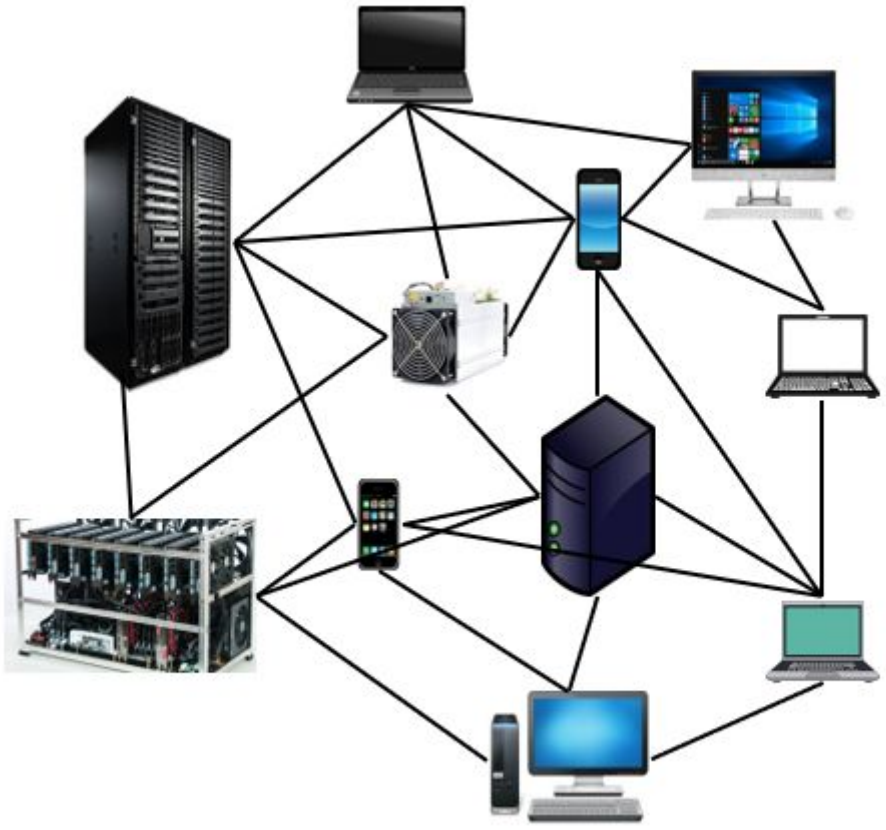

Figure 1.2 Decentralized Peer-to-Peer Network

A centralized network has an authoritative central point of control. All the clients are connected to this single point and all their data are stored in the central server. The client has not much control over how the central authority will use his or her data.

A good example is your bank account. The bank keeps your money, manages your account, and records all your transactions. They can also lend your money to other clients. Although this system has been quite reliable, it is prone to the vulnerability of a single point of failure. For example, if a bank's central server is hacked, all the accounts will be compromised.

On the contrary, in the peer-to-peer decentralized network, all the peers work together to upkeep the network via a consensus mechanism. The peers have 100% control of their data and how the data could be used. In addition, they do not need a third party or a middle entity to perform transactions.

More importantly, it eliminates the vulnerability of a single point of failure. If a node is hacked, only the data belonging to that node would be compromised while all other nodes would keep a copy of the ledger. Moreover, the cryptographic hashing algorithm makes it extremely difficult to hack the blockchain.

To ensure the nodes are motivated to maintain the network, blockchain incentivizes the nodes through a mechanism known as mining. By engaging in mining activities, the successful miners will be rewarded with cryptocurrencies such as Bitcoin, Ethereum or other coins.

1.4 The Composition of Blockchain

A blockchain is a chronological chain of blocks. The first block is known as the genesis block. A block refers to a set of transactions that are bundled together and appended to the blockchain. The second block is appended to the genesis block, the third block is appended to the second block and so forth, as shown in Figure 1.3.

Figure 1.3 The Blockchain Structure

Every node in the network stores a copy of the distributed ledgers, or the blockchain, as shown in Figure 1.4.

