GREAT BOUNT DEALER (GBD) WHITE PAPER

V1.0

OCT.2020

https://greatbountydealer.com

ABSTRACT

Smart contracts, applications that are deployed and executed in decentralized systems. Once a smart contract has been placed on a blockchain, changes cannot be made. Smart contracts, have a more secure structure compared to traditional contracts. Smart contracts, automatically perform the transaction securely without the need for any transaction based on the request and demand between the two parties. Smart contracts cannot obtain and transact off-chain data such as API data. This is due to the consensus mechanism of the blockchain, we offer our proposals to develop solutions to many problems with GBD.

GBD is an open source smart contract token traded on the decentralized TRON network. Decentralization reduces trust between parties and the rate of resolution of needs. GBD contracts allow you to pass many procedures easily with smart contracts that produce more reliable, transparent on-chain transactions and produce fast solutions. This is the prerequisite for connecting smart contracts to the real world, and this is how digital contracts are replacing traditional contracts. Real (physical) interactions with the crypto unit have become possible with the constantly developing technology. Crypto units, which are considered as blockchain-based valuable assets, which have shown great development in a decentralized manner in recent years, provide fast, cheap and easy transfers of large amounts. It is almost impossible to lose or damage smart contracts that are encrypted and signed in a completely digital environment.
Input/output data is required to apply smart contracts to a wider range of scenarios. We can follow the smart contracts like the following example:

- Secured smart contracts are similar to securities such as bonds, APIs that report interest rate derivatives and many other value derivatives, market prices and other market data references will be required. E.g; interest rates.

Insurance smart contracts, the insured event in question, will need to be fed with IoT data in the following cases. E.g ; Was the warehouse door locked? At the time of the breach, was the company's firewall online? Did you give the flight permit? Did you have insurance to arrive on time? Many similar problems bring problems and questions in insurance contracts.
Trade finance smart contracts will need GPS data on shipments. Supply chain ERP systems and customs data on shipped goods confirm whether contractual obligations are fulfilled.

Payment messages often have to be forwarded to off-chain institutions (for example, bank systems). GBD can securely output data to off-chain systems. The connection of smart contracts with the real sector strengthens its position very strongly and evidently with these applications. Transactions are carried out in a completely digital and completely secure manner, without the need for any physical contact in cryptocurrencies. Many problems experienced in real physical situations have aimed to minimize the risk and problem rates in crypto currency transactions.

2.WHAT IS CRYPTO CURRENCY?

Crypto currency (crypto-asset) is a digital element that is fully digitally encrypted to secure transactions, the way it works, designed as an alternative medium of exchange to cash. Crypto can also be considered as a kind of virtual currency, digital currency (alternative currency). The decentralization of each crypto currency comes from a block chain that functions as a public transaction database, a distributed ledger.

2.1. CRYPTOCURRENCY FEATURES

1. Decentralization
2. Transaction and owner records
3. New supply creation rules
4. Only the owner can prove the ownership with cryptographic techniques
5. Fulfillment of only one if multiple transactions are made for the same crypto currency at the same time.
6. Crypto currency can only change hands at the owner's order

3.ENCRYPTION TECHNIQUES

3. 1. SIMPLE ENCRYPTION TECHNIQUES

Block chain, the core technology of crypto currencies, is a distributed ledger. It is a digital payment system that uses a “Peer-to-Peer” network that is also fault-tolerant. It is the general name given to the currencies in which cryptography is used in the crypto units codes and coding ways that are widely spoken today. Cryptography, named after the Greek words for secret and writing; It is a field of science that aims to protect the content of existing data and that its content cannot be read or deciphered by other people. The process of hiding the content of a message is called encryption. This process converts plain text into cipher text using a key. Figure 3.1.1 below shows the encryption and decryption processes.

