Proof of Rounds

White Paper

TABLE OF CONTENTS

POR NETWORK OVERVIEW

Understanding PoR network

Distributed Ledger Technology was first described in the last decade of the twentieth century. Though, the first use case of Distributed Ledger Technologies (DLT) occurred only in the new century. The first project, which gained the attention of the wide public was Bitcoin, a peer-to-peer payment system. It was presented by Satoshi Nakamoto in 2008. Since then, DLTs has made several steps ahead. This paper assesses one of the approaches to the creation of Distributed Ledger Technologies called Proof-of-Round.

Proof-of-Round represents the newly developed consensus algorithm and network structure which combines the high speed of transactions with security and distribution of responsibility. Proof-of-Round (referred below as PoR) utilizes a hybrid approach to network architecture — it applies the best practices of partial centralization which gives a drastic increase in transaction approval speed.

Another unique feature of the Proof-of-Round network is its Round structure. Apart from the unique structure of the network, PoR uses the hierarchy of Nodes which allows to diversify the tasks of every participant and distribute the responsibility — crucial for hybrid networks. The structure of Proof-of-Round is assessed on a Fig. 1.1

Fig 1.1

The hierarchy of Proof-of-Round network has different levels. There is a number of Nodes which participate in transaction initiation and approval. They are Normal Nodes (every account in the network), Super Nodes (medium for decreasing the workload), and Master Nodes, which share the Root Node permissions one-by-one. Apart from this, there are Signal Nodes, which are responsible for producing timestamps and synchronization of the whole network.

Consensus

Proof-of-Round network synchronization occurs by taking advantage of the Directed Acyclic Graph (DAG). DAG is applied as a register for storing and writing down the information about every transaction which occurs in the network. The only contributor to DAG is a Root Node, which is shared by all Master Nodes.

In Proof-of-Round network, every Node is verifying the transactions in order. In turn, a transaction could be initiated by Normal Nodes. After initiation, the transaction is distributed to the number of Normal Nodes and Super Nodes. The Super Node does the same thing distributing the verified transaction to a number of other Super Nodes and Master Nodes. Finally, Master Node verifies the transaction and submits it to the Root Node, where it is finally verified and written to the DAG of the network.

MASTERNODES AND GOVERNANCE

General Structure

The stability of a network, its components, and the timely transfer of value inside the network is a priority to any Distributed Ledger Technology (DLT). Stability and usability of the network, along with its function to adapt to a constantly changing environment is strictly regulated by certain mechanisms of governance. These mechanisms are based on the distributed responsibility of network participants approving the decisions of the network and achieving a consensus.

Proof-of-Round suggests a hybrid approach to governance and network administration. Nodes are the main agents that ensure consensus and synchronisation is achieved across the network.There are 5 different types of nodes in Proof-of-Round - all of them have different roles within the network and can only operate properly as part of the network, following the Round Structure of Network. Decentralization is achieved in a number of ways, for instance, randomization of Root Node role delegation order, randomization of Signals (timestamps) distribution, and repeated double check of transactions validity by different types of nodes.

The hierarchy of Round Structure consists of 5 types of nodes and 3 levels. The first level consists of Normal Nodes, which are responsible for transaction initialization, and Signal Nodes, which provide timestamps and ensure the synchronization of the whole network. The second level consists of Super Nodes, which verify transaction consistency, ensure the similarity of distributed transactions to each network participant and discard any unnecessary (repeated and malicious) transactions. The network structure is assessed in Fig. 1.1:

Fig 1.1

This network structure, as shown above, allows us to distribute and verify information across the network within the fastest time possible. It is achieved by allowing a partial trade-off of decentralization while getting faster transaction verification speed and drastic decrease in consumed computational power and electricity. The roles of nodes in Proof-of-Round Network is assessed in Fig 2.1:

Fig 2.1

The information regarding all transactions and balance changes in a PoR network is only considered approved after the verification of the Root Node. At the same time, all the other types of operations in the network, which can be described as “governance” operations are added to the so-called Round Header. The type of information added to the Round Header includes:

- removing or adding of Nodes of any level
- participating Master Nodes
- Root Node role delegation order

All this information is added to the Round Header which is the only type of information in a PoR network, it is stored in blocks. It reflects the most crucial changes and helps increase the flexibility of the network. It also ensures the fastest possible delivery of the most crucial information to the whole network. It does this by appending to it only in the case that tangible changes to the network are committed. A round Header doesn't contain empty blocks, which would in fact be the vast majority, but rather it writes the actual timestamp into every block to ensure the precise network update time.

