

**BLOCKCHAIN TECHNOLOGY**

**Presented by:**

**Summiya saif ( 221243)**

Table of Contents

[1. Blockchain 3](#_Toc123674648)

[2. Blockchain Technology 4](#_Toc123674649)

[2.1 Block 4](#_Toc123674650)

[2.2 Digital signature 5](#_Toc123674651)

[2.3 Key characteristics of blockchain 6](#_Toc123674652)

[2.4 Taxonomy of blockchain systems 7](#_Toc123674653)

[3. Application of Blockchain 8](#_Toc123674654)

[Conclusion 8](#_Toc123674655)

[Reference 9](#_Toc123674656)

# 1. Blockchain

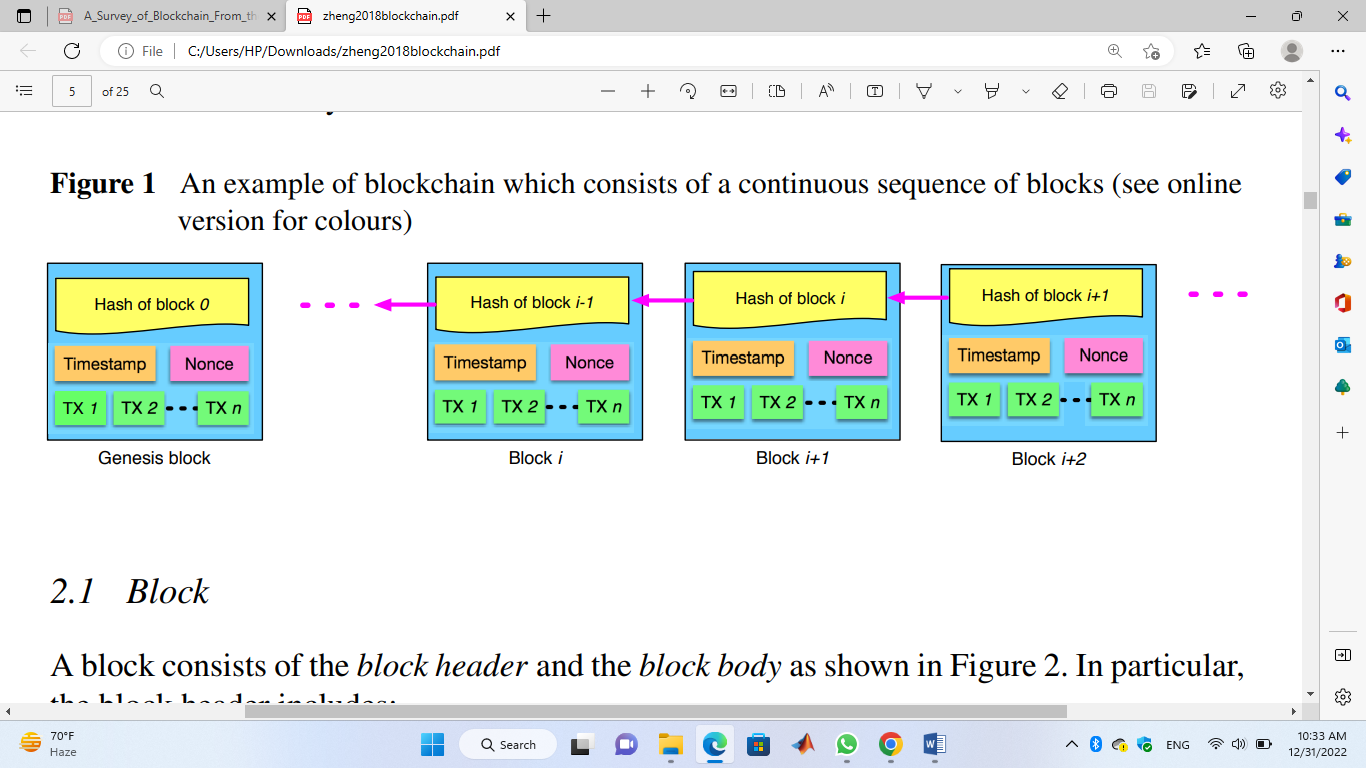
Recently, cryptocurrency has attracted extensive attentions from both industry and academia. Bitcoin that is often called the first cryptocurrency has enjoyed a huge success with the capital market reaching 10 billion dollars in 2016. The blockchain is the core mechanism for the Bitcoin. Blockchain was first proposed in 2008 and implemented in 2009. Blockchain could be regarded as a public ledger, in which all committed transactions are stored in a chain of blocks. This chain continuously grows when new blocks are appended to it. The blockchain technology has the key characteristics, such as decentralisation, persistency, anonymity and auditability. Blockchain can work in a decentralised environment, which is enabled by integrating several core technologies such as cryptographic hash, digital signature (based on asymmetric cryptography) and distributed consensus mechanism. With blockchain technology, a transaction can take place in a decentralised fashion. As a result, blockchain can greatly save the cost and improve the efficiency.