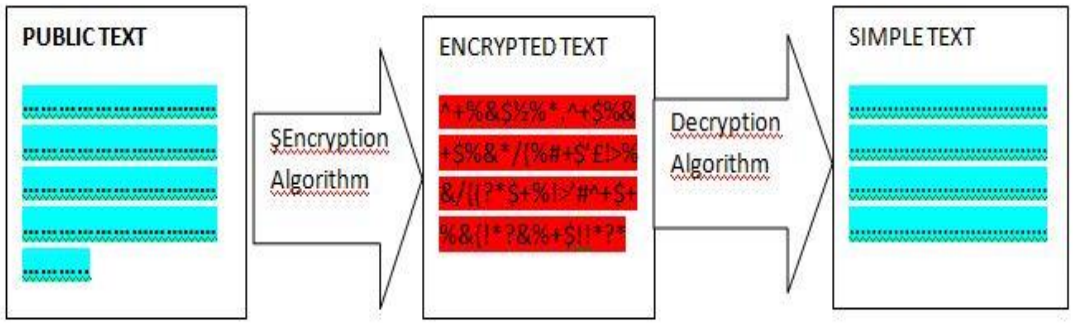
Figure 3.1.1 simple encryption process

Encryption algorithms are generally divided into two categories according to their key usage methods. These are: Private key (Symmetric) and Public key (Asymmetric) encryption algorithms. o briefly express the symmetric encryption algorithm: Although it is an encryption algorithm that works fast and is sufficient for small systems, the same key is used in encryption and decryption steps. This means that [n * (n-1) / 2] keys must be stored for a system with n users. In short, it is not scalable.

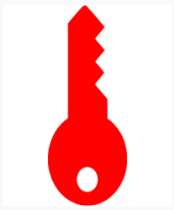
3. 2. ASYMMETRIC ENCRYPTION ALGORITHMS

Unlike symmetric encryption, there are 2 different keys in asymmetric encryption. These keys are called public and private. Public keys are distributed to everyone in the network (the network created by all participants), but private keys should be known only to the individual himself.

Public Key Systems



PUBLIC



PRIVATE

Emily susan

Susan's public key is known to everyone. However, Susan's secret key is private to Susan and is known only to her.

Figure 3.2.1 public key encryption technique

Secret Key Systems, sharing this private key is a problem as the sender and receiver use the same key. The secret key should be shared in such a way that only the receiver and only the sender can know the secret key. The solution to the key sharing problem in Private Key Systems has been found with Public Key Systems. Figure 3.2.1 above shows how a public key encryption process is performed. Asymmetric algorithms are used for privacy, signing, and key sharing. Asymmetric algorithms have a more complex structure than symmetric algorithms and therefore work much slower. The

most commonly used asymmetric algorithms are RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm) and Elliptic curve algorithm.

3. 3. CONCENSUS PROTOKOLS

Consensus Protocols, PoW (Proof of Work) and PoS (Proof of Stake): Consensus protocols; It is a set of rules that determine who will make changes in the block chain. In the PoW method, you earn as much as the block you dig. In addition, in this verification method, the first person to solve the necessary algorithm for adding the block to the chain receives the award. His type of mining requires investors to take an active role in verifying blocks of data. This ensures that transactions are verified and new coins are generated. If you do not actively work for block verification in this type of mining, you will not receive any rewards. The PoS method is considered as an alternative to Pow and is another type of verifying transactions on the network.
This method is actually not even mining because users do not need to take any action to generate new coins. For this reason, it is not considered as mining, but as printing money. In order to earn money in this method, you must have money in your electronic wallet. The prize you will win is directly proportional to the amount of money you keep in your wallet. The more money you have in your wallet, the more rewards you get, that is, you generate new money.

