Blockchain

Muhammed Said Kaya
Department of Computer Science
Hacettepe University
Ankara, Turkey

Remzi Çiçek
Department of Computer Science
Hacettepe University
Ankara, Turkey

Ali Kayadibi
Department of Computer Science
Hacettepe University
Ankara, Turkey

1 Introduction

Blockchain is a new technology that is been around last ten years and it is trending in Information technology industry.,It has gained worldwide popularity with a new cryptocurrency unit Bitcoin.The main is a new idea to keep data on distributed network instead of centralized network.This way this technology is adapted to other industries. It is commonly used in banking, investing and cryptocurrency topics. Blockchain is a set of distributed databases known as "blocks" that contain records of digital transactions. These interconnected blocks support the decentralization of systems and ensures that data is securely distributed and publicly visible. Many refer to blockchain as a public distributed ledger. It is continuously growing list of blocks which are connected with hash codes, secured with cryptographic methods.Blockchain is maintained by peers in P2P transaction network, where peers record transactions in a period of time and packaged them together into a block to join the blockchain In the last years, many companies are trying to adapt to this technology because many innovations have been developed on the Blockchain technology. Some of these innovations are supply tracking systems , crowd funding systems that make donations and transactions publicly visible.

2 Features of Blockchain

2.1 Distribution Ledger Technology

Blockchain uses distributed ledger technology. With distributed ledger technology, there will no longer be a central node. Participants on each node of the network can access the records shared on that network and store a copy of the same records. In addition, any changes or additions made to the book can be reflected to all participants in a short time. In other words, all transactions made on the blockchain can be registered on the nodes in this chain. Thus, there will not be a central structure where records are kept. In this decentralized system, a single node will no longer have any pressure on other nodes.

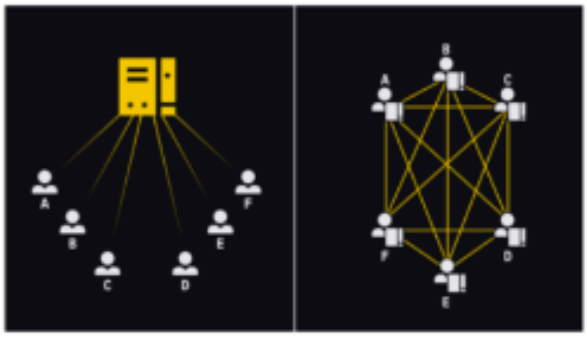

Fig. 1. Decentralized versus Centralized Networks

2.2 Transparency

Blockchain technology provides a decentralized structure and provides transparency. Every transaction recorded on the blockchain can be stored or tracked by anyone on that network. Thus, any node can control the data in the blockchain and develop applications based on this system. In addition, the private information of the parties that make transactions is encrypted, taking into account personal privacy. Thanks to this transparency offered by the blockchain, it enables the monitoring of all blocks and transactions up to the genesis block. It creates a trust environment of its decentralized structure with traceability that provides transparency in the blockchain.

2.3 Immutable

With its decentralized structure, blockchain technology allows everyone in the chain to store the information in the node and thus provides the possibility of unchangeable. Once transactions on the blockchain are verified and added to the chain as a block, they are stored forever. Because records are kept in multiple locations, information is not lost if a single network is damaged or cyber attacked. Also, interference with this chain in one place will not match the chains of other nodes, so it is immediately noticed and considered invalid. In order for such an attack to be successful, it is necessary to control more than 51 percent of the entire system. Considering that the data is copied and stored on many different nodes, this attack possibility is almost impossible. This shows how reliable the data on the blockchain is.

2.4 Low transaction cost

The decentralized distributed structure of blockchain technology eliminates the possibility of a single center to manage transactions. Each node in this network can perform peer-to-peer transactions without the need for an intermediary. Commissions paid to intermediaries in traditional systems also disappear. In addition, transactions can be carried out faster because intermediaries are eliminated.

2.5 Security

It provides confidence with features such as immutable and transparency provided by blockchain technology. Thanks to its distributed structure, every person, every computer who can access the network using the internet is like a center. All data is stored on all these computers, and it is necessary to capture many nodes of the network in order to change or delete data or stop the system. Since this is very difficult or even impossible, a security is provided against attacks.

