Introuduction

In 1946, the world's first computer ENIAC [1] was invented, kick-starting the era of general-purpose computers. In 1981, IBM introduced the world's first personal computer (PC), and Microsoft ushered in a new era of PCs. Proposed by Google in the 21st century, major Internet companies created the era of cloud computing. Therefore, it has become evident that the evolution of computing is changing forms gradually.

In 2015, Ethereum was the first to develop a blockchain-based distributed world computer [2]. Over the past two years, the successful developments of DeFi and NFT have further verified the commercial value of distributed world computers. Ethereum is just the beginning for distributed world computers. But, the decentralized future needs a greater leap in computing evolution.

With the rapid development of NFTs, Web 3.0 applications, and the metaverse, various decentralized applications have an increasing demand for storage, and there is no blockchain that can meet this demand well. With the exploration and continuous implementation of application concepts, higher requirements are also placed on the performance of the blockchain.

At this point, what the world needs is a high-performance world computer with highly integrated distributed storage.

1. Mission and Vision

1) The first ultra-high-performance decentralized world computer that deeply integrates distributed storage functionality to realize the mission of becoming the ultimate world computer.

In the first phase, Topia will be the first blockchain with highly integrated distributed storage, and by utilizing the development and accumulation of blockchain technology up until now, through innovation of the consensus mechanism and optimization of the P2P network and on-chain transactions, the efficiency of transaction processing on the chain is greatly improved. Therefore, Topia will be the first high-performance world computer with integrated distributed storage.

However, the final form of the distributed world computer does not stop at the deep integration of distributed storage and the improvement of on-chain transaction performance. The final form of the distributed world computer will be extremely friendly to developers and the user experience, with lower hardware requirements for operating node devices, supporting more nodes, hence resulting in the node distribution being more decentralized. Using the initial phase as a model, Topia will gradually realize the final form of distributed world computing.

The Bitcoin protocol is the first-generation of blockchain technology, which introduced native digital scarcity. Ethereum is a second-generation blockchain protocol designed to introduce smart contracts interoperable on the base layer, which helps provide a better solution for application scenarios. In essence,Topia is the third-generation blockchain protocol, which mainly introduces distributed storage on the basis of smart contracts. The combination generated by the integration of smart contracts and distributed storage on the base layer will directly open doors to a new world for the exponential growth of the decentralized application era.

2) Developing the infrastructure of WEB 3.0 [3] applications: secure ownership of personal data and allow control by individuals

The birth of Bitcoin realizes ownership of personal assets. Users hold the private key of the wallet, which cannot be transferred by anyone else, and the assets are truly in their hands.

Data is the "oil" of the digital economy era, and the right to own your data is the only way to avoid “data dictatorship” from bringing devastating disasters to the new world. In recent years, , the oil of the new age, and its safety concerns are growing. Whether it is Facebook or Google, its core business model is to use the massive personal data at its disposal to achieve accurate advertising. Is this really the final form of personal data value utilization? Is it really the best form? Should personal travel data, shopping data, web browsing data, and social media data really be in the hands of big tech firms and sold against our will? Clearly, this is neither the definitive nor the best form of personal data.

Your personal privacy data should not be archived on a company's servers but should be in your own "hands". Like bitcoin, you should have complete control over your personal data, just as you do with your bitcoin wallet.

With Topia’s privacy computing, commercial companies can pay you for the right to use your specific data to send customized commercial advertisements. But in the whole process, it still can't access any of your shopping, travel, web browsing, and other metadata. If, for example, a commercial company wants to know whether you are interested in a specific product, it only needs you to authorize the commercial company to use your data for that purpose, and it can get a 'yes' or 'no' result without accessing your personal data. A fee is required from the commercial company to obtain this 'yes' or 'no' result.

Personal data ownership will become a core feature of Web 3.0 applications as one of the most essential concepts in the era of Web 3.0. Topia, by its very nature, will realize the personal ownership of data and become the most important infrastructure in the Web 3.0 era.

3) The best infrastructure for the metaverse[4].

Digitization has been a significant technological trend over the past three decades, which is unstoppable and is only expected to increase exponentially as time goes on.

The evolution of information transmission through the ages has always been toward greater efficiency. From the first sounds of Homo sapiens millions of years ago to the beginning of human use of language 50,000 years ago; from the time humans began writing 5,000 years ago, to the invention of paper in the 19th century; then to the invention of the telegraph and the telephone in 1876, Information transmission has evolved efficiently . Every change in the carrier in which information is encoded and disseminated has had a huge impact on the world. In every instance where the connection between people and things is improved, it will have a positive effect on the efficiency of operational processes.

Internet development over the past three decades has also followed a similar pattern. With communication tools, such as chat software, that originally used text and then started supporting pictures, voice, and then real-time voice chat, and now supports video, we can imagine that a virtual reality metaverse may also emerge in the future. From the early stages of verbal communication to the invention of writing, the transmission of information depended on "written text", but now an array of new senses might be incorporated into the new age of communication. Hence, relying on the immersive experience to directly transmit and receive more dimensional and comprehensive information. Metaverse technology is ushering in a world in which people-to-people and people-to-things are connected by "sensing".

The development of a metaverse will allow for an easier connection between people and things, and as such will lead to a digitized virtual world. The question is: how should it be built on? Should it be built on a company's server or hosted on Amazon Web Service? Neither, it should be built on a new generation distributed world computer with higher security requirements and higher decentralization. A decentralized metaverse cannot be changed at will, it is irreversible, and is less likely to disappear due to hacker attacks. The various current infrastructures available such as cloud computing platforms cannot meet the higher requirements for metaverse's security and decentralization. The best and most suitable infrastructure for the metaverse is the decentralized distributed world computer based on blockchain technology.

NFT technology guarantees the uniqueness of cryptographic metaverse assets. The irreversible characteristics of the blockchain ensure the order in which the virtual world of the metaverse runs, and it will also ensure the security of a large number of digital and virtual characters that will appear in the metaverse. The decentralization of the blockchain is a powerful guarantee for the security of the entire metaverse virtual world. Toward the development of a best metaverse infrastructure, Topia will tap into the power of distributed technology, the characteristics of blockchain technology, and the support from underlying protocols such as NFT.

4) Building a more decentralized world with true equality and freedom.

It has always been one of the ultimate pursuits of human society that every individual can develop fully and freely, but due to the limitations of technology and ideas, all this still exists in a hypothetical utopian world. Topia is committed to bringing human society infinitely closer to a new world of freedom, openness, justice, and equality.

(1) Make finance more decentralized

Throughout history, economic development has undeniably been a driving force behind human development. As the jewel in the economic crown, financing occupies a central position in the economy that is closely related to everyone. However, not everyone can enjoy the convenience brought by the traditional financial system.

Statistics show that there are still approximately two billion people worldwide without access to these traditional financial services. Due to the access threshold and service cost, and the profit-seeking nature of capital, centralized financial institutions are still incentivized to accommodate the rich at the expense of the poor. On the other hand, Decentralized Finance (DeFi), emanating from its decentralized nature and powered by blockchain technology, has been adopted and used by early adopters and enthusiasts. Topia, through a more secure and high-performance distributed network, enables people all over the world to access decentralized financial services without authorization, restrictions, and thresholds, and firmly control their financial assets and data.

The core logic of Bitcoin is to truly establish the ownership of personal assets through technical means. As long as you have the private key, no one can seize your assets. On the one hand, Topia will help people better protect their private wealth, and on the other, it will make it easier for people to obtain inclusive and flexible financial services.

(2) Make the world more free and open

Decentralization is not the purpose of blockchain, it is just a means for us to achieve a more free, open, fair, and equal world. The Internet has changed the way of information transmission, and the blockchain, as a machine for constructing trust, has changed the value transmission mechanism in the entire human society. What is worrying is that the original free and open spirit of the Internet is increasingly being eroded. Large companies and government departments hold massive user data and store it in their own centralized servers, which can arbitrarily be tampered with, sell user data or even confiscate assets. The entire Internet is in the control of a few centralized institutions, becoming more and more fragmented, and even gradually getting out of control. Topia will uphold and fully protect users' rights to freedom and equality in a decentralized manner. The data is in the hands of the user, and only the user can decide to whom the data is shared, how it is used, and where it exists. People's privacy will also be greatly protected.

2. Current issues

As of now, the existing blockchain architecture and cloud services are only outstanding in certain aspects, but there are many deficiencies in supporting enterprise-level applications, and enabling NFT, metaverse, and Web 3.0 in the future.