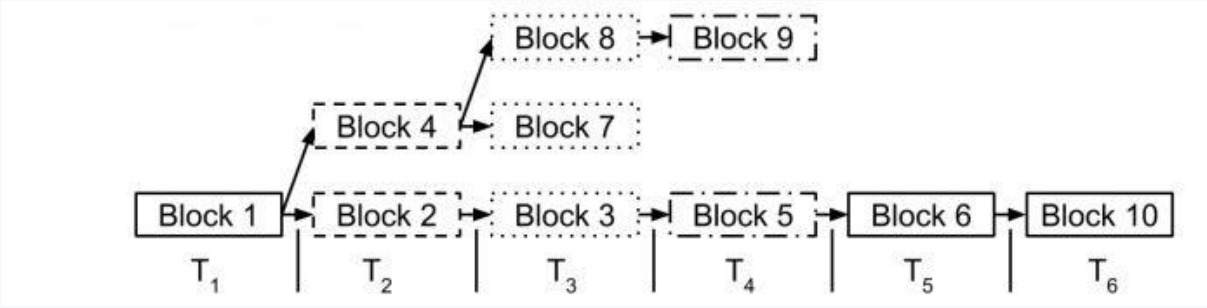


Figure 3.3.1 Blockchain Consensus Model

4. BLOCKCHAIN TECHNOLOGY

Blockchain is defined as a distributed database that keeps an ever-growing list of transaction records protected from dangers such as theft or alteration. In Figure 4.1,

the image of the distributed network architecture of the blockchain is shared.

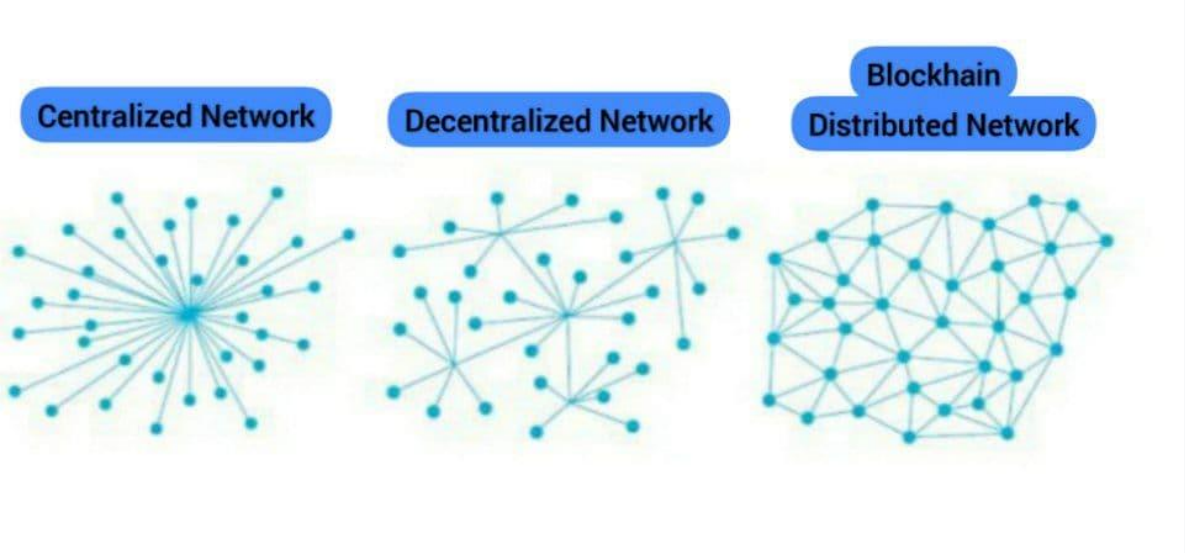


Figure 4.1 . Centralized, Decentralized and Distributed Networks

Blockchain; What we need; It is designed as an electronic payment system, based on cryptographic evidence rather than trust, where two parties can transact directly with each other without the need for a third trusted person. Blockchain was first proposed in 1991 by the cryptographers Stuart Haber and W. Scott Stornetta, who were looking for a solution to ensure the validity of official documents in the computer environment. Considering its current state, the work of Haber and Stornetta in 1991 is the prototype of the blockchain. Today's blockchain system can be thought of as an accounting book. When any peer-to-peer transaction is made, this transaction is recorded in an encrypted form. Anyone can join this network. Free participation in this network is due to the feature of the blockchain system as an open ledger. The term "chain" actually refers to a block of data. These data blocks are recorded by writing transactions as they arrive. These written data cannot be changed and are final. This feature is one of the most important features of the blockchain. Transactions are broadcast to all nodes in the peer-to-peer (P2P) network. blocks are of a limited size and when full, a new block is created next to the chain. If someone cheats and tries to change the data in the block, the system pushes this chain out of the system and preserves the integrity of the network. When the cheated chain is reinstated, that is, when the cheating ceases, the blockchain is reconnected. Anyone can see the entire transaction history. The completeness of the transaction history also ensures the validity of each virtual currency and all virtual currencies can be traced from the moment they are created. In addition, it provides retrospective transparency by providing resolution thanks to its technology. Prevents current records from being modified.