3 Brief History on Blockchain

The roots of Blockchain technology stem back to the year 1980s. First application of Blockchain is Bitcoin, which peer-to-peer electronic cash system, created by Satoshi Nakamoto in 2009. Before we deep into Bitcoin History , let's understand the brief history of blockchain and how it came into being. Pre Bitcoin-2009; There has been libertarian dreams and ideals by a group named Cypherpunk and with the advance of technology in 1980s. They published Manifesto "Privacy is necessary for an open society in the electronic age." because of since 1980s in electronic age , all transactions digitized and are free from government such as privileges and also by big companies like Google, Facebook. As a conclusion, Secure Communication was provided in the presence of third parties by using Cryptography. David Chaum who is one of the Cypherpunk attempted a centralized untraceable cash system is named DigiCash in 1988. Also worked on some new technologies like public key encryption while creating public and private keys. But the attemption was failed and also experiments of Cypherpunks continued to resulted in failure. In 2009, Who is unknown Satoshi Nakamoto is the creator of Bitcoin. He published a white paper that brilliantly combined all previous Cypherpunks efforts to create peer-to-peer electronic cash system and digital currency. In Blockchain technology transactions being stored in blocks which contains transactions and first block is called Genesis Block. Hal Finney received the first bitcoin transaction from Bitcoin's creator Satoshi Nakamoto on Jan 12,2009 and thereby Genesis block mined on Jan 3,2009. Exchange of first ever Bitcoin happened on May 21,2010 by a human is named Laszlo Hanteczwhile purchasing 25 dollar worth of pizza for 10,000 BTC. Anonymity in Bitcoin disappears during the exchange of real money and illegal works are followed. Bitcoin has basic and technical problems, such as its speed, preventing its use in daily life (without exchanging). (LO used in Turkey for Exchange: Bians, Coinbase and they are controlled by the government) In 2015, Ethereum Platform was created by Vitalik Buterin for programmable blockchain. Ethereum enables to develop applications on decentralized networks using by Ethereum Virtual Machine and Smart Contracts and Decentralized Autonomous Organizations (DAO). DAO is a fully autonomous organization. In 2016, DAO had maken up 14 of Ethereum network. The hackers attacked the DAO tokens and stolen nearly 50 million. The Ethereum communities fall into disagreement about deleting transactions and it caused the fork.So It was divided into Ethereum(ETH) and Ethereum Classic(ETC) which is the first Ethereum using the original blockchain. Bitcoin and Ethereum Platforms are permissionless blockchain systems. For enterprise applications , Permissioned network requires. There are some platforms like Quorum which is fork of Ethereum and also Hyperledger by used companies.

4 Blockchain Structure

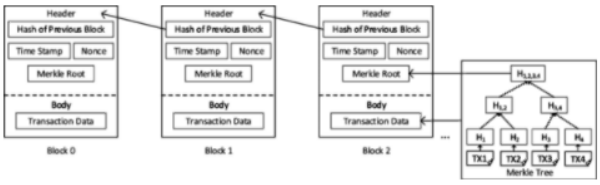

Fig. 2. Block Structure

Blockchain concept is formed by connecting multiple blocks to each other. Blocks are created to record transactions. Transactions that should be registered on the blockchain are recorded in blocks. By connecting these blocks to each other, a transaction record chain is formed. The act of linking the blocks that make up the blockchain concept is done using cryptographic techniques. If we explain this cryptographic technique simply; The hash value of the generated block is taken and this value is placed in

the next block. Since the hash value consists of data that includes all the information in a block, when a data in the block changes, the hash value changes and it can be easily determined that the block has been changed. This hash value is generated by miners in a way that certain rules are followed. Thus, the creation and validity of the block is ensured. Those who do this mining are called miners.

The blockchain stores all transaction data recorded in the chain since the block that stores the initial transaction. Thus, the records are kept under record until the starting block called Genesis and all records can be accessed. There is also the concept of block height here. This notion indicates the number of all blocks formed from the genesis block.

A block consists of a header and a body part. Timestamp, the hash operation information of the previous block, merkle root and nonce values are kept in the header of block. In the Body section, the transaction information to be recorded, which is the purpose of creating the block, is kept.

4.1 Header

4.1.1 Hash of Previous Block

When a block is added to the blockchain, it stores the hash value of the previous block in its header. Thus, whichever of the previous blocks is changed, the calculated hash value of the changed block changes, and this also affects the hash value of the block that stores its hash value. Because the previous hash value kept there changes, that is, because any data is changed in a block, the hashing value of the block also changes and this affects the hashing value of the block holding its hash value. This effect occurs in chain form until the last block. Thus, it is determined whether any block has been changed or not.

Hashing is the process of creating a fixed size output from different sized inputs. This operation is a mathematical operation called hash functions. Through functions called cryptographic hash functions, blockchains have a high level of data integrity and security. The most important feature of hashing algorithms is that they are designed as one-way functions. In other words, when a hash function is applied to a data, a hashing value is created. Reverse engineering to access the data from this hashing value cannot be done without spending huge amounts of computing time and resources. Another feature of hashing is that it is deterministic. So a hashing algorithm always gives the same output as long as the input is not changed. The security of the hash algorithm is equivalent to the difficulty of doing this reverse engineering process. So, the harder the input is to find, the more secure the hashing algorithm is considered to be.

4.1.2 Timestamp

Timestamps indicate when a block was created. The timestamp must be protected from being altered. As explained in the hashing section, if a data in the block changes, the hashing result will change, so the change in the time stamp is detected immediately. Timestamp plays the role of a notary and is more reliable than a traditional notary.

4.1.3 Nonce

While creating the proper hash value for a block, the data in the block needs to be protected, so an updateable data is needed to obtain a canonical hash. This data is called nonce. By changing this nonce value, miners find the proper hash value and are entitled to include the block in the chain.

