WHAT IS CRYPTO CLASSIC?

The Blockchain Technology is a technology protocol where information, payments, contracts or transactions can be identified, verified and signed one-on-one on a digital platform while providing more anonymity and safety than centralized servers. Today, no matter how good the security measures taken by all centralized servers that do not use the Blockchain technology are more open and vulnerable to cyber-attacks. Today, where the digitalization process continues rapidly: nearly all transactions such as contracts, signatures, exchange of money or information take place in the cyber world, and physical transactions, contracts, signatures and negotiations are also transferred to the cyber environment. To us, one of the most important features offered by the Blockchain technology is that it takes any data that others can access from centralized servers and connects the data flow between the parties who own/will own the data, and records the process uninterruptedly. Everyone in the Blockchain network has a wallet (account book) of their own, so that they can see all their data from here. In the Blockchain Technology, each block is associated with the previous block and is protected by an encrypted reference, and in this way, it becomes almost impossible to access the data flow consisting of numerous blocks from the outside, hence eliminating one of the main problems of the cyber world, unreliability. The technology that Crypto Classic (CRC) aims to bring is one of the most powerful and secure payment methods in the Blockchain network in terms of security, privacy and transparency of payments that can be directly transferred between people who have an address on the Blockchain. As a project, our aim is to make it possible to make payments and data transfers fast, low-cost and without intermediaries by providing direct communication between people. Crypto Classic will provide a technology that will directly affect the methods of payment that will take place between individuals in a developing and changing world, and speed up data transfers by reducing unnecessary processes. Just as the internet emerged in the 90s and has become widespread today, directly affecting all kinds of payment activities, this project that we built upon the Blockchain technology aims to implement payment and data transmission methods in à decentralized, secure, anonymous way by including all the sectors that require transfer of any kind of data or non-physical assets in the future. Crypto Classic has been designed in such a way that it can constantly update itself by constantly following the latest technologies on the Blockchain and adapt to new technologies that will emerge with the Blockchain. In this way, you will be able to continue to use Crypto Classic's technology, which we are presenting to you as a result of long periods of research, for many years without any problems, in the fastest and most advantageous and secure way. Within the scope of the innovations emerging with the Blockchain technology; Crypto Classic aims to be used as a payment method among many large- medium-small-sized brands, companies, organizations and even countries in the world. For this reason, Crypto Classic invites everyone to this revolutionary project that offers to create reliable payment methods with its innovative and up-to-date technology. As Crypto Classic team; aiming to replace all existing primitive, slow and vulnerable payment methods by combining the centralized payment methods used in the world with the Blockchain technology; we are proud to present to you a system that can adapt itself to new technologies as a fast, secure, cost- effective, confidential and transparent payment method. We set out this project with dream of a better world where financial freedoms will be better understood and implemented for everyone. Thus, we are pleased to present this innovative project, which has an unchangeable supply, to all investors who want to keep it as an investment or payment tool. To our investors who prefer Crypto Classic project as an investment and payment tool; we would like to announce that we will take our place in the stock markets with the highest trading volume right after the end of the pre-sale. We will continue to move forward with the support, responsibility and confidence that the future and our investors give us, and we will work hard to make Crypto Classic a project that will potentially solve the problems that people experience, especially in terms of the payment methods used in centralized finance. Crc serves as a futureproof middleware that enables enterprise systems to interact with smart contracts on any public or private blockchain network that exists today or in the future.

Crypto Classic New-Generation Technology Sets to Disrupt Payment Methods and Mining Processes

In today's world, the digitalization process keeps rising rapidly, and nearly every transaction, exchange of information, negations, contract, etc., takes place in cyberspace. Centralized transactions and payment methods are marred by slow processes, single points of failure, and a whole lot of other pitfalls. The advent of blockchain technology has disrupted and revolutionized virtually every sector of the global economy. Many projects are leveraging technology to provide innovative services that transform industries and businesses. A good example of these blockchain-based projects is the Crypto Classic project. The project is deploying innovative and revolutionary technology to solve the shortfalls of the payment industry as well as some of the major problems of mining. Before we go ahead with the Crypto Classic technology, let us take a look at the project itself.

Overview of the Crypto Classic Project

Crypto Classic is a blockchain-based project that is designed to unify different blockchain infrastructures and top Binance Smart Chain Protocol. These will be achieved by standardizing all communications between these blockchain infrastructures to create and execute complex financial transactions. The project is also built to ensure that every transaction is confidential to transaction parties whose identities are also protected.

The Crypto Classic project consists of a blockchain ledger, a native cryptocurrency robust system of on-chain services and applications. Crypto Classic team believes that the project will become the secure payment method of the future. As a pointer that the team is putting in the needed work into the project, the Crypto Classic coin just got listed on five different crypto exchanges in November alone.

The New-Generation Technology

The underlying technology of the Crypto Classic project is one of a kind and arguably the first in the blockchain ecosystem. This technology is designed to make payments and data transfers fast, efficient, relatively cheap, and without middlemen. There will be a direct line of communication between all transacting parties using the protocol to achieve this.

Just the same way the internet made its debut in the 90s and has risen to become widespread today, affecting virtually every aspect of our lives, the technology is built to self-update itself. This is where it gets very interesting. By self-updating itself, the Crypto Classic technology will always be needed within the blockchain industry. Whatever becomes of the blockchain industry tomorrow, and whatever the new trend becomes, this technology will self-adapt. This is a great milestone of achievement by the founding team.

Beyond the scope of financial transactions, technology also plays a vital role in crypto mining processes. Many analysts and environmental activists have come out to say that the negative impact of crypto mining on the environment is growing exponentially. The Crypto Classic technology will help to reduce carbon footprint with a fork-out that shortens the crypto mining processes. This technology will certainly be a game-changer once it is fully deployed.

Proof-of-Work Blockchains are Energy Inefficient, Indirectly Harming the Environment

Besides high trading fees due to scaling challenges, Proof-of-Work networks like Bitcoin and Ethereum have been blamed for being energy inefficient and wasteful. The high carbon footprint left for every transaction confirmed is alarming for environmentalists.

Trackers show that the entire Bitcoin network uses 192.80 TWh, the equivalent of Thailand. At the same time, the carbon emitted from fuel sources to sustain the platform, keeping it immutable and operational, is the equivalent of 91.58 Mt of Co2, the size dispensed by Chile. The energy wastefulness of Bitcoin is due to the deployment of miners who depend on energy sources to power their hungry gear—which is frustratingly rare and, when available, sells for thousands of dollars.

The same trend can be observed in all other proof-of-work networks dependent on miners. Unique, the BSC adopted a different approach anchoring their primary objectives to ensure environment preservation and boost governments' climate conservation efforts while remaining scalable, decentralized, and most critically, interoperable.

The Assurance of Code Security

According to the developer, CryptoClassic is launching a platform for creating and launching complex financial transactions reliant on the distribution and security of the base layer.

As a payments system, the portal's code must be secure and trusted, although working in a trustless environment reliant on the self-execution of deployed code. It is critical considering the exploitation of unaudited code by some projects which have seen millions of user funds lost in the BSC and the broader crypto community.

Already, there are over 2.6k holders of CryptoClassic's CRC token less than a month after launching. Trading at over $0.29 after peaking at around $0.80, the CryptoClassic project has a market cap of more than $24 million. As such, it is one of the most notable projects in the expanding BSC's ecosystem.

With multi-millions at stake and over 2.6k holders whose interests need to be protected, developers of CryptoClassic have gone ahead to prove that its code is secure and approved.

The public declaration and confirmation, complete with an audit certificate, is a confident booster.

Besides, this is a proof-of-document that the decentralized community, believing in the value proposition and their vision-mission statement, will always demand before doubling down. The auditing of CryptoClassic's code and assurance from security experts that its smart contracts function as designed would potentially accelerate the expansion of CRC in the near future while building a strong reputation for the upcoming and highly potent project.

CryptoClassic Launching on an Eco-Friendly Layer

The CryptoClassic project is riding on the eco-friendly BSC blockchain and aiming to leverage the ledger's features to deliver its value proposition.

Already, CryptoClassic's strategic decision to opt for the BSC over Ethereum and Proof-of-Work smart contracting platforms aligns with the recent global objectives on climate change.

During the latest U.N. conference in Glasgow, Scotland, global leaders agreed to prioritize programs to preserve the environment and shift to renewable energy.