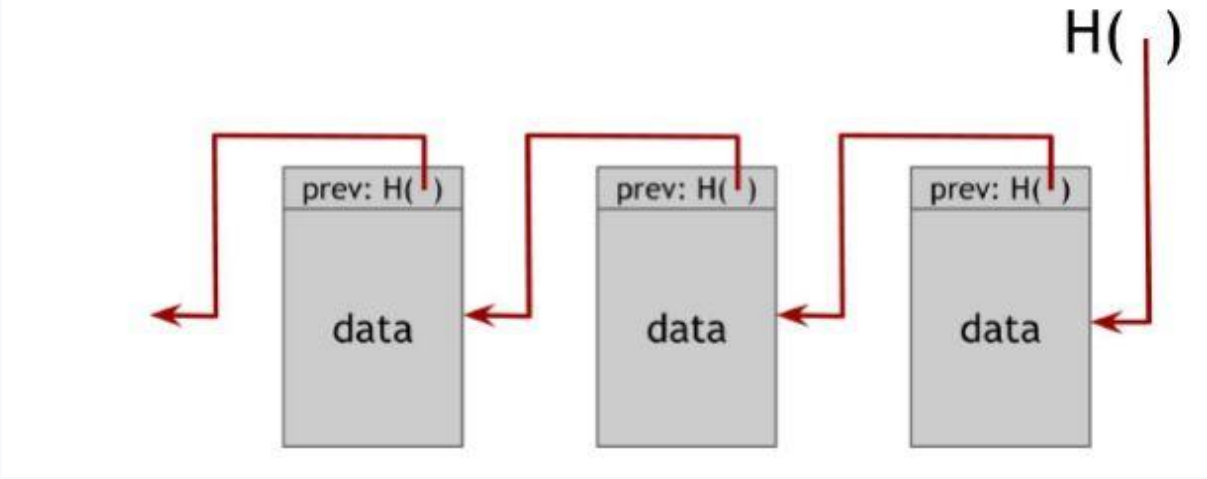


Figure 4.2. Blockchain Data Structure

There can be more than one transaction in a block. In the blockchain system, each user uses his own computer resources. Each node in the network has an exact copy of the entire ledger.

Magic Number	The unique number that identifies the block chain remains constant for all subsequent blocks.
Block Size	The number of consecutive bands to the end of the block.
Version Number	Block format type
Previous Block Link	Extract from previous block
Process Extract	The root node of the merkle tree is a descendant of all the extract pairs in the tree. The root node is the 256-bit hash linked to all transactions in the block.
Timestamp	Block creation time
Digging Difficulty	A measure of the relative difficulty of finding a new block. The difficulty is updated periodically as a function of how much hash power miners on the network consume.
Nonce	The number used once is used in the POW calculation.
Number of Processing	The Number of transactions in this block.
Transactions	Transaction list (cannot be empty)

Figure 4.3. Block Content

In the application of the blockchain, the systems called miners hold the entire blockchain, which includes all transactions so far. The selection of the node that will form the block is done with the consensus protocol. Creating a new block and adding it to the blockchain in a scenario where a transaction will be made between Computer1 and Computer2 machines via an application using a blockchain structure is shown in Figure 4.4.