Although Bitcoin is the most famous application of blockchain, blockchain can be applied into diverse applications far beyond cryptocurrencies. Since it allows payments to be finished without any bank or any intermediary, blockchain can be used in various financial services such as digital assets, remittance and online payment. Additionally, blockchain technology is becoming one of the most promising technologies for the next generation of internet interaction systems, such as smart contracts, public services, internet of things (IoT), reputation systems and security services.

Despite the fact that the blockchain technology has great potential for the construction of the future internet systems, it is facing a number of technical challenges. Firstly, scalability is a huge concern. Bitcoin block size is limited to 1 MB now and a block is mined about every 10 min. Subsequently, the Bitcoin network is restricted to a rate of 7 transactions per second, which is incapable of dealing with high-frequency trading. However, larger blocks mean larger storage space and slower propagation in the network. This will lead to centralisation gradually as users would like to maintain such a large blockchain. Therefore, the tradeoff between block size and security has become a challenge. Secondly, it has been proved that miners can achieve larger revenue than their fair share through selfish mining strategy. Miners hide their mined blocks for more revenue in the future. In that way, branches can take place frequently; this hinders blockchain development. Hence some solutions need to be put forward to fix this problem. Moreover, it has been shown that privacy leakage can also happen in blockchain even when users only make transactions with their public key and private key. User’s real IP address could even be tracked. Furthermore, current consensus algorithms like proof of work (PoW) or proof of stake (PoS) are facing some serious problems. For example, PoW wastes too much electricity energy while the phenomenon that the rich get richer could appear in the PoS consensus process. These challenges need to be addressed in the blockchain technology development.

# 2. Blockchain Technology

The blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger. Figure 1 illustrates an example of a blockchain. Each block points to the immediately previous block via a reference that is essentially a hash value of the previous block called parent block. It is worth noting that uncle blocks (children of the block’s ancestors) hashes would also be stored in ethereum blockchain. The first block of a blockchain is called genesis block which has no parent block.