4.1.4 Merkle Root

The hash values of all blocks in the blockchain are reduced to a root value using the tree structure. Thus root keeps the hash of all blocks' hashes. This root is called merkle root. Any changes in the blocks are detected more quickly. In addition, the storage value of this merkle root is more efficient than storing the hash values of all blocks. Thus, the Merkle tree increases security in a more practical way. Merkle Root makes it easier to process large amounts of data. The merkle tree in the blockchain is used to configure transactional data using less resources. A Merkle tree keeps blockchain data aggregated efficiently and securely. It provides rapid verification of blockchain data and rapid movement of large amounts of data from one computer node to another in the peer-to-peer blockchain network.

Merkle tree application method: A hashing value is obtained by hashing the hash results of two separate blocks that have been hashed. The process of combining hashing values is repeated until a single hashing value is generated. The last hash value is called Merkle root. Merkle roort provides a summary of the hash values of all blocks so far. The Merkle root summary is then added to the block header.

4.2 Body

4.2.1 Transaction Data

It is a process performed. Blocks are generated and put on the blockchain to prevent these transactions from being changed.

https://blockgeeks.com/guides/ethereum/

5 Ethereum

Ethereum is a blockchain platform for decentralized applications. Although often associated with Bitcoin, blockchain technology has many other applications that go beyond digital currencies. Until relatively recently, building blockchain applications required a complex background in coding, cryptography, mathematics, and important resources. From electronic voting and digitally recorded property assets to regulatory compliance, previously unimaginable practices are now actively developed and implemented faster than ever before. Ethereum makes all this possible by providing developers with tools to build decentralized applications.

5.1 History

Ethereum was initially described in a white paper by Vitalik Buterin who is a programmer ,in 2013 for creating decentralized applications. Buterin had argued that Bitcoin needed a scripting language for application development. He

proposed the development of a new platform with a more general scripting language. Development of Ethereum software project began in early 2014 .The basic idea is putting executable smart contracts in the blockchain needed to be specified before software could be implemented.Olympic which the Ethereum testnet released on May 2015. The first stage of Ethereum's development "Frontier" was released on July 30, 2015. Homestead, the first stable ethereum release , went out on block 1,150,000 on March 14, 2016.

5.2 Ethereum Virtual Machine

The Ethereum Virtual Machine (EVM), Ethereum's core innovation, is the complete Turing software running on the Ethereum network. This allows anyone to run any program, regardless of enough time and memory. The Ethereum Virtual Machine makes the process of building blockchain applications easier and more efficient than ever. Ethereum allows thousands of different applications to be developed on a single platform, instead of creating a completely original blockchain for each new application. The Solidity language itself is the tool we use to generate machine-level code that can be run in the EVM, it is a language.

5.3 Smart Contract

One of the best things about blockchain is that since it's a decentralized system between all permitted parties, there is no need to pay intermediaries (Brokers) and it saves you time and conflict. Although blockchains have problems with the process and speed of structural transaction approval, the cheapness of the transactions and the elimination of the 3rd structure leads states, governments and banks to use this technology. The fact that smart contracts can be used in people's property exchange or any action that requires a mediator is one reason to choose. For example, instead of the notary who is a mediator in real estate purchase and sale transactions, whenever payment is made with a smart contract on the blockchain, the owner of the real estate can be changed.

Fig. 3. Vitalik Buterin's Opinions About Smart Contract[1]

As a result ,Smart contracts can be used for all sorts of situations that range from financial derivatives to insurance premiums, breach contracts, property law, credit enforcement, financial services, legal processes, and crowdfunding agreements.

5.4 Ethereum vs. Ethereum Classic

There are both ethical and ideological differences between the Ethereum and Ethereum Classic chains. However, before explaining the differences, it is necessary to focus on the attacks and changes on decentralized autonomous organizations in 2016, which is an important point in the history of the Ethereum platform.

5.4.1 DAO : Decentralized Autonomous Organization

The Decentralized Autonotom Organization would create an event that had never been seen before on the DAO Ethereum Platform. With this organization, all future decentralized applications would be financed and a capital fund would be established. The way it works was as follows: If it was desired to have a say over the centralized applications to be financed, the distribution of funds in exchange for a certain amount of Ether would be given in return for the approval provided by that decentralized autonomous organization. How would you leave this organization if you wanted to? The split function was created by the system in order to realize this process and the exit door was opened to people. Never before has there been such a flexible, controlled and transparent system. People flocked to these decentralized autonomous organizations. After this influx, 150 million dollars of ether accumulation was realized in bulk sales within 28 days. While everything was going well, there was a situation like this. The condition for people to exit the system was that they could not spend their investment for 28 days. While most people argued that this could be a nuisance, decentralized autonomous organization creators assured that it would not be a problem. However, the attack caused by this situation caused the formation of Ethereum and Ethereum Classic chains in the future.

5.4.2 DAO Attack

On 17th June 2016, someone took advantage of this backdoor in the DAO and stole one third of the DAO's funds. Thats nearly $50 million dollars.The backdoor found by the hacker(s) was very simple in retrospect. If someone wanted to abandon the DAO, they can do so by submitting a request. Than the splitting function will give the user's ether in exchange of DAO tokens and register that transaction in the ledger and update the balances.What hacker did was, he recursively sent the request so splitting function did these two things over and over. He took 50 million worth of Ether by doing that and this was noticed by ethereum community. Community and the team wanted to take action and they have found three possible solutions. The options are nobody does anything, soft fork, hard fork.