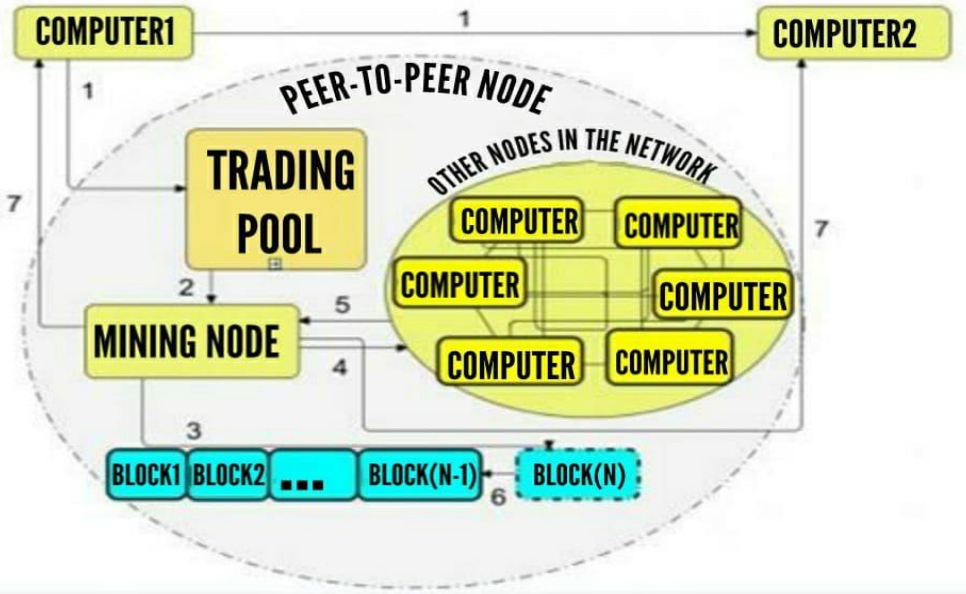


Figure 4.4. Adding a New Block to the Chain in a Blockchain Based Application.

1.Computer1 broadcasts the operation to the peer-to-peer network, including Computer2. 2. The use of the transaction pool in the system can be optional and transactions can be learned by broadcasting. Unconfirmed transactions are called by nodes. 3. According to the protocol used in the network, n transactions can be written to a block in bulk. A new block is created by the nodes. 4. Broadcast to computers on the peer-to-peer network for verification. 5. Information that the verification information has been completed is transmitted within the network. 6. In the peer-to-peer network, a miner node is selected by consensus protocol. The selected miner node adds the new block to the blockchain. 7. The information that the requested operation has been completed is transmitted to the machines that perform the operation.

Blocks are linked to previous blocks with the hash value. In this process, the general hash value is created from the hash value in the previous blocks. A summary of the previous block is also kept. In the block; If 4 transactions are collected and written in a block, the formation of a root hash (Merkle tree) from the hashes is shown in Figure 4.5.

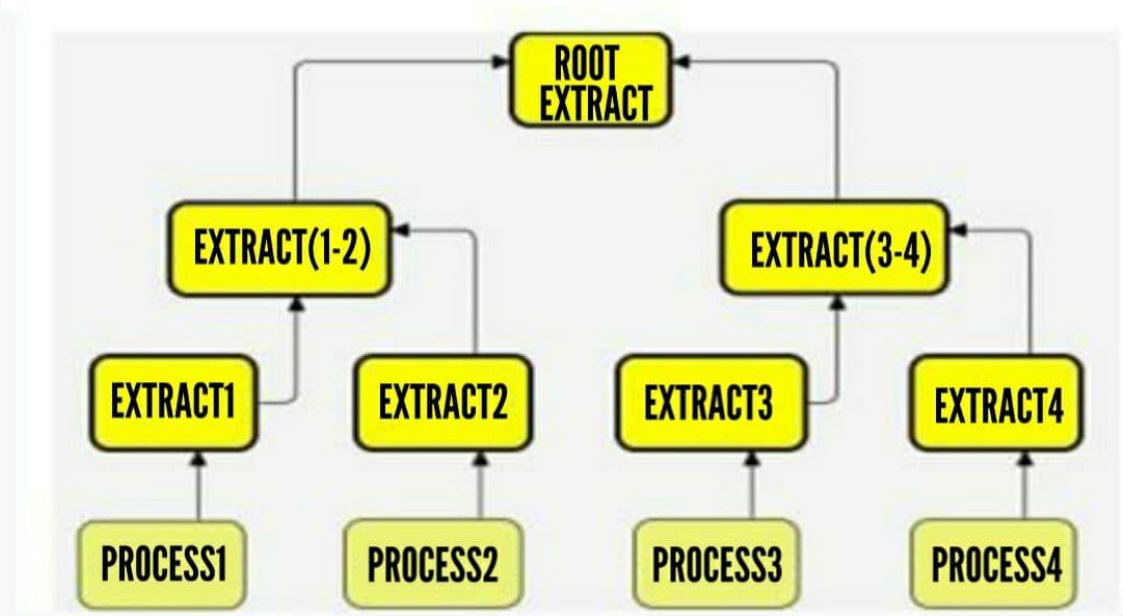


Figure 4.5. Creating a Merkle Tree

A block contains at least one transaction, and a block is 1 MB in size. The block header is 80 Bytes long and contains information about the block. Each transfer transaction is at least 250 Bytes long and there is an average of 350-500 transaction information in a block.