Normal Nodes

Normal Nodes represent the Lower Level of a PoR network structure whilst, Proof-of-Round give Normal Node permissions to every network participant. In other words a Normal Node represents ordinary accounts in a PoR network whose main function is to initialise transactions over the network. Normal Nodes also receive the initialized transactions by other nodes at the same level, verifying and submitting to all network participants of lower and middle level.

Any Normal Node can have a different amount of connections on a PoR network although, the recommended amount of connections is 9: 4 with the Lower level Normal Nodes, and 5 with Middle Level Super Nodes. This division is perfect in terms of the speed needed to spread the information regarding the transaction across the whole network. It is also optimal to ensure the adequate amount of computational power is used in order to validate and discard repeated transactions, which will occur on a Middle and Higher Level of Maternodes. The transaction verification process is assessed in Fig 2.2:

Fig 2.2

Similarly for the amount of connection for every node, PoR leaves the requirements of qualifying for a normal node open. Each project is unique and it will be up to individuals to decide on their own exact requirements, there are however, certain recommendations that will help reduce possible emergencies happening on the network and increase stability.

-The KYC procedure: Taking into account the fact that PoR is a hybrid network, some network participants might want to take advantage of their status. KYC will help to decrease the amount of malicious actions.

Super Nodes

Super Nodes represent the Middle Level of the PoR network. Their main function is to be a transaction distribution hub between Master and Root Nodes and Normal Nodes. They are designed to decrease the load on Masternodes by discarding the repeated transaction which are submitted to them by Normal Nodes. Also, Super Nodes verify unique transactions and send them to a Higher level of the PoR network.

As previously stated any node in a PoR can have various amounts of connections to each other although the recommended amount is still 14 for every Super Node of Middle Level: 5 with Normal Nodes, 4 with Super Nodes, 5 with Master or Root Nodes.

With the proposed amount of connections, the role of every Super Node is to accept and verify the transaction from the Normal Node that initiated it. . After verifying the transaction the Super Node distributes it to the Master Nodes and Root Node if a connection

is made at that exact moment. After this process the Super Node receives repeated transactions and discards them as necessary, decreasing the workload on the Master and Root Nodes. The workflow of this process is as follows:

Fig 2.3

Similarly to Normal Nodes, it's up to each project that utilises a PoR network to decide on the unique requirements needed to become a Super Node. Though, utilising a KYC procedure such as those described above are recommended, additionally it is necessary to provide an economic Incentive. Every Node has to freeze a certain amount of digital assets. In the case of malicious activities by a network participant, the frozen stake will be taken as a measure of preventive control. Aside from this a flawless operation track of Normal Node for a certain amount of time is a recommended requirement to qualify for a Super Node

Master Nodes

Master Nodes represent the Higher Level of a PoR network. They are the crucial elements of a network. They accept the verified transactions of Super Nodes and then sign and distribute them to each other to confirm the uniqueness and consistency of submitted transactions. Every second, Master Nodes share the function of the Root Node, one by one.

Similarly to other levels of architecture, PoR doesn't provide a strict limit on the amount of connections established by every Master Node although the suggested amount of connections is (N-1), where N is amount of Master Nodes. The suggested model of network with 5 Master Nodes is as follows:

Fig 2.4

Master Nodes are essential participants of a PoR network. By sharing the role of the root Node with the flow of time, Masternodes together represent the core center of the network. That is why the safety of the network is a priority, accounting to the hybrid structure of it. To ensure the flawless operation of the whole Proof-of-Round network, Master Nodes have to follow strict rules consisting of at least these points:

- Precise KYC procedure with video interviews should be applied to every participant of a Higher Level of PoR.
- Economic incentive in the form of freezing a concerning stake is also recommended.
- Checking the track record of the applicant on the roles of Normal Node and Super Node for at least 2 months.

These are the minimum suggested requirements needed to decrease the risk of malicious activity in a PoR network although they shouldn't be limited to only those above. Each project is encouraged to apply additional rules that are tailored according to the unique features of the project and product.

Root Node

A Root Node is the center of the PoR network; It's function is to act as a final verifier for all transactions. The issue of a possible concentration of power is avoided by applying a randomized mechanism of switching the Root Node role among all Master Nodes every second. After the final verification of the transaction, the Root Node responds to all Master Nodes, notifying the new status of each transaction. Final verification can only occur when every Master Node has submitted the information about certain transactions to the Root Node and all the entries that have been submitted are similar.