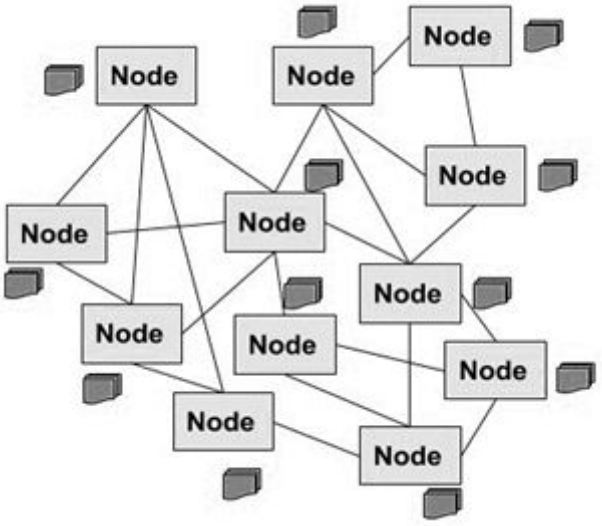

Figure 1.4 The Blockchain Network

1.5 The Block Structure

A block consists mainly of the block header containing metadata and a list of transactions appended to the block header. The blockchain metadata consists of information such as Hash, Block Height, Nonce, Difficulty, Timestamp and more, as shown in Figure 1.5.

Figure 1.5 The Block Structure

Moreover, there is other information in the block, such as rewards, transaction fees and so on. If you want to find out the latest Bitcoin block information, you can browse the following link:

https://www.blockchain.com/explorer

Figure 1.6 shows the real data of Bitcoin block #631977

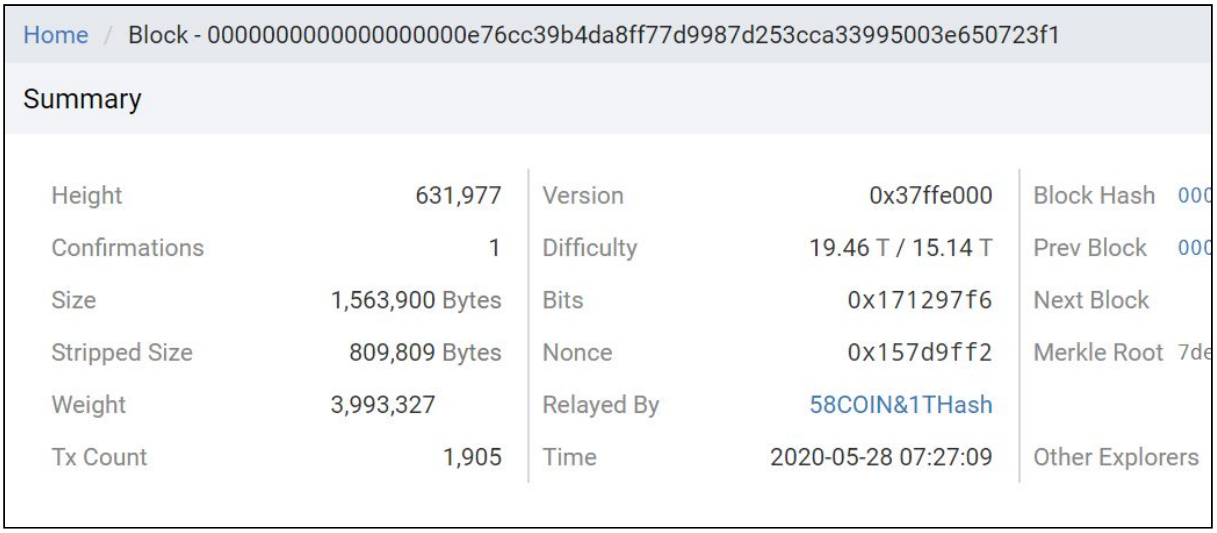

Figure 1.6

1.6 Block Height

The block height of a block is defined as the number of blocks preceding it in the blockchain (Investopedia). It is calculated as the length of the blockchain minus one. Genesis block has a block height of zero as it does not have preceding blocks. For example, the height of block 631977 is 631977.