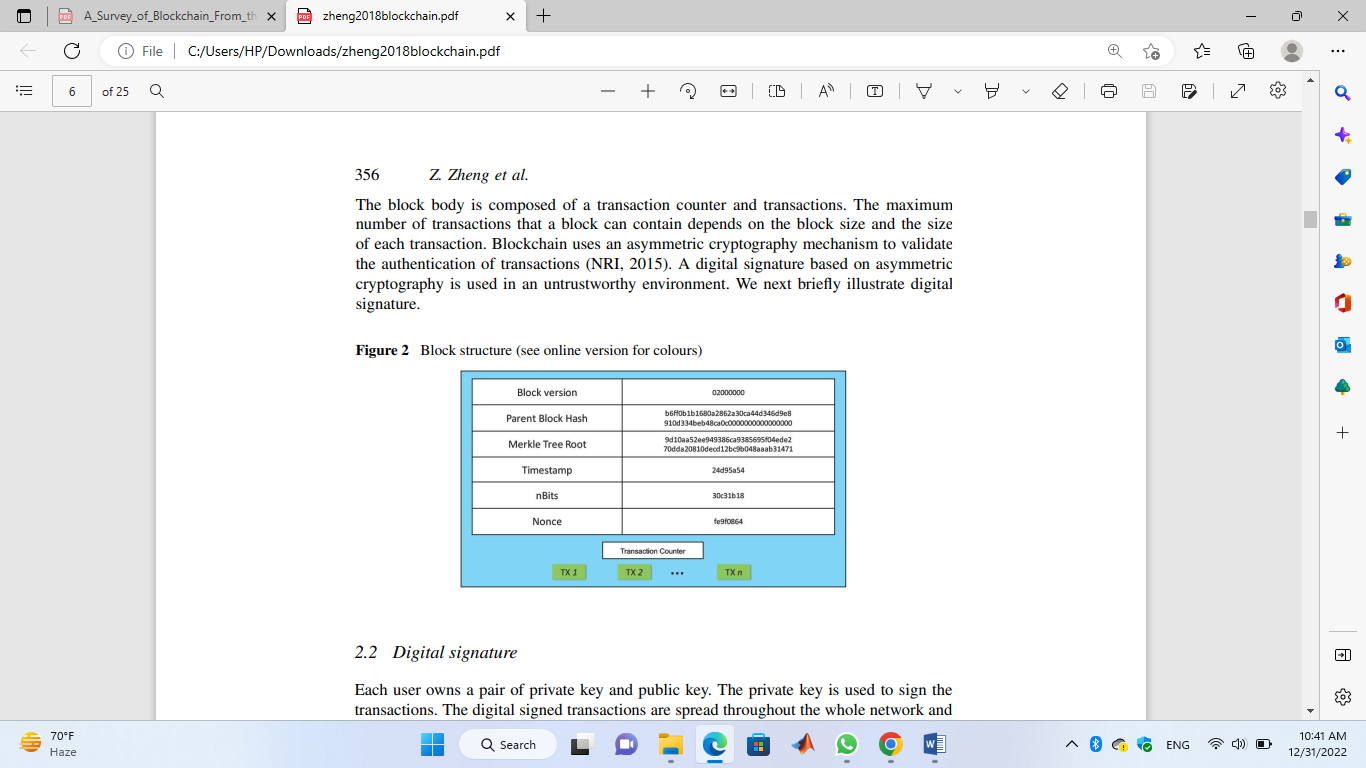
**Figure 1** An example of blockchain which consists of a continuous sequence of blocks.

## 2.1 Block

A block consists of the block header and the block body as shown in Figure 2. In particular, the block header includes:

* Block version: indicates which set of block validation rules to follow.
* Parent block hash: a 256-bit hash value that points to the previous block.
* Merkle tree root hash: the hash value of all the transactions in the block.
* Timestamp: current timestamp as seconds since 1970-01-01T00:00 UTC.
* nBits: current hashing target in a compact format.

