Blockchain

**Blockchain**

Presented by yooval yosef

avigail hagay

Racheli ben

TZ: 320818008

Lecturer: Dr Martin Land

Computer Networks and Distributed Systems Seminar, HAC College, 2021

Submitted August 29, 2021

**Table of Contents**

List of Illustrations and Tables……………………………………………………………………..2

1. Introduction………………………………………………………………………………………..…4
2. Background. ………………………………………………………………………………………….5
3. **Popularity and Practicalit**………………………………………………………………………….6
4. basic Concepts……………………………………………………………………………………..…7
5. Blockchain Components……………………………………………………..……………….…9
6. Ledgers………………………………………………………………..…………………….9
7. Blocks ……………………………………………………………………………..9
8. Transection……………………………………………………………………………………..…11
9. Realibility………………………………………………………………………………………..…11
10. Blockchain classification. ………………………………………………………...11
11. Cryptographic Hash Functions………………………………………………….…12
12. Asymmetric Key Cryptography……………………………………………………12
13. Consensus Models……………………………………………………………………..14
    1. Proof of Work Model…………………………………………………..….15
    2. Proof of Stake Model……………………………………………………...16
14. Blockchain Limitations and Misconceptions…………………………………………..18
15. Conclusion……………………………………………………………………………………………..19

Bibliography………………………………………………………………………………………………...21

**Illustrations**

Illustration 1 – Generic Chain of Blocks ………………………………………………………………………. 3

Illustration 2 – an example of a cryptocurrency transaction ………………………………… 6

Illustration 3 – demonstration of the blockchain………………………………………………………8

Illustration 4 –puzzle solution explained. ……………………………………………………………. 8

Illustration 5 – A Guide to understand the need in Blockchain……………….…. 111

**Table**

Table 1 – Pros/Cons of Presented Consensus Models………………………………………………...10

**Introduction-**

Blockchains are a type of digital ledger that allows for decentralized recording of transactions without the need for a central repository. Unlike traditional ledgers, blockchains are not governed by a central authority and are maintained by a group of users who record transactions on a shared ledger. Once a transaction is published on the blockchain, it cannot be altered. Due to its decentralized nature, any attempt to tamper with the ledger will be immediately detected and rejected by other users. This makes blockchains tamper-resistant and tamper-evident, ensuring the integrity of the recorded transactions. [1]

**Background**

The concept of a consensus model, which is a set of predefined rules for validating computational output, was introduced in the 1980s and 1990s. This became particularly important for digital transactions, where the validity of each transaction needed to be verified for the entire computer network to function correctly. In 2008, this idea was implemented in the form of "electronic cash," which led to the founding of Bitcoin in 2009.

The blockchain technology underlying Bitcoin allows for decentralized and distributed transactions without the need for a trusted third party to validate them, such as a bank. This means that there is no central authority governing the currency. The users of the blockchain, called "miners," receive cryptocurrency as a reward for successfully publishing new blocks containing transactions into the blockchain.

With the adoption of blockchain and consensus models, a self-policing mechanism was established, eliminating the need for a centralized authority to validate and maintain a transaction ledger. All transactions are transparent to all users, providing a layer of reliability as malicious activity can be easily recognized by all. Blockchain also offers pseudo-anonymity, as identification is generally not required to participate in a blockchain network, unlike other financial systems where identification is often a legal requirement to open a bank account or perform other similar functions. [2]

**Popularity and Practicality-**

Cryptocurrency is currently the most widespread application of blockchain technology. To illustrate the workings of blockchain, we will use examples from the world of cryptocurrency. The media often portrays blockchain technology in a hyped-up manner, likening it to magic. However, a more practical approach is needed when considering whether or not to use this technology. Its pros and cons should be weighed carefully against one's specific needs before deciding whether or not to implement blockchain. Despite the need for caution, blockchain's popularity continues to grow. This can be attributed to its unique way of functioning, which we will explore in the next section. Smart contracts are another way that blockchain is utilized, with software programs being stored and run on a blockchain network. Furthermore, businesses may use blockchain as a way of keeping records in a distributed fashion. It's worth noting that there are other modern-day applications of blockchain technology that we have not touched upon in this section. [3]

**Basic Concepts**

Blockchain - the digital ledger that records all transactions.