1.7 Nonce

A nonce is a random number the miners use to solve a mathematical puzzle in the mining process, which is also known as proof of work. The nonce in the Bitcoin block is a 32-bit (4-byte) field whose value is adjusted by the miner to make the hash of the block smaller than or equal to the current target of the network. The concept of proof of work will be explained in a later chapter.

1.8 Difficulty

Difficulty is a value that measures the degree of difficulty to find a hash value for a given target, which represents the difficulty of mining. The value of difficulty will be changed once every 2016 blocks. The value will usually increase.

1.9 Timestamp

A timestamp is a sequence of characters or encoded information identifying when a certain event occurred, usually giving date and time of day. The term derives from rubber stamps used in offices to stamp the current date, and sometimes time, in ink on paper documents, to record when the document was received, as shown in Figure 1.7.

Figure 1.7 Timestamp (Image adapted from Wikipedia)

In this digital age, the term has been expanded to refer to the date and time information attached to digital data. For example, computer files contain timestamps that tell when the file was created and when was it last updated. Digital cameras add timestamps to the pictures by recording the date and time the pictures were taken.

The Unix timestamp is the number of seconds passed since midnight on January 1, 1970 (UTC / GMT), ignoring leap seconds. When I wrote this book, the Unix timestamp was 1540130658. You can check the current timestamp at the link below:

https://www.unixtimestamp.com/

Timestamping is an important feature of blockchain technology. Each block is timestamped, with each new block referring to the previous block using the cryptographic hash. Combined with cryptographic hashes, this time stamped chain of blocks provides an immutable record of all transactions in the blockchain, as shown in Figure 1.8:

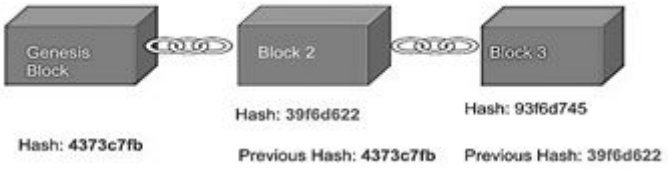

Figure 1.8

1.10 Hash

A hash or hash value is the result of a hash function. A hash function takes an input of any length, performs an algorithmic transformation, and produces an alphanumeric value of a predetermined length. The input could be a spreadsheet file, a music file, a video file, an image file, a financial statement, an invoice, a contract and more.

A hash value consists of 256 randomly generated bits, which are represented with 64 hexadecimal characters. Here is an example:
“4373c7fb1437035365d9228c77eca2cfd240523e274163e78c1eba11effd8b38”

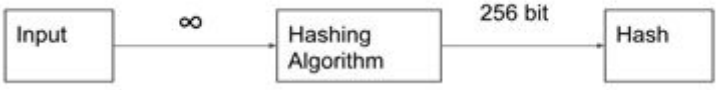

Figure 1.9 Hash

You can generate a hash online using the following link:

https://passwordsgenerator.net/sha256-hash-generator/

A hash has the following properties:

- A given input has a precisely predictable output of a specified length, usually but not necessarily much shorter than the input.
- Even if the input is only slightly changed, the output differs dramatically.

- If the hash function is of the cryptographic variety, it is exceedingly difficult, if not practically impossible, to infer the original input given only the output. The degree of difficulty/impossibility depends on the strength of the encryption used.

Every transaction occurring on the blockchain network is encoded with a hashing algorithm to produce a hash that is impossible to decrypt. Hashes are used to represent the current state of the blockchain. It means all the transactions that have taken place so far have been hashed, and the resulting output hash represents the current state of the blockchain. The hash is used for all parties to agree that the state is the same.

The purpose of the hash is for validation. Data on the blockchain is “hashed” in each block. Each block is linked with the previous block via the hash value. If someone tampers with a block, everyone will know the block is corrupted. Therefore, it preserves the integrity and immutability of the blockchain.