Bitcoin and Ethereum, for instance, depend on fossil fuel energies to power their energy-inefficient gears. Because of the energy wastage of Bitcoin, the Chinese government banned cryptocurrency mining in their territory, profoundly impacting Bitcoin's security.

The BSC, on the other hand, is energy efficient, interoperable, and, most importantly, cheap to transact on. This is why CryptoClassic is deploying on its rail, a move that would quickly give it a solid base in eventually actualizing its objectives.

CryptoClassic (CRC) Listed in 5 Cryptocurrency Exchanges, Two More Listing Scheduled by December 2021

Moreover, due to their specific vision and goal to disrupt payment via an interoperable blockchain whose ecosystem is expanding, the CRC token has been quickly listed in several centralized exchanges, including CoinTiger and Azbit.

According to CryptoClassic, the project is in talks to launch in two other centralized exchanges by December 2021.

This exposure to liquidity channels and support from reputable cryptocurrency exchanges is a direct endorsement of the project, pointing to its potential and possibly undervaluation at spot rates.

INTRODUCTION

In addition to being a building block to be designed to be evaluated, money is the most important player that plays a role in all commercial and economic features between societies and societies. Money is a means of commerce; It enables the sale of goods and services to be carried out quickly and effectively. Money is a standard of value; all tangible and intangible assets are expressed by it. Money, which is also a store of value, also fulfills the function of protecting wealth. Despite being a financial asset, money has the ability to revive the real sector through investments. Although there is no change in the functions it carries out, the concept of money has undergone various transformations throughout the history of humanity. As it is known, before the invention of money, trade was based on barter and goods and services were exchanged with each other. However, since there was no common value unit in this system, difficulties were encountered in the exchange of various commodities and services. Over time, many commodities that could be considered money (such as seashells, copper, gold and silver coins) were derived, but the Lydians invented the first coin in the sense known in history. So, people have come to use this generally accepted value in return for the goods and services they want to buy. The exchange of money was not limited to this. Paper banknotes invented by the Chinese spread around the world through explorers. With the development of technology, human beings, who experience changes and developments in every aspect of their life, have combined the concept of money with technology. Thanks to electronic money, people today do not have to carry physical money to shop. With the technology reaching people's pockets with smart phones, payments can be made in the place where they are. However, all these mentioned systems have always been open to abuse. Although measures have been developed in order to protect both physical money and electronic money against the intervention of fraudsters and fraudsters, it has not been fully successful. Bitcoin, which emerged in 2009, brought a new perspective to the concept of money. Unlike known electronic money, Bitcoin allows transactions to take place without an intermediary. Bitcoin makes it possible to keep records encrypted with its Blockchain technology in “Distributed Account Books”. In this way, both transaction costs are reduced and possible confusions are eliminated. Despite the innovations it brings, the independent structure of Bitcoin reveals some audit vulnerabilities for nation states. At this point, international organizations and state authorities have different perspectives and applications for this new technology. In this study, this new money phenomenon (cryptocurrencies) that emerged with Bitcoin was examined and the evaluations of national and international authorities on the subject were given.

Crypto Classic has worked on how Blockchain technology, which emerged with cryptocurrencies, can improve financial services and what changes can occur in transaction costs. The results and evaluations on this issue show that with this new technology, transaction costs will decrease significantly and therefore efficiency will increase. There will also be benefits in the field of transaction security, as transactions will be carried out at high speed and without the possibility of intervention. The most important feature of Industry 4.0, which started in the middle of the 20th century and is also called the digital revolution, is that data and records are kept and stored in a digital environment. These developments have brought some problems with them. Keeping records/data on more than one computer and electronic devices jeopardizes the security of the data as it is not encrypted. In addition, the fact that the data is publicly accessible also leads to the fact that that data can be changed by anyone who wishes. This is where Blockchain technology comes into play. Blockchain is a technological structure that prevents data from being changed and ensures data security by encryption method, as well as creating, recording and distributing data in the digital environment over multiple networks. Therefore, the most important contribution of Blockchain technology is to ensure data security and prevent it from being changed.

The technology, which is seen by some scientists as the biggest innovation after the internet, is called blockchain. The concept takes its name from the working logic. Because Blockchain refers to data blocks that are cryptographically chained to each other in the form of rings. At this point, it is useful to state what the concept of data block and cryptographic chaining mean. A data block is a kind of database that contains raw, unprocessed information. The database is the unit that provides the storage of the data it contains. While explaining the concept of blockchain, "cryptographically chaining" is essentially a concept for data security and refers to the encryption of data for the purpose of providing access to data only by authorized parties. Thus, data security and confidentiality is ensured. Although the blockchain has a database feature in the basic sense, it has some different features from standard databases. A standard database has a central administration or network where data is stored and managed. The central network is the owner and administrator of the database. Therefore, it is the central administration itself that provides access to the data. However, since there is no such network where data is stored in Blockchain, it has the feature of a decentralized database. Although the concept of blockchain has a short history of 10 years, structures similar to blockchain technology have been suggested since the 1980s. In this structure, the digital signature is verified by comparing the original signature, and the content can be viewed as a result of the verification. There is a technology that does not need cryptography, digital signature and central server, which is also available in the blockchain structure. The basis of the studies on the secure transfer of data by encryption, in the blockchain technology, dates back to 1991. In this structure known as “PGP (Pretty Good Privacy) algorithm”, data security and encryption expert Phil Zimmermann suggested the asymmetric encryption algorithm. The biggest contribution of the algorithm is that it prevents access to the content of the document even if the data is captured by unauthorized persons. The PGP algorithm is applied in the transfer of digital currencies in Blockchain technology. The article “Bitcoin: Peer-to-Peer Electronic Cash Payment System” published in 2008 by a person or group who introduced himself as Satoshi Nakamoto, forms the basis of the history of the Blockchain. Although “Bitcoin” is a digital currency using the Blockchain platform, the emergence of the Blockchain philosophy is based on “bitcoin”. Bitcoin is also considered to be the first application of Blockchain technology. Considering the examples that make the entire blockchain system look like a ledger, it is possible to explain the concept of the block as each page of this ledger. In other words, the Blockchain system is a structure consisting of blocks where data is stored. The blocks in question are arranged by adding them to each other as a linear chain when they are created.

Considering the examples that make the entire blockchain system look like a ledger, it is possible to explain the concept of the block as each page of this ledger. In other words, the Blockchain system is a structure consisting of blocks where data is stored. The blocks in question are arranged by adding them to each other as a linear chain when they are created. The initial block created in terms of time in the chain ring is called "genesis". Each block after the Genesis block contains a summary of the previous block. This feature is behind the inability to change the data in the Blockchain system in the previous sections. Because in order to change any data, it makes it necessary to change all previous blocks.

Blocks consist of the data contained in them and the block header describing the block. Block header,

> When the block was created (Timestamp)
> Summary records, also known as the Hash value of the previous block,
> Nonce data required for proof of labor,
> Merkle root

shows four different information. The purpose of this structure, also known as the Merkle root or Merkle tree, is the aggregation of large data sets and the verification of them quickly and securely. Considering that there are numerous data blocks in the blockchain system, the summary information of a certain number of data blocks is combined into a single package, and then the data in these combined packages are collected under a single package in the final stage. Therefore, a single hash value is created for the data blocks in the said group, and this hash value is called the Merkle root. Proof of work is a method used to prove that a computer is working for a job. The nonce in the block header, which is used as a one-time key in computer science, represents the data required for proof of work. In other words, it is the modifiable number value used to generate the desired block hash value. If a suitable block hash value is not formed, the nonce value is increased to create a suitable hash value.

Distributed ledger technology is one of the main features of Blockchain systematics. As it is known, Blockchain technology is a database that does not need a central network or server. In other words, a copy of the data is kept on all devices included in the Blockchain network. In addition, when a new data or transaction is entered into the system, the verification of this data is verified and approved by all devices within the network, not by a central administrator. For example, bank passbook is kept both in print by the account holder and electronically in the bank. Therefore, a unilateral change by the account holder on the passbook will not be respected. In order to approve the change in account information, it is necessary to reach an agreement between the parties. Blockchain's distributed ledger technology has a similar structure. Since a copy of the records is available on all devices included in the network, any change or deletion of records made by either party will have no validity.