5. WHAT IS THE GREAT BOUNTY DEALER (GBD)?

The GBD project was created by Turkish entrepreneurs using the Tron Blockchain infrastructure, and was designed as a smart contract TRC20 open source code. It aims to be a virtual and real exchange and commercial unit in the crypto money market. It aims to make the change happen faster and more smoothly with the merger of the developing technology and the real sector. Being a non-repetitive, open to development, safe and rapid change tool, it has also been designed as a pioneer and solution producer in all necessary changes by focusing on developing technology. It is aimed to eliminate the problems that arise in all changes, virtual and real, and to complete the changes in a transparent, fast and reliable way in transportation and transfer processes, away from physical intervention. While efforts are being made to legalize cryptocurrencies globally for various reasons, many restrictive factors are put forward and there is a contraction in many aspects such as crypto unit distribution, transaction volume, and transaction transfers. However, although this restriction continues, crypto units are improving day by day and proving themselves with speed, security and low transaction fees.

5. 1. VISION

As a production and market vision, it aims to develop itself day by day and to find a solution to the problems that occur in payment systems and to move forward in an open way. To strengthen the value and service structure in technologically developing global economies, to minimize time and physical expenditures, to reduce physical labor force, to provide a pioneering and innovative service scope in the transfer of economic values with secure and provable data. To find more permanent solutions to the problems experienced in payment methods and to reduce the existence of these problems to a certain extent, to evaluate and improve every progress and every technological development.

5. 2. GBD PAY SYSTEM

Although it is not the right approach to state that the development of the PAY system, its announcement to the world, and that it will be easy and/or in the short term, we can accept that it will take place within a certain period of time. While electronic payments are made in many areas around the world, we aim to start a new era by adding a new one to these payment types by opening the payment system with Cryptocurrency. Improvements were made to use the designed system as a payment

system in 5 different ways. PAY system, payment types are listed as follows. The system order will be developed as equivalent to sorting.

a. Payment with crypto currency
b. Manual payment (by entering address)
c. Payment with QR code
d. Payment with instant fiat currency conversion
e. Contactless (app) payment (crypto & fiat)

The specified payment methods will continue to be developed depending on the roadmap. Contrary to what is thought, the PAY system will not only be an online payment method, but also a real payment method. The example is designed to be used in any shopping mall and/or X product payments. In the period when technology is rapidly advancing, it has become inevitable to make payments using crypto units. Considering the development of network systems, the innovations brought to the blockchain and the speed of transfer, the fact that it is much faster, reliable, provable and cheaper than a normal payment system reveals the necessity of a payment system. Many payment system experiments developed so far have remained in theory. The reason for this to remain in theory has not been successful since development has been made to make it payment-based only as a crypto unit. GBD aims to design the PAY system in 5 different ways to provide instant service as wallet, mobile application, pc application and website.

5. 2.1. VIRTUAL PROBLEMS

2.1.1. Considering the problems caused by fiat currencies in the changes made in virtual environments in today's technology; Instantly eliminating the problems that arise due to the required speed, transparency and physical transfers with the crypto unit.

2.1.2. Many problems are encountered in real exchanges, such as physical conditions, transfer, high transaction fees, data proof, acceptability. Instant transfer transactions with crypto unit, low transaction fee, provable data, acceptability value, resolution with no physical conditions, untouchable and fully encrypted data.

2.1.3. One of the biggest problems in online payments is that virtual cards are used in terms of security rather than physical card transactions in virtual payment systems and virtual cards are made via API. Since it is done through the API, an error may occur

every second due to the connection in the communication network and the operation fails. It is the necessity of physical information necessary for the continuation of the transaction. Our aim with the crypto unit is to eliminate these problems and to make instant payments without the need for any API connection and error-free. With the designed PAY system, it is possible to transact as crypto currency or nominal money.