1.11 Merkle Tree

Merkle tree is one of the metadata in a block of the blockchain. In computer science, the Merkle tree is a branching data structure that is used to store hashes of individual data in a large dataset. The purpose is to make the verification of the dataset efficient and fast. It is an anti-tamper mechanism to ensure that the large dataset has not been tampered with.

In blockchain, the Merkle tree(also known as the hash tree) encodes the blockchain data in an efficient and secure manner. Every transaction occurring on the blockchain network is subjected to a hashing algorithm to produce a hash, as shown in Figure 1.9. Therefore, every transaction has a hash associated with it.

As there are thousands of transactions stored on a block, it will be very time consuming if every node must deal with hundreds of thousands of transactions across the blockchain, synchronization and mining will take a long time. To solve this issue, all the transactions hashes in the block are also hashed. As illustrated in the following figure, two hashes are hashed into a single hash, as shown in Figure 1.10

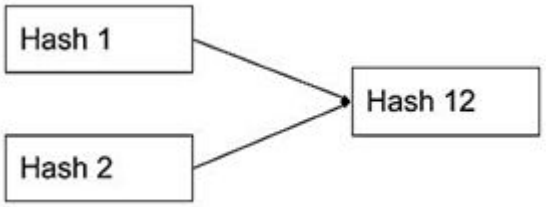

Figure 1.10

These hashes are not stored in a sequential order on the block, rather in the form of a tree-like structure such that each hash is linked to its parent following a parent-child tree-like relation. The hashing will go on until it produces a singular hash, the **Merkle root**. This

Merkle root is the hash of the block and it is stored on the header of the block. The process is illustrated in Figure 1.11.

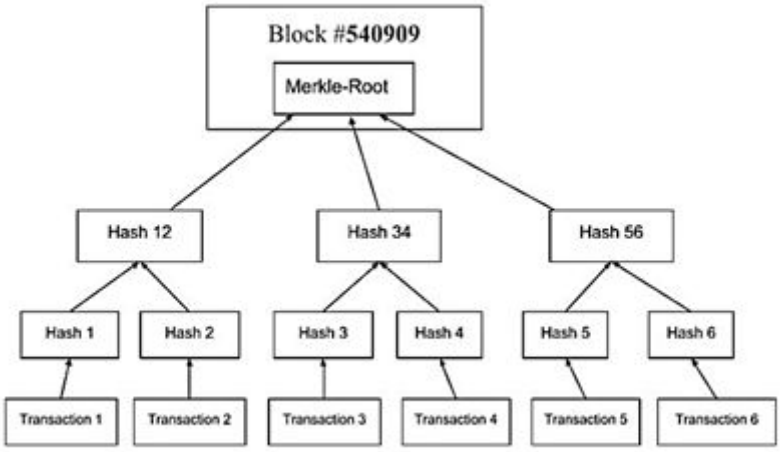

Figure 1.11

The Merkle Tree structure will enable the quick verification of blockchain data and quick movement of large amounts of data from one computer node to the other on the peer-to-peer blockchain network.

Chapter 2

Bitcoin- The First Application of Blockchain

2.1 A Brief History of Bitcoin

In contrast to popular belief, the idea of creating digital money without a trusted third party was not conceived by Satoshi Nakamoto, but was proposed by advocates such as Wei Dai and Nick Szabo more than a decade before the successful launch of Bitcoin. The biggest issue surrounding the implementation of a decentralized digital currency is double spending. Double-spending is a potential problem in which the same digital currency can be spent more than once.

As we know, we can send any number of an electronic copy of a digital asset to anyone. This includes sending emails, documents, music files, video files and more. However, we cannot do the same with digital money. If you pay someone using cash, the value of money is transferred to another party and the money no longer belongs to you. However, if you send someone digital money, you still can retain the same amount of money and can send it to someone else. In fact, there is no limit to how many copies of the digital money you can send.