Block - a record of one or more transactions along with additional metadata. Multiple blocks are linked together to form the blockchain.

Blockchain Network - the distributed network where the blockchain is used.

Node - a system within the blockchain network that can be associated with a specific user. There are three types of nodes: full nodes, lightweight nodes, and publishing nodes. Full nodes hold a copy of the entire blockchain or have access to the root copy of it. Publishing nodes can publish new blocks to the blockchain, while lightweight nodes only contain metadata of the blocks.

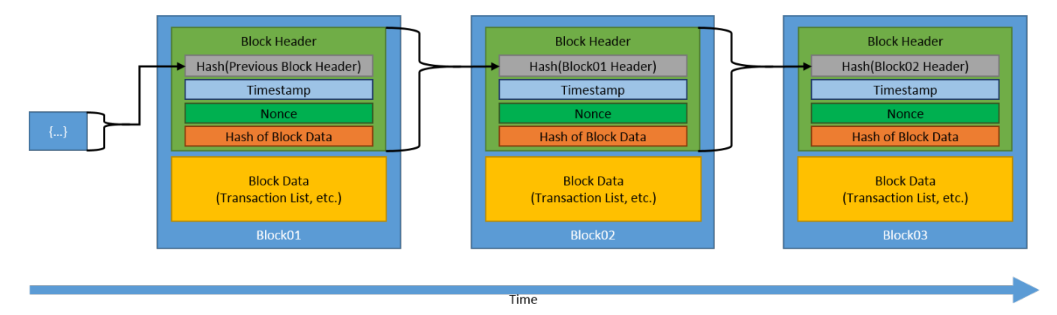
****

Illustration 1 – Generic Chain of Blocks

To illustrate the concept of blockchain, take a look at Illustration above, which displays blockchain visualization. Each rectangle represents a block with all its contents. The blocks are linked together in a chain, with each block chained to its succeeding block. Blocks are never removed, only additional blocks are added. The chaining of each block is done through cryptography, which is explained in detail in the following section. As more blocks are added, it becomes increasingly difficult to access and modify older blocks due to the computationally infeasible obstacle presented by the cryptographic chain of each block. To access older blocks, each block succeeding it must be successfully decrypted.

Another important concept in blockchain is the consensus model. This refers to a universally agreed upon set of rules and validations by all blockchain users, which must be met for a new block to be published in the blockchain. The consensus model was briefly mentioned in the Background section, but it is important to elaborate on it as it is a fundamental aspect of blockchain technology. [4]

**Blockchain Components [5]**

**Ledger**

A ledger is essentially a collection of transactions that documents the exchange of goods and services between parties. In the past, people used pen and paper to record these transactions. But with the advent of technology, digital ledgers came into existence. Typically, these ledgers are owned and operated by centralized trusted third parties, who manage them on behalf of the users in a community. These ledgers with centralized ownership can be implemented in a centralized or distributed fashion, depending on the requirements of the system.

However, there are several concerns related to trust, security, and reliability with centrally owned ledgers. For instance, the ledger may be lost or destroyed, and users must trust that the owner is properly backing up the system. Also, the ledger may be located entirely in specific geographic locations, which can result in network outages, rendering the ledger and services that depend on it unavailable.

Furthermore, the transactions on a centrally owned ledger are not always made transparently, and there may be a risk that they are not valid. Users must trust that the owner is validating each received transaction. Additionally, the transaction list on a centrally owned ledger may not be complete, and users must trust that the owner is including all valid transactions that have been received. There is also a risk that the transaction data on a centrally owned ledger may have been altered, and users must trust that the owner is not altering past transactions.

Blockchain technology has emerged as a solution to these concerns related to centralized ownership of ledgers. The technology enables distributed ownership and a distributed physical architecture of the ledger. This architecture involves a much larger set of computers than is typical for centrally managed distributed physical architecture. The nodes on a blockchain network all have a copy of the ledger, and they all update and sync with the same data, making loss or destruction of the ledger difficult. This makes blockchain technology inherently resilient to attacks and geographic diversity.