2.1.4. In payment transactions, especially in credit transactions accepted as Credit Card (KK) and given by banks, in case of foreign transactions in foreign transactions, some differences arise and the user is faced with an obligation or in some cases a rejection response. The general opinion reflects KK as instant fiat money/Currency in international payments, but the scenario does not always work in the same way and the transaction is rejected. Although these problems seem to have been overcome, in fact, instantaneous return transactions to their own currency, which are accepted in any country in the world, are reflected as unsuccessful. With the crypto currency and PAY system we have put forward as a solution, it has aimed to eliminate this problem with instant conversion to all fiat currencies and speed in payment.

5. 2.2. REAL (PHYSICAL) PROBLEMS

Although the real sector globally has closed itself to virtual environments and payment systems as it is accustomed to doing all its transactions in the physical environment, 50% of the transactions are actually done on virtual systems. There is a tradition that the general belief is that physical procedures will be healthier. This general opinion actually causes difficulties in many areas such as loss of time in physical transactions, data inconsistency, difficulty in processing, paper costs, loss, transfer, security and insurance. With the PAY systems developed by GBD in order to reduce the difficulties and expenses experienced in all these physical transactions, all these problems are overcome with just one transaction, data security and transfer operations are completed in a short time, both in value and in transaction speed. Data security and speed are important in crypto unit or fiat money transactions. With the project put forward in GBD pay systems, the ability to process data in seconds in data transfer, as well as the encryption of security with high cryptography ensures reliability in the transaction.

5. 2.3. PAYMENT SYSTEM THEORY

The PAY system is designed to function entirely with its own arithmetic algorithm. The necessity of the system emerges as a result of the globalization turning into the virtual payment system and the orientation towards developing technology. The most important feature is that it will provide convenience in many areas such as transfer load, data security, insurance, fund access, speed, transaction fees. In a high data transfer (can be specified as Amount), all freight and transfer will be between two main arteries only.