Wei Dai, a computer engineer and cypherpunk, tried to solve the double-spending issue by publishing a paper on cryptocurrency with the title "b-money, an anonymous, distributed electronic cash system" in 1998. In the paper, Dai outlines the basic properties of all modern-day cryptocurrency systems as "*a scheme for a group of untraceable digital pseudonyms to pay each other with money and to enforce contracts amongst themselves without outside help*". In the same year, Szabo designed a mechanism for a decentralized digital currency he called "Bit Gold". Though Bit Gold was never implemented, it has been called a direct precursor to the Bitcoin architecture.

Satoshi sent an email to Wei Dai in the year 2008 to announce that he had solved the double-spending issue and was ready to implement the first decentralized digital cash without the need of a trusted third party. His email (Branwen) is as follows:

"From: "Satoshi Nakamoto" <satoshi@anonymousspeech.com>

Sent: Friday, August 22, 2008 4:38 PM

To: "Wei Dai" <weidai@ibiblio.org>

Cc: "Satoshi Nakamoto" <satoshi@anonymousspeech.com>

Subject: Citation of your b-money page

I was very interested to read your b-money page. I'm getting ready to release a paper that expands on your ideas into a complete working system. Adam Back (hashcash.org) noticed the similarities and pointed me to your site.

I need to find out the year of publication of your b-money page for the citation in my paper. It will look like:

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, (2006?).

You can download a pre-release draft at

http://www.upload.ae/file/6157/ecash-pdf.html Feel free to forward it to anyone else you think would be interested.

Title: Electronic Cash Without a Trusted Third Party

Abstract: A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures offer part of the solution, but the main benefits are lost if a trusted

party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power.

As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Satoshi”

Later in the same year on 31 October 2008, he published the Bitcoin whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System". This whitepaper is now available for download from the link https://bitcoin.org/bitcoin.pdf.

Bitcoin’s peer-to-peer electronic cash system allows a party to send payments to another party directly using digital signatures, without the need to go through a trusted third party such as a bank or a financial institution. However, digital signatures alone still cannot avoid the issue of double spending. Therefore, Satoshi proposed a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate

computational proof of the chronological order of transactions (a.k.a. proof of work), in a process generally known as mining. The system is secure if honest nodes collectively control more CPU power than any cooperating group of attacker nodes. We shall describe digital signatures and mining in the following paragraphs.

2.2 What is a Digital Signature?

The Bitcoin whitepaper defines an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

According to Wikipedia,

"*A digital signature is a mathematical scheme for presenting the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).*"

A digital signature is generated using asymmetric cryptography, which is more secure than handwritten signatures that can be easily forged. It is used to prove that a message originates from a specific individual and not from someone else.

Asymmetric cryptography, also known as public key cryptography (PKI), uses public and private keys to encrypt and decrypt data. In the asymmetric encryption system, a user generates the key pair, which comprises a public key and a private key using a known algorithm. The public key and private key are associated with each other via a mathematical relationship.

The public key is meant to be distributed publicly to serve as an address to receive messages (including cryptocurrencies) from other users, like your Bitcoin or Ethereum address. The private key is meant to be kept secret and is used by the sender to send digitally signed messages to other users. The signature is included in the message so that the recipient can verify using the sender's public key. This way, the recipient can be sure that only the sender could have sent this message key pair, which is a public key and a private key using a known algorithm. For example, every transaction on the blockchain is digitally signed by the sender

using their private key. This signature ensures that only the owner of the account can move money out of the account.

The steps are explained below:

Step 1 Signing the message with the private key

To create a digital signature, the user can use a signing software to create a one-way hash of the electronic data. The private key is then used to encrypt the hash. The encrypted hash, along with

other information, is the digital signature. The process of creating a digital signature is illustrated in Figure 2.1.