A peer-to-peer network or protocol (Peer to Peer) is one of the consequences of not having a central database in the blockchain system. Because in systems where there is a central server and data is controlled and recorded from a single center, users trust the central server for the accuracy of the records. However, in order for the decentralized Blockchain system to work effectively, it requires the existence of a protocol or contract between the participants in the network. Only in this way will the element of trust be ensured. This technology was introduced in 1999 by Torrent, a file sharing application where files such as music or movies are stored on multiple computers. The peer-to-peer protocol provides simultaneous updating of data on the entire network in Blockchain systematics.

The agreement mechanism generally means that in order for any transaction to be valid in Blockchain technology, the transaction must be accepted by the majority of the system and work within the framework of certain rules determined in the infrastructure of the system. When blockchain technology is evaluated in terms of data privacy and security, which is one of its greatest contributions, four different types of networks emerge. These are open, private, semi-private and consortium Blockchain networks. In the “Open Blockchain” system, all participants in the network have the right to access all information, and every transaction made within the network is seen by all participants. In this system, the authority to create new blocks belongs to all participants. The validity of the transactions and the blocks created on such platforms depend on the approval of all participants. “Bitcoin” and “Ethereum”, which have contributed greatly to the emergence of blockchain technology, are the most important examples of the open Blockchain network. Although the Open Blockchain network has the mentioned features, which raises doubts about its reliability, its features essentially ensure the security of the network. Because the free participation in the network ensures that the number of participants increases continuously, and this ensures that the copy of the data is kept as much as the number of participants. Keeping a copy of the data on more devices is one of the factors that prevents it from being changed. On the other hand, although the access authorization to the data is open to all participants, personal data cannot be viewed because they are encrypted. As a result, in the “Open Blockchain” system, participation in the network and access to the information in the network are free. In this respect, it is classified among networks that do not require permission. The 'Consortium Blockchain' system is the type of network in which participants are subject to permission to access data and participate in the agreement process, although participation in the network is free. The “Fast Track Trade” platform, which was created by Singapore for the development of international trade and connects the buyer and seller without intermediaries, is an example of the consortium Blockchain application. The Private Blockchain system is the Blockchain network with the most limited authorizations in terms of network participation and access to data. Although it is possible to provide data security with encryption method in the Open Blockchain network, the possibility of decrypting the passwords necessitated the production of new network structures. In this framework, in the private Blockchain network, participation in the network, access to data, and participation in the consensus process depend on permission. It is especially preferred by public institutions where confidentiality must be kept at a high level, military and police organizations responsible for ensuring security, international finance and regulatory institutions. For example, the “web” site of a public institution is accessed only by the officials of that institution and is not open to the public. However, only those authorized by the employees of the institution can enter data on the site, and other users can only access this data. The working systematic of the Private Blockchain network is similar to this. In the semi-private Blockchain network, where only participation in the network is subject to permission, all participants in the system can enter data and access all data. Therefore, its difference from the private Blockchain network is that access to data and new data entry are not subject to permission.

While the emergence of the Bitcoin digital currency enabled Blockchain technology to become widespread, "smart contracts", called "Blockchain 2.0" and showing that this technology can be used in many areas besides payment systems, started a new era for Blockchain. The concept of smart contracts, which was first mentioned in an article published by Nick Szabo in 1994, is based on the fact that the agreement between the parties is realized by a contract that is coded over a computer, where the terms are determined in the digital environment and automatically actuated, instead of a contract in hard copy. In other words, the realization of a transaction made on the Blockchain platform occurs automatically if all the conditions specified in the smart contract are met.

Within the scope of the “Smart Port” project developed within the Port of Rotterdam, which is of great importance for European maritime trade, Blockchain-based smart contracts have been integrated into maritime transport. Within the scope of the application, it is ensured that the departure information, transportation conditions and arrival information of the transported goods are presented to the interested parties in a transparent, safe, fast and cheap manner according to the general characteristics of the smart contracts. The project, which also reduces the workload in the ports, provides time and cost savings. Considering that more than 85% of the goods traded worldwide travel on a ship at least once during their life cycle, it is thought that Blockchain-based smart contracts will make a significant contribution to the development of international trade.

Digital identity has the potential to be used in a wide range of industries. These sectors are utilities, retail merchandising, financial services, housing and housing, health, mobility, education, culture and entertainment, communications, commerce, transport and accommodation, and insurance. A digital identity system with Blockchain infrastructure is used by a company providing international payment infrastructure to be used in cross-border payments. With the application called "Business to Business - B2B", it is aimed to carry out the international payment transactions of financial institutions in a secure and intermediary manner.

Digital identity application can be applied in many areas. In Estonia, this technology is used in the provision of citizenship services. Estonian citizens can benefit from many rights such as the right to vote with a digital identity, the notification of tax returns, the right to benefit from health services, the right to establish a business, the realization of payment transactions, the right to use banking services and the right to public transport. In the same context, the Australian government is preparing to adopt a digital identity application.

The ability to make transactions without intermediaries, one of the most important contributions of blockchain technology, has added a new dimension to financing transactions. Although financing is a process that occurs as a result of the meeting of those who supply funds and those who request funds, today these transactions are carried out through banks and financial institutions. The fact that blockchain technology provides direct money transfer between individuals without an intermediary institution has also been a guide in terms of financing transactions. Common financing methods using the blockchain infrastructure are P2P Financing, Crowdfunding, Micro Finance, Syndication Loans, and Donation and Aid collection methods.

According to the researches, the use of Blockchain technology in international payment transactions saves between 40%-80% in transaction costs, while the transfer process takes between 4 and 6 seconds. Blockchain-based global payment system was established with the project developed by an enterprise (IBM) operating in the international information sector. Within the scope of the study, transfer transactions are carried out within seconds in 48 countries and 72 currency corridors. Thus, the fact that banks were not needed also reduced transaction costs. In addition, this system provides time and cost savings in order to include new markets in the capital flow. Among the general problems are the fact that many people and institutions such as customs administration, banks, logistics companies, public authorities, apart from the buyer and seller, participate in the traditional supply chain process, a large number of documents are processed for the process to work, and the risk of loss or copying of printed documents. The excess of intermediaries and the need for document management cause transaction costs to increase. In addition, the lack of transparency of the supply chain process makes it impossible to determine the true value of the goods or services between the buyer and the seller, as well as compliance with laws and ethical rules. The ability of blockchain technology to make transactions without intermediaries or to minimize intermediaries and to allow documents to be recorded in a reliable and transparent manner in the digital environment can provide solutions to the problems of supply chain management. In this context, the values that Blockchain technology can add to supply chain management; It is possible to specify as reducing transaction costs, shortening processing times and reducing manual interventions, increasing transparency and traceability.

People have given importance to information privacy by using different methods in communication, starting with the invention of writing. Today, with the increase in internet and computer usage, traditional communication methods have left their place to electronic communication. With this change, the concept of security in electronic environment and especially cyber security has gained importance. The global spread of communication between information systems is important for the protection of information against many possible attacks. Cryptography is a set of techniques that keep information confidential and transform it into a form that cannot be understood by undesirable parties. It uses mathematical methods to provide information security concepts such as confidentiality, integrity and non-repudiation. Cryptanalysis is a method of decoding meaningless encrypted texts. Cryptology encompasses the whole of cryptography and cryptanalysis. Cryptology is an interdisciplinary branch of science such as electrical and electronic engineering, computer science, mathematics, which investigates the reliability of crypto devices that provide data security in communication and the algorithms used in these devices. Cryptographic methods, which were monopolized by military and official institutions until the 1970s, gained a new dimension by revolutionizing the public-key systems proposed by two researchers, Diffie and Hellman, in 1976. With the discovery of public key systems, it has emerged that secure communication can be achieved without knowing the public private key. Since the emergence of Bitcoin, the popularity of cryptocurrencies has continued to increase with the convenience and reliability provided by blockchain technology to customers. Blockchain technology stands out with its basic features. The first feature is the prevention of single point error (SPoF) by sharing the same ledger among peers, thanks to its distributed structure. Thanks to this feature, more reliable and continuous information can be obtained without the need to rely on a single point. The second feature prevents changing historical data, thanks to its write-only structure. Cryptology is used for this feature and it is shown as the technology of the century thanks to its high security feature. The third feature is that transactions are managed by consensus algorithms between nodes on the network, so there is no need to rely on a third party. Adding a block to the chain occurs after most nodes have verified the block. As a final feature, the blockchain uses asymmetric keys for encryption and authentication. One of the most successful applications of blockchain technology is smart contracts. When predefined situations occur in the smart contract, the action to be taken as a result of this situation is automatically performed. Blockchain technology can be used in different areas such as health, public services, finance, logistics. One of the building blocks of blockchain technology is public key cryptography. In Blockchain technology, public key cryptography is used in basic functions such as signing transactions with a private key, using account addresses as public keys, and verifying transactions signed with a private key with a public key. The AAA defines the policies and procedures required for the creation, management, distribution, use, and revocation of digital certificates to securely use encryption, along with the methods and technologies used together to provide a security infrastructure. One of the most widely used applications in public key systems is electronic signature. When creating electronic signatures, after determining the algorithm to be used, such as RSA, ECDSA, it is important with which hardware to use. Status information of electronic certificates can change for many reasons. The certificate can be revoked in different cases such as losing the private key of the certificate, changing the certificate owner's information, or requesting the user's revocation. In addition, requests are met by certificate service providers for situations that require a certificate status change, such as suspension of the certificate that will not be used for a certain period of time, re-validation of the suspended certificate. Traditional AAA systems are based on SM and revocation information of certificates is published by the respective SM. The most common use for certificate revocation information is the methods in which SMs periodically issue CRL files and/or receive instant OCSP responses. Different types of certificates such as SSL/TLS certificates, NES, code signing certificates, security certificates are all X.509 certificates based on AAA technologies. SSL/TLS certificates and NES, which are based on X.509 certificates, serve different purposes. SSL/TLS certificates are often used to authenticate the server resource using the data. Unlike other certificates, the features that QCs must provide are detailed in RFC 3739 and in electronic signature laws enacted specifically for NES by countries using this technology. This study has been prepared specifically for the NES used in electronic signatures according to the X.509 v3 certificate standards, but it can also be used in other X.509 v3 certificates.