Nobody Does Anything

Making any changes from outside might go against the nature and idea of crypto blockchain(immutable). And people didn't choose this.Majority choosed going with Soft Fork.

What Is A Soft Fork?

Soft fork works as an update in software.It is backward compatible.It is your choice to update or not and you can still communicate regardless this fork. They wanted to soft fork so that they can lock down the stolen ether by ignoring the blocks that contains hackers transactions.

What Is A Hard Fork?

Unline soft fork, hard fork is not backward compatible.There is no coming back and if you dont join you dont access updates or interact with users of the new system. And this is the part where the battle between Ethereum and Ethereum Classic comes out.

Ethereum vs Ethereum Classic

Some people wanted to stay in the original chain and did not accept the fork. They are called ethereum classic. Even founders moved onto new chain but why don't these people want to move to new chain? Their reason was, it was a stance against financial corruption. This is why blockchain is immutable. They wanted that to remain the same and untouched by humans from outside.

6 Permissioned and Permissionless Blockchains

The difference between Permissioned and Permissionless Blockchains is permissioned Blockchain(private blockchain) needs approval before using the Blockchain network meanwhile permissionless Blockchain lets anybody join and participate in the system.This is why they are used in different things. As one of the big disadvantages of crypto is that no one has power over how it operates, people will not be keen about using a permissioned cryptocurrency. For example some companies, banks who tracks shipping logistics, who keeps medical informations about patients don't want to store hidden information into a permissionless Blockchain. There are some similarities between Permissioned and Permissionless Blockchains.For example they both are distributed ledgers, both are theoretically immutable meaning that the data they store cannot be modified and both make us of consensus algorithm.

1. **Permissionless blockchains:** These blockchains allows anyone to transact and join as a validator. The data is publicly avaible and copies of the ledgers are stored across the globe. Some of the popular blockchains are Bitcoin, Ethereum, Litecoin, Dash, and Monero.
2. **Permissioned Blockchains:** These blockchains knows as private blockchains. They are closed to public and only who are allowed to access can access these blockchains. Anyone who wants to see the data or to validate the transaction needs an approval from central authority. This is useful for banks, companies which concerns about complete control over data. Ripple is one of the example of permissioned blockchains.

6.1 Problems on Permissionless Blockchain

While a secure transparent structure is provided thanks to the cryptography on which blockchain technology rests, the emergence of enterprise-based requirements reveals some of the problems of permissionless blockchains.

These problems are listed below.

Privacy: Transparent visibility of shared data or the content of transactions made without authorization by everyone is a problem that can cause problems in the corporate industry. For example, the requirement that the patient's own data in the health sector can only be seen by the authorized persons reveals this problem.

Performance: The long transaction confirmation period experienced on platforms such as Ethereum and Bitcoin is a problem in institutional functions. Also, the fact that volumetric and blockchain data cannot be scaled horizontally creates a problem.

Permissioning: One of the problems with the permissionless blockchain technology is that organizations must have a special place so that no one can view their data, and only authorities can transact on this platform.

6.2 Quorum

Quorum is a fork of the Etherum client geth. Quorum is an open source enterprise blockchain platform. Being open source increases the trust in this platform and enables many developers to contribute to the development of this platform. The Quorum blockchain platform is a platform that can attract corporate businesses to benefit from blockchain technology. Thanks to this platform, it is possible to create a permission blockchain network and use it within the organization. Blockchain technology provides a reliable, decentralized platform through its immutable, secure and transactional features. In addition to these features of Blockchain, corporate companies have some additional needs for extra security. For example, in order to ensure the security of private information within the organization, requirements such as preventing access by unauthorized persons to the network like transaction privacy and enterprise permissioning, multiple pluggable consensus mechanisms suitable for enterprise use cases, enterprise-grade permissions management (access control) for network nodes and participants, Enterprise-grade performance . The Quorum blockchain platform has been developed to provide these desired features.

6.2.1 Quorum Architecture

Quorum Node

Despite the Quorum Ethereum client is a geth fork, the Quorum node contains many different features that distinguish it from Etherum.

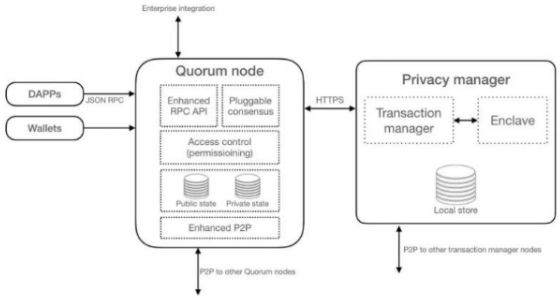

Fig. 4. Quorum high level architecture[12]

- **Consensus algorithm:** RAFT or Istanbul BFT consensus algorithms are used instead of Proof-of-Work to ensure consensus.
- **The Peer to Peer (P2P) layer:** It is arranged in such a way that only the allowed nodes can access the network and these nodes can perform the allowed tasks.
- **The block creation:** Block generation logic is done by ”global public state root” instead of ”global state root”.
- **The block validation:** Block validation logic is made by ”global public state root” instead of ”global state root”. Also, block validation is set as private transaction.
- **The State Patricia:** The State Patricia trie is split into a public-state trio and a private-state trie.
- **Transaction creation:** Data contained in Transaction may need to be kept encrypted to protect it. The opportunity to provide this was given as the transaction was created.
- **The Gas:** Although the gas itself remains, the value of gas is determined as zero.