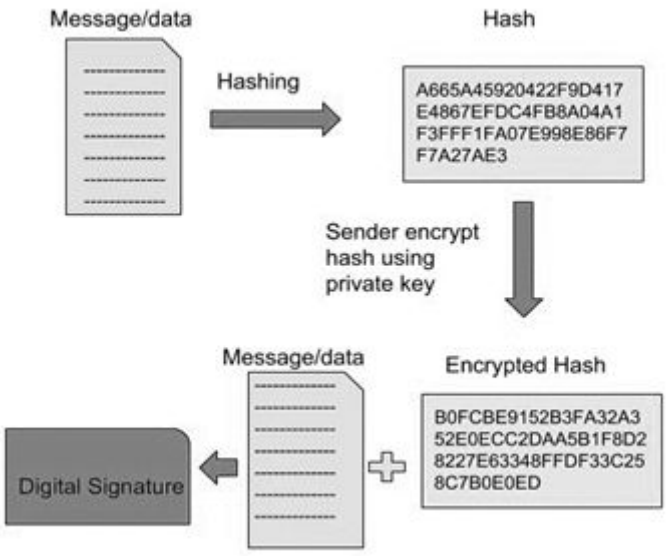

Figure 2.1 Creating Digital Signature

Step 2 Verifying the message with the public key

To verify the message, the receiver uses the sender's public key to decrypt the hash. If this decrypted hash matches a second computed hash of the same data, it proves that the data has not changed since it was signed. If the two hashes do not match, the data has either been tampered with in some way or the signature was created with a private key that does not correspond to the public key presented by the sender. The verification process is illustrated in the following figure:

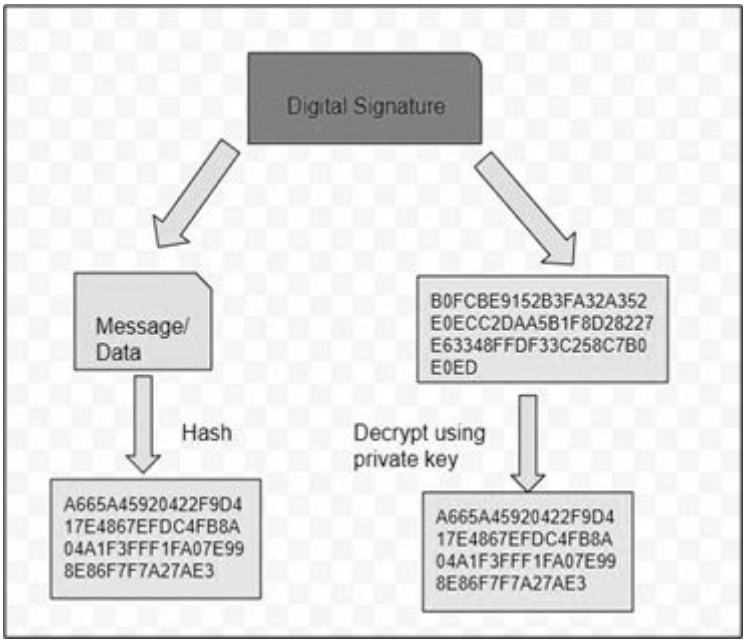

Figure 2.2 Verification Process

To sum it all, blockchain could not exist without hashing and digital signatures. Hashing provides a way for everyone on the blockchain to agree on the current world state, while digital signatures provide a way to ensure that all transactions are only made by the rightful owners. We rely on these two properties to ensure that the blockchain has not been corrupted or compromised.

2.3 What is Mining?

According to Investopedia,

"*Bitcoin mining is the process by which transactions are verified and added to the public ledger, known as the blockchain, and the means through which new bitcoins are released. Anyone with access to the internet and suitable hardware can participate in mining. The mining process involves compiling recent transactions into blocks and trying to solve a computationally difficult puzzle. The participant who first solves the puzzle gets to place the next block on the block chain and claim the rewards. The rewards, which incentivize mining, are both the transaction fees associated with the transactions compiled in the block as well as newly released bitcoin.* "

As quoted in the Bitcoin whitepaper, the continuous addition of a constant amount of new coins is like gold miners expending resources to add gold to circulation, therefore the term mining.