Blockchain technology has entered our lives and attracted the attention of many people economically, the concept of blockchain has begun to be investigated. In its most general definition, blockchain can be called a distributed ledger technology. In other words, it is a digital account book that is protected against alteration or tampering. It is a data structure model where data is securely interconnected, which makes it possible to create and share this ledger instantly.

This data structure consists of data-transaction blocks that are cryptographically linked to each other. As the transaction takes place, a new ring is added to the chain to record transactions, and the process continues. It is extremely difficult to change or remove the data blocks recorded in this ledger, and this operation is performed with the knowledge of all participants. It is this degree of difficulty that makes the blockchain the center of attention. It gives endless confidence to the users as it cannot be changed or interfered with.

The security-privacy couple, which is the biggest problem that arises with the internet of things and the transfer of personal life data from devices other than people to the internet, always leaves a question mark in mind. The Internet of Things has become an indispensable technology, as it allows users to remotely and incident-specifically control all the equipment they use in their lives (He ve ark, 2014; Yang, 2014). According to Gartner, the value-added product and economic contribution of IoT technology is expected to reach $263 billion by 2020. With the internet of things, the solution market size will reach 7 trillion dollars in 2020 (MAcGillivray ve ark, 2013). For such a rapidly growing technology, security means the existence or non-existence of the technology in the future.

In this study, it is argued that blockchain technology will create a strong technological infrastructure for the problem of security and privacy in IoT applications. A key disadvantage when looking more closely at the architecture of the IoT technology is that they cannot be trusted on a centralized cloud. The blockchain method provides a high security policy for objects connected to the Internet. In fact, to support this approach, the concept of blockchain for objects (BcoT) has been put forward for the industrial internet of things (IIoT).

In the process of incorporating the blockchain into the Internet of Things, many security measures are supported. A different setup has been created by customizing the blockchain to ensure that devices connected to the Internet of Things are kept in a common ledger with unique identities. In fact, it can be called creating a smart device chain. Devices included in this chain will be able to communicate with each other, execute smart contracts and include result data in the chain. It is desired to create a more efficient and safer structure that is not based on traditional methods with an architectural method that will be presented based on the blockchain.

In this thesis, it is argued that the landlord-tenant relationship, which is realized through an intermediary in real life using blockchain technology, is implemented autonomously with a smart contract. The confirmation software, which is based on the contract terms determined by the landlord and the tenant, opens the door to all services in the house after the transfer of the amount in the contract between the tenant and landlord accounts is confirmed. In this proposal, in the system that proceeds independently of an authority or an intermediary, transfer costs are minimized, and an endless trust and transparent trade is ensured. In addition, since this transaction is stored in the blockchain for years, a strong logging process will also be provided.

PAYMENT METHOD WORKING LOGIC

Cryptography simply means the encryption of data. While doing this encryption, it ensures that the data is rendered useless for undesired recipients. In this context, making data useless means preventing three basic actions. These actions are attempts to reveal information in the data, change the data, or add false information to the data. These are called confidentiality and integrity problems, respectively. In addition, a situation can be assumed where the sender encrypts and sends data only to subsequently deny that he is the sender. Another purpose of cryptography is the nonrepudiation of a sent specific data, called "nonrepudiation". At its core, cryptography is a theoretical concept, but has a wide practical scope, used to prevent and detect fraud or prevent access to data.

The basic concepts that make up the structure of the blocks in the blockchain can be expressed as follows.

I. **index:** Data showing the block's position in the blockchain. For example, the index information of the first block of each blockchain is 0.

ii. **hash:** It is the summary result obtained after the data in the block is inserted into a hash function.

iii. **previousHash:** It expresses the hash value of the previous block.

iv. **timesamp:** The timestamp of the time the block was created.

v. **nonce:** 32 or 64 bit integers used in mining operations.

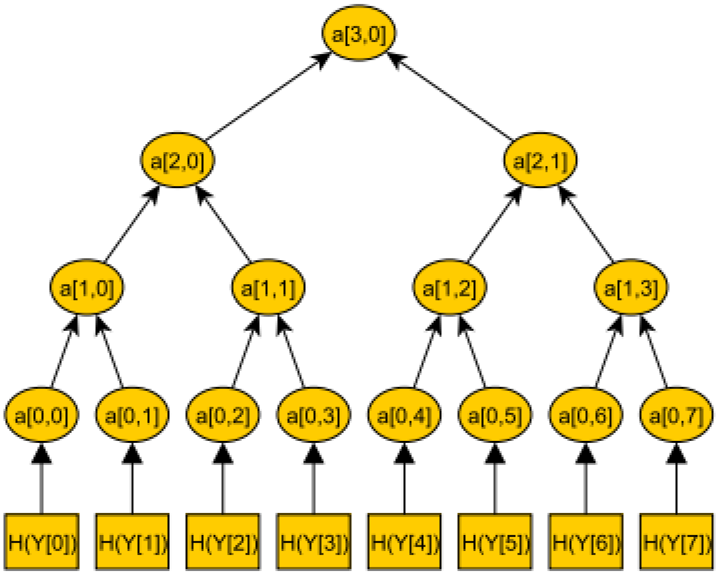
vi. **numTx:** The total number of transactions in the block.

vii. **Transactions:** It is a sequence of all transactions in the block. Transactions contain the following information:

Hash: is the summary of data, transaction outputs and input data in a transaction.

Type: is the type of the transaction. It has 3 different types. Of these, Coin Base Transaction refers to the transactions that take place for the cryptocurrency token issuance mechanism. Fee Transaction refers to the transactions of the rewards that the transaction owner pays to the miners. Regular transaction refers to the transactions performed to transfer token ownership.

Merkle Tree: The hash values of each transaction in the block form the last leaves of the Merkle tree. The hash of all these leaves as pairs forms the parent nodes of these leaves. The process of calculating hash values in binary groups and creating half the number of nodes at the next level continues until the last node of the tree, the Merkle Root node, is formed.



Blockchain Network Types

Blockchain projects are divided into types according to the communication and consensus preferences in the usage scenarios.

Open (Public) Blockchain Networks

In such networks, anyone who wishes can read the data, verify the transactions, and create the block to be added to the chain according to the consensus algorithm. Participation in this type of network is expected to be high. A blockchain network consisting of a large number of nodes, on the other hand, has become highly reliable with the increase of nodes that will function as the confirmation and verification mechanism and the impossibility of realization of centralization. Open blockchain networks can be divided into two subgroups:

Completely Permissionless Open Blockchain Networks

If a new node, after joining an open blockchain network, does not need permission to read the data in that network and to approve transactions and create new blocks according to the current consensus algorithm used in the network, this blockchain network is a completely permissionless blockchain network. Since the participation in such networks will be high, the number of nodes where peer samples of the data are kept will be proportionally high. This means that the blockchain network becomes more reliable. For example, the Bitcoin blockchain network is a completely permissionless open blockchain network.