Moreover, a blockchain network must check that all transactions are valid. This means that if a malicious node was transmitting invalid transactions, others would detect and ignore them, preventing the invalid transactions from propagating throughout the blockchain network. Additionally, a blockchain network holds all accepted transactions within its distributed ledger, and to build a new block, a reference must be made to a previous block. If a publishing node did not include a reference to the latest block, other nodes would reject it.

Finally, a blockchain network utilizes cryptographic mechanisms, such as digital signatures and cryptographic hash functions, to provide tamper-resistant ledgers. This ensures that the transaction data on the ledger cannot be altered by malicious actors. In summary, blockchain technology offers advantages over centrally owned ledgers, including resilience to attacks, geographic diversity, and increased transparency.

**Blocks**-

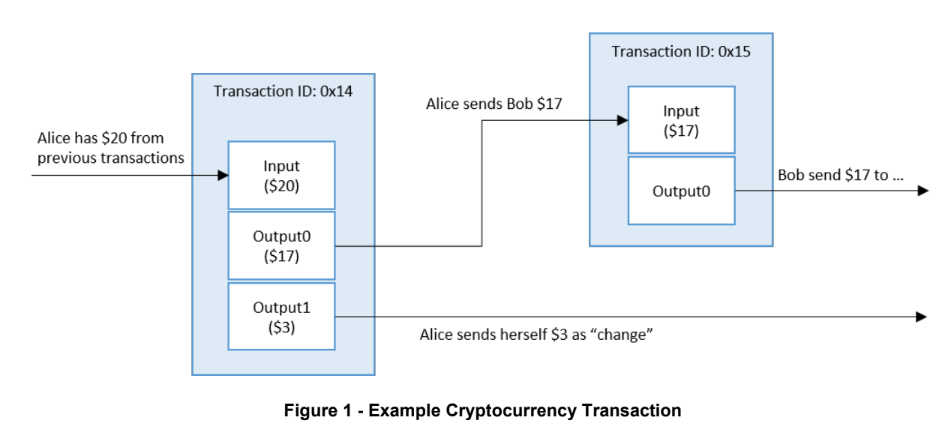
A blockchain consists of interconnected blocks, and the users of the blockchain submit transactions to the network. This is usually done through web or phone applications. Once a transaction is submitted, it must wait until a publishing node adds it to a block on the blockchain.

Each block on the blockchain has a header that contains information about the block, and the block data itself contains a list of verified transactions. To verify a transaction, the blockchain network checks that both parties involved in the transaction have digitally signed it using cryptographic functions. This ensures that the transaction is valid and cannot be tampered with.

**Transaction-**

In a blockchain, a transaction refers to the exchange of assets between two parties. While in the context of cryptocurrency, this typically involves the transfer of digital coins from one user to another within the network, transactions can also encompass any recorded activity involving digital or physical assets.

For a blockchain transaction to occur, the sender (party A) must provide a list of the assets they wish to transfer to the recipient (party B), along with details about the source of the assets and proof of access using digital signatures. The recipient's details and the amount of assets to be transferred are also included in the output data.



For instance, suppose Alice wants to send Bob $17. In this scenario, Alice's assets' source is $20, and she intends to send only $17 to Bob. Therefore, the transaction will have two outputs - the first one with $17 sent to Bob and used as an input for Bob's future transaction (transaction ID 0x15), and the second output will be the "change" Alice sends herself, which is the remaining $3 from the original $20 input.

**Reliability-**

In a blockchain network, reliability is paramount as it ensures the integrity of the network. The blockchain network operates on a system that does not require users to undergo an identification process, and therefore a trust mechanism is required to ensure the validity of the transactions. Unlike traditional ledger systems where a trusted mediator such as a bank is used, the blockchain network relies on various methods to establish trust among its users.