As it has been mentioned, the proposed structure of a network is 5 Master Nodes with each being eligible to become a Root Node, although PoR isn't limited to this amount, similarly to all other levels of network. With this proposed structure, every Master Node will become a Root Node once every five seconds, according to the timestamps from the Signal Nodes. The structure of the Higher Level which consists of 5 Master Nodes is depicted in Fig 2.5:

Fig 2.5

A Master Node, which is currently possessing the role of Root Node, is responsible for the final approval of all transactions in a PoR network. On the basis of timestamps, the Master Nodes replace each other in position. The process of deciding which of the Master Nodes will approve the transaction depends on the hash time or in other words, timestamp of creating the transaction. The Master Node that possessed the Root node role at that moment is the one to provide the final approval of the transaction. The process of Root node role changing and transaction approval is assessed in Fig 2.6:

Fig 2.6

This diagram shows how the Root Node role is obtained by every Master Node. The priority of becoming a Root Node is determined every second as a timestamp occurs. If the amount of Master Nodes doesn't change, the order of becoming a Root Node is one-by-one. The priority in the network is given to Master Nodes based on 2 factors with decreasing significance:

- Total time of operation in the network
- Approved amount of transactions.

However, when changes to the amount of active Master Nodes happen, for instance, a new one becomes active, it is then placed in the order with the same rules - based on the total amount of operation and amount of approved transactions.

Signal Nodes

Signal Nodes are unique in the structure of PoR. They settle into the lower level and along with Normal Nodes form the basis of the network. These types of Nodes are the only ones which do not participate directly in transaction approval, instead they just refer the obtained information from other nodes to other network participants.

The main and perhaps only function of Signal Nodes is to provide Signals i.e. timestamps for network synchronization. They have a broad enough pool of functions:

- Changing to Root Node role.
- Synchronization of the network.
- Deciding on the Master Node which will finalize the verification process of each transaction.

All these functions are assessed in more detail in Fig 2.6.

These functions also have a crucial value to the whole PoR network and is a reason why Signal Nodes will always be the subject of malicious attacks.The generation of false timestamps or the elimination of this process could lead to extremely diverse results and status of PoR network. That is why all the Signal Nodes are interconnected and initiate the timestamp, which is firstly delivered by Signal Node initiator to other Signal Nodes. After the

internal timestamp verification, the Signal is distributed to all other network participants. The interconnectedness of Signal Nodes is what decreases their risk of being attacked by hackers.

Another way to increase the security and safety of Signal Nodes is to disguise them as Normal Nodes since, Signal Nodes also participate in the transaction verification process (though not really checking the consistency of transaction). At the same time, when a Signal Node releases timestamp information, it distributes this information to the connected Normal Nodes and Super Nodes. When a Normal Node is redistributing timestamp information, the Nodes of different levels, connected to it, will only see the signed timestamp information, but not the exact Node that submitted it.

Similarly to all other types of Nodes, a PoR network doesn't limit or restrict the requirements of becoming a Signal Node. As is the case with other Nodes, there are certain recommendations like stake freezing and KYC procedure, which are the necessary safety measures for hybrid networks.

Network development and changes

The functions of the four types of Node frames and their operational activity in Proof-of-Round Network. The provided information states how the system operates, while regulation of network and changes in it needs assessment.

The most relevant information in the network is stored in the Round Header which, carries essential information about the network, specifically:

- Removing or adding of Nodes of any level
- Participating Master Nodes
- Root Node role delegation order and priority of Master Nodes

The Round Header always carries the current participation status. The past data of the Header is a deciding factor in the Root Node role delegation priority.

When any of the Master Nodes submit a change to the network, for instance, new Master Node initialization or kick of the existing Master Node for low participation, the Round Header reflects the process of voting for initialized changes to the network.

Voting for initializing a new Master Node could happen, should any Super Node fit the requirements necessary to become one. Similarly to initialization, kicking the Master Node can occur because of low participation in transaction confirmation. However, the rules are not limited to these factors and PoR leaves room for each new project to add its own requirements to the list, allowing it to be tailored specifically for each project.