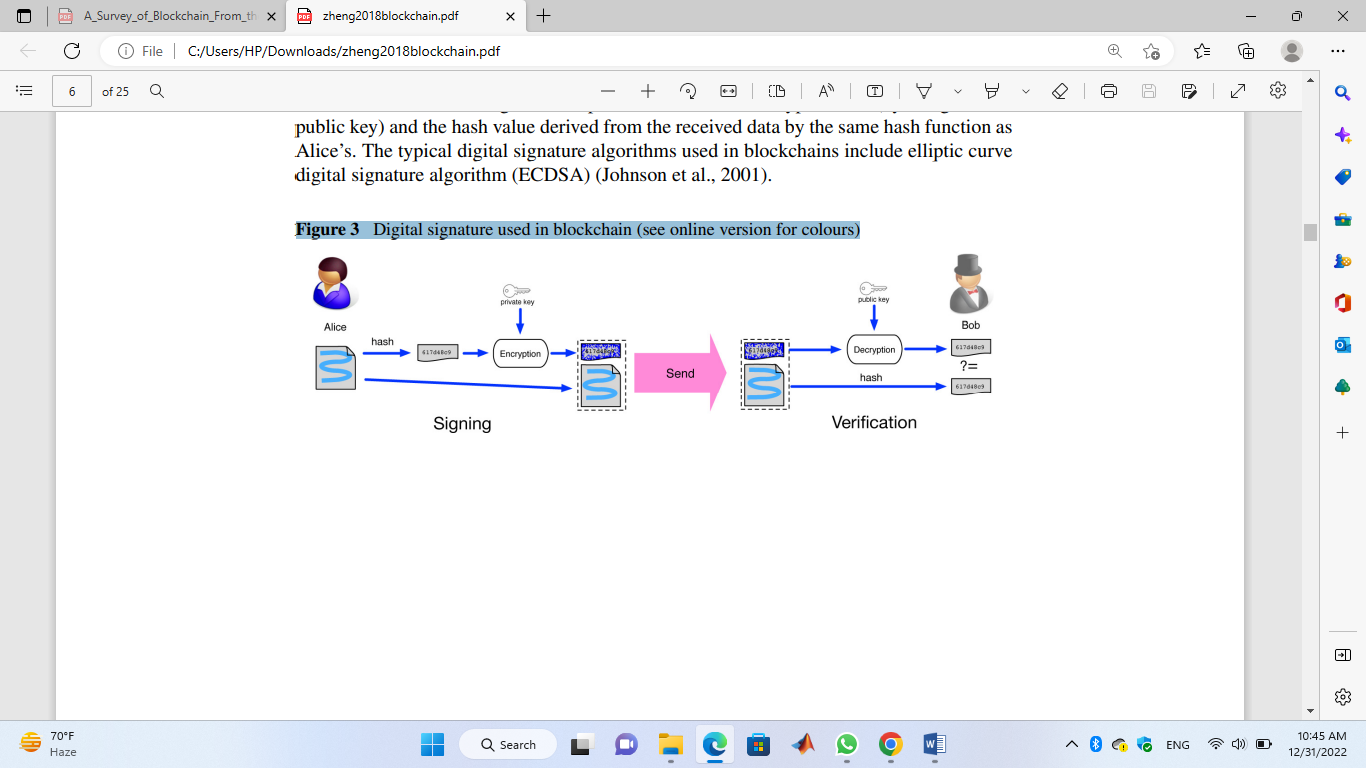
The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions. A digital signature based on asymmetric cryptography is used in an untrustworthy environment. We next briefly illustrate digital signature.



**Figure 2** Block structure

## 2.2 Digital signature

Each user owns a pair of private key and public key. The private key is used to sign the transactions. The digital signed transactions are spread throughout the whole network and then are accessed by public keys, which are visible to everyone in the network. Figure 3 shows an example of digital signature used in blockchain. The typical digital signature is involved with two phases: the signing phase and the verification phase. Take Figure 3 as an example again. When a user Alice wants to sign a transaction, she first generates a hash value derived from the transaction. She then encrypts this hash value by using her private key and sends to another user Bob the encrypted hash with the original data. Bob verifies the received transaction through the comparison between the decrypted hash (by using Alice’s public key) and the hash value derived from the received data by the same hash function as Alice’s. The typical digital signature algorithms used in blockchains include elliptic curve digital signature algorithm (ECDSA).



**Figure 3** Digital signature used in blockchain

2.3 Key characteristics of blockchain

In summary, blockchain has following key characteristics.

* Decentralisation. In conventional centralised transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank) inevitably resulting the cost and the performance bottlenecks at the central servers. Differently, a transaction in the blockchain network can be conducted between any two peers (P2P) without the authentication by the central agency. In this manner, blockchain can significantly reduce the server costs (including the development cost and the operation cost) and mitigate the performance bottlenecks at the central server.
* Persistency. Since each of the transactions spreading across the network needs to be confirmed and recorded in blocks distributed in the whole network, it is nearly impossible to tamper. Additionally, each broadcasted block would be validated by other nodes and transactions would be checked. So any falsification could be detected easily.
* Anonymity. Each user can interact with the blockchain network with a generated address. Further, a user could generate many addresses to avoid identity exposure. There is no longer any central party keeping users’ private information. This mechanism preserves a certain amount of privacy on the transactions included in the blockchain. Note that blockchain cannot guarantee the perfect privacy preservation due to the intrinsic constraint (details refer to Section 5).
* Auditability. Since each of the transactions on the blockchain is validated and recorded with a timestamp, users can easily verify and trace the previous records through accessing any node in the distributed network. In Bitcoin blockchain, each transaction could be traced to previous transactions iteratively. It improves the traceability and the transparency of the data stored in the blockchain.