While Bitcoin is the first cryptocurrency generated using the mining process, it is certainly not the only platform that has adopted this algorithm. Most of the alternative coins (altcoins) are using the mining algorithm to generate their crypto money.

2.4 The Purpose of Mining

Generally, people think of mining in blockchain to obtain bitcoins or other cryptocurrencies. While this is partially true, it is not the main purpose of mining. In fact, the main objective of mining is to ensure the perpetuity and security of the decentralized network. The network comprises nodes that store the distributed ledgers in the form of the blockchain. Bitcoins are awarded to the miners for their effort in maintaining the integrity of the blockchain by validating the transactions in the blockchain. Because of the reward system, miners (nodes) will stay on in the network and help to prevent network downtime. Just imagine: if there was no reward, nobody would want to connect to the network, and it would just cease to exist.

2.5 How Does Mining Work?

The mining process starts when miners are trying to validate new transactions and record them on the blockchain. The miners are competing to solve a difficult mathematical puzzle based on a cryptographic hash algorithm. The solution found is called the **Proof of Work**, a.k.a. **PoW**. When a block is 'solved', all the transactions contained in the candidate block are considered validated, and the new block is confirmed. This new block will be appended to the blockchain. The time taken to confirm a new block is approximately 10 minutes for Bitcoin, but for other coins it is much faster. So, if you send or receive bitcoins, it will take approximately 10 minutes for the transaction to be confirmed.

Miners receive a reward when they solve the complex mathematical problem. There are two types of rewards: new bitcoins and transaction fees. The number of bitcoins created decreases every 4 years, or every 210,000 blocks to be precise. Today, a newly created block creates 6.25 bitcoins. This number will keep going down until no more bitcoin will be issued. This will happen around 2140, when

21 million bitcoins will have been created. After this date, no more bitcoin will be issued. However, miners can still receive rewards in the form of transaction fees. The winning miner can collect all the transaction fees in the block. As the amount of bitcoin created with each block diminishes, the transaction fees received by the miner will increase. After the year 2140, the winning miner will only receive transaction fees as their reward.

2.6 Technical Explanation of Mining

Let us examine the technical aspects of crypto mining. In the blockchain, every block has a previous block except the very first block or the genesis block. Miners are competing to validate a new block by solving a complex mathematical puzzle. Let us look at the latest Bitcoin mined block, block # 631977 at the time of writing. This block is shown in Table 2.1.

Table 2.1 Block 631977

Hash	0000000000000000000e76cc39b4da8ff77d9987d253cca33995003e650723f1
Confirmations	1
Timestamp	2020-05-28 07:27
Height	631977
Miner	Unknown
Number of Transactions	1,905
Difficulty	15,138,043,247,082.88
Merkle root	7de3e90dad93273ac22d1db9c1721264790cd1e6ca2eec4b6d73799f7f37b0a0
Version	0x37ffe000
Bits	387,094,518
Weight	3,993,327 WU
Size	1,563,900 bytes
Nonce	360,554,482
Transaction Volume	6633.39891611 BTC
Block Reward	6.25000000 BTC
Fee Reward	1.36240641 BTC

Notice that the block height is 631977, which means there are 631977 blocks in the Bitcoin blockchain that have been confirmed since the genesis block.

Let us call the successful miner for this block Mr. John. Before John successfully mines block #631977, he was competing with other miners in mining the previous block #631976. However, he lost in the contest and block #631976 was mined by a fellow miner. As soon as block #631976 was mined, he needs to quickly update his blockchain and start mining for a new unvalidated block, known as the candidate block.

In fact, while John's computer (also known as a node) was searching for the Proof of Work for the previous block, it was also searching for new transactions. Those new transactions are added to the memory pool or transaction pool. The memory pool is a node's temporary storage area for

transaction data. This is where transactions wait until they can be included in a new block and validated.

In constructing the candidate block, John's node starts gathering the transactions in the transaction pool. It removes the transactions already present in the previous block if there are any. The block is called a candidate block because it does not have a valid Proof of Work yet.