POR CONSENSUS

DAG in PoR

DAG refers to a directed graph with no closed chains based on graph theory. The DAG data structure has already been implemented in several projects to date as demonstrated by IOTA and Byteball, which have proven its stability and benefits over the previous blockchain technology. The DAG system approves each transaction without creating blocks at all. This allows for major improvements in scalability by eliminating the need to create blocks. Omitting blocks eliminate s the block size restrictions and, in doing so, makes waiting for blocks to be created unnecessary.

Within existing DAG technology, transactions are approved by a system in which the past transactions are checked and approved by the creator. In this system, the repeated creation and approval by an unspecified number of nodes causes the chain to expand, guaranteeing the consistency of past transactions. The DAG system has made it possible to solve problems such as small block sizes inherent to blockchain technology; however, it does not directly solve every problem. The problem of transaction approval time being dependent on the volume of transactions on the network, and the transaction finality problem, caused by the occurrence of forks still remain.

Stable network status and timestamps

In Proof-of-Round networks the synchronization happens every second. This means that every transaction hash is tied to the Signals of Signal Nodes. Through the cooperation of Signal Nodes and Transaction Nodes (Normal, Super, Master, and Root) the networks achieves synchronization of the system and ensure that all the participants have the same status of network.

The lifecycle of the network is looped every second. It starts from the stable status when all the transactions are finally verified. Occurring every second, the Signal Nodes distribute a timestamp to the network. At the same time, Root node role is passed to the next Master Node in the order and all the transactions submitted to Root Node during this second are finally verified and added into the DAG. After completing all these processes, a network achieves the stable status - that is where the new lifecycle starts. The lifecycle of network is assessed on Fig 3.1:

Fig 3.1

DAGs in PoR networks are utilized in Root Node as a measure of secure storing and recording of all the approved transactions. Timestamps helps to organize the DAG and make it more readable for every network participant. It drastically decreases the response time of DAG to any network participant, adding the two-step navigation with the basis in timestamp and hash of transaction.

Transaction Lifecycle

A transaction in a Proof-of-Round network can be initiated by every Normal Node in the system. The process starts from creating the transaction and hashing the data which it contains using the SHA512 algorithm. When the hashing process is over, a Normal Node signs the transaction with both a public and a Private key. At this state, a transaction is ready for distribution to the Proof-of-Network network.

The Normal Node distributes the transaction to a predetermined number of same level nodes and a similar amount of Super Nodes. Out of X similar distribution channels of transaction, only X/2-1 channels reached the Middle Layer, represented by Super Nodes. Fig 2.3 from “Masternodes and Governance” section shows how the transaction distribution occurs between Lower and Middle Levels of Network.

When the first Super Node receives the transaction, it verifies its uniqueness and signs it with the Public key, owned by the Super Node. After committing these actions, the Super Node distributes the transaction to other Middle Level participants, according to the required amount of same level connections.Furthermore, the transaction is distributed to the Higher Level, where Master Nodes and Root Node receive it. Fig. 2.4 from “Masternodes and Governance” section shows the process of verifying the transaction by Super Nodes.

In case the transaction already exists in the record of Super Node, it neither signs nor verifies it. It discards the transaction as a repeated one, because there is a record of it in the previous activity of the Super Node, which means that at least some of the Master Nodes have obtained this transaction’s information and handled it properly: signed and distributed it to the Root Node. Fig 3.2 shows how the discarding process of Super Nodes work.

Fig 3.2

Similarly to Super Nodes, when a Master Node receives a transaction, it checks the uniqueness of it. In case the transaction is already present in the track record of this exact Master Node - the transaction is discarded, which happens with the same workflow as Super Nodes discarding. In the opposite case, if the transaction is unique, a Master Node signs the transaction with the public key, writes down its information, and redistributes it to all other Master Nodes and Root Nodes.

Lastly, the transaction gets to the Root Node. At this point where the transaction finalized obtains approval of consistency and achieves verification. The Root Node also includes the hash name and other information about the transaction in the DAG to reflect the balance changes or any other contributions to the network and Normal Node statuses.

If the transaction was already submitted to the Root Node and was verified by it, all the other repeated transactions are discarded. The discarding algorithm is similar to that of the Super Nodes and Master Nodes.

Centralization and consensus

The previous sections described the theoretical aspects of Proof-of-Round consensus along with the Nodes hierarchy and round structure of network. As it was stated before, there are many independent variables which the network does not specify strictly. It is an intentional feature to leave these variables flexible - so every project could implement the structure and decentralization level which is required for their exact case.