2.4 Taxonomy of blockchain systems

Current blockchain systems can be roughly categorised into three types: public blockchain, private blockchain and consortium blockchain. We compare these three types of blockchain from different perspectives. The comparison is listed in Table 1.

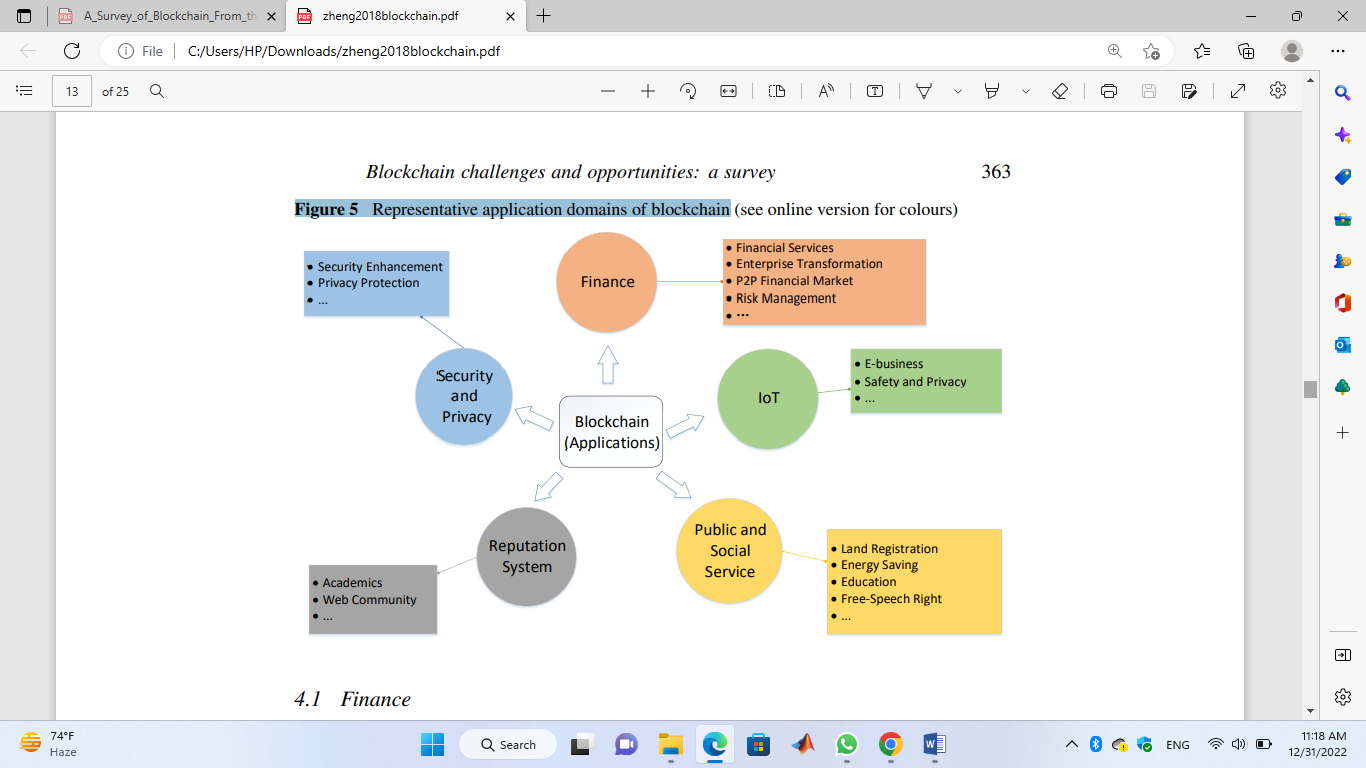
**Table 1** Comparisons among public blockchain, consortium blockchain and private blockchain