One of the key components of the blockchain network is its "append only" ledger, which is shared among all users. This means that all users have access to the entire history of transactions, making it virtually impossible for anyone to modify previously published blocks. In contrast, in traditional databases, data modification is allowed, which leaves the system open to the risk of malicious modification.

Another way in which the blockchain network establishes trust is by ensuring that each block is cryptographically secure. This is achieved through various cryptographic functions that ensure the security of the data contained in each block. Additionally, the blockchain network is built on a distributed architecture, with ownership and consensus models in place to ensure the validity of each transaction. This means that a set of predefined rules and validations are followed to determine whether a new block will be added to the blockchain. As the network is run across multiple nodes, all following the same consensus models, it becomes difficult for a malicious user to try and bypass the consensus models to publish a new block.

**Blockchain classification-**

In blockchain, there are two main permission models that determine who has the ability to read and write on the blockchain. The first is the permissionless model, which allows anyone to participate in the network and contribute to the consensus models. This model is typically implemented using open-source software, and users who follow the rules can receive cryptocurrency as a reward.

The second permission model is permissioned, which is managed by a central entity such as a company's executives. This model limits the read/write privileges of users and is usually implemented using closed-source software. Although the permissioned model may limit the freedom of users, it allows for the use of cheaper consensus models for publishing new blocks.

The advantage of a permissioned model is that users are individually granted permissions and are identified by a managing entity, which increases trust and reliability. This allows for the bypassing of resource-heavy rules that are necessary for trust purposes in a permissionless model.

**Cryptographic Hash Functions**

Hashing is a cryptographic technique used to generate a unique digital fingerprint or "digest" of data. The hash function takes the input data and produces a fixed-length output that represents the original data. Hashing is deterministic, meaning that the same input data will always produce the same output hash.

The security of the hash function comes from its one-way nature, meaning that it is computationally infeasible to find two different inputs that produce the same output hash. Additionally, the hash function is "image resistant," which means that it is impossible to determine the original data from its hash value alone.

In blockchain, hash functions are used to secure data and ensure the integrity of the blockchain. Before data is hashed, a nonce value is added to increase the difficulty of cracking the hash. The hash function is frequently used to secure the block header and the block data in a blockchain network.

**Asymmetric-Key Cryptography**

In blockchain, transactions are signed digitally by the involved parties using cryptographic keys. Asymmetric key cryptography is used, which involves a pair of mathematically related keys - a private key and a public key. The private key is used to encrypt the transaction, and any user holding the corresponding public key can decrypt it. The public key is available to all users, and thus a decrypted transaction proves that the encrypter holds the corresponding private key, providing validation.

Symmetric key cryptography, on the other hand, uses the same key for both encryption and decryption. This results in faster computations but is less secure, as there is no individual private key to prove identity. In a permissioned blockchain model, where trust is established, symmetric key cryptography may be a more suitable option. However, in a permissionless model, asymmetric key cryptography is preferred to ensure secure and validated transactions.

**Consensus Models**

Blockchain technology relies heavily on the concept of consensus to determine which user publishes the next block in the chain. This becomes particularly important in a permissionless blockchain where any user can read/write and potentially attempt to publish a new block. This is where the concept of "mining" comes in, where users are awarded cryptocurrency for successfully publishing a block or for validating transactions through transaction fees.

The consensus model of a blockchain is critical in managing the many attempts at publishing blocks. In order for a new block to be added to the blockchain, it must be individually approved by each user in the network. This approval process is usually automated through software.

There are multiple consensus models in practice within blockchain networks, each with their own advantages and disadvantages. Two common models are the proof-of-work (PoW) and proof-of-stake (PoS) models. These models differ in how they select the user to publish the next block, and how they incentivize users to participate in the consensus process.