Quorum is designed to perform both public and private transactions. Public transaction is activated via private transaction manager as in public ethereum chain. Private transactions are also activated by the private transaction manager.

Privacy Manager

The Private Privacy manager is responsible for providing and handling private transactions on Quorum Network. It allows Quorum nodes to share transaction payload securely between authorised parties of the transaction. It includes Transaction Manager and Enclave.

Transaction Manager (Tessera,Constellation)

It is a restful and stateless service that is mainly responsible for the following activities.

- Automatic identification of other network transaction controller nodes
- Exchanges encrypted payloads with other network transaction managers
- Stores and enables access to secure transaction details

There are two types of transaction manager we can choose in our networks. It is Constellation and Tessera. Constellation is the original privacy manager that is developed in Haskell. But no more development is made for Constellation to support Tessera which is more feature rich and actively developed.

The Transaction Manager provides a general purpose system for the safe exchange of information.It is similar to the MTA network (Data Transfer Agents) where PGP offers message encryption. The private transaction manager is not a block-chain-specific technology. It can be used in any application where an independently sealed and safe message exchange within a network of participants is necessary.

Tessera

Tessera is an Enterprise transaction manager. It is a java based stateless software used to enable the encryption, decryption, and distribution of private transactions for Quorum. Tessare can support following functions :

- Generate and host several public/private key pairs.
- Automatically finds all nodes on the network (i.e. their public keys) by connecting to as few nodes as every other node.
- Provides two-way SSL with TLS certificates (mutually authenticated TLS).
- Links to any SQL database that is provided by the JDBC client
- Synchronizes a public key directory mapped to receiver hosts with other network nodes.
- Exposes a shared API that is used for Tessera peer node communication.
- Provides a private API to connect with the Quorum node
- Requires one or more public keys to send a byte string, returning a contents-addressable identifier.
- Allows to receive a decrypted payload based on an identifier.

Tessera can be used as a combination of a distributed key server, PGP encryption(using modern cryptography) and Mail Transmission Agents (MTAs)

Enclave

Enclave Distributed Ledger protocols usually use cryptographic techniques for validity of transactions, identification of members and protection of historical records (i.e., through a chain of cryptographically linked data). Most of the cryptographic tasks, including symmetric key generation and data encryption/decryption, are assigned to the Enclave to accomplish the’ division of concerns.As a result due to modularisation, this differentiation increases security and also facilitates performance enhancements by the parallelisation of some cryptographic operations. In collaboration with the Transaction Manager, the Enclave acts to improve security by handling the cryptographic operations independently. It retains private keys and can be considered segregated from other components of the device as a ”Virtual HSM”. Only with its own linked transaction manager does an enclave interact.

The enclave manages the data below:

1. Access to the Public/Private key
2. Extra recipients' public keys
3. Identity default of connected nodes
4. Retrieving the default identities for nodes connected (default public key)
5. Providing all transfers with forwarding keys
6. Returning all enclave-managed public keys
7. Encrypting a packet for the sender and receiver specified (s)
8. Raw payload encryption for a specified sender
9. For a given recipient, decrypting transactions (or sender)
10. The inclusion of new recipients for current payloads

6.2.2 How Quorum Works

The transaction process takes place as follows, respectively as you see in Figure 5 and Figure 6. Party A, by using symmetric key encrypts the transaction and get encrypted transaction. After, for providing an immutable structure uses hash operations SHA3-512 and get digest value. This value stored on chain. In the end, using Party B's public key value, encrypted symmetric key obtained. Party B gets encrypted transaction and using encrypted symmetric key firstly gets digest value and compares it with digest that is stored on the chain. If it is correct using own private key gets symmetric key and decrypt the ciphertext and gets plaintext.

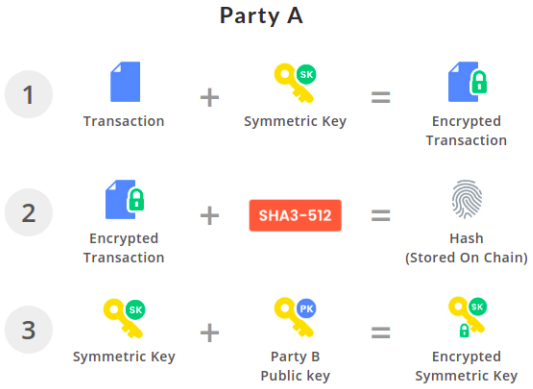

Fig. 5. Quorum Transaction Process 1 [15]

6.2.3 Use cases

Quorum is used in not just logistics but many more use cases such as healthcare, Identity, property, payments, capital markets and post trade. Here are some examples we have found:

- Tokenised cash — Developed by IHS Markit, is a distributed ledger that keeps record of all cash movements.
- JPM Coin — Developed by J. P. Morgan, is intended to allow for the instant settlement of contracts between customers of the wholesale payments company of the bank.
- Marketplace for Loans —It is a decentralised loan marketplace. It is developed by StreamSource technologies.
- Proxy voting — It increases the visibility of AGM voting between issues and investors.
- Post trade processing platform — A forum for post-trade distribution for oil trading.
- Interbank Information Network — IIN helps member banks on the network to share information in real-time concurrently to validate payments.
- Supply chain tracking — A website for cryptographic provenance that allows the validity of high-priced items to be proven.
- Mediledger — Detection of counterfeit drugs is now being developed using Quorum.

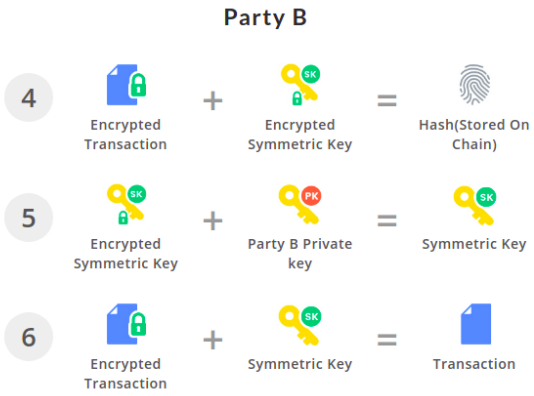

Fig. 6. Quorum Transaction Process 2 [15]

These are just some of the many use cases that Quorum has been used in. A more general list is shown on the official Quorum website under section "Built on Quorum".

6.3 How Quorum Solved Problem

6.3.1 No Transaction Pricing

A certain gas value is paid for each transaction made to prevent spam attacks and Sybil attacks on the Ethereum platform. In Quorum, the awareness of the people in the system ensures that this situation is not necessary and the gas value is assigned as 0.

6.3.2 Permissioned Participation

Providing the authentication and authorization mechanisms in the Quorum network, only transaction confirmation and smart contract execution features are given to people who are a part of this network.

In the Quorum network, Role Based Access Control Protocol is used to provide enterprise level access control mechanisms. In terms of the validity and usability of this protocol, we can give an example of Windows, one of the most used operating systems today, using this protocol in its own system. With this protocol, it is concluded that who can

join the network and that the participants can perform their transactions in accordance with the roles assigned to them.

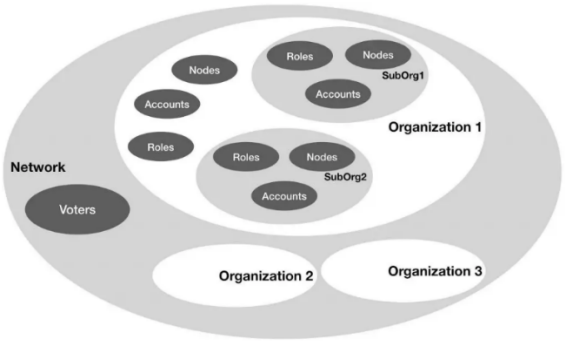

Fig. 7. Organizational Structure of Quorum Blockchain[12]

In order to understand the role-based permission mechanism operating in the system, it is beneficial to master some terminological concepts.

- Network: Enterprise Quorum Blockchain
- Organisation: Accounts and the roles that can be assigned to these accounts are also a set of nodes. The existence of this cluster provides the authentication and authorization mechanism of this organization.
- Account: Ethereum Wallet Account
- Voter: Approver the manager's proposal of organisations adding.
- Role: Tags that provide the authorization mechanism of the accounts.
- Node: In organizations includes ethereum client nodes.
- Permission: Description of the functions that accounts in the system can perform according to their roles.

The authorization mechanism in the Quorum network is provided by smart contracts. These smart contracts are responsible for managing the basic rules associated with the permit logic. Here behind the decision-making mechanism are the roles assigned to the units. These roles are responsible for the permissions of what a unit in the network can do. These roles can extract information about what the accounts can do. For example, an account with a system administrator role can run a smart contract, while a person with a different role can only access data. The smart contract providing this mechanism is also written in the Solidity programming language.
The Enterprise Quorum Blockchain network is made up of organizations, and admin accounts in this network can propose and approve new organizations to join the system. In addition, organizations can have their own managers. The administrator of the network can also make these assignments. In addition to these, organizations can include suborganizations. This requires each sub-organization to have a separate authorization mechanism. Because of this situation, roles, accounts and nodes are kept separately.

6.3.3 Consensus Mechanisms

PoW provides various cryptographic transactions to prevent sybil attacks in the public permissionless blockchain ethereum. Certain fees are defined for some transactions and defined amounts are paid for each transaction to be made. These payments create reluctance to commit spam and denial of service attacks. In addition, nodes (miners) are needed to generate blocks in the permissionless blockchain. PoW provides the necessary mechanism for generating blocks, but Miners must consume excessive power to produce blocks. This poorly affects the performance of the blockchain platform. In the permissioned blockchain, this power consumption is unnecessary. Therefore, consensus mechanisms that are created to work in the unauthorized blockchain network such as PoW are not used in the permissioned blockchain network. Slower public chain consensus mechanisms are not suitable for consortium chains as it is more important to improve performance in a permissioned blockchain. As such, Quorum offers different consensus mechanisms that are more suitable for private blockchains. Consensus algorithms such as RAFT and IBFT run faster, improving performance and ensuring process precision. For these reasons, such consensus algorithms are used in the Quorum Blockchain platform.

RAFT

There are three types of nodes in the RAFT consensus mechanism: Leader, Verifier, and Learner. During the leader selection, there are Leader node, follower node (verifier node) and candidate node concept. When establishing a RAFT, a set of verifier nodes is determined. These verifier nodes choose leaders among themselves. RAFT is used to manage logs. Here, all diary entries are reported to the leader. Since RAFT does not offer any reward mechanism to create a block, blocks are created in a controlled manner and unnecessary empty blocks are not created. In addition, RAFT is crash fault tolerant (CFT) consensus model that generates faster and optional blocks.. It is a consensus algorithm that is preferred when Byzantine fault tolerance is not mandatory and when faster block generation is desired. Raft offers a fault tolerant mechanism, and a certain amount of (2f + 1) nodes must be present in the network to tolerate faulty nodes.

Server states. Followers only respond to requests from other servers. If a follower receives no communication, it becomes a candidate and initiates an election. A candidate that receives votes from a majority of the full cluster becomes the new leader. Leaders operate until they fail.[13]

Leader[14]

- mints blocks and sends the blocks to the verifier and learner nodes
- takes part in voting during re-election and can become verifier if it does not win majority of votes
- the network triggers re-election if the leader node dies.
- can add/remove learner/verifier and promote learner to verifier.

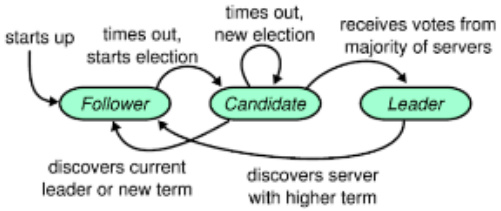

Fig. 8. Raft Consensus Mechanisms Leader Election[13]

Fig. 8. Raft Consensus Mechanisms Leader Election[13]

Verifier[14]

- follows the leader
- applies the blocks minted by the leader
- takes part in voting during re-election and can become leader if it wins majority of votes
- sends confirmation to leader
- can add/remove learner/verifier and promote learner to verifier

Learner[14]

- follows the leader
- applies the blocks minted by the leader
- cannot take part in voting during re-election
- cannot become a verifier on its own
- it needs to be promoted to be a verifier by a leader or verifier
- it cannot add learner/verifier or promote learner to verifier
- it cannot remove other learner/verifier but it can remove itself

IBFT

Istanbul Byzantine Fault Tolerant (IBFT) algorithm is an algorithm based on Practical Byzantine Fault Tolerant (PBFT). Each validator has to keep a state machine duplicate to reach block consensus. In other words, IBFT is also defined as a state machine replication algorithm. IBFT inherits three phases from PBFT called PRE-PREPARE, PREPARE and COMMIT.

Validators initially choose a proposer at Round 0. Thus, the IBFT consensus protocol is started. The Proposer offers a new block proposal with the PRE-PREPARE message. Validators receiving the PRE-PREPARE message verify the incoming proposer and enter the PRE-PREPARED state. Then the validators broadcast the PREPARE message. This step is done to make sure that all validators are running on the same role. Validator switches to PREPARE state when ceil (2N / 3) of PREPARE messages is received from other validators. After the Validator switches to the state of PREPARE, COMMIT broadcasts the message. The validator informs other validators that it accepts the proposed block and is going to insert the block to the chain. After all validators receive the ceil (2N / 3) of COMMIT messages, the block is added to the chain.

IBFT consensus algorithm supports immediate transaction finality. It provides liveness and safety under standard Byzantine fault threshold assumptions of n-1 / 3 under a partially synchronous network and 3f + 1 network configuration.[12]

6.4 Analysis

Quorum is a new way of adapting to blockchain among companies and industries. It is a ethereum focused permissioned blockchain platform designed to use among enterprise companies and financial industries. It is used to ensure privacy of data among parties that are on the network. This is provided with using different consensus algorithms in a platform that is fork of Ethereum.These are the reasons the Quorum has increased performance than public Go-ethereum(Geth) protocol.

If we examine the number of consensus mechanisms, RAFT requires 2f + 1 node while IBFT requires 3f + 1 node to provide a fault-tolerant mechanism and tolerate faulty nodes. In this case, the RAFT consensus mechanism can be used if it is desired to establish a blockchain network that requires a small number of nodes. In the IBFT consensus mechanism, blocks are always generated at a fixed interval, regardless of whether there are pending transactions. Therefore, it is generated in empty blocks that do not contain transactions. The RAFT consensus mechanism generates blocks if there are pending transactions. In other words, the block is not created unless there is any transaction load. This saves storage. In RAFT, the block production process is faster than in IBFT. In the RAFT mechanism, according to IBFT, it is a very fast process to create a block and collect the majority approvals required to add it to the chain. The RAFT consensus assumes that the leader always acts with honestly. Therefore, all entries suggested by the leader are accepted by the followers. In the IBFT consensus, the blocks produced are created by collecting signatures from bidder and voting validators, so honest entries are provided in a strong way. Thus, it ensures the immutability of the blockchain.

In terms of the immutability of the data, a preventaion has been taken against dictionary attacks created by performing a minimum of 2 to the power of 256 operation transactions with the Asimetic Key, SHA-3 512 hash operation and Transaction manager structure used for the Private Transaction structure in Quorum Network Quorum guarantees that the private transactions that it provides through transaction manager are smoother and their content is not changed.

For authorization mechanisms, this authorization mechanism in the Quorum network is provided with a role based access control mechanism. This situation provides a level access control mechanism. However, this autho-

rization mechanism is provided by smart contracts. In case of incorrect setting of the roles accounts and nodes authorities in a sub organization, it may reveal the situation of making changes on the data in the system. person can cause security vulnerabilities to occur, and this necessitates the Consensus mechanisms to be more robust and reinforced.

Authorization mechanisms can be analysed like Permissioned blockchains are actually a constrained version of public blockchains. However, the fact that some people have powers that can affect the network may cause some drawbacks. This situation may lead to the limitation of the network by the people who have a say in the network, the decrease in trust in the network and security weaknesses due to the failure to manage the network properly.

7 Conclusion

In this article, we have examined the basics of blockchain, the immutable structure behind the blockchain, and the reliability of the data brought by these structures in a technical sense, and we have seen how these are achieved. Starting from the historical structure of the blockchain, we first examined the Bitcoin structure. Then, we examined these organizational weaknesses and attachments and forks performed in the face of these situations, where programmable smart contracts on the ethereum chain came with Blockchain 2.0. Until now, what we've done was on permission blockchain.

Then, we entered permissioned chains with the quorum network, which is the soft fork of ethereum, and examined their needs, goals, pros and cons. We explained step by step how the private transaction structure is formed with transaction managers, tessera and enclave components, and how this process works. We examined in which use cases this network can be used. We have seen how the authorization mechanism works, while participating in the system, there is a change according to the consencus mechanism. Finally, as a result of our analysis, we have seen that consencsus mechanisms work faster due to the authorization mechanism in the quorum network, but require a minimum number of nodes, and in terms of the accuracy and unchangeability of the data, the sha3-512 hash operation used by the transaction manager may be vulnerable to dictionary attack with minimum 2 to the power of 256 operation ,is one of the measures taken against attacks. Lastly, permissioned blockchains work faster in every respect, but the authorization mechanism is based on the fact that the system administrators of the organizations do not misuse these authorities and are reliable. If these situations are not taken into account, it is a permissioned blockchain that can be easily used in situations such as enterprise resource planning that can be used in financial industries.

References

[1] https://blockgeeks.com/guides/ethereum/

[2] https://en.wikipedia.org/wiki/Ethereum: :text= Ethereum

[3] https://blockgeeks.com/guides/solidity/

[4] https://blockgeeks.com/guides/smart-contracts/

[5] https://blockgeeks.com/guides/what-is-ethereum-classic/

[6] https://academy.binance.com/tr/articles/what-is-blockchain-technology-a-comprehensive-guide-for-beginners

[7] https://academy.binance.com/en/glossary/block

[8] https://academy.binance.com/en/glossary/block-height

[9] https://academy.binance.com/en/glossary/genesis-block [10] https://en.wikipedia.org/wiki/Timestamp

[11] https://www.investopedia.com/terms/m/merkle-root-cryptocurrency.asp

[12] https://blockgeeks.com/guides/quorum-a-blockchain-platform-for-the-enterprise/

[13] https://raft.github.io/raft.pdf

[14] https://docs.goquorum.consensys.net/en/stable/ Concepts/Consensus/Raft/

[15] https://www.blockchainappfactory.com/quorum-blockchain-development

A Resources

- Performance Evaluation of the Quorum Blockchain, https://arxiv.org/pdf/1809.03421.pdf
- Raft Consensus Mechanisms, https://docs.goquorum.consensys.net/en/stable/Concepts /Consensus/Raft/
- Quorum Architecture, https://blockgeeks.com/guides/quorum-a-blockchain-platform-for-the-enterprise/
- Private Transaction Mechanisms, https://www.slideshare.net/Chainstack/how-do-private-transactions-work-on-quorum
- Sybill Attacks, https://academy.binance.com/tr/articles/sybil-attacks-explained
- IBFT and RAFT, https://www.kaleido.io/blockchain-blog/consensus-algorithms-poa-ibft-or-raft
- IBFT and RAFT, https://www.freecodecamp.org/news/in-search-of-an-understandable-consensus-algorithm-a-summary-4bc294c97e0d/