The first set of variables which is left flexible is the amount of network participants, especially of Middle and Higher Levels. The amount of Super and Master Nodes has a direct correlation to the decentralization of network - the more independent nodes are present in the network, the higher is the level of decentralization. However, the variable amount of nodes does not meant that the rule of communication and transaction verification between them could be changed in any way. Projects utilizing PoR only have an option to decide the amount of network participant for each level.

Another set of variables,left blank in Proof-of-Round is the amount of connections for each node. In previous sections of this paper and on all prior figures, the amount of connections was 5 for different level connections and 4 for same levels. Generally, the only rule for establishing the amount of connections is quite simple - the amount of inter-level connections should be equal to X, while intra-level connections should be equal to X-1 (1 Node is the initiator of connections). In some cases, it is acceptable for Super Nodes to have an unlimited amount of connections with Normal Nodes. This exclusion is made because Normal Nodes in Proof-of-Round network are used as user accounts and the amount of them is limited only with amount of network participants. Though, PoR methodology still suggests keeping the amount of connections regulated in X inter-level connections and X-1 intra-level ones.

PoR vs PoS/PoW

Feature	PoR	PoS/PoA etc	PoW
Consensus confirmation time	In theory 0.2 seconds. Realistically 0.2-0.8 seconds. Fluctuation occurs depending on the master node settings and the number of transactions occurring at any given time.	Configurable depending on a network	Configurable depending on a network
Consensus confirmation time example	Best time recorded was 0.064 seconds.	PoS- (Dash 2.5 minutes)	Bitcoin - 10 minutes Ethereum - 15 seconds Litecoin - 2.5 minutes, Dogecoin - 60 seconds
Number of consensus nodes	Flexible. System is dynamic and can adapt to the business goals of any project at exact time	Configurable, yet fixed amount in each network	N/A
# of tolerated malicious nodes	50% Hybrid nature of network allows the business organization to possess certain amount of Nodes	50%	N/A
Resource Consumption	Moderate	Moderate	High
Manageability	Because we are a hybrid P2P network, the network is extremely	PoS is transparent and users vote to implement changes	Changes to protocol can be changed very rarely

	easy to change and it can be done in a short space of time	on the system.	

TPS in PoR

Proof-of-Round platform contains a hybrid nature: a solid trade-off of decentralization. However, on the other hand, the network benefits by the huge Transaction-per-Second capacity of it as a benefit of the mentioned trade-off. The network architecture and testnets are developed and the current status on scalability of network and TPS parameter cannot be provided precisely.

At the same time, in the test environment of Proof-of-Round network with 3 Master Nodes and X parameter of connections equal to 3, the network performed quite impressively. With the industrial hardware used as a platform for every Node in the test network, the maximum achieved TPS was equal to 300,000.

The Proof-of-Round engineering team expect this number to grow together with increasing the amount of participants in the network of Higher and Middle Level.

CRYPTOGRAPHY

Despite the fact that Proof-of-Round uses a hybrid approach to network structure, it is still focused on decentralization, cryptography and irreversity of the network statuses, all of which constitute the main points of decentralized networks. PoR achieves partial decentralization by applying encryption algorithms as a basis of network functioning.

Hash Functions

A hash function is a function that creates a bitstream of a fixed length and no fixed form out of a bitstream of arbitrary length.

PoR uses a function called SHA-512, which creates a hash value of 512-bit length. This secure hash algorithm is considered the safest cryptographically among the “SHA-2” hash function standards established by the National Institute of Standards and Technology.

SHA512 has a number of different characteristics which are crucial for the distributed ledger technologies functioning.

Irreversibility is the inability to return a converted hash value to its original form using a function. SHA-512 makes it impossible to revert, read, or manipulate transaction content that has been converted to a hash value.

A collision of hash values occurs when two hash values are identical. It is possible to switch the legitimate text with illegitimate text through a preimage attack to avoid a likely hash value collision. PoR converts extremely important and large-volume transactions to hash values using SHA-512, which has a high collision resistance, so that calculated hash values can not be manipulated.

Digital Signatures

Digital Signature is a technology that verifies that there is no error in the destination of data received and that data has not been manipulated during the transmission route. This technology is guaranteed by a pair of encryption keys - Public and Private. Proof-of-Round uses these digital signatures to ensure its transaction consistency.