Partially Permissionless Open Blockchain Networks

If a new node does not need permission to read the data in that network after joining an open blockchain network, but needs to approve transactions and add new blocks according to the existing consensus algorithm in this network, this blockchain network is a partially permissionless open blockchain network. For example, the Ethereum blockchain network is a partially permissionless blockchain network.

Private Blockchain Networks

Companies, public institutions or organizations may not want their data to be tracked by everyone in the open blockchain network. In order to read the data in the private blockchain network developed for such situations, the permission of the owner of the network or the rules set by him is required. Private blockchain networks can be divided into two subgroups:

Partially Permission Private Blockchain Networks

If a new node joins a private blockchain network and needs permission to read the data in that network, but every node in the network is allowed to approve transactions and create new blocks according to the current consensus algorithm used in this network, then this blockchain network is a partially permissioned private blockchain network.

Entire Permission Private Blockchain Networks

If a new node, after joining a private blockchain network, needs to get permission to read the data in that network and confirm transactions and add new blocks according to the current consensus algorithm used in the network, this is a private blockchain network that requires full permission to the blockchain network.

Consortium Blockchain Networks

Partially private are blockchain networks. The ideal number of nodes is chosen to perform this transaction, rather than giving the authority to verify transactions to anyone with an internet connection or leaving it entirely to a company. Consortium blockchain networks, which have many common advantages with private blockchain networks, operate under the leadership of a group of selected nodes, not under a single institution as in private blockchain networks. It can be said that this platform is cut out for inter-company cooperation.

Semiprivate Blockchain Networks

Deserving users are granted access by a company running semi-private blockchain-based applications, as opposed to everyone joining the network in public blockchain networks and tightly controlling requests to join the network in private blockchain networks. In such networks, B2B (business-to-business) users are usually targeted (Radanović & Likić, 2018). Cook County, located in Chicago, USA, has developed a pilot application that uses this type of blockchain network in collaboration with Velox.re to track and reliably record assets where changes in ownership may occur, such as land property.

Hybrid Blockchain Networks

It is a type of blockchain network where the strengths of public and private blockchain networks are taken and the weaknesses are tried to be limited. Therefore, in a hybrid blockchain network, the entire ledger can be accessed by everyone in the world with the open blockchain network logic, while access to the changes in the ledger can be controlled with a private blockchain network running from the background (Sagirlar, Carminati, Ferrari, Sheehan & Ragnoli, 2018). The XinFin project is a hybrid blockchain project developed for the supply chain. This project used both the Ethereum blockchain, which is an open network, and the Quorum blockchain, which is a private blockchain. In this project, the private blockchain network is used to generate hashes of transactions, which are then validated on the public blockchain network.

Comparison of Blockchain and Linked Lists

In each node forming the linked lists, the data to be kept as a basis and the address information of the next node are kept. In computer science, linked lists correspond to a data structure. The fact that each node is connected to the next is similar to the interconnection of blocks in a blockchain. In each block in the blockchain, the hash information of the previous block is kept. By looking at this information, it can be reached up to the first block of the chain. In the blockchain, as in linked lists, there are genesis blocks that do not keep previous Hash information, that is, the first blocks that make up the chain. In the blockchain, the previous block is reached with the hash function, while in linked lists it is reached with the pointer function. While the data is kept in a linear structure in linked lists, transactions and the data associated with these transactions are kept in trees called Merkle trees in the blockchain. While there is a validation mechanism in blockchain, there is no such mechanism in linked lists.

Comparison of Blockchain and Centralized and Distributed Database Systems

Traditional database technologies use client-server architecture. A client can edit data held on a central server. Control of the database remains with a competent authority who verifies a customer's credentials before gaining access to the database. Since this authority is responsible for the management of the database, data can be changed or even deleted if the security of the authority is compromised. In distributed databases, trust is mandatory for all machines that make up the database. It is assumed that no machine will take a malicious approach to the integrity, accuracy and security of data, and this structure is completely centralized.

Blockchain consists of multiple nodes that are decentralized. More than 51% of the nodes in the blockchain network must reach a consensus for data to be added to the blockchain. Thanks to this agreement, the intangibility and security of the data are guaranteed.

Consensus Algorithms

A block to be added to the blockchain can only be added after the majority of the nodes that make up the blockchain network reach a consensus. This process is called consensus. Consensus algorithms are decision-making mechanisms that help the group of nodes that make up the blockchain network to reach consensus on the addition of the new block to be added to the blockchain.

Some consensus algorithms and working logics are as follows:

Proof of Work

It is the first consensus algorithm introduced in the Proof of Work blockchain network. Many blockchain technologies use this algorithm to confirm all their transactions and generate their blocks. According to this consensus algorithm, nodes in the network try to solve a difficult problem given to them. There is a value called nonce that they are trying to find. The value created by hashing together this nonce value, which is tried to be found with the data to be written to the block, is available at the nodes. Nodes spend all their power on the question of which nonce value we hash with the data at hand, we will reach this final value. This process is called mining. The first node to find the nonce value announces to all the nodes in the network that it has found the correct nonce value. All other nodes check whether this nonce value is true. If a sufficient number of nodes accept that this nonce value is correct and share this nonce value with all nodes in the network, it is added to the block chain and the system-specific cryptocurrency (coin) with an incentive reward is given to the node that finds the nonce value.

The PoW algorithm has been refined over time. The reason for this is that the system is gradually slowing down, the time taken for a block production is too long, and therefore the requests cannot be fulfilled in a timely manner. Making the problem solved by the nodes easier means that the system is open to DDoS attacks.

The first and most popular blockchain to use the Proof of Work algorithm is the Bitcoin blockchain. The approximate time it takes to create a block in this algorithm is 10 minutes. This time can be seen as a disadvantage of this algorithm, as there is no speed to meet the demand of client nodes. Another issue that can be considered as a disadvantage is the excessive energy consumption of the nodes trying to solve this difficult problem. According to a study, the energy consumption statistics of the Bitcoin blockchain, which is the most popular blockchain using the PoW algorithm, are expressed in the table below.

Explanation	**Value**
Bitcoin's estimated annual electricity consumption (TWh)	64.37
Annual Global Mining Revenues	$3,218,288,371
Estimated annual global mining activities	$3,218,288,371
Current Cost Percentage	100.00%
The country closest to Bitcoin in terms of electricity consumption	Switzerland
Total Network Hash Rate PH/s (1,000,000 GH/s)	49,367
Electricity consumed per transaction (KWh)	640
Number of American households that can be powered by Bitcoin	5,959,793
Number of US households working for 1 day with electricity consumed for a single transaction	21.64
Bitcoin's electricity consumption / the world's electricity consumption	0.29%
Annual carbon footprint (kt of CO2)	31,539
Carbon footprint per transaction (kg of CO2)	313.74

A 51% attack is when at least one more than half of the miners in the network create new rules that work for them and take over the system. Regardless of the consensus algorithm, 51% of the nodes in the blockchain network can decide together in terms of operational power and try to continue on a new chain according to themselves. This situation is called fork. To explain with an example, 51% of the processing power in the blockchain may want to jointly decide and prevent the transfer of the crypto money that person A wants to transfer to person B and share this money among themselves. In this case, there will be a difference between the chain in which the nodes that are on the minority side of the transactional power add their blocks and the chain added by the group with the majority of the transactional power. There are two types of bifurcation, hard and soft. While the old structure is no longer valid for the nodes using the new rules in the hard fork, the new rules do not make sense for the nodes using the old rules. Bitcoin Cash (BCH) and Bitcoin Gold (BTG) are examples of hard forks made of Bitcoin (BTC). Ethereum Classic (ETC) is an example of a hard fork made of Ethereum (ETH). Soft fork, unlike hard fork, can work with old versions. In other words, the blocks produced with the old rules are also accepted by the new rules and continue with a single chain. After a certain period of time, the majority of the nodes in the network switch to the new separation and the fork is completed successfully.