|  |  |  |  |
| --- | --- | --- | --- |
| ***Property*** | ***Public blockchain*** | ***Consortium blockchain*** | ***Private blockchain*** |
| Consensus determination | All miners | Selected set of nodes | One organisation |
| Read permission | Public | Could be public or resisted | Could be public or resisted |
| Immutability | Nearly impossible to tamper | Could be tampered | Could be tempared |
| Efficiency | Low | High | High |
| Centralised | No | Partial | Yes |
| Consensus process | Permissionless | Permissioned | Permissioned |
|  |  |  |  |

Since public blockchain is open to the world, it can attract many users. Communities are also very active. Many public blockchains emerge day by day. As for consortium blockchain, it could be applied to many business applications. Currently, Hyperledger is developing business consortium blockchain frameworks. Ethereum also has provided tools for building consortium blockchains (ethereum, n.d.). As for private blockchain, there are still many companies implementing it for efficiency and auditability.

# 3. Application of Blockchain

There is a diverse of applications of blockchain technology. In this section, several typical applications of blockchain are summarised.



**Figure 5** Representative application domains of blockchain

# Conclusion

The blockchain is highly appraised and endorsed for its decentralised infrastructure and peer-to-peer nature. However, blockchain could be applied to a variety of fields far beyond Bitcoin. Blockchain has shown its potential for transforming the traditional industry with its key characteristics: decentralisation, persistency, anonymity and auditability. Researchers also investigate typical blockchain applications. Nowadays smart contract is developing fast and many smart contract applications are proposed. However, as there are still many defects and limits in smart contract languages, many innovative applications are hard to implement currently. As the blockchain technology is acquiring immense attention from public and private sectors, more smart contract-based applications would be put into use.

# Reference

* T. Aste, P. Tasca, and T. D. Matteo, ‘‘Blockchain technologies: The foreseeable impact on society and industry,’’ Computer, vol. 50, no. 9, pp. 18–28, Jan. 2017.
* S. Nakamoto et al., Bitcoin: A Peer-to-Peer Electronic Cash System. Citeseer, 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf
* K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, ‘‘Blockchain for AI: Review and open research challenges,’’ IEEE Access, vol. 7, pp. 10127–10149, 2019.
* A. Litke, D. Anagnostopoulos, and T. Varvarigou, ‘‘Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment,’’ Logistics, vol. 3, no. 1, p. 5, Jan. 2019.
* M. Kouhizadeh and J. Sarkis, ‘‘Blockchain practices, potentials, and perspectives in greening supply chains,’’ Sustainability, vol. 10, no. 10, p. 3652, Oct. 2018.
* Akins, B.W., Chapman, J.L. and Gordon, J.M. (2013) A Whole New World: Income Tax Considerations of the Bitcoin Economy. antshares (2016)
* Antshares Digital Assets for Everyone, <https://www.antshares.org>.
* Atzori, L., Iera, A. and Morabito, G. (2010) ‘The internet of things: a survey’, Computer Networks, Vol. 54, No. 15, pp.2787–2805.
* Axon, L. (2015) Privacy-Awareness in Blockchain-based PKI, CDT Technical Paper Series. azure (2016) Microsoft
* Azure: Blockchain as a Service, https://azure.microsoft.com/enus/solutions/blockchain.
* Barcelo, J. (2014) User Privacy in the Public Bitcoin Blockchain.
* Bentov, I., Lee, C., Mizrahi, A. and Rosenfeld, M. (2014) ‘Proof of activity: extending Bitcoin’s proof of work via proof of stake [extended abstract]’, ACM SIGMETRICS Performance Evaluation Review, Vol. 42, No. 3, pp.34–37.
* Billah, S. (2015) One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner