CRISPMIND™
INTELLECTUAL PROPERTY MANAGEMENT

123 N. Wacker dr. Suite 250 Chicago, IL 60606
phone: +1-415-670-9800 contact@crispmind.io
https://www.crispmind.io

TECTUM BLOCKCHAIN

As a Third Generation Blockchain – a Smart-Node Grid Network

White Paper

Author:
Alexander Gusev
Date: 2021.03.18

123 N. Wacker dr. Suite 250 Chicago, IL 60606
phone: +1-415-670-9800 contact@crispmind.io
https://www.crispmind.io

INTRODUCTION

While developing centralized applications where software is offered as a service to an end-user, the information can be hosted on cloud computing platforms, stored in the cloud, and used in web services for text messages, phone calls, payment processing and many other applications.

In the world of decentralized applications, it is possible to create a new type of software based on the BLOCKCHAIN NETWORK OF SMART-NODES, or the SMART-NODE GRID NETWORK (SNG), which will provide the calculation, storage, transfer and indexing of network blocks for each client individually. The advantage of the SNG approach is that users personally control their identity and data, and also have the choice to become both consumers and service providers in this system. On top of that, each level has a built-in motivation mechanism to maximize the network effect and trigger the community's self-development framework.

THIRD GENERATION BLOCKCHAIN NETWORK

TECTUM, is a SMART-NODE GRID NETWORK (SNG NETWORK) based on the architecture that uses DISCRETE DYNAMIC TOPOLOGY (DDT) and CELLULAR AUTOMATA (CA) technologies proposed by von Neumann in the 1940s (https://embryo.asu.edu/pages/john-von-neumanns-cellular-automata). DDT BLOCKCHAIN NETWORK is a network of nodes grouped into clusters (BRANCHES), which operate as an organized grid comprised of interconnected SMART-NODES with virtual channels utilizing DISCRETE DYNAMIC TOPOLOGY. This new generation of the highly scalable, self-developing and self-regulating network infrastructure of Blockchain Network is the Blockchain of 3rd generation and is embodied in the TECTUM platform.

TECTUM is a new generation Peer-to-Peer Infrastructure based on the SMART-NODE GRID principle, which aims to revolutionize the Internet through true decentralization and its motivation mechanism for the operation of NODES.

TECTUM BLOCKCHAIN is based on SMART-NODE GRID or BLOCKCHAIN NETWORK OF SMART-NODES and is designed to mark the network connection and the possibility of data transmission as a useful Proof-of-Utility. A BLOCKCHAIN NETWORK OF SMART-NODES solves the problem of the "efficiency" of the Blockchain networks, equalizing the status of all the nodes in the network.

Each node in the SNG NETWORK follows a SMART-NODE rule and updates its state based on local rules. SMART-NODE GRID is a generic term for a type of model, a finite automaton characterized by discrete time, space and interaction. It is a discrete system that self-develops locally according to certain rules. The development of such a network has been proven to mimic the evolution of complex systems well described by von Neumann. The SMART-NODE GRID has the characteristics of decentralization, equity and parallelism. We offer a SMART-NODE GRID that will work as a universal NODE (NODE) creating and storing block chains in conjunction with the network.

Local rules govern the transition of SMART-NODES from one state to another. The state of the NODE and local rules are some of the main factors affecting network topology.

123 N. Wacker dr. Suite 250 Chicago, IL 60606
phone: +1-415-670-9800 contact@crispmind.io
https://www.crispmind.io

The concept of SMART-NODE GRID OF CELLULAR AUTOMATA is a decentralized data transmission network that consists of several independent and self-organizing SNGs that enable clients to connect, read, write and transmit data. This coordination is decentralized and does not require the trust of any centralized systems (third party) involved. The safe operation of the SNG NETWORK is achieved through an agreed mechanism that coordinates and verifies the operations performed by each node. BLOCKCHAIN NETWORK OF SMART-NODES opens an opportunity to various strategies for decentralizing server, desktop and mobile applications.

Unlike a centralized network connection and data transfer, there are several efficient connections between nodes in the SNG NETWORK that can be used to increase data throughput.

Network Tokens stimulate the sharing of network resources and ultimately minimize the loss of connections and bandwidth, and the owners of NODES are motivated to increase resources. Thus, a development mechanism arises, this property of the NETWORK is the "Self-Motivation".

All Nodes in the blockchain network are analogous to each other due to the decentralized nature of the Blockchain. The lack of trust in the systems of the blockchain network deserves special attention, since any node can send any information to any node in the network. For Blockchain to work properly, peers must evaluate the information and coordinate their actions.

All Nodes are equal, have equal rank, and each is capable of sending, receiving and transmitting data. The principle of CELLULAR AUTOMATA allows for SNG NETWORKs to enjoy simple local rules that can generate highly dynamic and highly scalable topologies that can be created within the WAN via virtual circuits and that are independent of the underlying physical and logical infrastructure. The simplicity of local rules allows for cost-effective implementation on all types of devices on the network, from Internet of Things (IoT) devices, including smartphones, routers, to high-performance server clusters.

Despite its apparent simplicity, SMART-NODE GRID-enabled routing can be very random and unpredictable, providing superior security and privacy. Nodes are rewarded for providing connectivity and transmission power, resulting in a fully competitive market optimized for increased network capacity. The SNG NETWORK will increase the utilization of connectivity and data throughput by sharing the unused bandwidth of the network nodes - more and more new nodes join the network to receive rewards, thus the network expands rapidly and maximizes utilization. Existing Nodes are interested in increasing resources and increasing data transmission capacity.

By creating the Third Generation Blockchain Network, the SNG NETWORK will bring fundamental changes to the Blockchain ecosystem. Third-generation blockchain networks are capable of supporting a new type of decentralized applications that have much more powerful data collection, storage and transmission connectivity. The purpose of the SNG NETWORK is not only to revolutionize the structure of the decentralized networks, but also to improve the basic technologies of the Blockchain Networks in general:

123 N. Wacker dr. Suite 250 Chicago, IL 60606
phone: +1-415-670-9800 contact@crispmind.io
https://www.crispmind.io

1. Blockchain Networking of Computing Infrastructure: SMART-NODE GRID NETWORK represents the concept of a decentralized data network and uses a truly decentralized blockchain to provide network connectivity and data transmission using massive independent Relay Nodes.
2. NODES in the form of SMART-NODES united in SMART-NODE GRID with dynamic topology use the idea of CELLULAR AUTOMATA for the development and self-organization of the network. The intrinsic characteristics of SNG NETWORK such as decentralization, node equality and concurrency allow us to build a truly decentralized network for storing and managing blockchains.
3. SNG NETWORK effectively achieves high resiliency Consensus in large-scale distributed systems based on what is important for decentralized systems without trusted third parties.
4. Proof-of-Utility as the useful proof of work: SNG NETWORK offers a Proof-of-Utility (PoU) mechanism that encourages participants to contribute actively to the network, improving connectivity, data handling and bandwidth for great rewards by improving network connectivity and data throughput. Proof-of-Utility is proof of work and data transfer - similar to the concept of Impulse, which is mass times speed, where mass is the amount of data and speed is the transfer rate.
5. Tokenization of the effective work of the SNG NETWORK NODES for processing, transmission, and storage: SNG NETWORK Tokenizes the work of NODES for processing, storing and transferring data, encouraging participants to increase resources (volume of storage, processing speed, transfer speed) and share their resources in exchange for Tokens. Free network resources can be better utilized through such a sharing mechanism. SNG NETWORK stimulates the build-up and sharing of the network resources.
6. SNG NETWORK becomes the infrastructure for applications specially designed for decentralized networks, application developers will have a new networked toolkit to quickly and easily create truly decentralized applications. APP developers can focus entirely on creativity, innovation, user interface / user experience, and business logic. This network toolkit fully complements the toolkit of other BLOCKCHAIN projects (based on the SNG NETWORK, various applications can be launched in parallel: identification, loyalty programs, training, payment, data storage, etc.)

SNG NETWORK uses CELLULAR AUTOMATA methodologies to achieve complete decentralization. All Nodes are equal, truly peer-to-peer, and each is capable of sending, receiving and transmitting data. CELLULAR AUTOMATA allow you to create simpler local rules that make it possible to generate a highly dynamic and easily scalable topology using virtual links installed in the WAN, which are independent of the underlying physical and logical infrastructure. The simplicity and locality of the rules allow for cost-effective implementation on all types of networked devices capable of becoming part of the Internet of Things - from smartphones to routers. Despite its apparent simplicity, CELL-enabled routing can be very random and unpredictable, providing superior security and privacy. The nodes in the SNG NETWORK are rewarded for processing, storing and transmitting data, which leads to the automation of self-regulation of the INFRASTRUCTURE. More and more new nodes will join the network to receive rewards quickly expanding the SNG NETWORK. Existing Nodes are interested in upgrading and increasing data transmission capacity. All of the above will further increase the overall bandwidth of the network, as well as improve the dynamic topology, since the network has many more degrees of freedom in route selection.

123 N. Wacker dr. Suite 250 Chicago, IL 60606
phone: +1-415-670-9800 contact@crispmind.io
https://www.crispmind.io

FEATURES OF THE BLOCKCHAIN 3.0

1. Any NODE can connect to a completely open network from anywhere.
2. Network Topology facilitates efficient network sharing.
3. Safe net neutrality from network-level innovation.
4. BLOCKCHAIN 3.0 is always open and scalable.
5. Automatic efficient and dynamic routing.
6. Tokenization mechanism (automation of the settlement process using the Token (COIN) accounting mechanism as a payment for maintaining and expanding and optimizing the network and network connections and data transfer assets and stimulating the participating nodes.
7. Layoff opportunity for users unable to keep up with network performance.

BLOCKCHAIN 3.0 CONSENSUS MECHANISM

SNG NETWORK offers new and more useful proof of work. Unlike the traditional type of Proof-of-Work hashing calculation, which does not take into account any additional actions, SNG NETWORK introduces the Proof-of-Utility (PoU) based on many useful actions, including being online for an extended period, expanding the number of peer-to-peer connections, ensuring high data rates, etc. The Consensus Algorithm is second to none and is designed from the ground up to improve efficiency and fairness of rewards, based on the establishment of local rules.

MECHANISM OF MOTIVATION

SNG NETWORK is designed to encourage network sharing and network ownership by its users. The economic and management model of the SNG NETWORK takes this factor into account when developing a market model. These innovations in technology and economic models complement each other and together add to the power of the SNG model.

PROOF OF WORK

As a pioneering cryptocurrency, Bitcoin is driven by mining, a Proof-of-Work mechanism that encourages miners to inspect transactions by granting them with a BTC reward for solving complex hashing problems. The downside to Bitcoin mining is that it requires specialized and expensive hardware and a lot of energy to mine effectively. According to Digiconomist, Bitcoin's energy consumption exceeded 83 TWh/year at the end of 2020 (https://digiconomist.net/bitcoin-energy-consumption/) and continues to grow, while for the Ethereum network this number is close to 29 TW/h/year (https://digiconomist.net/ethereum-energy-consumption/). It is very important to use a less expensive way of proving the work done, with minimal waste of resources. SNG NETWORK offers an alternative to the existing Proof-of-Work by providing a more decentralized, dynamically evolving, self-organizing and self-evolving network infrastructure and developing an entirely new set of Consensus Mechanisms. The new Proof-of-Utility does not waste resources. Instead, it is a peer-to-peer exchange mechanism at the blockchain level. Members are rewarded by providing more network resources than they consume. SNG NETWORK uses the Proof-of-Utility mechanism to guarantee network connectivity and data throughput.

123 N. Wacker dr. Suite 250 Chicago, IL 60606
phone: +1-415-670-9800 contact@crispmind.io
https://www.crispmind.io

NETWORK TOPOLOGY AND ROUTING

SMART-NODES are a natural extension of the SNG NETWORK, capable of simulating networks with non-geometric adjacent junctions. It is effective in modelling networks that evolve topologies based on local rules. Since the goal is to build a decentralized blockchain system with a dynamic topology, the BLOCKCHAIN OF SMART-NODE GRID is a natural model for the system.

Consider a dynamic network with N nodes. Network connections at time (t) can be described by an N × N adjacency matrix A (t) that evolves over time. Connections between nodes can be added, removed or changed at each time step. If the dynamics A is Markov, the update process can be written as:

A (t + 1) = f [A (t)], (2)

Where f is the network topology update rule. To keep the update rule local, f should be chosen so that when updating its connections, only information about the neighbors of each node is used. The above update rule does not contain the states of the nodes, so the evolution of the topology does not depend on the state of any node. The more general Markov update rule must take into account both the network topology and the states of the nodes in order to:

A (t + 1) = f [A (t), S (t)]

(3) S (t + 1) = g [A (t + 1), S (t)]

Where S (t) is a vector representing the states of all nodes in the network at time t, f is the topology update rule, and g is the state update rule. Likewise, f and g should be chosen so that the update uses only information about the current neighbors.

The state may contain historical information. An example of a state in a blockchain system is all the blocks that a node stores locally. Note that although we describe the system formally using the global state S and the global connectivity A, each node I only needs to know and store its local state S and its neighbors {j | Aij 6 = 0}.

Consider the SMART-NODE in the Blockchain network where blocks are generated. Each time a block is received, the node updates its state and sends the block to its digitally signed neighbors.

Neighbors will decide whether to forward a message based on their state, for example if it received a block, whether the block is valid or conflicts with another block in state, effectively affecting the topology of the entire network without changing the physical layer or the underlying protocol.

As an example, to illustrate how we model a network, consider a general network machine that allows an arbitrary number of neighbors. For simplicity, a minimalist approach is taken to emulate blockchain expansion and data relaying from a small set of microscopic rules. Initially (at time zero), the network is a three-dimensional cubic structure with 8 nodes, each of which has 3 neighbors:

123 N. Wacker dr. Suite 250 Chicago, IL 60606
phone: +1-415-670-9800 contact@crispmind.io
https://www.crispmind.io

EFFECTIVE DECENTRALIZATION

Due to the dynamic nature of the SMART-NODE GRID NETWORK, the network topology between nodes is constantly being updated. The correct update mechanism is critical to achieving decentralization of the resulting topology. If, for example, the update mechanism is chosen so that a newly joined node has a higher chance of choosing a node with more neighbors to be its neighbor, and the probability of selecting a node is proportional to the degree of that node, then the resulting network will be scaleless, the degree distribution follows a power law. Such networks have centralized hubs defined by the nodes to an enormous extent. While hubs have the potential to improve efficiency, they make the network less resilient because hub failures will have a much larger impact than other host failures.

One of the goals of the SMART-NODE GRID is to design and build networks that are decentralized, but at the same time efficient in information transfer procedures. This must be done with the correct topology update mechanism that randomly selects neighbors based on their performance and data rate and is stimulated with a reward. Data transfer rewards must be sub-linear (rising slower than a linear function), so hubs have no advantage. A SPARSE RANDOM NETWORK is one of the possible topologies that can be generated based on such a mechanism. It is decentralized and therefore resistant to failure of any node, but still efficient in routing due to the small diameter of the network. TECTUM BLOCKCHAIN utilizes a proprietary FLASHGRID technology to accommodate the SNG with efficient in information transfer procedures.

SMART-NODE GRID: OVERVIEW OF THE CONSENSUS CONCEPT

SNG NETWORK is designed as a futuristic Blockchain network infrastructure that requires low latency, high bandwidth, extremely high scalability and low cost of reaching Consensus. These properties are critical for future APPLICATIONS. Thus, the SNG NETWORK needs new consensus algorithms that can meet such high demands. Currently, there are several approaches to achieve Consensus on the Blockchain: Byzantine Fault Tolerance Algorithm (BFT), Practical Byzantine Fault Tolerance Algorithm (PBFT), Proof-of-Work (PoW) Algorithm, Proof-of-Stake (PoS) Proof of Stake Algorithm and Delegated Proof-of-Stake (DPoS) Proof of Stake Algorithm.

Practical Byzantine Fault Tolerance (PBFT). Byzantine Fault Tolerance is a model proposed by Leslie Lamport in 1982 to explain the Consensus problem. It discusses Consensus on a scenario in which some Nodes may be HARMFUL (the message may be tampered with) and provides a worst-case guarantee. In Byzantine fault tolerance, let the total number of nodes be N and the number of faulty nodes equal to F. If $N \geq 3F + 1$, then the problem can be solved using the Byzantine fault tolerance (BFT) algorithm. Lamport proved that there is a valid algorithm, so that when the share of bad nodes is less than one third, good Nodes can always reach Consensus, no matter what messages the bad Nodes send. Practical Byzantine Fault Tolerance (PBFT), first proposed by Castro and Liskov in 1999, was the first BFT algorithm widely used in practice. PBFT is much more efficient and runs asynchronously:

123 N. Wacker dr. Suite 250 Chicago, IL 60606
phone: +1-415-670-9800 contact@crispmind.io
https://www.crispmind.io

1. Proof-of-Work (PoW): The Bitcoin blockchain network has introduced an innovative Proof-of-Work (PoW) algorithm. The algorithm limits the number of offers, increasing their cost, and eliminates the need for final confirmation of compliance by agreeing that everyone will accept the longest known chain. Thus, anyone who tries to launch an attack has to incur large economic costs. That is, to pay more than half of the computing power of the system. Later, under this idea, various algorithms of the "PoW" series are proposed, using economic penalties to limit spoilers. Proof-of-Work is the Consensus used by the Bitcoin network and also the earliest one used on the Blockchain. In short, Proof-of-Work connects how much work a miner puts in and how much he gets. Working here is the computing power and time that the miner provides for the Blockchain Network system. The process of providing such services is called "mining". In Proof-of-Work, the reward distribution mechanism is that mining income is proportional to computing power. The more powerful the machine is, the more expected rewards miners will receive.
2. Proof of Stake, Proof-of-Stake (PoS): Initially, PoS reduces the difficulty of computing the hash according to the number of Tokens held. PoS is similar to financial assets in a bank, which distributes financial returns in proportion to the value of assets held by stakeholders for a given period. Similarly, in PoS, the Blockchain Network system distributes "interests" according to the number of stakeholder Tokens and retention times. In Delegated Proof of Ownership (DPoS), not every participant can create a block. Instead, the Nodes vote on trustees who represent them to enter parliament and create blocks. Users who would like to become trustees must earn the trust of the community.

SMART-NODE GRID CONSENSUS

The Scalability Problem of a Simple and Practical Byzantine Fault Tolerance Algorithm (BFT and PBFT): In large distributed systems, it is difficult to reach Consensus using the Byzantine Fault Tolerance Algorithm (BFT) and the Practical Byzantine Fault Tolerance Algorithm (PBFT). In the BFT algorithm, the total number of messages sent to the system is O (N!), Which makes it impractical. The PBFT algorithm has reduced the total number of messages to O (N2), which is processable but does not scale when N is large. Also, both BFT and PBFT require each node to have a list of all other nodes on the network, which is difficult for a dynamic network.

Consensus In Smart-Node Grid Network Based On Ising Model: SMART-NODE GRID is a large distributed system with local connections. The asymptotic behavior of the system is controlled by the update rule. It is possible to achieve a guaranteed global Consensus in a Cellular Automaton using a messaging algorithm based only on sparse local neighbors for a set of update rules. Using the mathematical framework originally developed for the Ising model in physics, we discovered and proved that the class of CA rules will guarantee the achievement of Consensus in no more than O (N) iterations, using only the states of sparse neighbors by an exact mapping from CA to zero temperature of the Ising model. Several studies have investigated the fault tolerance of the CELLULAR AUTOMATA and ways to improve reliability in systems based on the Cellular Automaton. In addition, we have shown that the result is resistant to DIVERSANTS and malicious NODES and calculates the threshold when the desired Consensus cannot be reached.

123 N. Wacker dr. Suite 250 Chicago, IL 60606
phone: +1-415-670-9800 contact@crispmind.io
https://www.crispmind.io

SMART-NODES

A SNG NETWORK is a finite state machine with a set of nodes, each of which changes its state under a local rule that depends only on its neighbors. Each node has only a few neighboring nodes. Spreading through local interactions, local communities of nodes will ultimately influence the behavior of the SMART-NODE GRID. The desired network openness is determined by the uniformity of the cellular machines, where all Nodes are identical, forming a fully decentralized P2P (peer-to-peer) network. Each node in the SNG NETWORK is constantly updated based on its current state, as well as the states of its neighbors. The neighbors of each node are also dynamically changing, so that the network topology is also dynamic without changing the underlying infrastructure and protocols.