Proof of Stake

According to this algorithm, all coins in the system are initially produced and coins are given to the nodes according to their investments. Nodes in the blockchain network now have as much power as their own coin. There are two methods to determine the node that will create the block based on their share. According to the first method, the node with the highest denominator according to the total number of coins has the right to share the first block to be shared. If it does not share this expected block within the specified time, the turn passes to the node with the second highest share, and in similar cases, the process continues in this way. According to the second method, a node is not determined initially, but similar to the PoW algorithm, while the nodes are given problems to solve, the nodes with a high share are given easier problems to solve, thus increasing the probability that the node that will create the block first will be the node with the largest share. An age concept has been developed in order to prevent the nodes with more shares from constantly creating more blocks and generating more income than the nodes with less shares, and to ensure that nodes with less shares can also create blocks. According to this concept, coins with a higher age value are more likely to create a block, and the age values of a node's coins used to create a block are reset after the block is created. The reset coins start to gain age again over time, and these transactions continue by repeating in this way. While the block generation process in the PoW algorithm is called mining, in the PoS algorithm it is called forging or minting. In the PoW algorithm, the nodes that produce blocks are called miners, while the nodes that produce blocks according to the PoS algorithm are called validators. Since the PoS algorithm is not an algorithm that requires computations with a high degree of difficulty like PoW, hardware-based centralization and high energy consumption, which is very likely in the PoW algorithm, will not occur. Nodes that want to generate blocks according to the PoW algorithm consume excessive electricity as a cost. Nodes that want to generate and/or verify blocks according to the PoS algorithm must initially load a certain amount of Ether as a deposit into a smart contract. Even though a node performs this loading, it can compete with other deposit loading nodes to produce blocks. If a node charging the deposit commits a fraudulent act, they will forfeit the entire deposit they have placed.

Delegated Proof of Stake

According to the DPoS algorithm, all transactions required by the blockchain network, such as the size of the transactions, the range of the blocks produced, and the pricing, are made by the witnesses (witness) chosen by the representatives (delegate) in the blockchain. Witnesses are responsible for adding blocks to the blockchain and are rewarded for this. Each witness has only one vote. It is said that whichever node has the highest vote among the witnesses is the most reliable node, and the priority for creating a block is given to this witness. Witnesses must keep their nodes running constantly and aggregate transactions on the network into blocks. They must digitally sign and publish these blocks they collect. They must approve transactions. If there is a problem with consensus, the DPoS algorithm ensures that these problems are resolved fairly and democratically. Delegates do not have the power to change the details of any transaction. The approximate time required for transactions to be written to a block is 10 seconds. In general terms, it is a consensus algorithm that functions as a digital version of democracy. According to the PoS algorithm, the node that will create the new block is initially determined by the amount of coins distributed to the nodes, while according to the DPoS algorithm, users vote to select a certain number of witnesses. Witnesses with the most votes are rewarded for verifying transactions and creating blocks. The DPoS algorithm is faster and more scalable due to fewer nodes verifying transactions and creating new blocks. Examples of blockchains using the DPoS consensus algorithm are ARK.io, EOS, Lisk, STEEM.

Proof of Elapsed Time

PoET is a blockchain consensus algorithm that prevents high resource usage and high energy consumption and ensures that transactions are carried out more efficiently with a fair lottery system. This algorithm is often used to determine mining rights and block creators in permissioned blockchain networks. It is imperative that every node in the network waits for a randomly chosen time slot. The first node to finish waiting for the specified time interval wins the new block. Each node in the network generates a random wait time and sleeps during this time. The node with the shortest waiting time, that is, the earliest to wake up, processes the new block into the blockchain and broadcasts the mandatory information to all nodes in the network. The same operations are repeated to produce the next blocks. There are two important factors that guarantee the fairness of this algorithm. The first is to ensure that the nodes in the network do not intentionally choose a short wait time to win the new block, but generate this waiting time truly randomly. The second is to ensure that the winner actually completes the cooldown.

Practical Byzantine Fault Tolerance

According to this consensus algorithm, which is designed to work in asynchronous systems, each validator node in the network waiting to verify transactions has a public-private key pair. Every validator node in the network has the public key information of all other validator nodes. After each node in the network checks a transaction information sent to it, if it approves this transaction, it shares it with other nodes in the network by signing it with its own private key. In the PBFT model, basically the nodes in the network are ordered as one primary node (leader) and the others as backup nodes. All nodes in the network are in communication with each other and the main purpose is to reach a common decision and agreement with all honest nodes in the network as a majority on the state of the system. Nodes in communication with each other must both prove that the message they received came from a particular node in the network and verify that this message has not changed during the transmission to them. This reconciliation has four main stages. In the first step, the client calls the leader node for a service operation. In the second stage, the leader node forwards this request to the backup nodes. In the third stage, the backup nodes implement the request sent to them by the leader node and each send a reply to the client. It waits until the client receives the same answer in sufficient majority. The result that reaches a sufficient majority is the result of the client's request. When honest majority nodes determine that the leader node is faulty and should be removed, they remove the leader node and replace it with the next leader node.

Simplified Byzantine Fault Tolerance

According to this algorithm, a designated block-generating node collects and validates the transactions suggested to it and periodically combines them into a new block proposal. Consensus is provided by this generator node, which implements rules accepted by the nodes and block signers. Other block signing nodes approve the proposed block by signing it. All members in the network know the identities of the block signers and will only accept a block if the majority of signers sign a block. A block signer verifies all transactions within each block. Only blocks that have been verified by a quorum are added to the chain.

Directed Acyclic Graphs (DAG)

DAG is not actually an example of a blockchain. There is no concept of block in DAG. It is a structure made up of nodes and faceted edges. In this structure, each node represents a piece of data. In the blockchain, blocks are kept unidirectionally linked and there is at most one way to go from one block to another. However, according to the DAG structure, there can be more than one way to go from one node to another. In order for a transaction to be valid in DAG, it must verify two different transactions at random. The reason why DAG is defined as acyclic is the absence of a bidirectional relationship between two nodes. That is, if there is an edge from an X block in the direction of the Y block, it is not possible to have an edge from the Y block to the X block, but a block can be unidirectionally related to more than one block. A root node is called a DAG node that has no ancestor, and a leaf node is a DAG node that has no children. Topological sorting is used in the DAG algorithm. That is, each edge is always routed from the previous edge to the next. Blockchain and DAG are examples of distributed ledgers, but blockchain is a linear distributed ledger, while directional acyclic graphs do not have a chain of interconnected blocks. Although blockchain and distributed ledgers are used as synonyms in the cryptocurrency world, DAG is also a distributed ledger without a blockchain.

We can list the advantages of DAG over blockchain as follows:

> DAG is more scalable and therefore faster compared to blockchain.

> DAG does not contain blocks. Nodes do the validation.

> DAG is highly reliable as all transactions are verified at least once by all nodes thanks to its structure.
>> There is no energy consumption. In other words, it is far from centralization compared to the PoW algorithm, which causes hardware centralization.
> DAG is ideal for small payment systems as it charges almost zero commission.
A disadvantage of this system is that DAG does not contain information about protection against system crashes.
Basically, Crypto Classic is trying to realize a unique payment system by combining DAG technology with Etherium codes.

Proof-of-Activity

It is a hybrid algorithm created by combining the two best features of PoW and PoS consensus algorithms, which are more reliable and do not require high energy consumption. According to the PoA algorithm, mining operations start just like in the PoW algorithm, but the difference between them is that while in the PoW algorithm (mine) blocks containing full transactions, in the PoS algorithm, miners only dig block templates containing header information and reward addresses for miners. After miners dig these block templates, the system switches to the PoS algorithm. Within the block, the header information points to a random node, which is then responsible for verifying previously mined blocks. Verifiers with more blocks to verify have a higher chance of validating blocks. A blockchain can be added to the chain after verification. The network pays miners and validators fairly.

Proof-of-Capacity

It is an improved version of the PoW algorithm. There is a nonce value that miners are trying to find. Nodes have to allocate hard disk space to mining operations before they start mining. This feature makes the PoC algorithm faster than the PoW algorithm. In the PoW algorithm, the nonce value is constantly produced and tried to be estimated, while according to the PoC algorithm, the nonce value is sought among the possible solutions kept in the memory of the nodes before starting mining. The more solutions the nodes have, the more likely they will naturally be to win the mining race. The Proof of Capacity algorithm basically consists of two stages. These are the plotting and mining stages. A list of all possible nonce values during the plotting phase is created by repeatedly combining data, including a miner's account. Each nonce has 8192 hashes in the range 0-8191. Adjacent hashes are divided into binary groups. The miner, who starts the mining process in the second stage, starts mining by generating a scoop number (N) given to the binary hash groups created in the first stage. The miner goes to the scoop number N produced by the nonce value 1 and uses the data in this scoop to calculate the deadline value. This process is repeated for each nonce value held on the miner's hard disk. The minimum deadline is selected by the miner after all deadline calculations. Deadline is the time from the last block production to when a miner is allowed to produce a new block. If no other node creates a block during this time, the miner can create his block and claim a reward for the block he created. The PoC algorithm allows the use of various systems, including Android-based systems. It consumes up to 30 times less energy than ASIC-based mining operations.