As you can see in Table 2.1, block #631977 has 1905 transactions inside it. This was the number of transactions present in John's transaction pool when he created his candidate block. The mining process is illustrated in Figure 2.3.

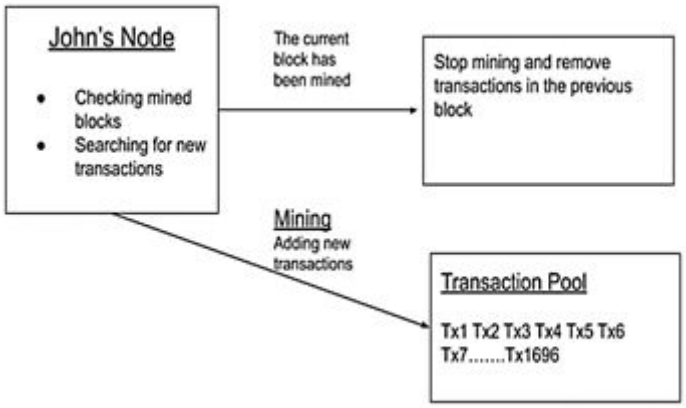

Figure 2.3 The Mining Process

In the mining process, John's node is creating a Coinbase transaction. This transaction will create bitcoins and deposit them into John's wallet as a reward for finding a valid Proof of Work. This transaction is different from the other ones because the bitcoins in the reward are created out of nothing. They do not come from someone's wallet. Besides that, John's node also calculates the transaction fees in the block.

John's reward for mining block #631977 is as shown in Figure 2.4 is

Total reward = Reward for mining block + Transaction fees

= 6.25 BTC+1.36240641BTC

= 7.61240641 BTC

**BTC block reward has been reduced to 6.25 BTC since Bitcoin halving occurred on 11th March 2020, down from 12.5 BTC.*

Figure 2.4

From Figure 2.4, you can see that it is a Coinbase transaction which means the newly minted Bitcoin does not come from anyone's wallet. You can only see the winning miner's wallet address here.

2.7 How to achieve Proof of Work?

Mining involves the process of producing a hash whose value is less than the target value. When this hash has been found, it is called a valid hash and hence proof of work is achieved.

The mining algorithm uses a counter known as the nonce to generate the hash using the SHA256 cryptographic function. A hash algorithm always produces the same arbitrary length data given the same inputs. It is impossible to compute the same hash with two different inputs. It is also impossible to predict the output of any given data in advance.

The value of nonce is initialized to 0. Mining is finding the nonce, the only input that changes every time we run the hash function. The goal is to find a value for the nonce that will result in a hash lower than the target. So, the mining node might need to try billions or trillions of nonce values before it gets a valid hash. As you can see, mining is like playing the slot machine, there is no way to predict when you can strike a jackpot.

It is quite easy to prove that the nonce found indeed produces a valid hash. All the information is available, everyone in the network can run the hash function and confirm if the hash is valid or not. Because it is also impossible to predict what the nonce will be, it also acts as a proof that the miner has indeed achieved Proof-of-Work.

Calculation of a valid hash is as follows (based on block #540909):

The formula to calculate the current target of the block is

Current target = Maximum target / Difficulty

Maximum target is

`0x00000000FFFF0000000000000000000000000000000000000000000000000000`

This is a hexadecimal number. After conversion to a decimal number, the maximum target is

`26959946667150639794667015087019630673637144422540572481103610249215`

Difficulty is (as given in the block)

`7019199231177.17`

Therefore, the current target is

`26959946667150639794667015087019630673637144422540572481103610249215)/7019199231177.17`

= 3.84089×10^54

The hash of the block is

`00000000000000000000ef17668e407e78c5a247f731b1138ad16f5bf79f1c0d`

Converted to a decimal number, the value is

`894547162054952395488710168460602647087185615849461 89`

The hash value is approximately 8.95×10^51**.** Clearly, the hash value is less than the current target, therefore it is a valid hash.