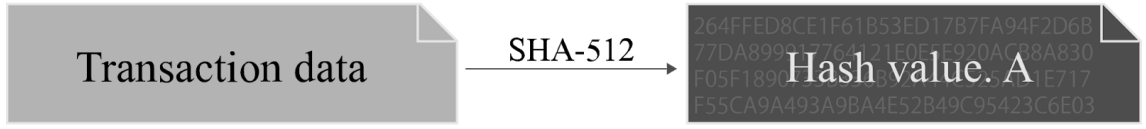
A Public Key is used to sign transactions and encrypt its data. Transactions signed with a Public Key can only be reversed with a Private Key.

A Private Key is used to initialize the transaction by signing it. Only Private Keys grant access to balance changes and decrypt the data signed by Public Keys. Further, a Private Key is the main method to get access to any account in the network rather than using the WEB 2.0 methods, like email and password.
As a general rule, each node has a pair containing one encryption key and one public key, and each node stores its encryption key so that only that node can locate it.

The process by which transaction consistency is verified is described as follows:

Step 1: Conversion using a hash function

First, the NN converts the transaction data to a hash value using the SHA-512 hash function.

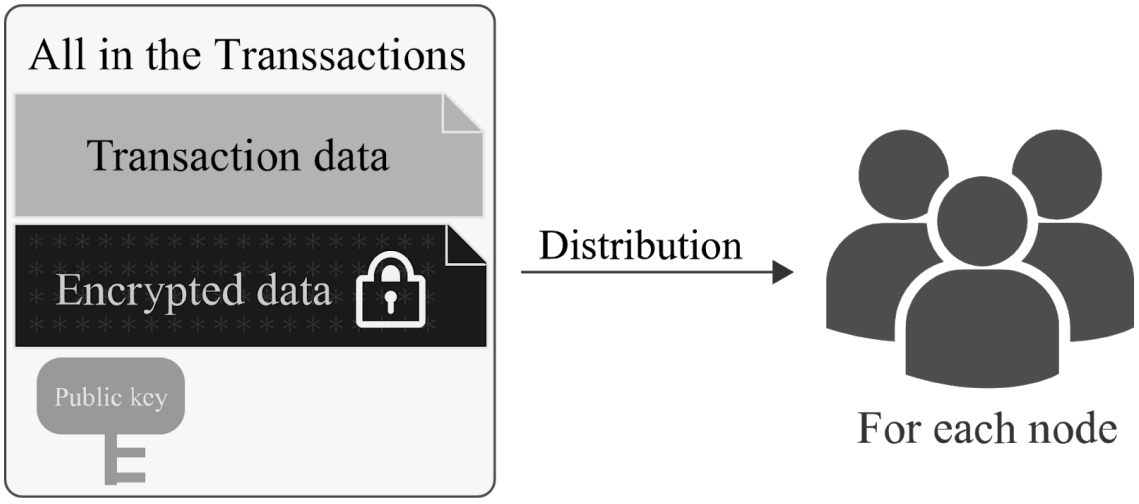


Step 2: Encryption

The NN then encrypts the calculated transaction hash value with its own private key.

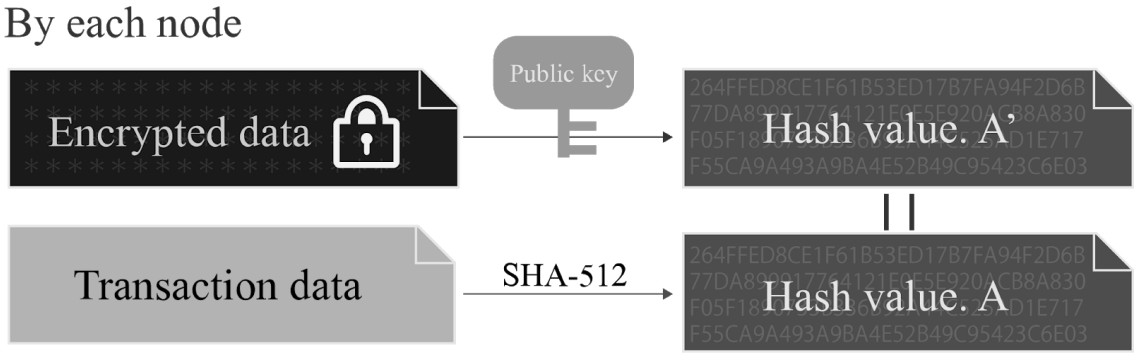
Step 3: Transaction distribution

The encrypted data and Public Key are packaged with the transaction data that has been converted to a hash value, then made into a transaction and distributed to each node.