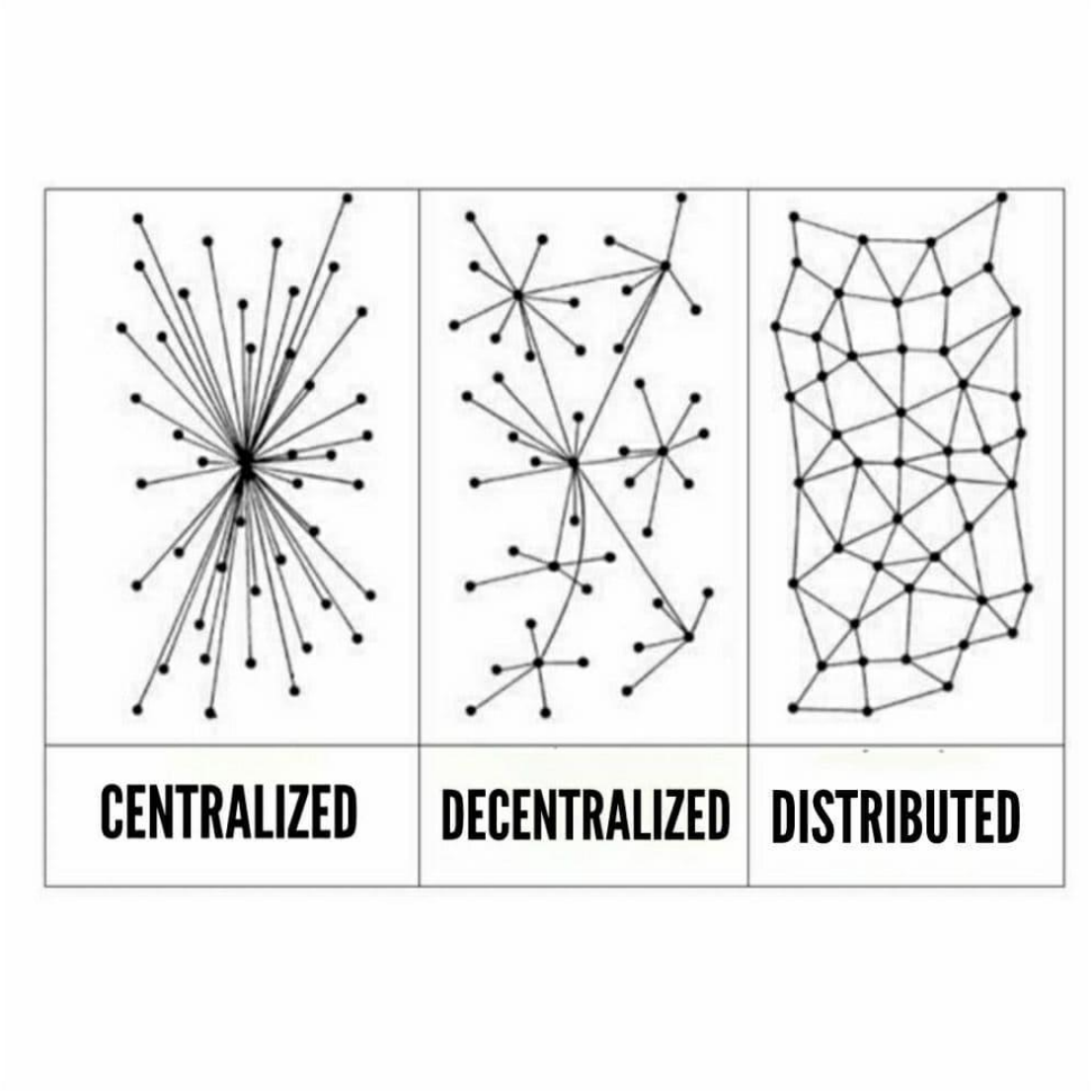


Figure 5.2.3.1. Crypto Unit Transfer systematics

As seen in the figure, crypto distribution systematics can be considered as two main arteries in general. In payment systems, these two main arteries will be formed by collecting the data collected over the distributed system on the two main arteries and

reflecting them at an equivalent rate. Sample data, Filiz; When she send one million Turkish Liras to Feride as fiat money, the crypto currency is automatically calculated over the distributed system and transferred to Feride with the encrypted key. Cryptocurrency/fiat money is transferred to Feride. What is the path followed when converting cryptocurrencies into fiat money? In general, any exchange process described is based on and data exchange takes place. However, the PAY system performs this exchange process by considering a slightly different data. By providing data on five main elements, artificial intelligence compares all value equivalents in milliseconds, determines the average value, determines the nominal money per unit, completes the conversion at the same time and makes it ready for the transfer process. No matter how high the amount of nominal money Filiz will transfer to Feride in return for the transaction, the system performs the transaction by dividing a certain number of bytes (bytes) in one go, and the transfer is deemed to have taken place as soon as the first byte transaction is made.

5. 2.4. PAY SYSTEM TRUST PROTOCOL

In the PAY system, the priority scenario is about how secure the transactions are. Since all transactions made on the blockchain are data encryption, it is impossible for third parties to decrypt them. Data transfers generally use SHA256 encryption technique. It is very reliable in data transfer.

Figure 5.2.4.1. Scheme of Security Protocol

In blockchain technology, each participant keeps a copy of all records from the start. Since changing these records will cause the summaries to change, the majority realize this when records are changed. Therefore, the need for a central database in a reliable environment is eliminated. With a distributed database system that can verify, it can be proven that correct information is kept without trusting anyone.

6. GBD ROADMAP


START
GBD preliminary works
Q3.2020
Determining project name,creating contract
Q1.2021
Project official announcement.
Q1.2021
First stock market listing
Q3.2021
Switching to BTR20 network
Q4.2021
Switching BSC network
Q2.2022
GBD network operations and testnet startup.
Q4.2022
GBD own network operations
Q1.2023
Project details and determinations of roadmap
Q3.2020
Generation the GBD Token.
Q1.2021
Private sales and pre-sale transactions
Q2.2021
Top 20 stock market listing
Q3.2021
Switching to ERC20 network
Q1.2022
PAY system studies
Q3.2022
Starting to set up the payment instrument app/wallet
Q2.2023

Connect to GBD Social Media