Proof-of-Burn

PoB is based on the principle of 'burning' or 'destroying' coins, which gives miners mining rights. It can be said that it is the version of the PoW algorithm without energy loss. Miners are given the right to produce blocks in proportion to the coins they have burned or destroyed. The miner burns his coins to get the virtual mining hardware, which gives him the power to mine blocks at the rate of the coins he burns. Miners can also burn alternative blockchain coins like Bitcoin, but are rewarded when they burn the network's native cryptocurrency. The power given to miners by burned coins decreases as new blocks are mined (Zheng etc., 2016).

Proof-of-Weight

It is a version of the PoS algorithm that has made great progress. According to the PoWeight algorithm, it looks at the so-called 'weighting factors' as well as the amount of coins owned. The main advantages of this system are that it is customizable and scalable. Being customizable means that the 'weighting factors' can be diversified.

Comparison of Consensus Algorithms

Consensus Algorithm	Blockchain Platform	Release Year	Programming Languages	Smart Contracts	Pros	Cons
PoW	Bitcoin	2009	C++	No	Low 51% attack chance	High energy consumption Centralization of Miners
PoS	Ethereum	2015	Solidity	Yes	Low Energy Consumption more decentralized	Nothing-at-stake issue
DPoS	Lisk	2016	Javascript	No	Low energy consumption Scalable Increased Security	Partially central Double spend attack
LPoS	Waves	2016	Scala	Yes	Fair Use Ability to rent coins	Decentralization Problem
PoET	Hyperledger Sawtooth	2018	Python, JS, Go, C++, Java and Rust	Yes	Cheapness of participation	Special hardware requirement Not good for open blockchains
PBFT	Hyperledger Fabric	2015	JS, Python, Java, REST and Go	Yes	No confirmation needed Low energy consumption	Communication Gap Cybil Attack
SBFT	Chain	2014	Java, Node and Ruby	No	High security with signature	For open blockchains

Disadvantages of Blockchain

In addition to the advantages of the Blockchain, the difficulties that can be considered as disadvantages can be listed as follows:

> Scalability: It has difficulty in responding to the demands of the large number of nodes in blockchain networks, offering slow transaction speeds and demanding high fees per transaction. Solutions to the future adaptation and efficiency problems of blockchain technology, which could not complete its development and expansion process, should be produced before the blockchain becomes fully widespread. While all transaction data are kept in blocks in the standard Bitcoin blockchain, a payment channel is opened between the parties who want to transfer according to this project. After the channel is opened, no transaction information is added to the blockchain until the channel closing request. However, while the payment channel is closed, a transaction containing the current balance information of the parties is kept in the block. In this way, the transaction data to be added to the blockchain is reduced.

> Inefficient Technological Designs: Ethereum's smart contract platform allows developers to run their own DAPPs. According to a study conducted at the National University of Singapore, a large number of smart contracts contain weaknesses due to their coding. In the Bitcoin blockchain, keeping all transaction data, whether important or not, causes this network to be heavy and slow.

> High Energy Consumption Consensus Mechanisms: PoW consensus algorithm is used in the majority of blockchain applications. Since the PoW algorithm is an algorithm that requires high computations, nodes need to consume high energy due to high computations to reach a conclusion.

> Privacy and Security Issues: In permissionless blockchain networks, transaction data and histories are visible to anyone in the world with an internet connection. While this is a good thing for the transparency of the blockchain, patient records etc. Privacy issues may arise in some cases where information is held on the blockchain.

> Cost: Blockchain technology is an effective tool to reduce costs. It reduces the fees associated with the transfer fee and can speed up the operational processes. But since it is a new technology, it will be difficult to integrate into old systems. Blockchain solutions using consensus mechanisms that require high computation have high costs due to the energy they consume.

> Regulations: Blockchain applications may need to operate within existing regulatory structures that are not outside of them, but this means that regulators in all industries must understand the technology and its impact on businesses and consumers in their industries. If the regulators do not fully understand the blockchain, various problems may arise due to inaccuracies in the regulations.

Technology

The technology sectors affected by the blockchain can be grouped under the following headings:
> Cloud Storage: Although cloud storage is effective because it works in a centralized structure, it is vulnerable to security threats. With blockchain, users can rely more on cloud storage as it moves to a decentralized system where it will prevent their data from being lost.

> Power and Energy Management: Blockchain will change how we store, distribute and generate energy in the first place. Currently, they charge high fees for energy transmission as there are many intermediaries when it comes to energy supply. With the blockchain, it is envisaged to get rid of intermediaries and reduce costs.

> Cyber Security: Thanks to the blockchain, institutions can keep their data encrypted in a decentralized way. In this way, they can protect their data from hacker attacks and DDoS attacks. Civic, Cambridge Blockchain and Gladius projects are examples of blockchain-based cybersecurity projects.

Law and Crimes

Blockchain maintains the integrity of data and hence is a great platform to store all evidence. It can also be deployed without worry and adds a layer of security to the security application.

Government Policy

> Governance: The number one purpose of the government wanting to use blockchain technology is to achieve governance rights, have a proper transparent voting system, ensure citizen rights, minimize fraud in the system, improve law and order decision making with blockchain solutions that can run smart contracts.

> Health Sector: Providing health services to citizens, one of the primary duties of governments, can become more sustainable, reliable, scalable and traceable with blockchain.

> Education: The central authority, which is the third party between the service requester and the service provider in online education services, will be eliminated with the blockchain. Those who request the service will be able to get service at a cheaper price.

Contracts

Contracts are the business agreement, payment, etc. between the two parties. It exists to determine the conditions on such matters and to ensure that the parties act by adhering to them. It is possible to examine contracts in three sub-categories;

> Inheritance: Thanks to smart contracts, inheritance transactions can be moved to the blockchain platform. Legacies can be digitally transferred to whomever they want after people die with smart contracts. A project called Digipulse is an example of this.

> Legal Contracts: With smart contracts, intellectual property rights can be protected against the risk of being stolen by others.

> Property and Land: Ownership of property and lands can be secured and their prices determined by smart contracts.

Crypto Classic Technical Accounts

Crypto Classic accounts will consist of addresses of 25 bytes. A CRC account holds the following 4 information:

> Nonce value, which is a counter used to ensure that each transaction runs only once

> Current CRC balance of the account

> The contract code of the account, if any

> Account's storage space (empty by default)

There will be two types of Crypto Classic accounts:

> Externally owned accounts: controlled by private keys.

> Contract accounts: controlled by contract codes.

Externally owned accounts do not contain codes. Externally owned accounts can create and sign a transaction and send it to a contract account. The code is activated every time the contract receives a message. Smart contracts in Crypto Classic should not be seen as rules to be fulfilled or followed. They can be seen as autonomous agents with direct control over their own CRC balances that run a custom piece of code when prompted by a message or transaction.

Running the Process

The most complex part of the CRC protocol is running a transaction. It is assumed that each run operation passes an initial test in which its intrinsic validity is tested. This test consists of the following items.

> The transaction should be a well-formed RLP output with no trailing bytes.

> The signature of the transaction must be valid.

> The nonce value of the transaction must be equal to the current nonce value of the sender's account, ie valid.

> The balance of the sender of the transaction must be at least the cost required for the down payment.

Y state transition function, T process, σ state and σ' post-process state;

$\sigma' = Y(\sigma, T)$.

The RLP function has an encoding/decoding algorithm developed for serializing complex data such as nested arrays in CRC, by adding a prefix byte specifying the data type and the length of the original data and offset, and returning from this state. This function analyzes the data type and the length of the offset with the actual data by first looking at the first byte of the input data during the decoding phase. It decodes the data according to the type and offset of the data. The same process continues for other serialized data.

During the execution of the transaction, the information that follows the transaction instantly is collected. This collected information is called substate and is represented by C.

> **C** consists of 4 components**: C ≡ (Cs, Cl, Ct, Cr)**

> **Cs:** It is a cluster where accounts that will not be used after the completion of the transaction are kept.