Step 4: Consistency check by digital signature

The node that receives the transaction calculates the hash value of the transaction data using a hash function. The node then reverts the concurrently attached encrypted data to readable data using the enclosed Public Key whereby the value is then checked.



Data encrypted with an encryption key can only be reverted with a Public Key. For this reason, the hash value of the reverted transaction data will match the hash value of the enclosed transaction data as long as there has been no

malicious rewriting. If these hash values do not match, it is determined that the transaction has been rewritten, causing the Super Node or Master Node to destroy the transaction. By verifying transactions with a digital signature guarantees consistency in the creation, distribution, and approval of transactions.

Elliptic Curve Cryptography

To create Public Keys from Private Keys, Proof of Rounds use an elliptic curve cryptography technology called “Secp256k1”. Secp256k1 is the encryption key technology used by Bitcoin which has operated without any system hacks since 2009 proving its effectiveness.

The Secp256k1 algorithm process for the creation of a Public Key is described as follows:

The formula for an elliptic curve in elliptic curve cryptography is as follows.

$$c^2 = x^3 + ax + b \ mod \ p$$

Step 1: Find a, b, and p in the above formula, then find the point of reference G(x,y).
Secp256k1 uses the following parameters:

a=
0x0000000000000000000000000000000000000000000000000000000000000000

b=
0x0000000000000000000000000000000000000000000000000000000000000007

p = 0xfffffffffffffffffffffffffffffffffffffffffffffffffffffffefffffc2f

Gx =
0x79be667ef9dcbbac55a06295ce870b07029bfcdb2dce28d959f2815b16f81798

Gy =
0x483ada7726a3c4655da4fbfc0e1108a8fd17b448a68554199c47d08ffb10d4b8

Step 2: Add the node’s G(x,y) to this G(x,y) and repeat that addition function n times (n=value of the node’s private key). This will give you the value nG.

After this the obtained value will be used as the Public Key.

It is easy to find nG from G by repeating the modulo operation n times, but when n is an extremely large value, it is considered extremely difficult to find n from G and nG using the modulo operation. This creates unilateralism in the key creation just as with a hash function, making it impossible to decipher the encryption. This extremely robust encryption key system guarantees the security of the private keys.

SECURITY

The Role of Signal Nodes in security

The hybrid nature of networks are often subject to criticism and although in the case of a Proof-of-Round network, the trade-off between decentralization and anonymity takes place to ensure improved security and transaction speed.

One of the mechanisms used to avoid centralization is the decentralization of Signal Nodes. Signal nodes are unique in their ability to create timestamps, which are crucial for a network and create the framework for it to synchronize every second. Notably, Signal Nodes are evenly spread across the network, while maintaining a link to deliver and agree upon timestamps.This measure together with proper requirements of becoming a Signal Node helps to ensure the security of the timestamping process, stability and security of the network.

It must be noted however, that to ensure the maximum level of security for Signal Nodes, the architecture of the Lower Level of the network is designed in a special way. Each Signal Node only participates partially in the verification process and does not actually check the consistency or uniqueness of the transaction. In other words, transactions are sent without being checked by Signal Node. This is done in order to disguise Signal Nodes as Normal Nodes. Each Signal Node is created in a way that makes it appear almost identical to a Normal Node. It is particularly important to the transaction approval process that the nodes have similar features as this means that the average user obtaining the signals will verify both. When Signal and Normal nodes are disguised to look alike, it helps spread the risk of any potential attacks by fray or black hackers.

A Signal Node can still be tracked on a time frame of hundreds of thousands of timestamps. To ensure that it is impossible to interrupt the timestamp creation, each Signal Node is required to change the Public and Private keys within a certain timeframe. This makes tracking the Signal Nodes impossible due to the Public and Private keys constantly changing. The combination of Signal nodes being able to disguise themselves as Normal nodes and their ability to constantly change their Public and Private key pairs ensures the highest level of security possible.

Measures against malicious activity in PoR

It is important to note that Signal Nodes are not the only target for potential attacks, the Nodes which validate transactions are also vulnerable. This is why a Proof-of-Round network utilizes repeated confirmation of any transaction by the nodes. This is the reason why the role of every Super and Master Node is to check the unique identity of each transaction.