RULES AS FORMULAS

The programming formula of SMART-NODE is called "local rule", which is a mandatory rule for the SNG NETWORK and has an important influence on the network topology. The correct choice of local rules leads to cellular automata with complex but self-organized behavior. Rules are important because they are formulas for programming CELLULAR AUTOMATA and automatic networks. Static characteristics of a cellular automaton is a discrete dynamic system defined as:

Cellular Automaton = (S, N, K, f) (1)

A finite number of nodes interact in a conventional network; S represents node states, where each node has a local state. The state of all nodes determines the global state; N denotes the number of nodes in the network; K denotes a set of neighbors, that is, which neighboring Nodes are taken into account in local state transitions; f denotes a state transition function that has a significant impact on the global evolution of the system. The dynamic evolution of the SNG NETWORK starts from the initial state. Nodes change their states based on their current state and the states of their neighboring nodes. The global state is completely determined by the local states of all nodes and develops accordingly.

THE ANALISYS OF ETHEREUM NETWORK

In short, the Ethereum network is a platform for creating decentralized online services based on smart contracts (Smart Contract). Also, this platform can be called a single decentralized virtual machine. The eponymous cryptocurrency Ethereum or Ether (ETH) runs inside the system. Network operation is based on 3 fundamental principles:

1. The presence of cryptographic protection means that the internal currency is created based on complex mathematical algorithms that are extremely difficult to crack.
2. Singleton transaction recording mechanism. That is, the system contains only one correct algorithm responsible for conducting transactions. This digital mechanism can be called a single truth, accepted by all users of the site. To prevent the emergence of new mechanisms within the platform, the GHOST protocol is used. According to this protocol, the one that requires the

123 N. Wacker dr. Suite 250 Chicago, IL 60606
phone: +1-415-670-9800 contact@crispmind.io
https://www.crispmind.io

most computation is considered canonical. The open state of the mechanism means that the network can be used by all its participants at any time.

3. The Ethereum network mechanism systematically analyzes the incoming information and, relying on it, changes its state. The starting point for the system under consideration is the so-called "State of Genesis". This is the initial status of the platform before any money transfers are made. After the transactions are carried out, the network transitions to the phase of a new final state, which will be the current state of the Blockchain Network at a specific point in time.

Today, the Ethereum blockchain consists of hundreds of thousands of transactions grouped into blocks. Each new element of the network is connected with the previous one, due to which a chain is formed. Any block has its own number all going in strict sequence. Despite the fact that these networks are open, they cannot be changed or deleted from the database. As mentioned just above, the entire lifecycle of the Ethereum network is based on a constant change of state. For such changes to take place, there must be valid transactions in the system. Transfers receive the status of valid after passing the validation, which is part of mining. Mining on the Ether network is the process of creating new blocks of transactions, which is performed using the computing power of hundreds of computers (or nodes). In fact, each miner claims to form and test a new element of the Blockchain Network. Thousands of users around the world are non-stop generating and approving blocks. When recording a new blockchain element, each miner provides mathematical proof that the block is formed and includes only valid transfers. This algorithm is called Proof-of-Work (that is, proof of work done). For each confirmed block, "miners" receive a reward in the form of a certain number of Ethereum coins (ETH). Since today colossal capacities are required to form new elements of the network, users practically do not mine (extract) one by one. They are pooled and work together to form one block. After creating a new component, the reward is distributed among all participants in the process. Its size directly depends on the contribution of a particular user to the creation of the block. The Ethereum network has, on average, the following key metrics:

- Total network hash rate: 282.395 THash/s.
- Average time spent on block generation: 14.5 sec.
- Total number of blocks: 6 186 719.
- Size of one network element: 25.134 Kb.
- Ethereum Blockchain network size: 667.10 GB.
- Average number of blocks generated per day: 5,945.
- Block reward: 3 ETH.

Based on the above information, we can conclude that the size of the Ethereum Blockchain is increasing daily by 148.6 MB. Thus, over a year, the network database will “grow heavier” by about 54 GB.

123 N. Wacker dr. Suite 250 Chicago, IL 60606
phone: +1-415-670-9800 contact@crispmind.io
https://www.crispmind.io

TECTUM SMART-NODE GRID NETWORK

CHARACTERISTICS OF THE NETWORK ACCOUNT:

1. Account balance.
2. The number of Harvesting units (“harvest”).
3. The number of the first transaction associated with the account.
4. List of multi-signed accounts and co-signers.
5. Transaction types related to multi-signature)
6. Information about the status of the delegated account.
7. The importance and rating of the NCD.
8. Active (matured) balance.

CRYPTOGRAPHY

Blockchain technology requires the use of some cryptographic concepts. TECTUM, like many other Blockchain networks, uses technology based on Elliptic Curve Cryptography. The choice of this curve is important in order to guarantee safety and speed. TECTUM uses the TWISTED EDWARDS CURVES:

$x2 + y2 = 1- 121665121666x2y2$

Above a finite field defined by prime 2255-19 along with a digital signature algorithm called Ed25519. It was developed by DJ Bernstein et al. It is one of the safest and fastest digital signature algorithms [2]. The base point for the corresponding G group is called B. The group includes q = 2252−27742317777372353535851937790883648493 elements. Each element of group A can be encoded into a 256-bit integer A, which can also be interpreted as a 256-bit string, and A can be decoded to get back A. For the hash function H mentioned in the article, NEM uses 512- bit SHA3 hash function.

PRIVATE AND PUBLIC KEYS

The private key is a random 256-bit integer k. To extract the public key A from it, you must perform the following steps:

$H\ (k) = (h0, h1,\ldots, h511)$ (1)

$a = 2254 + \Sigma 2ihi3 \leq i \leq 253$ (2)

$A = aB$ (3)

Since A is afloat, it can be encoded into a 256-bit integer A used as the public key.

123 N. Wacker dr. Suite 250 Chicago, IL 60606
phone: +1-415-670-9800 contact@crispmind.io
https://www.crispmind.io

SIGNATURE AND VERIFICATION OF SIGNATURE

Given a message M, a private key k, and a public key A associated with it, the following steps must be taken to create a signature:

$H\ (k)$ = (h0, h1,…, h511) (4)

$r = H\ (h256,\ldots,\ h511,\ M)$, where comma means serial connection (5)

$R = rB$ (6)

$S = (r + H\ (\text{R, A, M})\ a)\ mod q$ (7)

Where (R, S) is a message M signed with a private key k. Note that only signatures where $S < q$ and $S > 0$ are considered valid to prevent signature malleability.

To verify the signature (R, S) for a given message M and public key A, you must first check the condition $S < q$ and $S > 0$, and then calculate:

$\tilde{R} = SB - H\ (\text{R, A, M})$

A and check the condition:

$\tilde{R} = R$ (8)

If S was calculated, as shown in (7), then $SB = rB + (H\ (\text{R, A, M})\ a)\ B = R + H\ (\text{R, A, M})$ A

Thus, (8) will be fulfilled.

OPERATING MODES

This network has three modes of operation: Regeneration mode (TOPOLOGY change), Reading mode and Write mode (See GLOSSARY).

Regeneration of blocks always occurs on a read or write request (At the end of a read or write request). If the network is idle, then no regeneration occurs. In this mode - the network stops processing requests (READS, WRITES) and the network NODES (NODES) analyze the work of the previous cycle - the processing time of blocks, access speed (SPEED OF COMMUNICATION CHANNELS), the number of processed transactions (in each new cycle, each node processes its own block, the same for everyone). Based on the results of this analysis, the optimal NETWORK TOPOLOGY (hierarchy, rating) is compiled for the next cycle by the ELECT NODE. The ELECT NODE is selected randomly based on the proprietary RANDOM CIRCLE STOP (RCS) algorithm, from among MASTER NODES at the very beginning of the regeneration mode. The RCS algorithm is a ROCK-PAPER-SCISSORS GAME. During the designated period, the MASTER NODES perform sequential calculations (GENERATION OF RANDOM NUMBERS, WITH A SHIFT). After the specified time has elapsed, the ELECT NODE is selected (according to the specified criteria), which has generated a random number.

123 N. Wacker dr. Suite 250 Chicago, IL 60606
phone: +1-415-670-9800 contact@crispmind.io
https://www.crispmind.io

The choice of the ELECT NODE comes from the group of MASTER NODES, the number of which depends on the size of the network. MASTER NODES are selected from the NOMINAL NODES. In each cycle, the circle of MASTER NODES is updated. (You cannot be a MASTER NODE for two consecutive cycles). The conventional NODE TOPOLOGY has a binary structure of a binary tree.

NETWORK TOPOLOGY

Form clusters in such a topology, in which the highest transmission speed is important (SELF-GROWING BRANCHES). Each MASTER NODE could have its own cluster (BRANCH). The ELECT NODE calculates (verifies, approves, signs) each new BLOCK of transactions aggregated (COLLECTED, COMBINED) by MASTER NODES in the previous cycle. After checking and verifying this block by MASTER NODES and reaching a Consensus (CRITERION), the block is written into the CHAIN and transmitted down to the rest of the NETWORK along with the topology. BLOCKS are collected only by MASTER NODES. The new NETWORK TOPOLOGY (HIERARCHY) is calculated by the ELECT NODE at the end of the current cycle and propagates through the network from the NODE to the NODE under the current topology for the current cycle from each MASTER NODE along the corresponding branch.

ENCRYPTION ALGORITHM

It is a SHA-1 Proprietary JUMP METHOD that uses an undetectable STACK OVERFLOW ERROR for one-way hashing.

GLOSSARY

1. ALGORITHM OF COUNTER SELECTION RCS (RANDOM COUNTER SELECTION): Simultaneously all MASTER NODES, including the ELECT NODE, generate random numbers. The elect nodes transmit the received numbers to the ELECT NODE. The ELECT NODE sorts them in ascending order and chooses from the received MASTER NODE list in accordance with the number that was generated earlier.
2. STACK: The entire bundle of transactions received by the ELECT NODE from MASTER NODES.
3. CLUSTER: A group of NODES connected by a binary-tree NETWORK TOPOLOGY.
4. DELEGATE NODE: A peer-to-peer network node with a high-performance rating and high speed of communication channels. DELEGATE NODE has a complete database of transactions. Any NODE can request access to the DELEGATE NODE of its CLUSTER to the archive (LEDGER) of transactions (EVENTS).
5. ELECT NODE: The main node of the CLUSTER selected by the pool of MASTER NODES to process the STACK; a peer-to-peer network node that performs the following functions:
    a. The MASTER NODE for the next cycle is selected by the current ELECT NODE of the CLUSTER among the other MASTER NODES at the end of the current cycle using the RCS (Counter-Choice) algorithm.

123 N. Wacker dr. Suite 250 Chicago, IL 60606
phone: +1-415-670-9800 contact@crispmind.io
https://www.crispmind.io

b. Receives blocks from MASTER NODES and forms a STACK that includes all transactions in the network.
c. Distributes the received and signed block through the MASTER NODES to the network.
d. Defines a new binary tree topology in each fiefdom for the next cycle using the Proof-of-Relay algorithm.
e. Distributes a new NETWORK TOPOLOGY through the MASTER NODES. Each node of the CLUSTER receives the address of the next ELECT NODE, the address of the upper MASTER NODE and the addresses of the two lower MASTER NODES.
f. Transfers a NODE from one CLUSTER to another.

6. NOMINAL NODE: A node that can form, perform a transaction sufficient for writing it into the Blockchain, and also issue a READ REQUEST to a DELEGATE NODE.
7. MASTER NODES: The STACK processing NODES elected from the group of DELEGATE NODE at the end of the CURRENT CYCLE using the RCS algorithm; perform the following functions:
   a. Participate in the selection of the ELECT NODE.
   b. Determines the performance rating of NODES of its CLUSTER based on an algorithm that takes into account the work done earlier, as well as the performance of the node.
   c. Transfers the performance rating of NODES to other MASTER NODES, who, based on the rating, forms the topology of the NETWORK.
8. TRANSFER OF DATA PATHS:
   a. BOTTOM-UP: Transfer of information about transactions.
   b. UP-DOWN: formed and signed blocks are transferred, as:
      i. The node directly sends the transaction(s) to the ELECT NODE, the ELECT NODE forms and signs the BLOCK from the received transactions and sends directly to each MASTER NODE.
      ii. The NODE sends transactions to the MASTER NODE through the ELECT NODE, the MASTER NODE receives the transaction blocks from the MASTER NODE, forms the final block, signs, and sends down the network also through the MASTER NODES.
   c. UP to the MASTER NODE through the ELECT NODES, DOWN directly.
   d. UP to the MASTER NODE directly, DOWN through the ELECT NODES.
9. READING MODE: Any node forms a request to READ the required block from the BLOCKCHAIN NETWORK. Request either directly to the ELECT NODE, or to any DELEGATE NODE of his CLUSTER.
10. RECORDING MODE: Any NODE who has received information for recording from the BLOCKCHAIN transmitting it over the network. RECORDING MODE forms a block based on the information received, writes it to the Blockchain, and transmits it to all DELEGATE NODES for recording in a BLOCKCHAIN LEDGER.

END