> **Cl:** A log series of archival and indexable 'checkpoints' found in the execution of the VM code, which allows contract-calls (eg a Dapp interface) to be easily tracked.

> **Ct:** is a set of accounts touched, contacted, empty ones deleted at the end of the process.

> **Ct:** Repayment balance.

Executing the Message Call

To execute a message call, sender (**s** - sender), transaction originator (**o** - transaction originator), receiver (**r** - recipient), account to run the code (**c**, usually the same as receiver), available gas (**g** - available gas), value (**v** - value), gas fee (**p** - gas price), an arbitrary-length array of bytes with the input data of the message call (**d**), depth of the message-call/contract-creation stack (**e**), and permission to change state (**w**) data is required. Besides evaluating the new state and substate of a process, message calls have as an extra component a byte array that holds the output data represented by o. This o data is ignored when running processes.

$Yz(\sigma, T) \equiv z$, where Yz is the status code of the operation.

In the light of the above data, it would be correct to write an equation in which which output data is calculated by inserting which input data into a function as follows:

$(\sigma' , g' , A, z, o) \equiv \Theta(\sigma, s, o, r, c, g, p, v, d, e, w)$.

Crypto Classic State Transition Function

The state of a CRC calculation consists of the following four fields, σ = location, a = address:

> **Nonce:** The number of transactions sent from the address owned by this account, or the number of contracts created by this account for accounts associated with the code. It is formally represented by this expression: $\sigma[a]n$. (n = nonce)

> **Balance:** The amount of Wei the address has. It is formally represented by this expression: $\sigma[a]b$. (b = balance)

> **storageRoot:** 256-bit hash of the root node of the Merkle Patricia tree. It is formally represented by this expression: $\sigma[a]s$. (s = storage)

> codeHash: Equal to the hash of this account's CRC code. This code works in case of a message call to the account. It cannot be changed after it is created. It is formally represented by this expression: $\sigma[a]c$. (c = code)

Assuming the code is represented by b $KEC(b) = \sigma[a]c$.
The Crypto Classic state transition function, APPLY (S, TX) -> S' can be defined as follows:
> Checks if the transaction is well established (for example: there are the correct number of values), if the signature is valid, and if the nonce matches the nonce value in the sender's account. If one of the conditions is not met, an error is returned.
> The transaction fee is calculated with the formula STARTGAS * GASPRICE and the sender's address is decided by looking at the signature. The fee is subtracted from the sender's account balance and the sender's nonce is increased. If the sender's account does not have sufficient funds, an error is returned.
> The transaction value is transferred from the sender's account to the recipient's account. If the recipient account does not exist, it is created. If the receiving account is a contract account, run the contract code until it is complete or gas runs out.
> If the transfer of value fails because the sending account does not have enough funds, or there is no gas required to run the code completely, it will roll back all status changes except the fee payment and add the collected fees to the miner's account.
> Otherwise, the remaining gas is refunded to the sender and the gas fees used are also sent to the miner.

In terms of undoing the actions performed, the messages work equally to the actions: if the throttle is not enough while running a message, the execution of the message and any other executions triggered by it will be rolled back, but the applications before the execution of this message will not be rolled back.
Accounts that do not contain codes and that have Nonce and balance values of 0 are empty accounts.
$EMPTY(\sigma, a) \equiv \sigma[a]c = KEC\ (()) \wedge \sigma[a]n = 0 \wedge \sigma[a]b = 0$
If an account's state is empty or does not exist, it is a dead account:
$DEAD(\sigma, a) \equiv \sigma[a] = \emptyset \vee EMPTY(\sigma, a)$

Calculation and Full Compatibility

Because the CRC code can do any kind of computation reasonably, including infinite loops, the CRC code allows for loops in two ways. The first one, the JUMP command, allows the program to switch to the previous point in the code, and the JUMPI command is used to switch when conditions such as while a < 13: a = a * 2 are met. Second, contracts allow looping other contracts, potentially by recursion. As described in state transitions, the maximum number of steps a process will take is specified, and if the calculation takes longer, the calculation is rolled back but fees are still paid. Messages work the same way. The following example makes the logic behind this solution more understandable:

> An attacker runs a contract with an infinite loop and then sends a transaction to the miner that will capitalize that loop. The miner sees the transaction and runs the endless loop and waits until the gas runs out. Even if the gas runs out and the transaction is interrupted while this cycle is running, the transaction is still valid and the miner still charges the attacker their fees for each calculation step.

> An attacker creates a very long infinite loop, forcing the miner to calculate during this long time. When this very long calculation is over, other blocks will appear in the network that were dug by other nodes, and because of this situation, the miner who runs this long endless loop will not be able to charge for his calculations. But the attacker will need to specify a value that specifies how many steps the computation he wants the miner to perform consists of. Thus, the miner will know beforehand that the calculation to be made will take a very long time.

> An attacker send(A, contract.storage[A]); Suppose he sees a code contract.storage[A] = 0 and sends a transaction with only enough gas to perform the first step. In this case, the owner of the contract does not need to worry about such attacks, because if the transaction is interrupted, all changes will be rolled back.

> Suppose a financial contract works by taking the median of nine different data sources to mitigate risk. An attacker can manipulate one of nine different data sources with a variable-address-call, making it an infinite loop. In this case, the gas shortage problem will arise again. However, this problem can be prevented by placing a gas limit in a message to the financial contract.

Crypto Classic Token Standards

CRC tokens are digital assets represented by smart contracts. Each project developed on the Crypto Classic platform to be built can have its own token that complies with the specified standards. Tokens can be used for a variety of purposes and are often offered for bulk sale during an ICO. It can be bought, sold or traded.

Token Balance

Suppose the token contract has the following two token holders:
Let the balance 0x1151161181181131114111611114112111111111 be 300 units (A)
Let the balance of 0x2222222322222222222222232225222224222722222 be 400 units (B)
The balances data structure of the contract will return the following information down:

balances[A] = 300 balances[B] = 400
The balanceOf(. . .) function will still return the same values using the following:
tokenContract.balanceOf(A) will return 300, tokenContract.balanceOf(B) will return 400.
Balances and balanceOf concepts are balance learning methods in web3.js library. While their use may vary according to versions, it is also possible that the concepts of these rapidly developing and changing technologies have become obsolete.

Clients with a Graphical User Interface (GUI)

> Parity Crypto Classic

It is a CLI (command-line interface) based client developed with Rust programming language to ensure maximum loading speed and fastest synchronization securely. By default, JSON-RPC HTTP Server is running on port 8545 of this client.

JSON-RPC HTTP Server

JSON is a light weight data exchange format. It has a tree structure. It supports a collection of number, string, name and value pairs, objects, boolean and array data types. RPC (Remote Procedure Call) is a protocol used in distributed, decentralized networks. With this protocol, a program on one computer can call a function, method, or procedure on another computer in the network. JSON-RPC, on the other hand, is the RPC protocol in which the call to other computers in the network and the response to this call are transmitted in JSON format, which is light on the load. JSON-RPC HTTP Server is an HTTP server that receives or transmits RPC requests or responses in JSON format from the network.

Testnets

Testnets are networks developed to test whether developed smart contracts or DAPPs are written properly, error-free and smart enough. A Dapp or smart contract that has successfully passed the tests on these networks can now be run on the mainnet with peace of mind. If a Dapp is run on the mainnet without being tested on any of the testnets, there is a bug, lack of gas, etc. If problems occur, it will be to the detriment of the user. Therefore, these tests are made with cryptocurrencies that do not have a defined financial equivalent on testnets. When a transfer is made from mainnet accounts to any account in these networks, it is irreversible, the transferred cryptocurrency is burned. There should be a mechanism that encourages miners, like the mainnet, that validates transactions and writes them to blocks in exchange for ethers, which have no monetary value. Below is a list of Ethereum testnets developed for the Ethereum platform and how nodes in these networks are rewarded for their test operations:

Decentralized Applications (DAPP)

DAPP, short for Decentralized Application, means an application that does not have a central server and whose database cannot be changed or deleted by anyone. The main features of DAPP can be listed as follows:

> The source code is available to all users.
> Blockchain compatible and decentralized.
> The application has its own cryptocurrency.
> Provides consensus algorithm for its users.

NodeJS was used as the Backend service of the trial Dapp application developed for Crypto Classic, Solidity was used as the smart contract language, and HTML5, Jquery, Javascript and Bootstrap were used for web application development and design.