In the case that any Node sees two different sets of data in the hash for any transaction, it then checks the amount of submissions in each branch. The transaction with

the highest amount of confirmed distributions to any node is then double checked for it's consistency before being submitted to the network as the real one. Fig 5.1 shows the workflow for handling malicious transactions by PoR network participants.

Fig 5.1

Technical incentives against potential attacks

A preventative approach is used when trying to protect Proof-of-Network from potential attacks. Each node possesses Public and Private keys which are the only two things necessary to operate in the network. The removal of traditional methods of identification like a login/password and IP helps to conceal the node's location and makes it more difficult to detect the internet connection and IP address of the Node. Notably, an IP address is the key feature in almost all the attack vectors on Nodes.

It is however, still possible to detect a masternode through phishing social engineering or extensive research into every confirmed transaction in a Proof-of-Round network. This is the reason that every node is required to use a dynamic IP for functioning since this type of internet connection is created in such a way as to avoid any potential cyber threats. Together with the web 3.0 login which has no passwords or access to a centralized database, being a basis preventive cybersecurity for Proof-of-round network.

Economic incentives to safeguard the network against possible cyber attacks

Finally, the last aspect of malicious activity in a Proof-of-Round network is the economic incentive to prevent such attacks. The requirements of running any Node, participating in transaction approval is assessed in "Nodes and Governance" section. It is strongly recommended to have proper KYC for every participant of the network. This is done due to the hybrid nature of the network which gives more space to any account in it, including space in the shady field.

Apart from KYC requirements, almost every Node of Middle and Higher level is required to proceed with stake freezing the exact amount of the asset. In the case of any malicious activity in the network, the reserve serves as an additional warranty that every network participant is performing towards collateral success vector of network participants. This is achieved by simply increasing the price of the agent's dilemma. Obviously, in the case of any confirmed malicious activity by any participant, the stake is excluded from the balance and either burnt or redistributed by the projects team.

CONCLUSIONS

Benefits of PoR

Concluding, it is necessary to enumerate the Proof-of-Round benefits and functioning specifics.First of all, the hybrid nature allows improving the transaction speed and safety of the network from a partially centralized approach. Obviously, there is a solid trade-off of the ideas of total decentralization. Secondly, the hybrid network still allows any user to have total control of the assets stored in PoR network and handle them in any way.

Decentralization achievement

The partial decentralization is achieved through the distribution of responsibility to generate timestamps which are executed by Signal Nodes. This process involves the achievement upon certain conditions of delivering the Signals to network participants. Additionally, the Root node permission is also shared by Master Nodes which decreases the possibility of malicious transactions being approved and put into the DAG.

Every transaction goes through a number of Normal, Super, and Master Nodes before it gets final approval from the Root Node. Every participant is approving the consistency and uniqueness independently. If on any level a transaction's consistency or nature is doubted — the network takes actions to find out the malicious participant of the network and takes proper actions.

Encryption

Encryption in Proof-of-Network is executed on the basis of the SHA512 hashing function, which is one of the most resistant to collisions. Although, Public Keys of every Node is used to sign and verify the transaction which it processes to achieve the better distribution of responsibility.

Finally, the encryption of Public Keys and the process of creating them is Secp256k1. It was proved to be the best-secured method, which is utilized in the Bitcoin network since 2009 with no hacks and breaches.

Security

Security in Proof-of-Round is achieved through different incentives. The first one is technical limitations and requirements of the network. Every node is connected to the network via WEB 3.0 interface — removing the need to store logins and passwords in a centralized database and using Public and Private Key pairs for PoR network connection. Additionally, every Node is required to use a dynamic IP address instead of a static one. It decreases the chances of being tracked by third parties and the possibility of an attack on Node.

Apart from this, there is an economic incentive of diminishing the malicious activity of network participants. Every Node applicant is required to go through a KYC procedure and

freeze a certain amount of stake in digital assets. This increases the costs of possible malicious activity for any network participant with a simple financial incentive.

In general, Proof-of-Round strives to achieve the highest performing ratio in terms of transaction per second while not sacrificing a certain part of decentralization. Though, Proof-of-Round implements strict regulations of safety and security of the network.

APPENDICES

Images:

https://docs.google.com/presentation/d/1udljAvcN5BXAyD0b70Ho1DBf5ek0-11Xsox50Q0lCk0/edit#slide=id.g47d814f898_0_48