1. With the development of NFT, GameFi, SocialFi, metaverse, and Web 3.0, storage has become increasingly scarce, storage requirements will become more apparent, and the existing blockchains do not meet the needs of developers.
2. The previous generation of blockchains led by ethereum has a heavy technical and historical burden, hence the cost of updating and iterating is extremely high. The existing blockchain architecture makes it difficult to integrate a distributed storage solution on the base layer. However, products such as Filecoin and Arweave specializing in storage still have integration difficulties with existing blockchains.
3. The current blockchains either only provide computing functionality, or data storage functionality respectively, which causes difficulties for DApp development. When developing a DApp, it is necessary to pay attention not only to the logic on the chain, but also to the problem of data storage.
4. In the metaverse, everyone can send transactions and transactions can be effectively confirmed. The metaverse needs a capable blockchain to record information.
5. As more people begin to understand Web 3.0 and its concepts become popular, a series of Web 3.0 applications will grow exponentially, and the blockchain built and customized for Web 3.0 is about to emerge.
6. At present, cloud services are too centralized, there is a greater risk of user data leakage; and users have no control over their own data; these are contrary to the principles advocated by Web 3.0;

3. Technical Architecture

Based on the current problems of blockchain and cloud services, we propose the following architecture for Topia:

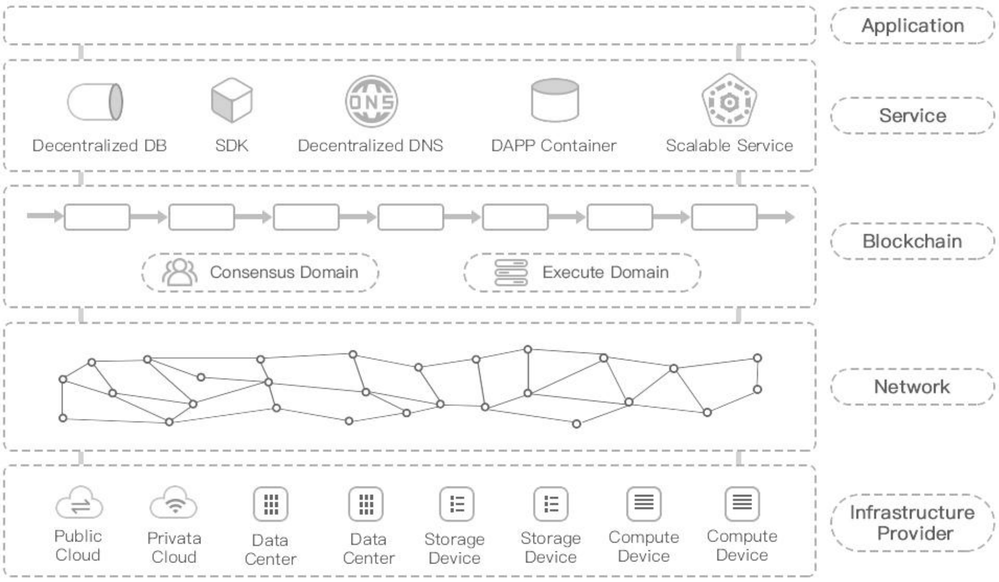

Figure 1: Topia’s overall architecture diagram

The overall architecture divided into 5 layers: Infrastructure Provider, Network, Blockchain, Service, and Application;

Infrastructure provider: We will not provide our own infrastructure, but rather cloud service providers, data centers, and idle storage and computing equipment of individuals and organizations will join and contribute to the Topia network by staking Topia tokens. This framework will distribute a certain amount of Topia token rewards according to the service provided, and it obtains a certain reputable value according to the quality of service provided.

Network: The network not only refers to the P2P network provided for blockchain consensus and message broadcasting, but also refers to the point-to-point network for mass data transmission between any two nodes, the encrypted transmission network between cloud services, and the CDN that accelerates the edge node [5] network; among them, the blockchain consensus and message broadcasting nodes are based on the double-layer distributed hash table (DHT) [6] algorithm to accelerate the message data being broadcasted to the target node;

Blockchain: The blockchain layer is based on the Topia network, which provides service quality assurance for applications; according to different functionalities, the chain layer divides the nodes into two domains, the consensus domain and the execution domain. The consensus domain represents the set of consensus confirmations, including block proposers nodes and block verification nodes. The consensus domain is dynamic and is maintained by the native contract and updated for every epoch (24 hours); the block proposer and block verification nodes are selected from the consensus domain by the VRF (verifiable random function). The execution domain represents the set of transaction executors, which are divided into different sub-domains according to different transaction types.

Service: In the service layer, Topia will provide a decentralized database and DApp container based on Topia distributed storage, which ensures that DApp data is stored in a user-controlled manner, so that it has its own autonomy over its own data; each DApp corresponds to a DApp container, through which user data is stored in a location controlled by the users themselves, the DApp needs user authorization to read the data; each user has its own access to the DApp URL, which is passed through the decentralized DNS resolution. In addition, at the service layer, SDK services and scalable services for interacting with other chains such as cross-chain services are also provided.

4. Consensus

The consensus in Topia is called POM(Proof-Of-Multifactor), based on VRF (Verifiable Random Function), threshold signature BLS (Boneh–Lynn–Shacham), and DKG (distributed key generation); based on these technologies, Topia's consensus, POM, is divided into the following parts:

4.1 DKG and BLS

The DKG used by the POM consensus consists of two parts: running a brand new DKG from scratch, using the algorithm[7]; redistributing the old private key to a different set of new nodes, using the algorithm[8]. The process is described as follows (as shown in Figure 2, assuming that the number of participants is *n* and the threshold is *t*):

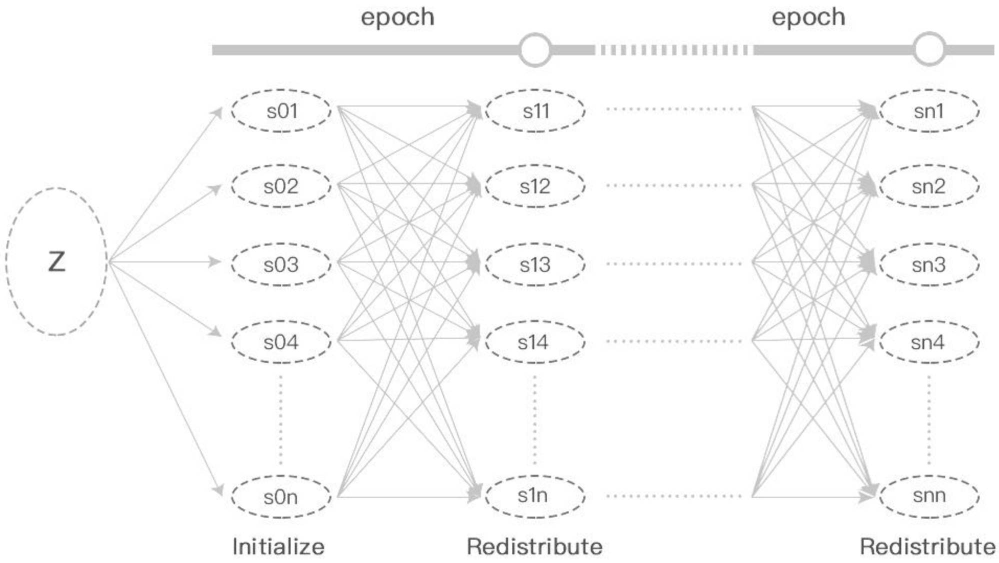

Figure 2: DKG process

Initialization process:

At the beginning of the system, each member of the selected consensus domain runs an instance of Feldman VSS (Verifiable Secret Sharing) as a dealer;

Each member, *i*, generates a random *zi* and constructs a polynomial function *fi(x)* such that *f(0)* = *zi*, then allocates the private key according to the VSS protocol, calculates the public key for the private key, and broadcasts the commitment.

Once each participant receives *t-1* (t is the threshold) commitments, it sends the locally-generated private key and the corresponding public key to other participants, where the private key is sent in encrypted form;

Each participant can verify the received private key according to the received commitment; in the end, each participant's private key, denominated by *si*, is the sum of the received private keys, and the public key *pub*, corresponding to the consensus domain, is the sum of the public keys of all participating members.

Reassignment Process:

At the end of each epoch, once it is detected that the consensus domain members and parameters have changed (adding new members, leaving members, threshold changes), the redistribution protocol will be run to recalculate the private key of the consensus domain members.

The above DKG-related protocols have the following advantages:

1. There is no need to choose the trustee who distributes the private key;
2. Each participating member can verify whether the private key he shared corresponds to the public key.

In the above description, the consensus domain represents the set that is eligible to participate in the consensus, managed by the native contract. DKG is mainly used to generate the signature private key and corresponding public key of BLS participants.

4.2 VRF

In the POM consensus, VRF is mainly used to randomly select block proposers. The current VRF algorithm is based on Elliptic Curve VRF (ECVRF) [9], which satisfies trusted uniqueness, trusted collision resistance and full pseudorandomness.

It mainly includes the proof generation process (ECVRF_prove) and the proof verification process (ECVRF_verify); The main principle of the proof generation process is to first convert the random seed data into points on the elliptic curve, and derive a pseudo-random number from the input private key and other inputs, and then perform a hash calculation based on the generated points and pseudo-random values. The main principle of the verification process is to verify whether the parameters required for the hash calculation of the elliptic curve points (these points are generated by the public key and the seed data) are equal to the results based on the previously generated proof data, the input public key, and the random seed data.

Different elliptic curve proofs have different generation and verification processes, as such, Topia network will implement edward 25519, secp256k1 curve, and bls12381 curve to adapt to different application scenarios;

In the VRF proof generation process, the random seed data is critical, hence it is necessary to ensure that the generated proof is unpredictable and difficult to change; in the POM consensus, taking into account various aspects, the random seed data is based on hashing the current and latest confirmed block through the aggregated signature *AggSig*, generated after the block verification domain BLS signature, and the VRF proof:

$$\text{RandnessSeed}_{j} = \text{hash}(AggSig_{\lhd-1} \;\|\; VRFProof_{\lhd-1})\ (j = 1,2,3, \dots)$$

When *j* = 0; *AggSig* and *VRFProof* are the corresponding values of the genesis block.

4.3 Block Proposal

Every 0.5s, block proposers are randomly selected from the block proposer domain by drawing lots.

Currently, the random selection algorithm is based on the poisson distribution:

$$\mathbf{P(X = k) =} \frac{\lambda^{k}}{k!} e^{-\lambda}$$

Among them,

$$\lambda = \text{weight}_{j} / \text{totalweight*blockNumRound}$$

where weight $_{j}$ is the weight of the block proposer, totalWeight is the weight of all block proposers in the block proposer domain; blockNumRound is the expected number of proposers per round.

The generation process of a block proposal right is as follows:

1. The block proposer calculates the current VRF proof based on ECVRF_prove, and obtains its corresponding hash integer value (the value being in the range [0, 2^256))
2. vrfINT = hash(VRFProof).Int
3. Calculate P(j) = (1-P(X=0)-P(X=1)-…-P(X=j)) * 2^256
4. Execute for (j=0; vrfINT<P(j) && j<MaxElectionCount; j++); *MaxElectionCount* is the maximum election value of the block proposer; after this loop is executed, and if the last *j* is greater than *0*, the block proposers have the right to propose blocks

5. Once a block proposer has the right to propose a block, it selects compliant messages from the transaction pool, constructs the proposed block header and the packaged transaction, and then broadcasts the message to active verification domain members selected by a random algorithm from the verification domain groups.

In the above process, the weight of each block proposer is related to the proposer's reputation and the amount of staked Topia tokens (refer to the token economics section for the calculation formula). The block proposal algorithm ensures that the block production rate is positively correlated with the weight of the block proposer, and the expected value of the block production rate is λ = weight $_j$ / totalweight. In addition, the use of VRF ensures randomness and verifiability and prevents collusion between block proposers and block validators, because no one except the block proposer itself can predict whether other block proposers have the right to propose blocks.

According to the above method, there will be multiple block proposers in each round with the block proposal right. In order to easily determine which submitted block is the accepted block, once the block proposer calculates j > 0, the priority weight of the block to be submitted will be calculated by the way of hash splicing.

$$\text{pri} = \text{hash}(\text{VRFProof}, j)$$

4.4 Block verification and submission

As shown in Figure 3:

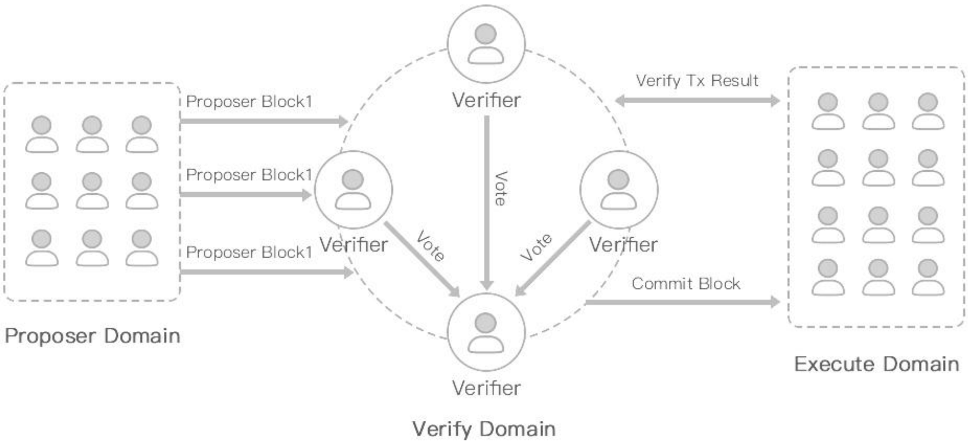

Figure 3: Block verification and submission

Once the randomly selected member of the verification group receives the submitted block, it will be cached, and then wait for a period of time (currently the time is set at 50ms), at this time, the block with the highest priority in the cache will be used for verification.

In addition to verifying the legitimacy of the basic information of the block and VRFProof, it also randomly checks the execution result of the transaction contained in the block through the execution domain, if an illegal block is verified, the block submitter will be punished (the rules of punishment can be seen in the Governance section).

The verified legal block will be signed by the member's private key and sent to the leader node of the verification group (the leader node is randomly selected).

Once the leader node receives the verification domain member's voting signature for the same block and reaches the specified threshold (BLS threshold), it will notify the execution domain to submit the previous execution result.

The execution domain receives the submission request, submits the previous execution results, adds the new block to the ledger, and simultaneously broadcasts the block to the entire network.

In conclusion, POM consensus has the following advantages:

1. Block proposal, block verification, and block execution (transaction execution) are divided into different domains, facilitating horizontal scaling.
2. The block proposal algorithm based on the VRF algorithm ensures randomness and verifiability, and prevents collusion between block proposers and block verifiers.
3. Based on the use of BLS and DKG, the communication complexity of block confirmation and the size of the consensus confirmation message are both reduced (because the consensus confirmation message is signed by the private key of the participating members, compared with the full private key signature, the signature message length is much less), thus reducing the bandwidth usage.
4. Block proposal, block verification, and block execution (transaction execution) are divided into different domains, facilitating horizontal scaling.
5. The block proposal algorithm based on the VRF algorithm ensures randomness and verifiability, and prevents collusion between block proposers and block verifiers.
6. Based on the use of BLS and DKG, the communication complexity of block confirmation and the size of the consensus confirmation message are both reduced (because the consensus confirmation message is signed by the private key of the participating members, compared with the full private key signature, the signature message length is much less), thus reducing the bandwidth usage.

5. Transaction Model

5.1 Basic flow of transaction processing

As shown in Figure 4:

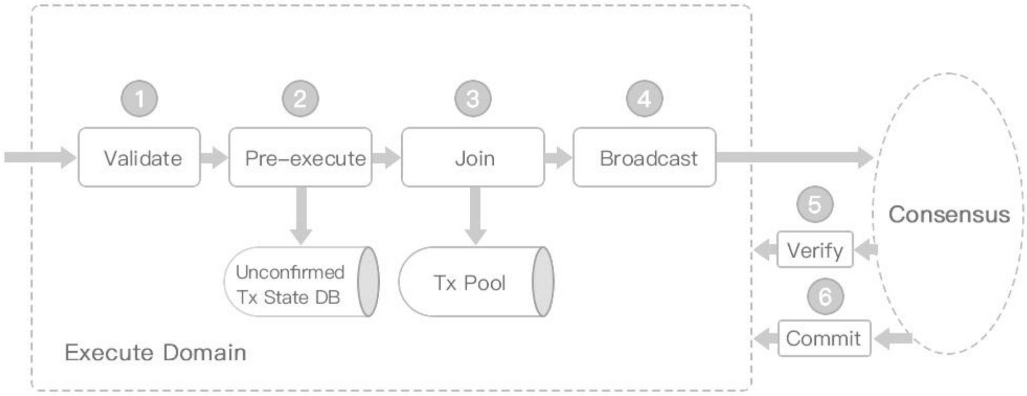

Figure 4: Basic transaction process

When any node in the execution domain in Figure 4 receives the transaction (forwarded by this node or other nodes), it verifies the basic information of the transaction first (including transaction type, signature, length, transaction address, etc).

A transaction verified by basic information will randomly select a node that can execute the transaction from the execution domain according to the transaction type, and pre-execute the transaction; the pre-execution will generate the gas required by the transaction and other results. These will be stored in the unconfirmed state database as an intermediate state, and a transaction attempt with an insufficient balance for the payment amount will be regarded as a failed transaction.

Once the transaction is pre-executed successfully, the transaction meta information will be joined with the transaction executor and transaction execution result information, collectively join the transaction pool (Tx Pool) to broadcast the transaction to other nodes outside the consensus domain node. After the transaction is received, it will be put into the local transaction pool after verification of validity.

When the block containing the transaction (obtained from the local transaction) submitted by the consensus node proposer is submitted to the verifier, a transaction will be randomly selected to verify the validity of the transaction to the execution domain. Once the verification fails, the executor of the transaction will be punished (see the governance section for details), and will enter the ‘complete verification’ mode of the block transaction (verify all transactions in the block);

Once the consensus module passes the verification of the submitted block, it will issue a commitment message to the execution domain to notify of the Tx State to be confirmed, and the corresponding node of the execution domain will update its state through other nodes in the entire network.

5.2 Scalable transaction executor

The Topia network will support many transactions. Different transactions require different node resources. For example, general node resource allocation can satisfy common payment transactions by default. Privacy computing and large computing power often have special requirements for CPU and GPU. If all transactions are configured with the same resources, the utilization rate of resources will be very low. Therefore, the nodes in the execution domain are grouped according to different transaction requirements, as shown in Figure 5.

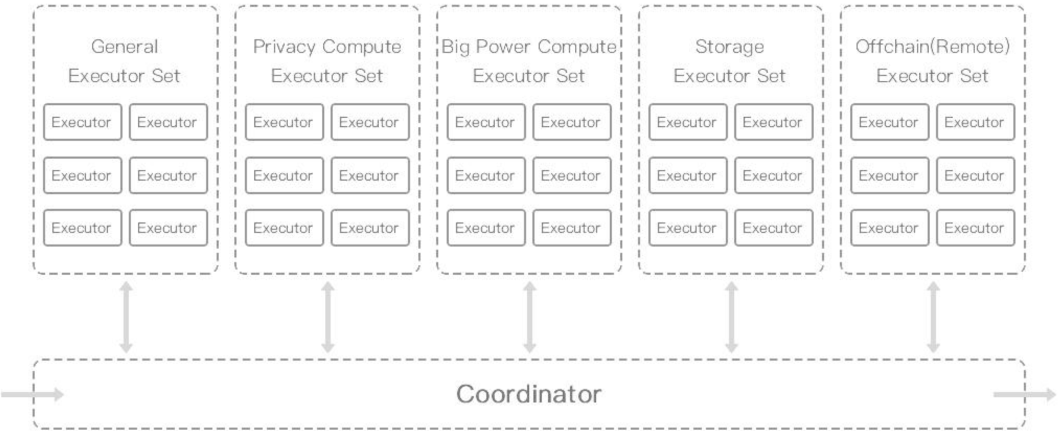
General Executor Set
Privacy Compute Executor Set
Big Power Compute Executor Set
Storage Executor Set
Offchain(Remote) Executor Set
Executor
Coordinator

Figure 5: Scalable transaction executor

The coordinator of transaction execution is only a module of each executor, not a single node, all executors have such a module, so all executors in the transaction executor domain are leaderless, these executors are maintained through native contracts; When a transaction executor receives a transaction, it will randomly select an executor from different execution sets to execute the transaction according to the transaction type; Topia supports dynamic expansion of different executors, which can either add new executors to the same executor class or create new executor classes.

5.3 Parallel execution of transactions

When receiving batch transactions, for the same transaction types, the coordinator distributes it to the same executor; The transaction list will be converted to DAG form.

In DAG transactions, a transaction with an in-degree of 0 is a ready transaction without any dependencies that can be executed immediately. When the number of ready transactions is greater than 1, ready transactions can be distributed to multiple CPU cores for parallel execution. When a transaction is executed, the in-degree of all transactions that depend on the transaction is reduced by 1. As the transaction is continuously executed, the ready transaction is also continuously generated. In the extreme case, if the number of constructed transaction DAG layers is 1 (that is, all transactions are independent without dependencies), the overall execution speed of the transaction will be improved by a factor that directly depends on the number of cores *n* of the processor. If *n* is greater than the number of concurrent transactions, the execution time of all transactions to be executed in batches is the same as the execution time of a single transaction. Figure 6 shows the DAG processing of the transfer transaction:

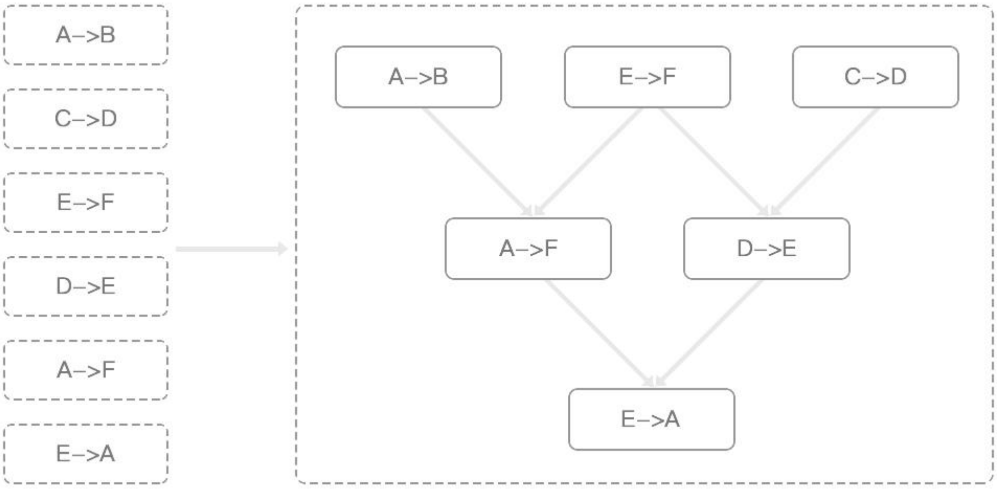

Figure 6: DAG processing of transfer transactions

6. Network

The Topia network not only includes the P2P network as the chain layer, but additionally includes the edge network and the application service network,as shown in Figure 7:

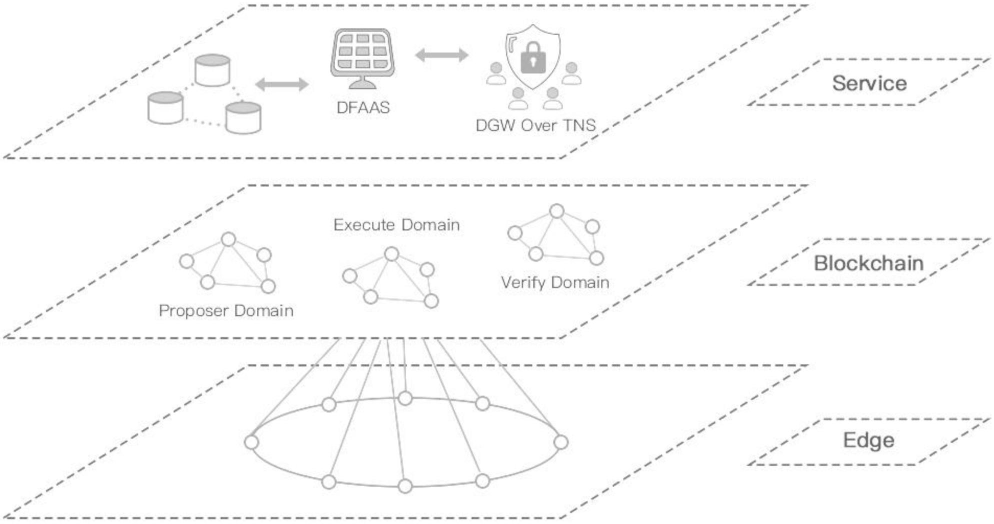

Figure 7 :Topia network

6.1 Edge Network

The edge network mainly interconnects edge devices and off-chain nodes, provides reliable data assurance for the chain layer, and can also serve as off-chain computing nodes. Edge network nodes consist of IoT devices, communication terminal devices, and off-chain computing and storage devices.

In Topia's edge network, tunneling technology is used for secure interaction between transmission devices, and it will be compressed and merged according to the content and size of the data stream. For example, some protocols will carry a large number of text characters, and compression thereof can greatly improve the transmission efficiency. For data streams carrying audio and video in the protocol, compression does not save bandwidth, but only increases CPU consumption, which reduces transmission efficiency. To improve transmission efficiency, it is also possible to combine and send data packets with a smaller amount of data.

In the edge device network, the node discovery mechanism is based on Kademlia[10], which is simple, flexible, high-performance and more secure than other DHT (Distributed Hash Table) routing algorithms.

The edge device is based on Topia's distributed storage and adopts the principle of close proximity for data storage.

In the edge network, edge devices interact with the chain layer to submit edge computing proofs. In order to speed up data transmission, some relay nodes are required to forward data between the edge network and the chain layer network, as these nodes have better stability and large bandwidth.

6.2 Blockchain Network

The blockchain network is divided into three types of node domains: Proposer Domain, Verify Domain and Execute Domain;

Each node of the same type first chooses log(n) committees in close proximity to where it belongs and then picks log(log(n)) nodes from each committee, and only stores the information of these nodes, not all nodes in the network. In this way, for the same type of nodes, each sender only sends to the target node he knows, and then the receiver sends it to the neighbor members of the committee through the broadcast protocol, in this decentralized way, we can ensure that some nodes will not be overloaded.

For nodes in different domains, log(n) other types of nodes with the closest proximity will be saved, that is, the block proposer node will save log(n) block verification nodes, and the block verification node will save log(n) block execution nodes.

Multiple block verification domains will exist. For legal block verification domains, the number of nodes in each domain will not exceed 100, but not less than 50. The newly added verification nodes follow the node joining random method shown in Figure 8:

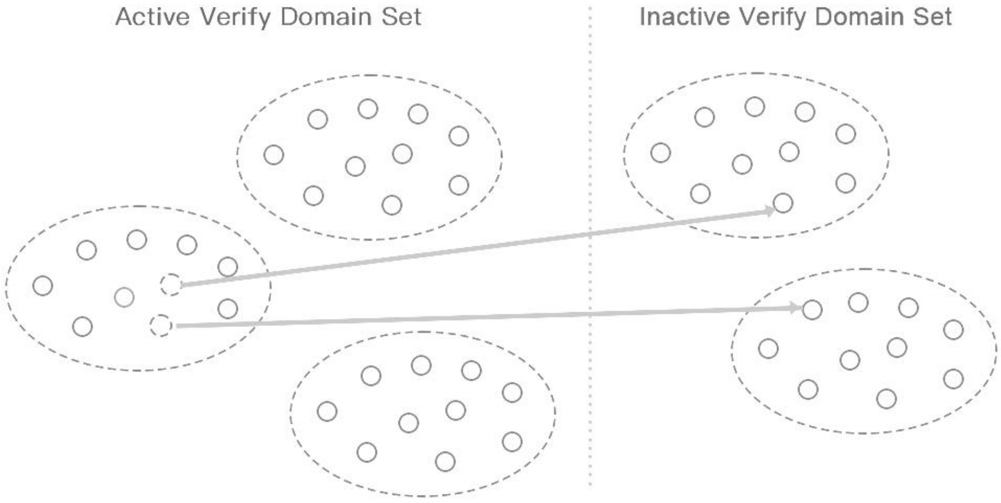

Figure 8 :Node joining random method

The verification domain as a whole is divided into the active verification domain set with the majority of active members and the inactive domain set with the majority of inactive members (active members are based on the positive contribution of verification nodes to block verification. Nodes that often go offline, periods of node network instability, or bad actors, can all be classified as inactive). When a new verification node joins, it will be randomly added to an active verification domain, and a fixed number of nodes in the domain will be randomly added to different passive verification domains. This method has the following advantages:

1. The balance of each verification domain can be guaranteed at any time; that is, the maximum number of nodes in each verification domain is O(log n), where n is the total number of verification nodes;
2. The number of city nodes in each verification domain can be guaranteed at any time; that is, the ratio of the number of honest nodes in each verification domain to the total number of nodes in the domain is not less than 0.5, thus ensuring that offline or malicious nodes are within the acceptable range, to avoid the occurrence of partition attacks.

In order to ensure stable and fast transmission between nodes, the transmission protocol will consider using quic[11]. quic has the following characteristics:

1. Using caching to significantly reduce connection establishment time;
2. Improve congestion control, congestion control from kernel space to user space;
3. Multiplexing without head of line blocking;
4. Forward error correction to reduce retransmission;
5. The connection is smoothly migrated, and the change of the network status will not affect the connection.

For the reliable information transmission of nodes, the network node reputation scoring mechanism will be used, that is, the nodes will be scored according to the stability, bandwidth, effective messaging, and data transmission success rate of the connected nodes, and the nodes connected to each other are highly scored. At the same time, for various p2p network attacks, data statistics will be carried out, and automatic and non-automatic processing measures will be taken.

6.3 Application Service Network

The application service network has two main functions in the entire Topia network:

1. providing convenient services for users to use Topia;
2. realizing decentralization at the application level;

it mainly includes:

6.3.1 TNS (Topia Name Service)

TNS is similar to the current DNS[12], but is based on the Topia blockchain, thus avoiding many shortcomings of the current centralized DNS. Its structure is shown in Figure 9:

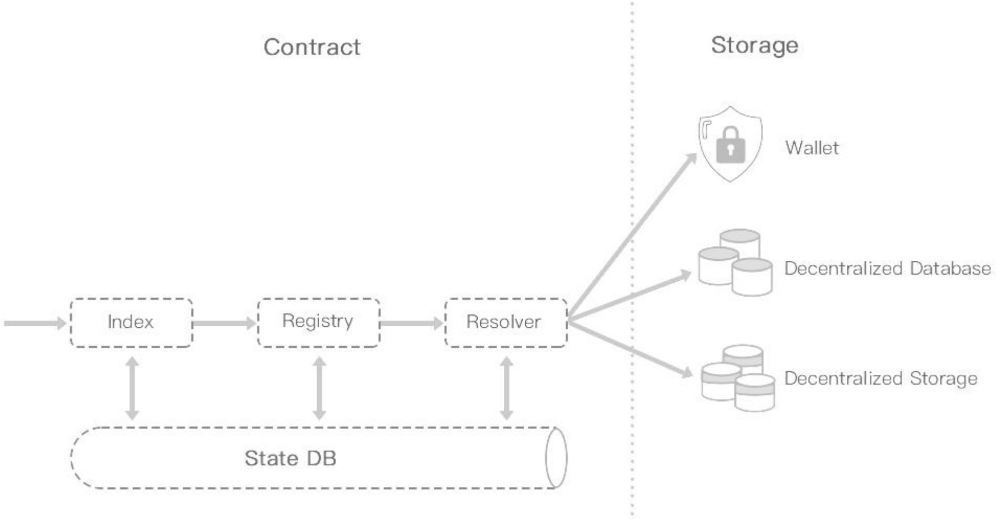

Figure 9 :Schematic diagram of TNS

TNS as a whole consists of two parts: a contract and data storage based on the Topia blockchain; the contract includes a name registration index contract, a name registration contract, and a resolution contract. Except for the first-level name Topia, each second-level name (such as x.topia) corresponds to a registry and has its unique Owner address. The registry includes all the name information and resolution contract addresses based on the second-level name. Including the specific resolution method of the name; the data content corresponding to the parsed information includes the chain address, some simple text information, and large files (such as files of a website), which are respectively stored in the wallet, Topia decentralized database, and Topia distributed storage.

In this way, TNS can map common names to wallet addresses, which facilitates the interaction with various DApps for users; in addition, users can access the sites through TNS in a way that is not controlled by third parties, thus preserving data privacy.

6.3.2 Decentralized gateway

The decentralized gateway utilizes the nature of the blockchain to provide users with a stable, reliable, and private access entry to Topia in a decentralized manner, as shown in Figure 10 below:

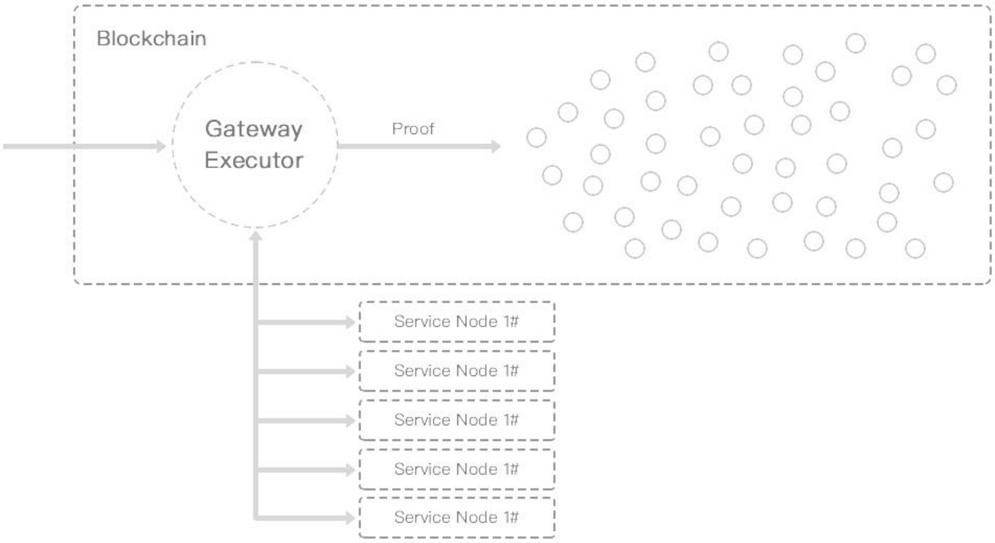

Figure 10: Topia Decentralized Gateway

Topia uses the gateway execution domain of the blockchain network as the entry point. Every time a user accesses Topia, a pair will be randomly selected from the gateway execution domain, and the executor will randomly select one from its own service node as a request-response. For the executor, a request is also called a relay. In order to ensure the reliability of the data, the gateway executor will connect to multiple service nodes, and in each epoch cycle, it will submit a relay proof to the Topia blockchain network. After passing the consensus verification, it will receive a reward in the next epoch cycle.

6.3.3 Decentralized FaaS (DFaaS, Decentralized Software as a Service)

Faas[13] is an event-driven execution model that runs in stateless containers, and these functions will leverage the services of a FaaS provider to manage server-side logic and state, as shown in Figure 11:

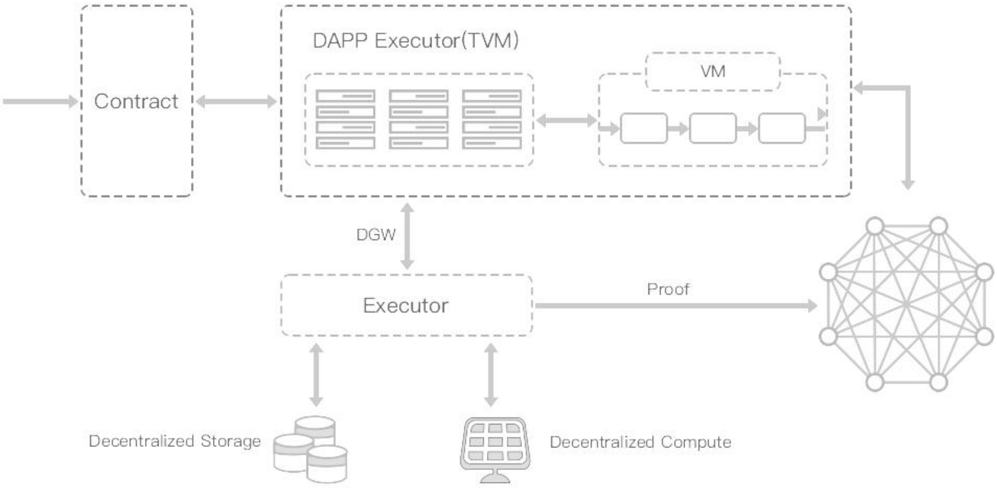

Figure 11: Schematic diagram of Topia DFaaS

Topia DFaaS is composed of a decentralized gateway, TVM built on the executor, and a blockchain network. DFaaS is triggered based on events and DWG connects users as a trigger for DFaaS. TVM extends the blockchain VM, computing based on On-chain deterministic and other non-deterministic computing, coexisting with the same DAPP container. On-chain computing is based on VM, and off-chain computing is based on Topia distributed computing and distributed storage, which can realize parallel calculation and storage. These calculations and proofs need to be submitted to the Topia blockchain in order to obtain rewards.

7. Smart Contract System

Smart contracts are user-defined transactional applications stored on the blockchain and guaranteed to execute as they were programmed. Smart contracts were first proposed by Nick Szabo: "a set of promises defined in digital form, including agreements on which contract participants can execute promises."[14][15]The Topia smart contract system is shown in figure 12:

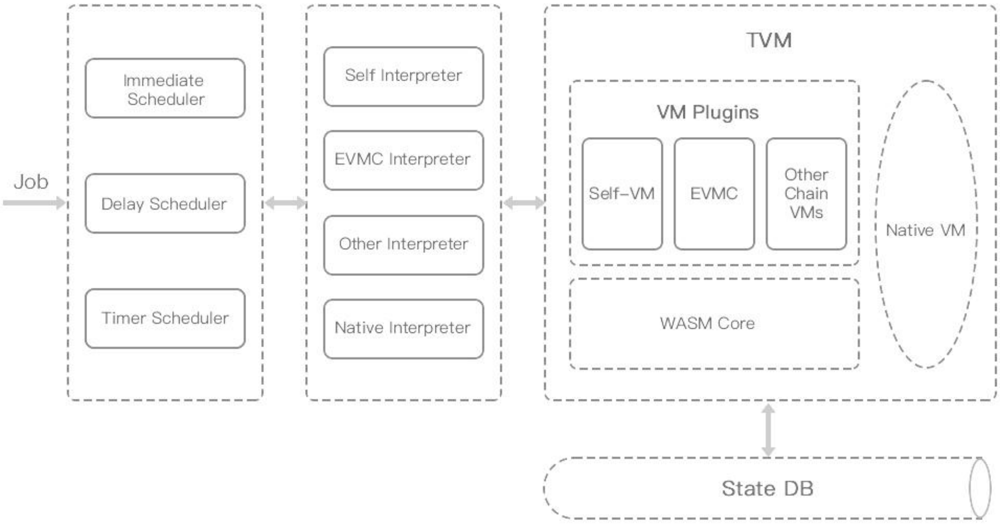

Figure 12: Topia smart contract system

The Topia smart contract system consists of job scheduler, contract interpreter, Topia virtual machine (TVM) and state DB;

7.1 Job Scheduler

The execution of the transaction becomes a Job, and the chain nodes will be put into different types of scheduler queues according to the different types of transactions; the schedulers are divided into three types:

- Immediate Scheduler: the scheduler that executes the transaction immediately;
- Delay Scheduler: the scheduler of delayed transactions;
- Timer Scheduler: the scheduler of timed transactions;

These Schedulers exist in the form of plug-ins in the architecture to adapt to the scalability of future transaction execution;

7.2 Contract Interpreter

Contracts exist in the form of bytecode, so the Job to be executed must pass the interpreter to execute the corresponding VM (Virtual Machine); according to the different VMs, the interpreter is divided into:

- Native Interpreter: Native contract Interpreter;
- EVMC Interpreter: A contract Interpreter compatible with Ethereum;
- Other Interpreter: As an extension, a contract Interpreter for other chains;
- Self Interpreter: Interpreter for Topia's own chain contracts;

These Interpreters also exist in the form of plug-ins in the architecture;

7.3 TVM

Topia virtual machine is called TVM, and consists of the following:

- Native VM
- On-chain VM, the on-chain VM is based on SSVM[16] (Second State Virtual Machine), a WebAssembly implementation provided by Second State

The two VMs provide a unified external interface that is invoked by the Interpreter and uses a unified interface to invoke the state database.

WebAssembly was invented as a client-side technology, but it has also proven to be very useful on the server-side. Server-side WebAssembly provides key advantages for modern web and service applications, namely:

1. Speed: WebAssembly achieves near-native performance. It can be 10x to 100x faster than Java, Python or JavaScript runtime. It is also much faster than docker, especially in terms of cold start and system access;
2. Security: WebAssembly is a sandbox with a capability-based security model. It is not only more secure than native binaries, but also more secure than OS-level containers such as docker; and, it provides access to the underlying system, including access to new hardware capabilities;
3. Portability: WebAssembly applications can be written in C, C++, Rust, Go and run on different operating systems and hardware platforms without changes;
4. Manageability: WebAssembly programs can be configured, started, stopped, and moved by other applications.

SSVM is developed based on standard WebAssembly, so it is faster (1000 times faster than docker in cold start), can be seamlessly integrated with existing application frameworks, and can securely access external resources (such as databases, message queues and AI hardware).

In TVM, EVMC will be integrated to fully support ethereum smart contract system, including contract language solidity, web wallet metamask, development tools remix, truffle and hardhat etc.

8. Distributed storage

8.1 System Structure

As shown in Figure 13:

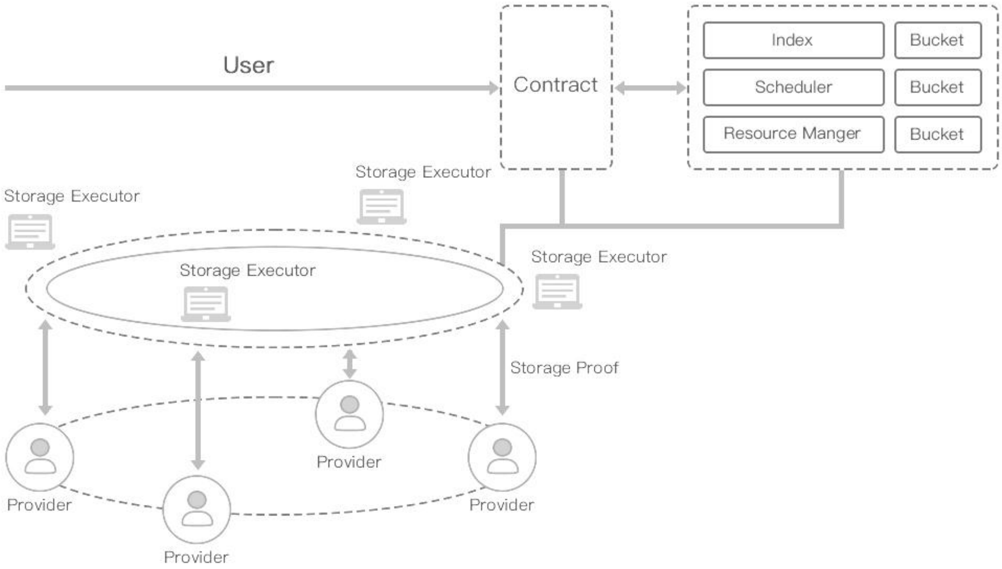

Figure 13: Topia distributed storage system structure

Storage executor maintains storage data, index metadata and performs storage resource scheduling and management.

For each user's storage request, a storage contract and corresponding bucket will be automatically created. The bucket represents a file grouping mechanism that allows all files belonging to a bucket to become part of the metadata structure, just like a file system, but only controls access at the bucket level.

In order to ensure data privacy, the specific data is randomly stored in provider storage node by the storage executor in the form of chunks, with each chunk having three redundancies. In order to effectively manage storage resources, chunk storage adopts erasure coding techniques.

According to the storage proof mechanism, the storage worker will periodically submit the storage proof to the chain; If the storage proof verification fails, the storage node will be punished;

8.2 Storage Protocol

As shown in Figure 14:

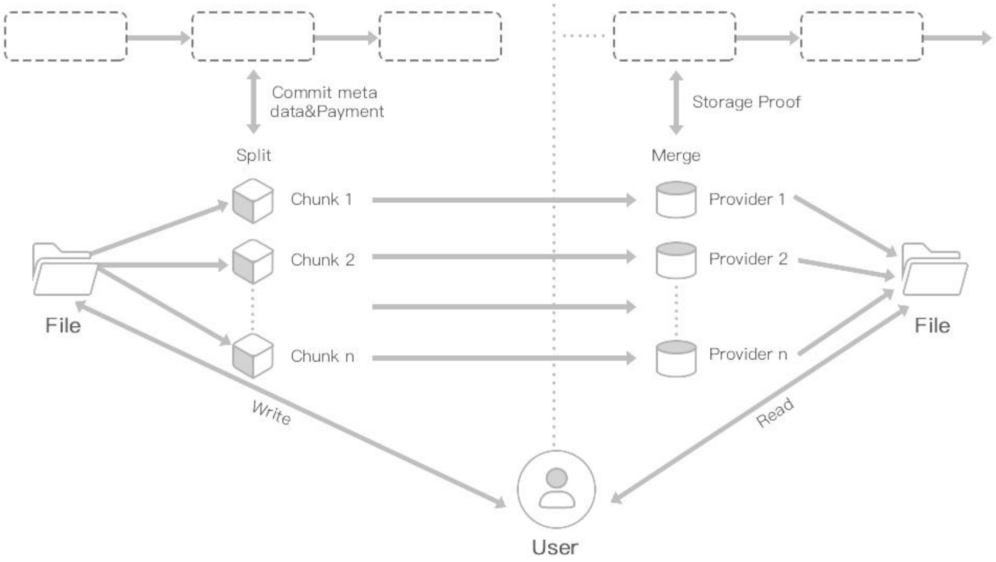

Figure 14:Schematic diagram of the storage protocol

The storage protocol is divided into the user end and the storage provider.

When a user initiates a storage data request (Write), the file is first divided into multiple chunks (the maximum size of each chunk is 256KB), and then a storage execution node is randomly selected according to the reputation of the storage provider. The execution node will select storage providers according to the reputation and resource status of each provider, pass these chunks to them, and then record the corresponding metadata on the chain.

Once the storage provider is selected, it needs to provide the storage proof to the chain periodically. Storage proof visual representation as shown in Figure 15:

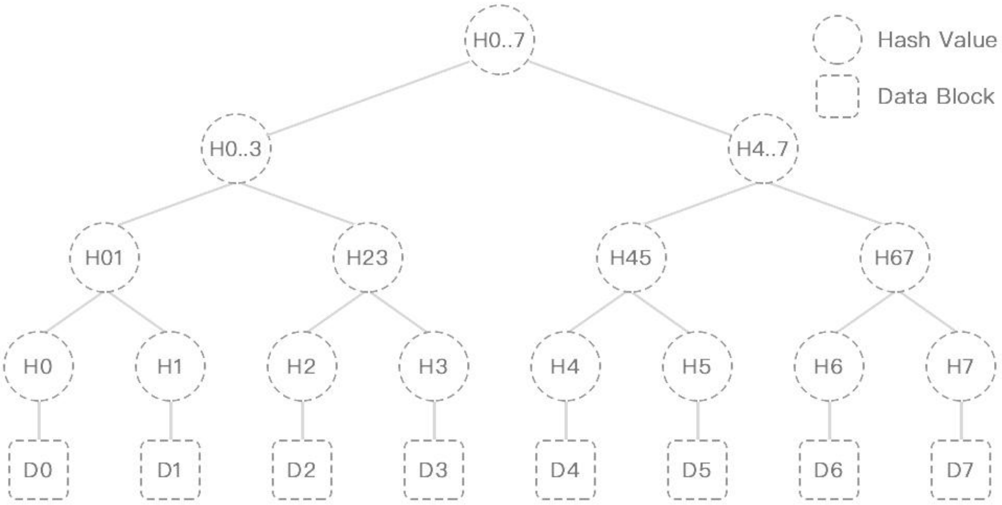

Figure 15:Schematic diagram of storage proof

The file is divided into segments of equal size and then hashed into a merkle tree; Storage hosts attest to their storage by providing a segment of the original file and a series of hashes from the file's merkle tree;

Since the proof is submitted to the blockchain, anyone can verify its validity. Each storage proof uses a randomly selected segment; and the proof has a certain validity window period, if the window period is exceeded, the proof will be considered “failed”;

When the user reads the file, the randomly selected storage executor will first search for the corresponding metadata information from the chain, then obtains the corresponding chunks according to the metadata information, and then combines these chunks into the required data.

9. Cross-chain

Cross-chain refers to the interoperability of different blockchains, but this interoperability is performed in a trustless and decentralized way. Cross-chains can be divided into cross-chain assets and cross-chain data according to their interaction content. According to the interacting chains, it can be divided into:

- isomorphic cross-chain (the interacting chains with the same security mechanism, consensus algorithm, network topology, and block verification logic, and the cross-chain interaction between them is relatively simple)
- heterogeneous cross-chain (the block and verification mechanism of the interacting chains are very different)

Most of the current blockchains only feature cross-chain assets, passing through insecure bridges. Based on the cross-chain verification node network and the cross-chain execution node network, Topia realizes the complete decentralized cross-chain in the way of BLS, and supports the cross-chain of data. The cross-chain to be discussed below is a heterogeneous cross-chain, as shown in Figure16:

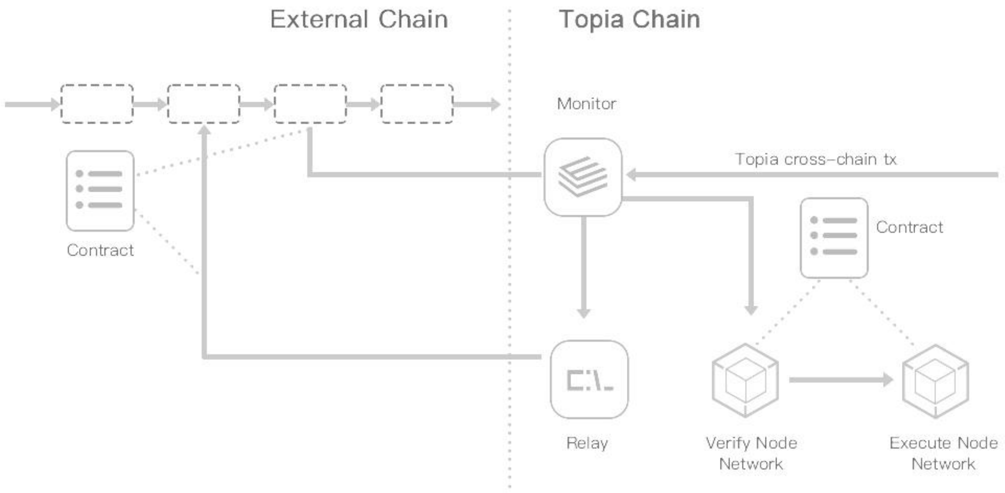

Figure 16: Topia cross-chain structure

Cross-chain functionality mainly involves the interoperability from Topia to other blockchains, and visa versa.

For the cross-chain interoperability from other chains to Topia, firstly, Topia cross-chain verification nodes once monitor the cross-chain transaction of the external chain, will verify the transaction and sign the private key, send the transaction to other randomly selected cross-chain verification node leaders, and broadcast the cross-chain transaction to the current cross-chain verification node. Other verification nodes will also verify the transaction and use their own private key to sign the transaction, and send it to the leader. Once the number of verification signatures received by the leader reaches the threshold specified by BLS, it is considered a legal cross-chain transaction and forwarded to the execution node to execute. For transactions from other chains to Topia, specifying which verification nodes monitor which chains are managed by native contracts;

For the cross-chain transactions from Topia to other chains, once Topia cross-chain verification node monitors the cross-chain transactions, it is directly relayed to other chains and recognizable transaction messages of other chains need to be constructed. After the transaction is executed successfully, Topia cross-chain verification nodes need to verify the legitimacy of the corresponding data. Specifying which verification nodes to monitor Topia's own cross-chain transactions, which are also managed by native contracts.

Cross-chain transactions need to be sent to Topia for verification and methods of verification. The verification and corresponding methods of each blockchain differ, and these will be registered and managed through Topia native contracts. Interaction with external chains mainly occurs in the form of contracts. These chains also verify the cross-chain transactions and response data initiated by Topia in the form of contracts. Cross-chain asset transfer adopts lock and mint methods. Cross-chain functionality needs to ensure the atomicity and consistency of transactions. Topia divides the entire cross-chain transaction into sub-transactions. If any transaction fails, a corresponding rollback operation will occur.

10. Privacy Computing

Topia will use the following means to preserve data privacy:

- **Zero Knowledge Proofs:** Zero knowledge proof refers to the concept where the prover can make the verifier believe that a certain statement is correct without providing any useful information to the verifier. The prover proves to the verifier and convinces it that it knows or possesses a certain message, but the proof process cannot reveal any information about the proved message to the verifier. In the blockchain, information cannot revealed usually refers to transaction information data, zero-knowledge proof can make transaction data more private, and no one except the trader can know the actual transaction information.

- **Homomorphic Encryption:** Homomorphic encryption is a cryptographic technique based on the computational complexity theory of mathematical problems. Homomorphic encryption is a method that can perform calculations without decrypting encrypted data in advance. Processing the homomorphically encrypted data to obtain an output and then decrypting this output, the result is the same output as the unencrypted raw data processed in the same way. [17]
- **Secure Muti-party Computation:** As a subfield of cryptography, secure muti-party computation allows multiple data owners to perform collaborative computations without trusting each other and guarantee that any party can not obtain any other information other than the calculation results due.[18] In other words, MPC technology can obtain the use value of data without revealing the original data content. The advantages of input privacy, calculation correctness, decentralization and other advantages of secure multi-party computing combined with blockchain can form the next generation of general computing platforms.
- **Proxy Re-Encryption:** In the proxy re-encryption method, the ciphertext of one user is converted that can be decrypted by another user through the proxy server, without revealing the user's private key and text information. This method is mainly used in end-to-end interactions. Proxy re-encryption solves the problems of encryption and non-interaction sharing of private data, as well as shared rights management. Proxy re-encryption combined with smart contracts can be used in trustless decentralized networks.

11. Governance and Economic Models

11.1 Governance

Among the main aspects of governance are software upgrade proposals, protocol upgrades, adjustments of economic parameters, network optimizations, and changes in incentives distribution plans. Governance participants include governance committee, community members, technical teams, investment institutions and TOP holders. Topia follows the following aspects in governance rules:

- **Decentralization:** Topia is a permissionless blockchain. This property allows Topia users to be autonomous. As stakeholders may not be willing to take responsibility for decision-making, and may require negotiation to reach agreements, conflicts of interest may become apparents. Therefore, permissionless blockchains often need to increase governance participation through incentives and utilize consensus mechanisms for final confirmation.
- **Transparency:** Ensuring the transparency of the decision-making process is crucial in blockchain governance, and stakeholders can monitor whether the decision is reasonable, thereby gaining the trust of the entire community. When a decision is made on-chain, the blockchain can help record the entire process. If there is an off-chain decision, it will take place in a formal channel open to relevant stakeholders. Whether on-chain or off-chain, when allocating decision-making power, both seek to enhance fairness and democracy from diverse stakeholders.
- **Supporting governance at the ecosystem level:** Governance is not only positioned on the Topia platform itself, but also needs to support the broader environment of the entire ecosystem. The chain ecosystem includes the underlying on-chain data, the superstructure of the blockchain-based application system, and the entire community composed of different stakeholders.
- **Compliance, social and ethical responsibility:** Compliance mainly includes local government regulatory requirements. Complying with the General Data Protection Regulation (GDPR) to protect personally identifiable information. Transactions and information included in the blockchain should ensure data quality and avoid malicious on-chain information.

11.2 Economic Model

11.2.1 TOP Token

As the native currency of Topia, TOP, plans to have a total issuance of 5 billion. 70% of the supply are generated by new blocks, and the remaining 30% will be further subdivided as follows:

Institutional investors : 25%, 375,000,000 TOP
Operations and marketing: 10%, 150,000,000TOP
Team: 20%, 300,000,000TOP
Community development: 20%, 300,000,000TOP

Foundation reserve: 25%, 375,000,000TOP

The initial unlocked amount will be 100,000,000 TOP, and 3% will be released every year thereafter. The TOP generated by blocks is 100,000,000 TOP in the first year, and then 90% of that in the next year, and following the second year, the inflation rate will stablelize at 3%. The ratio is controlled at 100,000,000 TOP; the inflation rate in the first year will be relatively high, about 30%.

TOP token is mainly used in the following aspects:

- Transaction fee, the minimum fee for each transaction is 0.00005 TOP;
- Node collateral fee;
- The cost of purchasing storage and computing power;
- Service fees, including fees for Decentralized Gateway (DGW), Decentralized Faas (DFaaS) and TNS;
- Block rewards;
- Developer rewards.

11.2.2 Node Weight

The entire Topia network is divided into the following node types:

Block proposer node: block producing node. Each round is elected by VRF, and this node type has a minimum requirement of 50 W(Weight).

Verification node: verify the proposed block in each round, with a minimum requirement of 200 W.

Execution node: nodes for round execution, including transaction execution nodes, service execution nodes, storage execution and scheduling nodes, computing execution and scheduling nodes, with a minimum requirement of 500 W.

Storage node: nodes that store various data and documents, with a minimum requirement of 1000 W;

Computing node: nodes that perform large computations, with a minimum requirement of 1000 W.

Topia uses a combination of Staking (S), Reputation (R) and Contribution (C_r) to determine the weight of a node:

$$W = \alpha S/10 + \beta R + \gamma C_r$$

Among them, α, β and γ are the weighting factors. In the initial stage of the mainnet, α and γ are set at 0.4, and β at 0.2. It will be adjusted according to the operational phases through the contract. S/10 means every 10 TOPs can be converted into 1 W, and the value of R is equivalent to W, and it is calculated as follows:

$$R = \sum_{i=1}^{n} R_i P_i + R_0 \ (i \geq 1)$$

R*i* is the reputation value of the *i*th item of the node, P*i* is the weight factor of the corresponding item, and the initial value of R_0 is 10. The factors affecting the reputation of nodes are:

- Double signature, deduction of 100;
- If a node is offline while it is their turn to execute, deduction of 50;
- Delayed network response, deduction of 20;
- If the correct storage and calculation proof is not provided, deduction of 50;
- Joint cheating, deduction of 50;
- Each epoch executed correctly, reward of 5：

The formula for calculating resource contribution is as follows:

$$C_r = tS + zQ$$

Among them, S is the effective data storage size per 1 T, Q is the computational power size per 1 KTCP/s , TCP/s is the computational power calculated by the Topia algorithm, 1 MTCP/s = 1000 KTCP/s = 1,000,000 TCP/s. *t* and *z* are weight factors, which are adjusted through the contract, and the initial value of t and z for all nodes in the mainnet are 1.

11.2.3 Calculation of Fees

The types of fees included in the Topia network are transaction fees, storage fees, and computing fees.

- **Transaction Fee:** The fee to process a transaction which includes sending tokens and executing a smart contract interaction.

  (TxSize * Gas/Byte + SmartGas) * GasPrice

  TxSize represents the size of the data contained in the transaction. SmartGas represents the actual gas consumed by the contract execution. The calculation of Gas is determined by the consumed CPU computing power, storage, and network. GasPrice must be greater than or equal to the specified minimum value. 20% of the transaction fee will be awarded to block proposers and 80% will enter the fee fund pool. The fee fund pool is used as part of the reward funds for Topia's ecological growth requirements.
- **Storage fee:** The storage fee is paid according to the size of the valid data stored by the storage provider. The minimum unit denomination is KB, data less than 1KB will be stored on the chain. Currently, the provision is 10 TOP/KB. The value can be dynamically adjusted through the native contract.
- **Computation fee:** The storage fee is paid according to the actual computing power consumed by the storage provider. Currently, 10 TOP/KTCP is temporarily specified, and this value can be dynamically adjusted through the native contract.

11.2.4 Rewards and penalties

Rewards include the following:

- **Block reward:** The block determined in each round will generate a certain number of TOP tokens, the value is dynamically adjusted by the contract according to the actual situation, and these rewards are distributed according to the following proportions:
  - Block Proposer: 30%
  - Block Verifier: 40%
  - Executor: 30%

Because the block verifier reward is shared by multiple nodes, it will occupy a larger proportion;

- **Additional rewards for nodes:** every 30 epochs (one epoch is currently set to be 24 hours), the native contract on the chain will automatically award the top 10 nodes with varying amounts of TOP tokens

Penalties include the following aspects:

The following consensus nodes (including proposing nodes, validating nodes and executing nodes) are all subject to different levels of fines:

- Double-signing blocks of the same height, confiscation of 5% of the total number of TOP tokens staked by nodes.
- Nodes selected for execution with delays or offline are subject to a penalty of 0.01% of the total number of TOP staked by nodes.
- Storage nodes and computing nodes failing to submit timely proofs are subject to a penalty of 0.05% of the staked amount.; if the number of failed submissions reaches 50% of the required submissions within 30 epoch cycles, all staked TOP will be confiscated.
- After verification, if the storage proof and calculation proof are wrong, 0.02% of the node stake will be confiscated. If the number of errors reaches 50% of the required submission times within 30 epoch cycles, all the staked TOP will be confiscated.

  50% of the confiscated TOP referred to above will be burned without reporting, and the remaining 50% will enter the fee fund pool.

11.2.5 Resource Service Trading Market

As shown in Figure 17:

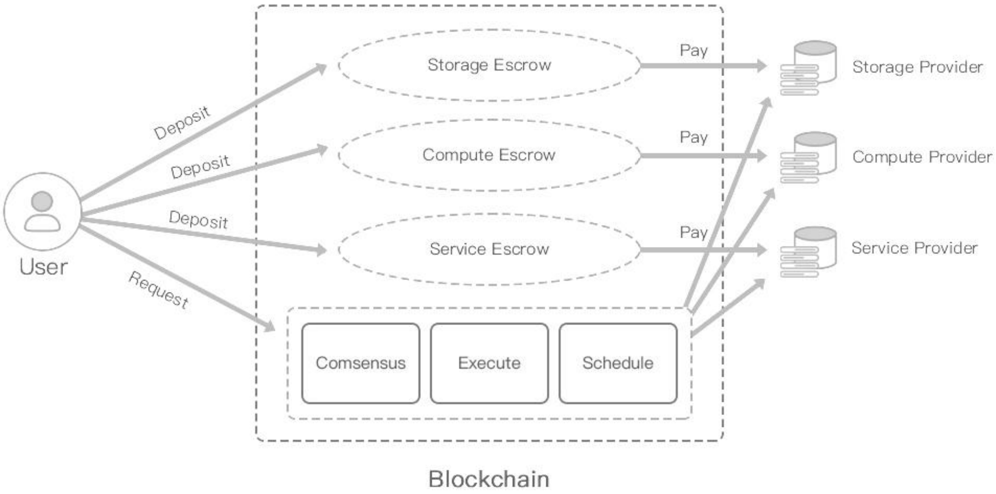

Figure 17: Resource Service Trading Market

Users who have a demand for resources (storage and computing) and services (services provided by the application network layer) in the resource service trading market, firstly, need to deposit enough TOP to the corresponding escrow contract, and then proceed to initiate a request transaction to the Topia blockchain.

Within an epoch, if Topia receives the service provider’s proof for the first time, that is, it proves that the provider has provided the corresponding service to the user, the escrow contract will pay the provider 25% of the TOP payable in each epoch.

After the payment is completed, the user can withdraw the remaining TOP from the escrow contract; if the TOP in the escrow contract is insufficient, the provider has the right to suspend the user's service.

References

[1] Weik, M. H. (1961). The ENIAC Story. Ordnance, 45(244), 571–575. Retrieved from http://www.jstor.org/stable/45363261

[2] Lipton, A., & Treccani, A. (2021). Blockchain and Distributed Ledgers: Mathematics, Technology, and Economics(pp. 205-232). World Scientific.

[3] Canorea, E. (2022, January 20). Web 3.0: The New Internet Revolution. Plainconcepts. Retrieved from https://www.plainconcepts.com/what-is-web-3/

[4] Robertson, A., & Peters, J. (2021, October 4). WHAT IS THE METAVERSE, AND DO I HAVE TO CARE? One Part Definition, One Part Aspiration, One Part Hype. Theverge. Retrieved December 29,2021, from https://www.theverge.com/22701104/metaverse-explained-fortnite-roblox-facebook-horizon

[5] Zakas, N. C. (2011, November 29). How Content Delivery Networks (CDNs) Work. Humanwhocodes. Retrieved September 22,2015,from https://humanwhocodes.com/blog/2011/11/29/how-content-delivery-networks-cdns-work/

[6] Girdzijauskas, Š., Datta, A., & Aberer, K. (2010). Structured overlay for heterogeneous environments: Design and evaluation of oscar. ACM Transactions on Autonomous and Adaptive Systems (TAAS), 5(1), 1-25. doi:10.1145/1671948.1671950.

[7] Pedersen, T. P. (1991, April). A threshold cryptosystem without a trusted party. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 522-526). Springer, Berlin, Heidelberg.

[8] Wong, T. M., Wang, C., & Wing, J. M. (2002, December). Verifiable secret redistribution for archive systems. In First International IEEE Security in Storage Workshop, 2002. Proceedings. (pp. 94-105). IEEE.

[9] Goldberg, C. S., & Vcelak, J. (2019). Verifiable Random Functions (VRFs).Retrieved from http://www.watersprings.org/pub/id/draft-irtf-cfrg-vrf-04.html

[10] Maymounkov, P., & Mazieres, D. (2002, March). Kademlia: A peer-to-peer information system based on the xor metric. In International Workshop on Peer-to-Peer Systems (pp. 53-65). Springer, Berlin, Heidelberg.

[11] Iyengar, J., & Thomson, M. (2021). RFC 9000 QUIC: A UDP-Based Multiplexed and Secure Transport. Omtermet Emgomeeromg Task Force. doi:10.17487/RFC9000. RFC 9000.

[12] Dilley, J., Maggs, B., Parikh, J., Prokop, H., Sitaraman, R., & Weihl, B. (2002). Globally distributed content delivery. IEEE Internet Computing, 6(5), 50-58.

[13] Avram, A. (2016). Faas, paas, and the benefits of the serverless architecture. InfoQ, Jun, 25.

[14] Morris, D. (2016). Bitcoin is not just digital currency. It’s Napster for finance. Fortune.Retrieved November 7,2018,From https://fortune.com/2014/01/21/bitcoin-is-not-just-digital-currency-its-napster-for-finance/

[15] Schulpen, R. R. W. H. G. (2018). Smart contracts in the Netherlands: A legal research regarding the use of smart contracts within Dutch contract law and legal framework. Master, TILBURG UNIVERSITY.Retrieved October 26, 2019,from http://arno.uvt.nl/show.cgi?fid=146860

[16] SSVM: https://github.com/qaz1wsx/SSVM

[17] Coron, J. S., Mandal, A., Naccache, D., & Tibouchi, M. (2011, August). Fully homomorphic encryption over the integers with shorter public keys. In Annual Cryptology Conference (pp. 487-504). Springer, Berlin, Heidelberg.doi:10.1007/978-3-642-22792-9_28. ISBN 978-3-642-22791-2.

[18] Yao, A. C. (1982, November). Protocols for secure computations. In 23rd annual symposium on foundations of computer science (sfcs 1982) (pp. 160-164). IEEE.