1.  
**Proof of Work Consensus Model**

The proof of work consensus model is based on the concept that the first user to solve a complex mathematical puzzle earns the right to publish the next block in the blockchain. This solution, called the "proof of work," requires substantial computational resources, such as energy, time, and hardware. In contrast, verifying that the solution is correct is relatively inexpensive and quick, allowing for immediate verification of the user's eligibility to publish the next block. One common method of creating a puzzle is to choose a hexadecimal number and require the solution to be the hash of the block header to be published, such that the hash is a number lower than the chosen number. Once a user finds a solution, they send it to the full nodes in the blockchain network for verification. The full nodes then quickly and easily verify the solution before publishing the new block to their copy of the blockchain, which then propagates throughout the entire network.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

The Illustration above demonstrates an example of a puzzle used in the proof of work consensus model, where SHA265 is the hashing function used in this specific example. The puzzle requires a solution to be any digest with six leading zeros. The first two examples in the illustration, “blockchain0” and “blockchain1”, do not contain the necessary six leading zeros and are not solutions to the puzzle. However, in the final example, the hashing on the data “blockchain10730895” results in a digest that meets the condition, and is therefore accepted as a solution to the puzzle. Once a user finds a solution, they send it to the full nodes in the blockchain network for verification. If the solution is verified, the user is granted the ability to publish their new block. To find a solution, users must continually modify the data slightly until they reach a digest that satisfies the puzzle condition. This process can be computationally expensive and time-consuming due to the large number of digest possibilities. In some cases, the puzzle conditions are changed periodically to increase the difficulty level and reduce the time available for users to solve the puzzle. In the case of Bitcoin, the puzzle conditions are changed every 2016 new blocks, resulting in an average of one successful new block published every ten minutes.

1. **Proof of Stake Consensus Model**

The proof of stake consensus model operates under the assumption that the more invested a user is in a blockchain system, the more they will prioritize its success and refrain from malicious activity. This investment is typically in the form of cryptocurrency that is locked into the system through a wallet.

Unlike the proof of work model, proof of stake does not require computationally intensive puzzles to be solved. Instead of receiving rewards for successfully publishing a new block, users are compensated through transaction fees paid by other users wishing to publish their own transactions in the block.

There are various methods for implementing the stake in this model, with two commonly used approaches being random selection and multi-round voting. With random selection, the probability of a user being chosen to publish a new block is proportional to the percentage of the total stake they hold. With multi-round voting, users with stake are selected to propose new blocks, and each round of voting results in the selection of one block for publication. It may take several rounds of voting to reach a sufficient number of votes to publish a block.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

**Blockchain Limitations and Misconceptions**

There are some limitations and misconceptions regarding blockchain technology that should be taken into consideration. One common misconception is the idea that no one controls a blockchain. However, this is not entirely true, as there is a certain level of control over the blockchain network, whether it is a permissioned or permissionless blockchain. [7]

Another limitation to consider is the possibility of a blockchain "death". Unlike centralized systems that can be easily dismantled and reconstructed, shutting down a blockchain network can be difficult due to its distributed nature. Even if a shutdown is successful, there may still be active nodes remaining, which can be exploited by malicious users attempting to modify blocks and bypass the consensus models and validation mechanisms. This is especially concerning if frequent reconstruction of the system is needed. [8]

Overall, while blockchain technology has its benefits, it is important to understand its limitations and potential vulnerabilities.

**Conclusion**

Blockchain technology, with its distributed architecture and ownership, has emerged as a promising tool for organizations. The popularity of blockchain applications has surged since Bitcoin. However, the current hype around the technology and the plethora of proposed uses may not accurately reflect its long-term impact. As with any new technology, it is essential to evaluate the advantages and disadvantages of blockchain before adopting it for a specific application. While some organizations may find blockchain's numerous features desirable, others may see them as obstacles preventing their adoption of the technology. [9]

תמונה שמכילה תרשים

התיאור נוצר באופן אוטומטי

**Bibliography**

Our work is based on the article:

*D. Yaga, P. Mell, N. Roby, K. Scarfone,*

*“Blockchain Technology Overview”, NIST 8208, October 2018,*

[*https://doi.org/10.6028/NIST.IR.8202*](https://doi.org/10.6028/NIST.IR.8202)

**References:**

[1]: 12.

[2]: 13-14

[3]: 6-14

[4]: 13-14

[5]: 7-27

[6]: 35

[7]: 36

[9]: 41-46