SKYRIM NETWORK

A Data Asset Network of distributed ledgers

Abstract

The aim is to describe why the Skyrim Network is created, what defines Skyrim Network and how it works. To build a trusted basis of the future globe, we have to solve the core data problem of finance and technology infrastructure.

To transact the data asset, we build a trusted network integrated with blockchain technology. The Skyrim Network core is a data protocol deployed on blockchain and its asset platform addresses security, capacity and reliability contradictions. Leveraging decentralized community services, governance and economics, we create a trusted data transactional ecosystem for digital generation.

This text is not intended to be the reference with respect to implementation details. Some particulars are going to change with the development and application phases.

Contents

1. Introduction & Overview

1.1 Introduction

Data is the real asset in digital world, also will be the most valuable asset for human future. Internet of Information realizes a variety of connection scenarios, such as connection between people-people, people-information, people-goods and people-things. The connections persistently produce valuable data asset. The decline in hard drive prices, the increase of cloud storage capacity and the optimization of Communications Protocol have significantly improved the efficiency of data production and reduced data storage costs.

Nevertheless, the gathered data do not bring a plenty of values to different industries but a lot of hidden troubles of data security, owing to the isolation of data and the lack of secure data streaming. A huge amount of data generated by users is dominated by various centralized organizations like Facebook, Amazon, Alibaba, Paypal, JP Morgan and Centralized Banks. The central platforms can make a profit from the user's data. However, it is the users who produce these data but not the organizations. There are many problems with the security and effective use of data assets among individuals and enterprises that generate and hold data. Also, for institutions handling with a big size assets, are faced with reliability problems. It is still challenging for them to seek a stable platform to store assets. The problem will be more serious when the data involves high-value private data, such as financial data, personal transaction data, etc.

The Skyrim Network project is dedicated to building a Data Asset Network of distributed ledgers. The project aims to provide a scalable and decentralized public chain together with a side chain system, an aggregated Communications Protocol and an optimized developer toolkit. It will help users and enterprises authentically store the data assets more secure. Moreover, it will make data streaming and collaboration more effective. So that stimulates data assets will generate more liquidity and encourage more data assets, then powered with AI technology, the future world will be more secure, incentive and reliable for real value creators. In data we empowered creations.

1.1.1 Current Problems of Data Assets Industry

Data Asset Security

With the continuous rise of data assets value and progressive grow of the big data market size, big data technology is not only bringing about improvement to social production and life, but also security issues. In January 2017, first floor big data software fell into a massive ransomware attack in which Hadoop cluster were targeted by hackers. At the same time, a study conducted by Shodan (an Internet-connected device search engine) revealed that nearly 4,500 servers with the Hadoop Distributed File System (HDFS) were found to expose 5,120 TB (5.12 PB) of data. A great number of global data security incidents have emerged in recent years. How to deal with data security issues in the era of big data has become a hot topic in the world.

For ordinary users, data leakage may be just receiving some harassing calls or scam calls. They only need to change their account password settings in most cases. In comparison, the data leakage for enterprises are serious. If the leakage involves the data of important client, design drawings or core technical data, then it might bring fatal crisis to the enterprise.

2. Data Privacy Violation

Social software, such as WeChat, Facebook and Twitter, is able to control the social relationships of users. The monitoring system records chat history, browsing history and travel history. Also, online payment and shopping websites history can track people's consumption behavior. In the era of big data, the threats faced by people are not limited to privacy leaks, but also the prediction of user's state and behavior based on the big data. These deliberate analyses and predictions may pose greater potential threats to the privacy of users.
Recently, the incident of 50 million Facebook profiles harvested for Cambridge Analytica in major data breach has triggered a crisis of public trust in Facebook's commitment to privacy and data protection. Multinational regulators have initiated investigation procedures.

As one of the world's largest social networking platforms, the success of Facebook's business model is based on more than 1.4 billion active users and an open platform built with massive third-party applications. The new economic model based on personal data determines that the profit of Internet platforms (such as Facebook) mainly comes from the analysis, utilization and sharing of massive user data.

3. Transactional Capacity

Big data has great value for risk control and marketing. Traditional retail financial institutions tend to record some descriptive data such as transactions and sales data only, but this part of data has not been fully utilized. From the bank's point of view, when users make online payment or swipe their physical bank card in offline retail stores, these consumption data will enter the banking system. Previously, the bank only focused on simple credit card records, there was no in-depth analysis. However, these comprehensive data, including financial data, consumption data, behavioral data, etc., from small data to big data, from static data to dynamic data, from thin data to thick data, is not so easy to collect. It is necessary to ensure the streaming and collaboration of data, thereby realizing data's maximum value.

In this industry, capacity also limits institutions' further application of data asset management. When big players like Paypal also wants to tackle with problems and use some chain services, it will be faced with lack of partners qualified in providing the capacity to support the huge network and tons of transactions. We expect better chain services with better performance in TPS and stability can bridge more providers and real needs.

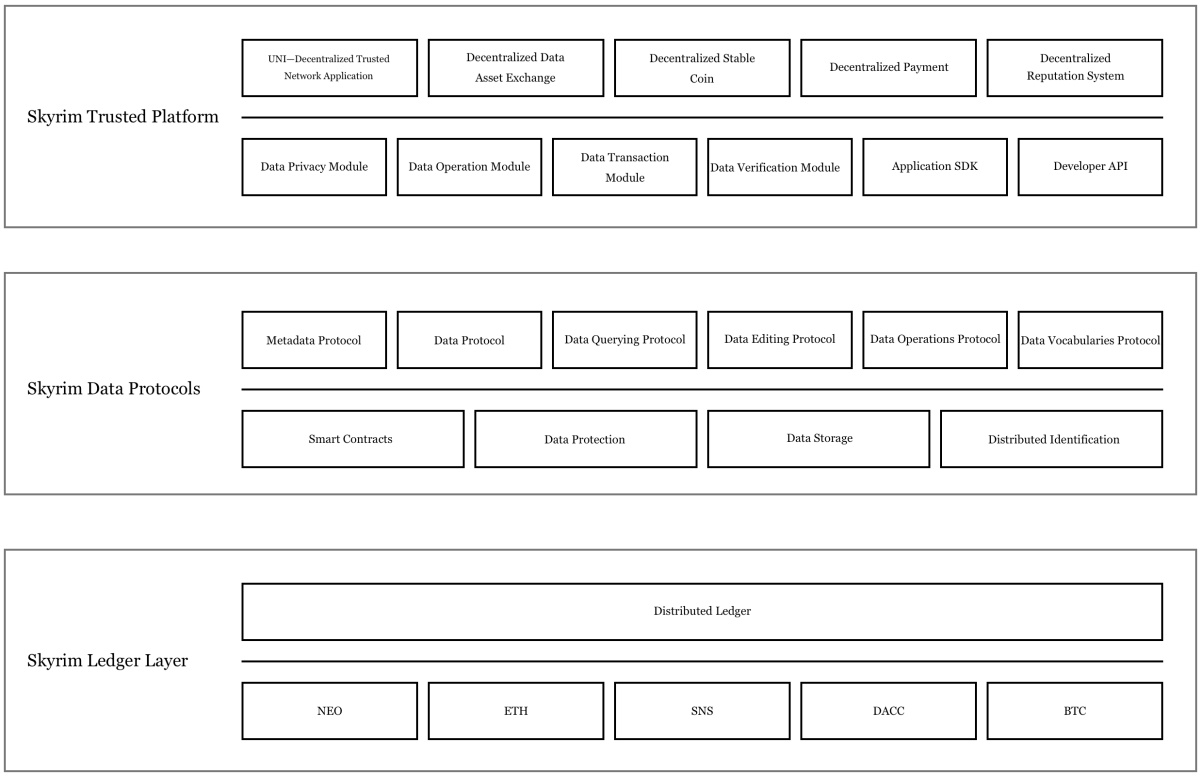
4. Reliability of Value Storage

Leading global financial institutions, such as JP Morgan, Fidelity, etc. have not found the best solution to store high value financial data in a convincing way. Ordinary data storage solutions cannot provide secure and stable services to these key financial clients with data relating to huge transaction numbers and surrounding high risks. When critical financial

players seriously seek a solution to combine their data with chain services. So far there is not a mature solution to meet their needs.

Therefore, we determined to create an infrastructural solution for data asset problem, and designed a trusted network protocol for data assets transaction in different layers to implement it and govern the ecosystem better.

1.2 Skyrim Network Architecture Overview



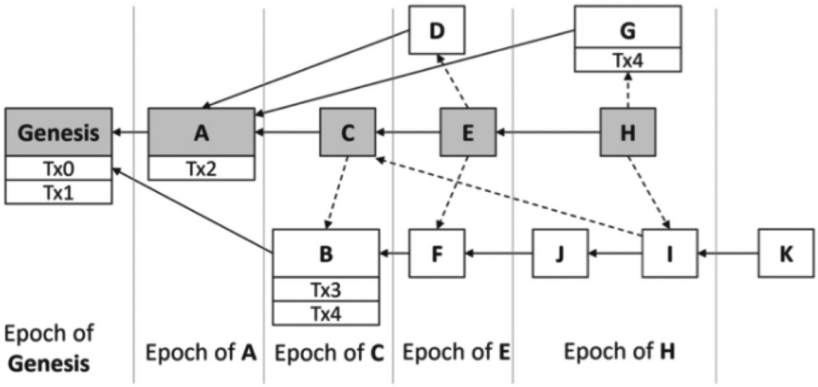
We display the architecture overview as the picture as below:

1.2.1 Skyrim Network Chain Structure

The Skyrim Network chain will support an ecosystem with tech highlights as well as support various services and DApps.
We present our blockchain structure as below:

Skyrim Network is a fast, scalable and decentralized blockchain system that optimistically process concurrent blocks without discarding any forks. Skyrim Network consensus protocol represents relationships between blocks as a direct acyclic graph and achieves consensus on a total order of the blocks. Then, Skyrim Network, deterministically derives a transaction total order as the blockchain ledger from the block order.

1.2.2 DHT P2P Network



We will use the DHT P2P Network as the major mechanism. A distributed hash table (DHT) is a class of a decentralized distributed system that delivers a lookup service similar to a hash table: (key, value) pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key. Keys are unique identifiers which map to particular values, which in turn can be anything from addresses, to documents, to arbitrary data. Responsibility for maintaining the mapping from keys to values is distributed among the nodes, in such a way that a change in the set of participants causes a minimal amount of disruption. This allows a DHT to scale to extremely large numbers of nodes and to handle continual node arrivals, departures, and failures.

DHT research was originally motivated, in part, by peer-to-peer systems such as Freenet, Gnutella, BitTorrent and Napster, which took advantage of resources distributed across the Internet to provide a single useful application. Particularly, they took advantage of increased bandwidth and hard disk capacity to deliver a file-sharing service.

These systems differed in how they located the data offered by their peers， but some central components are exposed to attacks.

DHTs normally emphasize the following properties:

- Autonomy and decentralization: the nodes collectively form the system without any central coordination.
- Fault tolerance: the system should be reliable (in some sense) even with nodes continuously joining, leaving, and failing.
- Scalability: the system should function efficiently even with thousands or millions of nodes.

A key technique used to achieve these goals is that any one node needs to coordinate with only a few other nodes in the system, so that only a limited amount of work needs to be done for each change in membership.

Some DHT designs seek to be secure against malicious participants and to allow participants to remain anonymous, though this is less common than in many other peer-to-peer (especially file sharing) systems; see anonymous P2P.

Finally, DHTs must handle more traditional distributed system issues such as load balancing, data integrity, capacity, and performance (in particular, ensuring that operations such as routing and data storage or retrieval complete quickly).

The structure of a DHT can be decomposed into several main components. The foundation is an abstract keyspace, such as the set of 160-bit strings. A keyspace partitioning scheme splits

ownership of this keyspace among the participating nodes. An overlay network then connects the nodes, allowing them to find the owner of any given key in the keyspace.

Once these components are in place, a typical use of the DHT for storage and retrieval might proceed as follows. Suppose the keyspace is the set of 160-bit strings. To index a file with given filename and data in the DHT, the SHA-1 hash of filename is generated, producing a 160-bit key k, and a message put (k, data) is sent to any node participating in the DHT. The message is forwarded from node to node through the overlay network until it reaches the single node responsible for key k as specified by the keyspace partitioning. That node then stores the key and the data. Any other client can then retrieve the contents of the file by again hashing filename to produce k and making any DHT node find the data associated with k with a message get. The message will again be routed through the overlay to the node responsible for k, which will reply with the stored data.

1.2.3 Skyrim Network Layer2

The Skyrim Network layer 2, as the physical infrastructure layer of Skyrim Network, is a P2P network provided and maintained by miners. It has two sub-networks.

- Skyrim Network Chain are consisted of a main chain and multiple service chains. It provides ledger, payment service and cryptocurrency for the Skyrim ecosystem.
- Skyrim Network Side Chain is a processor and ledger that stores and processes business data off the chain in a trustworthy manner, thereby reducing the workload and frequency of data processing on the blockchain ledgers.

1.2.4 Skyrim Network Data Protocols

Skyrim Network provides support of crypto asset trading. It is characterized by flexible pricing, which can make pricing and distribution flexibly. The entire trading process is automatic, there is no manual interference.

1.2.5 Skyrim Network Application Platform

Skyrim Network has the standard Library, chain service (Chain Data, Search, Indexing, and Value Ranking, Storage) It also supports Smart Contract tools.

Through creating a full suite of developer tools, end users, companies and research groups are allowed to easily create DApps for various purposes. Skyrim Network's DApp development framework will use simple and easy to use modular tools and functions to abstract the process of DAPP creation. Any token fee, incentive and reward system can be created and implemented to suit the needs of the content application and ecosystem being created as fully customizable token economy templates will be included. Skyrim Network's wallet application can provide a simple and easy solution for token transfer and storage with Skyrim Network DAPP through seamlessly integrating into any DAPP built on Skyrim Network's public chain.

1.2.6 Performance

The public chain performance is supported by following characteristics:

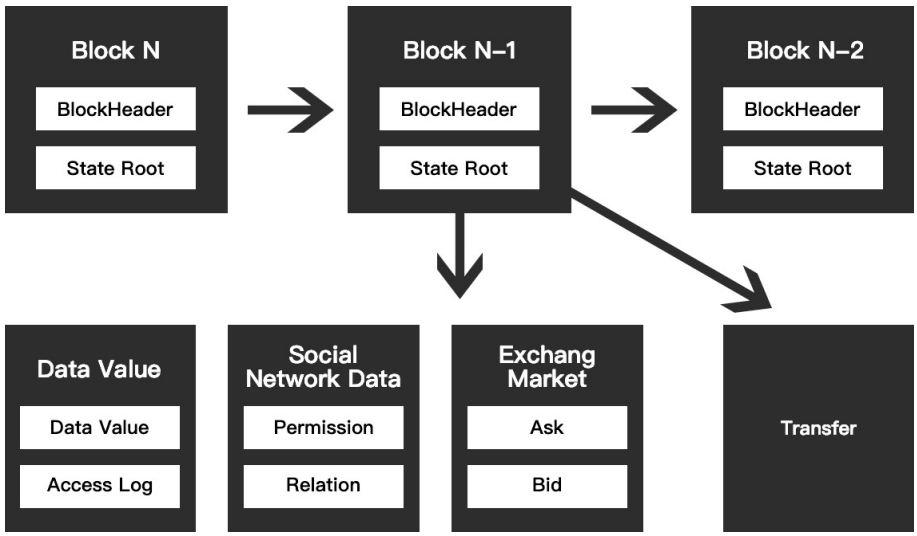
- Public Chain : Skyrim Network Chain on Amazon EC2 clusters with up to 20k full nodes. Skyrim Network Chain achieves a transaction throughput of 5.76GB/h while confirming transactions in 4.5-7.4 minutes. For typical Bitcoin transactions, the throughput is equivalent to 3000 ~ 6000 transactions per second. Our results also present that when running Skyrim Network, the consensus protocol is not the throughput bottleneck anymore. Instead, the bottleneck is at the processing capability of individual nodes.
- A new consensus model based on data value.
- User data security and privacy protection on the basis of access control contract.
- Side Chain: document storage, data index and news services.

2. Skyrim Network Ledger Layer

2.1 Skyrim Network Chain Structure

The Skyrim Network blockchain is a shared ledger records global states updated by transactions in Skyrim Network.
In general, the blockchain structure adapted by Skyrim Network consists of two components - a block header with a state root and a list of records (shown in Figure 3).

- Block Header
  Each block header provides a unique summary to the entire data (containing globe state and activity details) at current block. It is preserved in order with necessary information.
- Records
  Skyrim Network Chain stores not only transaction records in state root component, but also data values, social network data and exchange market data. This modification supports Skyrim Network realizing data value measurement and social network relation mapping, as well as providing a decentralized asset market.



2.1.1 Blocks

Blocks store all the on-chain information of Skyrim Network. A Block in Skyrim Network Blockchain consists of a block header, a list of comprised transactions Ts and a list of other unreferenced block headers, is denoted by

$B \equiv (BH, BTs, BU)$,
where
Note:
We call unreferenced block headers as *ommer* blocks or simply *ommers*.

- **Block Header, H**

The block header H is a collection of relevant pieces of information:

1. *parentHash*: The Keccak 256-bit hash of the parent block's header, denoted by

H*p* and H*p* ∈ B256.

1. *ommersHash*: The Keccak 256-bit hash of the ommers list part of the block, denoted by

H*o* and H*o* ∈ B256.

1. *beneficiary*: The account address of the participant who will receive a reward caused by successfully mined the block, denoted by

H*c* and H*c* ∈ B160.

1. *transactionRoot*: The Keccak 256-bit hash of the root node of the trie generated from the transaction list part of the block, formally denoted by

H*t* and H*t* ∈ B256.

1. *stateRoot*: The Keccak 256-bit hash of the root node of the state trie after all *stable transactions* are executed and finalized, denoted by

H*r* and H*r* ∈ B256.
Note:
Stable transactions are the transactions which were included in the blocks of past 5 epochs of pivot block, i.e. in .

1. *receiptsRoot*: The Keccak 256-bit hash of the root node of the trie generated from the receipts of each transaction executed when updating stateRoot of the block, denoted by

H*e* and H*e* ∈ B256.

1. *logsBloom*: The Bloom filter composed from indexable information (logger address and log topics) contained in each log entry from the receipt of each transaction in the transaction list, formally H*b*.
2. *difficulty*: A scalar value refers to the mining difficulty level of the current block, denoted by

H*d* and H*d* ∈ N64.
It is calculated from the previous block's *difficulty* and the *timestamp* and

1. *height*: A scalar value equals to the the number of parent blocks referred to reach the genesis block, denoted by

H*h* and H*h* ∈ N32.
Note:
The height the genesis block equals to 0.

1. *GasLimit*: A scalar value equals to the maximum amount of gas allowed in the current block, denoted by

Hl and Hl ∈ N64.
It is used to determine how many transactions can fit into the block.

1. *timestamp*: A scalar value equal to the number of seconds since the first of January 1970 (i.e. the output of Unix's time())at the inception of the block, formally denoted by

H*s* and H*s* ∈ B64.

1. *extraData*: An arbitrary byte array containing data no more than 32 bytes relevant to this block, denoted by

H*x* and H*x* ∈ BY32.

1. *Nonce*: A 64-bit hash is used to prevent a sufficient amount of computation has been carried out on the block, denoted by

H*n* and H*n* ∈ B64.

- **Well-formed Blocks**

A Skyrim Network block B (with header H = H(B)) is *well-formed* if and only if it is internally consistent and satisfies the following conditions:

$$Ho \equiv \text{KEC}(\text{RLP}(LH^{*}(\text{BU})))$$
$$\wedge\ Ht \equiv \text{TRIE}(\forall i < ||\text{BTs}||, i \in \mathbb{N} : (\text{RLP}(i), \text{RLP}(LT(\text{BTs}[i]))))$$
$$\wedge\ He \equiv \text{TRIE}(\forall i < ||\text{BR}||, i \in \mathbb{N} : (\text{RLP}(i), \text{RLP}(LR(\text{BR}[i]))))$$
$$\wedge$$

Intuitively, a well-formed block B has a header H consistent with the data stored in B. In other words, H effectively summarized the contents in the whole block B.

- **Serialization**

Recall the preparation function for transaction LT defined in previous discussion, we define another two preparation functions *LB* and *LH* for a block and block header respectively to assert the types and order of the structure as following:

$LH(\mathrm{H}) \equiv (\mathrm{H}p,\mathrm{H}o,\mathrm{H}c,\mathrm{H}r,\mathrm{H}t,\mathrm{H}e,\mathrm{H}b,\mathrm{H}d,\mathrm{H}h,\mathrm{Hl},\mathrm{H}g,\mathrm{H}s,\mathrm{H}x,\mathrm{H}n)$

$LB(\mathrm{B}) \equiv (LH(\mathrm{BH}),L\mathrm{T}^*(\mathrm{BTs}),LH^*(\mathrm{BU}))$,

where $L\mathrm{T}^*$ and LH^* refers to element-wise sequence transformations as before,
and the component types are defined as

In order to further serialize the block structure defined above into a sequence of bytes ready for transmission and storage, the RLP transformation can be adopted.

- **Valid Blocks**

Given a block B, the validity of the header of B is checked by whether the fields of BH follow the definitions and rules:

- the *height* is increased by one;
- the *timestamp* (in Unix's time()) is increased;
- the canonical *Gaslimit* does not change significantly (i.e. more than 1/1024) and it remains above 5000;
- the mining *difficulty* is properly set according to the formula (will be introduced in later section of Difficulty);
- the proof-of-work satisfies the mining difficulty;
- the extra Data is no more than 32 bytes;
- the parent block is chosen properly from the past view of B following the GHOST rule;
- the deferred state root *stateRoot* must be correct. More specifically, the state is committed right after executing the transactions included in the past blocks of the pivot block of 5 epochs ago.

  Formally, the block B has a valid header if and only if B satisfies (†):

Note:
In the TRIE function shown above, σ refers to the base state just before executing EPOCH P(5)(B), which is equivalent to the final state exactly after executing P(6)(B). Furthermore, the state root of σ is stored in the header of P(B) satisfying the following equation:
$\mathrm{TRIE}(LS(\sigma)) = \mathrm{P(B)H}r$.

- **Partially (In)Valid Blocks**

A block B with block header H = H(B) is called *partially valid* if it passes all the assertions stated in previous sub-section except for the following two:

- the deferred state root H*r* is incorrect;
- the parent reference P(B) is not chosen by the GHOST rule in PAST(B).

A partially valid block is unable to contribute to the security of Skyrim Network. It will not be a pivot block controlling by zero weight assigned to it following the consensus algorithm in Skyrim Network. Furthermore, partially valid blocks are entitled no rewards to the miners, then the front paid transaction fees from the transactions only collected in partially valid blocks will be burnt.
However, the partially valid block can still contribute to the throughput as long as the target difficulty is legitimate and the proof of work is valid. This is because partially valid blocks are allowed to be referred and the transactions inside will be processed as in any fully valid block.

- **Topological Consistency**

In a DAG built with a block B being a leaf block from the parent and ommer references of B, the referenced blocks are called *topologically consistent* if there is no explicit chronological order between any two of them, i.e. they appear in each other's inverse cone zones. This is required since otherwise a valid block B should only reference the one appears later, which would already reference the earlier block directly or indirectly.

2.1.2 Three Graph Structure

In Skyrim Network, the consensus algorithm is designed to resolve two issues:

- whether a block is valid and should be added to the Skyrim Network blockchain;
- these valid blocks should be processed in what order.

In an overview, the Skyrim Network construct a Tree-Graph blockchain instead of a chain structure following the Conflux consensus algorithm. Each vertex in the Tree-Graph represents a block, and each directed edge corresponds to a parent or ommer reference.
The consensus protocol optimistically accepts all formally correct blocks and specifies a total order of blocks. This total order will be agreed by all honest participants and it is hard to change (under reasonable assumptions). Once the order is determined, transactions inside blocks are executed accordingly. Invalid transactions are skipped by the consensus algorithm, such as duplicated transactions or transactions conflicted with previously processed transaction.

2.1.3 PoW Consensus Algorithm

Skyrim Network System, will be developed with PoW Consensus. Every full node maintains a Tree-Graph structure of accepted blocks, which are blocks that are valid in the node's local view. The full node is responsible for the verification of whether a newly receiving block is valid before adding it into the Tree-Graph.

The validation of a new block can result in three outcomes - acceptation, rejection or pending.

- Acception
  The block is verified to be valid, then it will be added to the Tree-Graph immediately.
- Rejection
  The block is verified to be clearly invalid, then and it will be discarded;
- Pending
  When the block references some blocks not in the current Tree-Graph, the verification of the block cannot be complete. The verification is pending until all the referenced blocks have been added to the Tree-Graph.

- **Validation Procedure**

Given a new block B, the validation is done in the following steps:

1. Header Validation

This step aims to testify that B has a valid header (or at least a partially valid one) following (†) stated in previous sub-section of **Valid Blocks**.
Note:
A Proof-of-Work Validation of B is embedded inside the Header Validation. The solution to the PoW puzzle is verified w.r.t. the legitimate target difficulty. The gas limit and ≥ 5000 is also checked here.
Furthermore, as the major mechanism against Sybil attacks, the Proof-of-Work Validation is usually performed before invoking more expensive steps of verification and execution. It is interchangeable with other steps of the validation for better efficiency. It will also be performed last and repeatedly when mining a new block.

1. Ommer Header Validation
   This step asserts that B only references existing valid blocks. Under situation that new block references the head of an unknown block, it is marked as pending until all its referenced blocks have been added to the Tree-Graph. Except for waiting, the node can also query its neighbors about the referenced unknown block.

2. Internal Consistency
   This step asserts that B is self-consistent, i.e. satisfying following conditions:

- The block header is well-formed.
- Every transaction $T \in BTs$ is locally legitimate. More specifically, this means:

a) T is well-formed RLP with no trailing bytes;
b) T has a valid signature by S(T).

Note:
The locally legitimate verification is the first test of the intrinsic validity of transactions.

- The total gas consumption does not exceed the block gas limit, i.e.

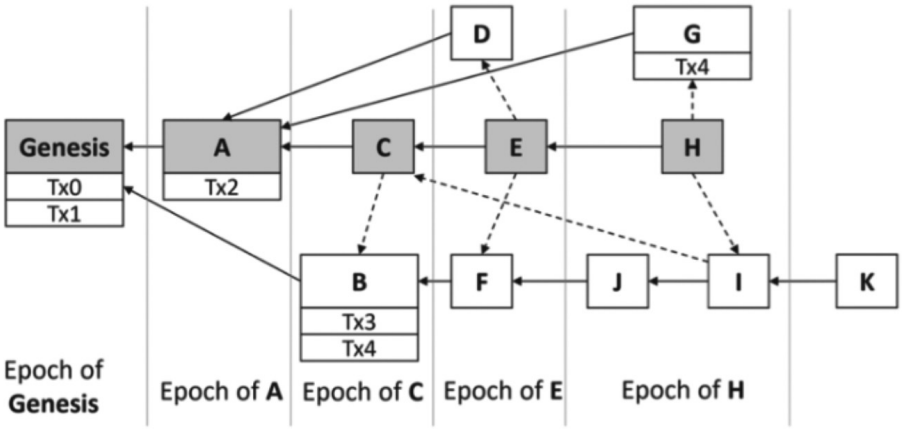
If B passes all above steps, then it is marked accept and added into the Tree-Graph structure, otherwise it is marked reject and discarded.

Note:
A valid block must pass all the above validation steps and there is no jump or loop, so all validation steps are interchangeable and parallelizable.

- **Deferred Execution of Transactions**

In Skyrim Network we check the validity of each transaction locally without a global test of whether it is a duplicate of some processed transaction or the sender has insufficient balance. Therefore, a block B being valid does not imply that all transactions in are valid or will be eventually executed. The validation of transactions will be deferred to the finalization of B. This forms the most important difference of Skyrim Network from other blockchains in validating blocks.

2.1.4 Tree-Graph



For convenience and a better understanding of the Tree-Graph constructed in Skyrim Network Blockchain, we show an example local Tree-Graph in Figure 4.
Recall that Each vertex represents a block and each directed edge represents the reference of another block in the Tree-Graph.

We can demonstrate following properties of the Tree-Graph from the above figure:

- Genesis block is the first block of the Tree-Graph. It is a special case in that it does not reference a previous block. Therefore, the vertex for the genesis block has no outgoing edges.
- Other than the genesis block, each block has exactly one parent reference (shown by the solid arrow in Figure 4) and multiple or zero ommer references (shown by the dotted arrow).

- This directed graph is acyclic since every directed edge reflects a clear chronological order of blocks, unless the referenced block is generated with a hash collision.

Every Skyrim Network full node maintains a Tree-Graph structure of accepted blocks. This leads to problem of how to decide the total order of all accepted blocks. In Skyrim Network, the consensus algorithm will first select a pivot chain based the Tree-Graph structures. A pivot chain defines the order of blocks on the chain, then the total order of all blocks can be determined.

2.1.5 The Pivot Chain

Since any block besides the genesis block has exactly one parent, all parent edges in the Tree-Graph together form a *parental tree* with the genesis block being the root. In the parental tree, the Conflux consensus algorithm selects a chain from the genesis block to one of the leaf blocks as the *pivot chain*. Blocks on the pivot chain are called *pivot blocks* and other blocks called *off-pivot blocks*.

In Skyrim Network the pivot chain is not necessarily the longest chain or the "heaviest" chain. Indeed, Skyrim Network Blockchain selects the pivot chain based on the GHOST rule (a simplified variant of the GHOST rule is used in Ethereum).
The Conflux selection algorithm starts from the genesis block. At each step, it computes the accumulated *total difficulty* of each child subtree in the parental tree and advances to the child block with the largest total difficulty of subtree. The selection algorithm stops when it reaches a leaf block.
The total difficulty of a subtree root at block B is denoted by and defined recursively as:

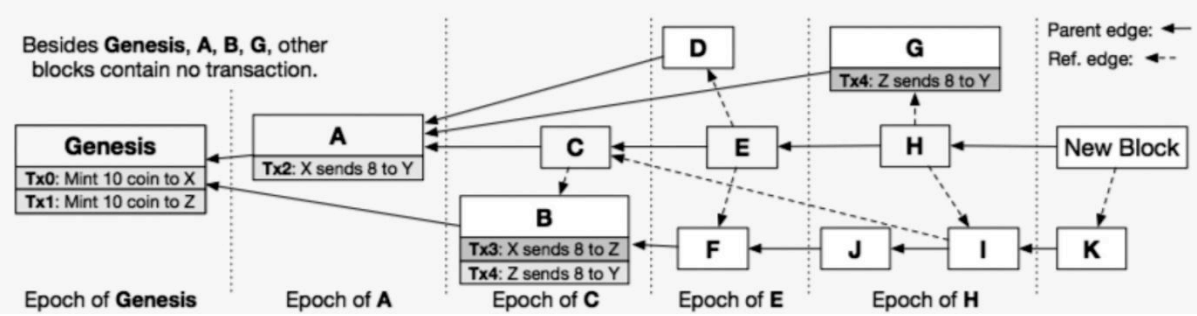
where denotes the target difficulty of B, and
P(B′) is the parent block of B′ (hence the summation is taken over B's children).
Note:

- B*t* is not a part of the block B. It is only used to describes a state of B in the local view and may increase as more subsequent blocks are included afterwards.
- The total difficulties can be computed from all block headers, since a block header contains the block difficulty and its parent block, which is all we need to compute the total difficulty recursively.

The GHOST rule guarantees the irreversibility of the selected pivot chain even in the occurrence of honest nodes forks due to network delays. This is because the blocks in the forks also contribute to the safety of the pivot chain.

Here we take the Figure 4 as an example to give a explicit comprehension of the pivot chain selection. We can suppose that all blocks have equal difficulty for simplicity.
In this example, Skyrim Network Chain would select Genesis, A, C, E, and H as pivot blocks, which is not the longest chain in the parental tree. Comparatively, the longest chain should be Genesis, B, F, J, I, and K. The subtree of A contains more blocks than the subtree of B, hence block A has a larger amount of total difficulty than B. Therefore, the chain selection algorithm selects A over B at its first step.

2.1.6 Epoch



Given the pivot chain in a Tree-Graph, Skyrim Network Blockchain splits all blocks into epochs as follows:

- Every pivot block B is at the *epoch of* B, which is denoted by EPOCH(B). In particular, the genesis block is at epoch 0.
- Every off-pivot block B is at the epoch of the first pivot block B that references it directly or indirectly. This means following rules satisfied:

1. Every block $B' \in BU$ is at the epoch of B.
2. If block B'' is referenced by B' and not included in an earlier epoch, then any such B" is at the epoch of B.
3. Recursively all blocks referenced by B'' is not at the epoch of B.

In other words, the epoch of B contains all blocks that are potentially produced after P(B) but before B at the local view of B. For example, in Figure 4, each of the pivot blocks Genesis, A, C, E, and H corresponds to one epoch. The block J belongs to the epoch of H but not E because J is reachable from H but not reachable from the previous pivot block E.

2.1.7 Total Order of Blocks

The sorting procedure used to find t
The total order of all blocks is extender from the total order of pivot blocks. The sorting process is shown as following steps:

1. Sort blocks according to their corresponding epochs, so that a block in an earlier epoch always precedes another block in a later epoch;
2. Sort the blocks inside each epoch based on their topological order, i.e. corresponding to the partial order implied by ommer references.
- In the case of no partial order relation between two blocks, breaks ties deterministically with the unique IDs of these two blocks.

More detailed rules are described with codes in Figure 5 shown below.

Figure 5. The Definition of ConfluxOrder().

For example, the local Tree-Graph in Figure 4 may give a total order as Genesis, A, B, C, D, F, E, G, J, I, H, and K. The order of D and F may change if the block id of F is smaller than D, and the same holds for G, J, and I.

2.1.8 Transaction Total Order

Input : The local Tree-Graph $\mathbf{G} = \langle \mathbf{B}, \mathsf{P}, E \rangle$ and a block $\mathsf{B} \in \mathbf{B}$
Output : A list of blocks $\mathbf{L} = \mathsf{B}_1 \circ \mathsf{B}_2 \circ \ldots \circ \mathsf{B}_n$, where $\mathsf{B}_1 = \mathsf{G}$ and $\forall 1 \leq i \leq n, \mathsf{B}_i \in \mathbf{B}$

$\mathsf{B}' \longleftarrow \mathsf{P}(\mathsf{B})$
if $\mathsf{B}' = \perp$ **then**
  return B
$\mathbf{L} \longleftarrow \text{ConfluxOrder}(\mathbf{G}, \mathsf{B}')$
$\mathbf{L}' \longleftarrow$ An empty list
$\Delta \longleftarrow \mathsf{PAST}(\mathbf{G}, \mathsf{B}) - \mathsf{PAST}(\mathbf{G}, \mathsf{B}')$
while $\Delta \neq \emptyset$ **do**
  $\Delta' \longleftarrow \{\tilde{\mathsf{B}} \mid |\mathsf{FUTURE}(\mathbf{G}, \tilde{\mathsf{B}}) \cap \Delta| = 0\}$
  Let B' be the block with maximum $\mathsf{Hash}(\mathsf{B}')$ in Δ'
  $\mathbf{L}' \longleftarrow \mathsf{B}' \circ \mathbf{L}'$
  $\Delta \longleftarrow \Delta - \mathsf{B}'$
$\mathbf{L} \longleftarrow \mathbf{L} \circ \mathbf{L}'$
return $\mathbf{L}$

The total order of transactions can be found based on the total order of blocks and the verification of conflicts among transactions. The determination of transaction total order is performed in the following steps:

1. Sort transactions based on the total orders of their enclosing blocks.
- If two transactions belong to the same block, sort them based on their appearance order in the block.
2. Check the conflicts of the transactions at the same time when deriving the orders.
- If two transactions are conflicting with each other, discard the second one.
- If one transaction appears in multiple blocks, keep the first appearance and discard all redundant ones.

Note:
The total order of transactions packs all the valid transactions into sequential blocks in the of an Ethereum-like chain.

For example, the transaction total order in Figure 4 is Tx0, Tx1, Tx2, Tx3, Tx4, and Tx4, where Skyrim Network Blockchain discards Tx3 because it conflicts with Tx2, and discards the second Tx4 because it is redundant.

2.1.9 Transaction Processing & Incentive Mechanism

Skyrim Network Blockchain implements similar virtual machine like Ethereum. The valid transactions are executed on the EVM, once the total order of transactions is determined. In this section, we focus on the execution of transactions.

2.1.10 Gas and Payment

As defined in Section 3.2.2 every transaction T has two fields of gas Limit and gas Price that declare the specific benchmark amount of gas and the price per unit gas. When the execution of a transaction T is initialized, the purchase of gas conducts at the price. If there is a shortage in the sender's account balance to afford such a purchase, the transaction will be considered invalid and be discarded. As in Ethereum, gas does not exist outside the execution of transactions.

However, in the current version of Skyrim Network, the unused gas at the end of the transaction execution is *not refundable*. It is the sender's responsibility to estimate the amount of gas to be consumed and carefully set an appropriate gas limit. This design makes it explicit for miners to calculate and compare the transaction fee when packing transactions into a new block, without actually executing any transactions. Since the execution of transactions is deferred to later blocks in the design of Skyrim Network, the non-refundable manner of unused transaction fees is particularly important for the efficiency of executing transactions in concurrent blocks.
The purchased gas of a transaction is added to the reward pool to motivate miners. It is miners who choose the transactions and form them into a 'block'. Therefore, a higher gas price on a transaction would cost the sender more but also increase the chance of being processed timely.

2.1.11 Transaction Validation

Before the execution, a transaction T in the processing queue must pass a group of secondary tests of intrinsic validity:

1. The transaction nonce is valid, i.e.

   where σ is the current world state.

2. The gas limit is no smaller than the intrinsic gas used by the transaction.
3. The balance of the sender account contains at least the cost required in up-front payment, i.e.

Note:
When T passes all previous tests but fails the last one, T will be considered as an invalid transaction and will not be executed. However, the sender's balance will be reduced by max{ *}* and nonce increased by one.

Note that the local legality of the transaction is not checked again in the secondary tests, e.g. the RLP format and the validity of signature. This is because it is already verified in the first intrinsic validity test before accepting the corresponding block into the Skyrim Network Tree-Graph, as discussed in the subsection of Validation of Blocks.

Once the transaction T passes both first intrinsic validity test and the secondary tests, it can never be invalid later on, though it may fail in the execution.

2.1.12 Execution Model

The execution model specifies the system state transition with inputs of a sequence of byte code instructions and a small tuple of environmental data. The state transition function is formalized as a virtual state machine. Thus, it is Turing-complete except that its running time is intrinsically bounded by the limited amount of available gas. In current version of Skyrim Network, we implement the well-known Ethereum Virtual Machine (EVM).

- **Basics**

The EVM is a stack-based architecture with 256-bit word size. The stack has a maximum size of 1024. The memory model is a simple word-addressed byte array. The machine also has an independent storage model which is a word-addressable word array (rather than byte array for the memory). The memory is volatile, and storage is steady and maintained as part of the system state. All locations in both memory and storage are initialized as zero. The program code is stored separately in a virtual ROM that is only interactable via specific instructions.
The execution of the virtual machine may reach exceptions for various reasons, including stack underflows/overflow, invalid instruction, invalid jump destination, out-of-gas, etc. Like the out-of-gas exception, the machine halts immediately and sends an exception to the execution agent. The execution agent is either the transaction processor or recursively the spawning execution environment, which will catch and deal with it separately.

- **Gas Consumption**

Recall the cost of execution is known as *gas*. It is charged under three distinct circumstances:

- the execution of instructions, where each type of instructions is assigned an intrinsic amount of gas;
- the generation of subordinate message call or contract creation;
- the increase in the memory usage.

In particular, the total gas for memory-usage payable is proportional to the smallest multiple of 32 bytes that are required to include all memory indices (whether for read or write). This is paid in a just-in-time manner. For example, referencing an area of memory at least 32 bytes greater than any previously indexed memory will certainly result in an additional cost.

Note:
In present version of Skyrim Network, there is no refund of gas fee even if an operation that clears a storage entry is executed. This is distinct from the gas refunding policy in Ethereum.

- **Execution Environment**

Besides the global system state σ and the amount of remaining gas g, the execution agent must provide the following important information used in the execution environment:

1. I_a: the address of the account which owns the code that is executing.
2. I_o: the address of the original transactor who initiated this execution.
3. I_p: the gas price declared by the transaction that initiated this execution.
4. I_d: the input data used in this execution in the form of byte array. If the execution agent is a transaction T, this would be the transaction data .
5. I_s: the address of the account that invoked the code. If the execution agent is a transaction, this would be the transaction sender's address.
6. I_v: the value passed to the recipient's account. If he execution agent is a transaction T, this would be the transaction value T_v.

7. *I*b: the byte array of the VM code to be executed.
8. *I*H: the block header of the current block.
9. *Ie*: the depth of the current message-call or contract-creation in the stack.
10. *Iw*, the permission to make modifications to the state.

The state transition is defined by the execution function Ξ. Function Ξ takes the current state σ , the amount of gas *g*, and execution environment information *I* as input, and returns the resultant state σ′, the remaining gas *g′*, the accrued substate *A* and the resultant output o. Formally, it is denoted by

$(\sigma', g', A, o) \equiv \Xi(\sigma, g, I)$,

where the accrued state $A \equiv (s, l, t)$ consists of the self-destruct set *s*, the log series *l* and the touched accounts *t*.

2.1.13 SGAS Incentive Mechanism

In Skyrim Network, miners get paid by Skyrim Network Gas Tokens (“SGAS” for short) from two sources: the newly minted SGAS as block award and the fees (a.k.a *gas*) paid by transaction senders. In this section, we discuss the incentive mechanism designed mining motivation.

2.1.14 Transaction Fee Reward

We define a block B *properly include*s a transaction T if and only if the following conditions are satisfied:

1. $\forall B' \in PAST(B), T \notin B'Ts$;
2. T is first included in the i-th epoch EPOCHi, and B belongs to EPOCHi.

The transaction fee rewarding mechanism specifies that the transaction fee of T is divided between all blocks that *properly include* T. Furthermore, the transaction fee is distributed proportionally to those blocks with respect to their weight defined by actual difficulty in section 3.5.2. Recall, a block with a fully valid header and actual difficulty above the epoch target difficulty gets weight 1, and other blocks with partially valid headers or lower-than-target actual difficulty gets weight 0.
Following the rewarding mechanism, the transaction fee is not distributed to any miners when the transaction T is only included in blocks of 0 weight. In such case, the transaction fee is burnt, but the transaction will still be processed.

2.2 Skyrim Network Side Chains & VM

2.2.1 Skyrim Network Side Chain

We use side chain technology to scale up computation Skyrim Network, called Skyrim Side Chain System. The Skyrim Side Chain System adopts a series incentive protocols to motivate Skyrim Network participants autonomously and transparently. It means the incentives are operated on the side chain without active state transition management but through smart contract, and the nodes themselves are incentivized to operate the chain.

In addition, significant scalability is achieved by the integration of a group of transactions represented in a payment from a contract into a single bit in a bitmap, so that a single transaction and one signature represent a effective payment coalesced with many participants. Furthermore, a MapReduce framework is developed to provide scalable computation enforced by bonded smart contracts.

Under the construction of Skyrim Side Chain System, an account to be managed by a series of external parties, and an contract to be computed by a groups of nodes in a similar behavior as miners. Instead of creating all trivial transactions for every state update, Skyrim Network coalesced state updates into an unitary update with minimal on-chain data on top of an existing blockchain, even if new users' ledger entries are added.

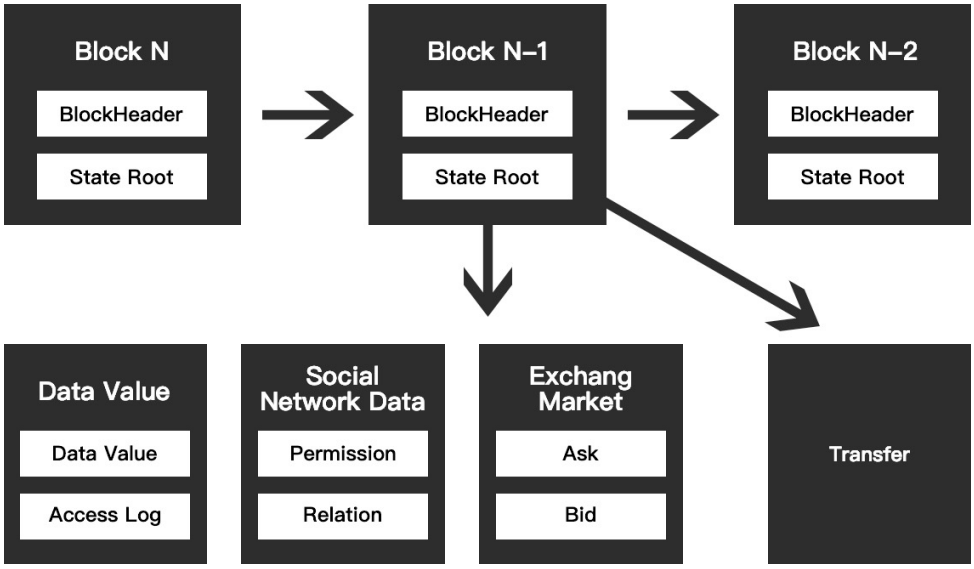
The entire Skyrim Side Chain System is built by a series of smart contracts for different purposes within a root blockchain, i.e. Skyrim Network main chain. The structure of the Skyrim Side Chain system is shown by Figure 6. The root blockchain enforces the state in the Skyrim side chains and working as a global enforcer of all computation. However, it is only computed and penalized if there is proof of fraud. Skyrim Network side blockchain can co-exist with their own business logic and smart contract terms. In particular of Ethereum-like design, the Skyrim Network side chain would be composed of EVM smart contracts with a small number of necessary commitments to achieve a significantly large amount of computation and keep the financial ledger entries in non-Byzantine cases.

Skyrim Side Chain System consists of following five crucial components:

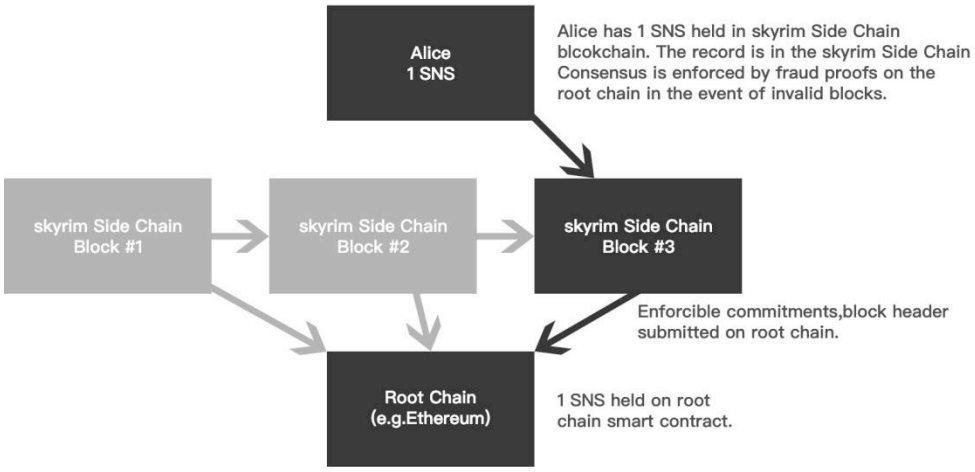
- An incentive protocol that encourage smart contracts to be computed in a cost-effective manner.
- A tree formatted structure of child chains that further upgrades low-cost efficiency and compacts net-settlement of transactions.
- A Map Reduce computing framework that conducts fraud proofs of state transitions within nested chains. It asserts child chains with compatible state transitions when they reconstruct into the tree structure to extend scalability.
- A consensus mechanism dependent on the root blockchain that attempts to provide incentives and accomplish a bitmap-UTXO commitment structure. It synchronizes state machine replicas and ensuring consistency among them. Also, it keeps powerful adversaries from derailing the system and successfully forking the chain, e.g. discarding unavailable data or prevent from other Byzantine faults.

The Skyrim Network Side Chain, or External Channels

In Skyrim Side Chain System, side chains (or called off-chain channels or external channels) can hold states on behalf of others. Transactions on the side chains are accounted with the root chain by matching and verifying the funds held in the root chain account. This accounting process is also called a fraud proofs of state transition. Note that Skyrim Side Chain System is not compatible with fractional reserve, i.e. a transaction on the side chains is only valid if there are sufficient amount of funds available in corresponding root chain account. However, an account on the side chain is not necessarily existing in the root chain. It can be a smart contract on the root chain that holds the associated balance and sufficient amount of funds. Therefore, transactions are flexible under the Skyrim Side Chain System,



either the recipient is existing or not, and either the transactions of side chain tokens or native root chain tokens.



Similar with all blockchain, the contents of side chains are encoded as blockheader to save memory space. It is the hashes of side chain blockheaders are stored on the root chain instead of disclosing data. If a fraud transaction is submitted on the side chain, the root chain will detect the fraud via proof of fraud. Then, the block of the side chain will be rolled back, and the miner of invalid block will be penalized. This is very efficient, as many state updates are represented by a single hash (plus some small associated data).

Skyrim Side Chain System allows light nodes to contribute to the root chain by acting as a node for concomitant side chain. A light node can manage a side chain without a full persistent ledger of the root blockchain. Further, no custodial trusts are required to be a node. In the worst case, only time-value is lost, since disputed funds are locked up for a period.

Similar to Lightning Network for Bitcoin, participants of Skyrim side chain can interactively transit infinite times of payment only if the transactions are investigated valid. However, Skyrim Side Chain System does not require all participants to be online to update the account states when transactions made. Also, participants can merely exist on the side chain without a direct interaction with the root chain.

In summary, a significantly large amount of transactions are processed in parallel on a number of side chains with minimal data hitting the root blockchain. This allows Skyrim Network to provide scalable throughput performance.

- Prevention of frauds

A series of fraud proofs are constructed as smart contracts on the root chain. These contracts protect the ledger from fraud attacks and any or non-Byzantine attempts.

- Fraud transactions

Any withdrawal from the side chain requires a period for censoring enforced by the fraud proofs. The censorship is designed as an interactive validation that the withdrawer of any funds on the side chain have to attests to a bitmap of the influential ledger outputs arranged in an UTXO model. More specifically, anyone among the side chain can submit a fraud proof of double spending or other Byzantine faults. During the censoring period, an incorrect proof can also be called back.
After the censorship and before the timestamp is committed, invalid transactions can be revoked for rapid exit of a faulty Skyrim Side Chain. In coordinated mass revocation events, a participant may be able to exit with less than 2-bits of block space consumed on the parent chain.

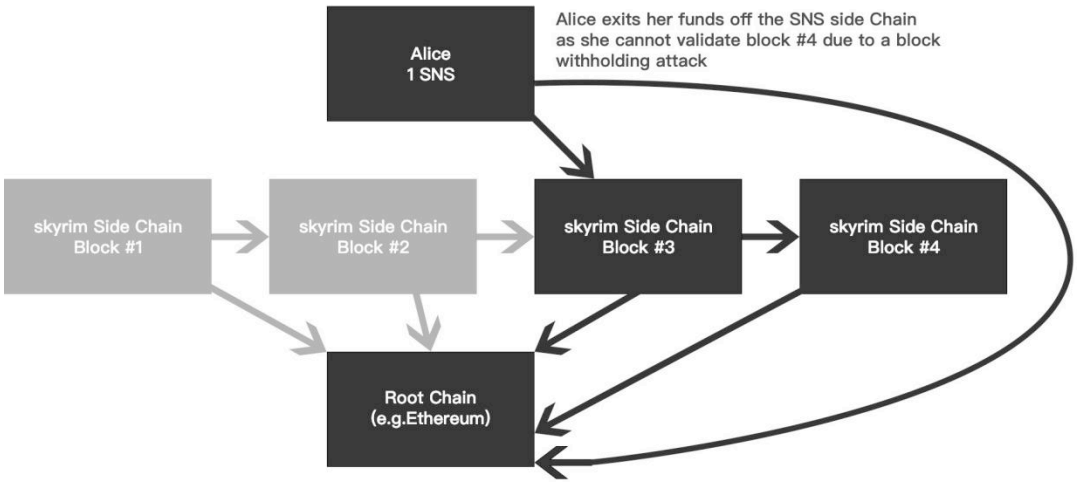
- Withholding attack

In the event of a block withholding attack, a mass-exit can be conducted without any custody of trust in the validator nodes. This protects the participant to exit the fraud rapidly and economically compared with other off-chain proposals.

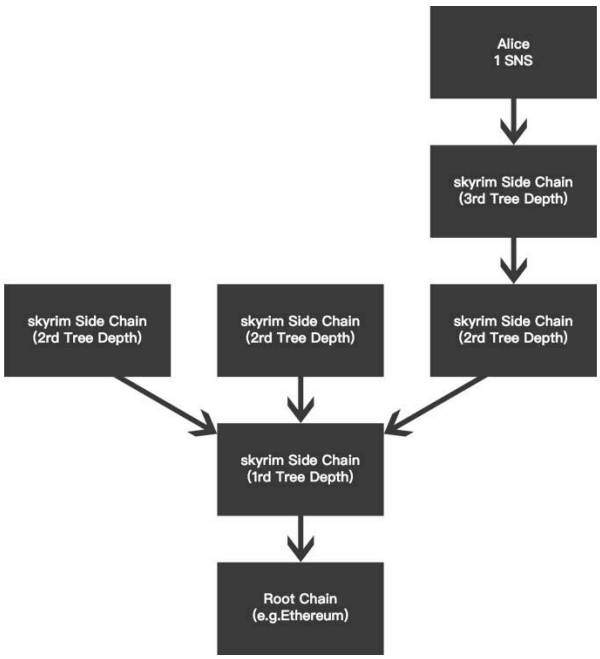
We show an example of an exit of funds in the event of block withholding in Figure 8. Block #4 is withheld by a malicious node and committed on the root chain. A participant of the side chain, Alice, is not able to retrieve block #4. She can withdraw the funds from the side chain by broadcasting a proof of funds to the root blockchain. After a delay for censoring. her withdrawal is going to be processed by the root chain directly.

Tree Structure of Skyrim Side Chain System

Recall a side chain is built by storing blockheaders and a corresponding smart contract stored a summarized ledger on the root chain. We further construct Skyrim side chains hierarchically in a tree structure in which child side chains can be built as smart contracts held on the parent chains. The parent chain can be the root chain or a side chain. Since each child chain stores its blockheader on the parent chain, the data of the whole Skyrim Side



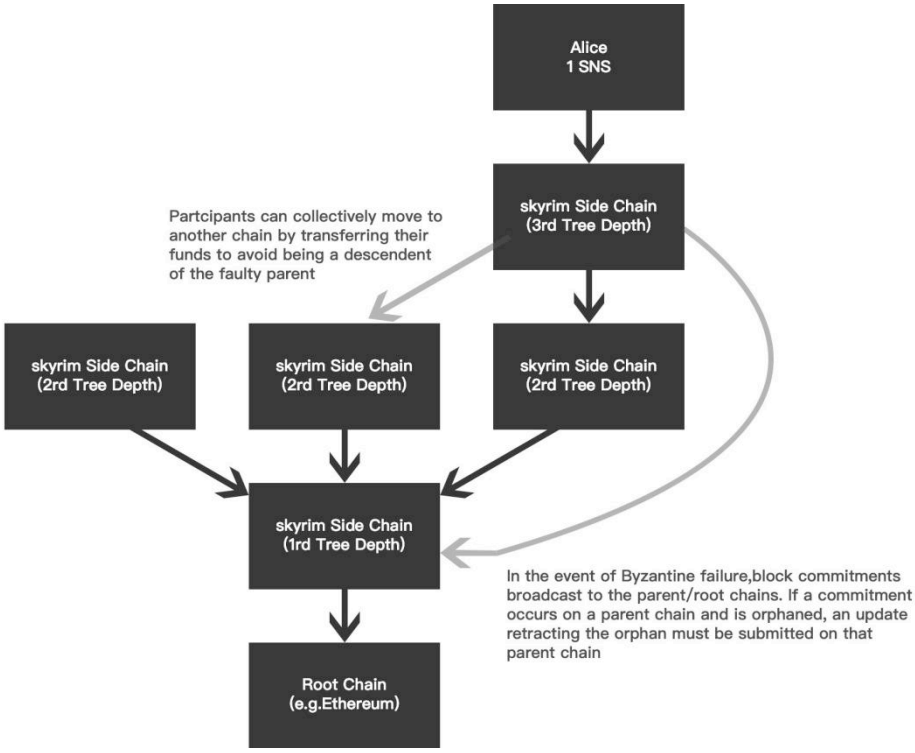
System is encoded compactly on the Skyrim Network main chain as the feature of a Merkle



Tree.

Similar enforcement of fraud proofs can be proposed to assure the balances and state transitions of these chain hierarchies as a higher and lower courts. This tree structure maximizes availability and minimizes costs in non-Byzantine states. If a child chain is in Byzantine condition, either an exit to any parent chain or a flow down commitment can be executed with the current committed state.

Each child chain runs on top of its parent chain. In effect, state transitions can be only periodically committed to parent chains (finally flows to the root blockchain). This provides Skyrim Network the ability to process enormous scale of computation and account state transitions due to the omission of intermediate side chain commitments without Byzantine



Validation of transactions involves two parts: validating if a transaction conforms to internal standards, and validating if a transaction has the necessary prerequisites such as sufficient transaction inputs. After a transaction is validated, then blockchain states can be updated. Skyrim's software will encourage parallel computing opportunities to the greatest extent possible by clearly defining blockchain state access rights for the validation of transactions and for the actual updating of application and blockchain states. Through this, Skyrim's platform can process transactions more efficiently.

Any software language or virtual machine can be compatible with Skyrim as long as they can be integrated with Skyrim's platform software API.
Currently, Skyrim virtual machine will mainly support WASM (web assembly), a more efficient system than EVM. WASM also supports JIT compilation, allowing developers to write C/C++, java code that can be run on Skyrim VM.

2.3 Decentralized Ledger

A fully distributed ledger system that includes smart contracts and protocols. Skyrim provides compatibility support for complex technological systems, whether that be existing blockchains or tradition information systems. All systems feature decentralized entity management with support for main protocols. It combines identity system, data exchange, data collaboration, procedure protocols and various industry-specific modules. Together this builds the infrastructure for a peer-to-peer trust network which is cross- chain, cross-system, and cross-application.

The distributed ledger within Skyrim's system support a highly effective version of the DBFT consensus protocol. It has reached near-infinite scalability and requires a relatively low hashing rate, making it highly unlikely to experience forks of the network.
As a decentralized protocol, users have consensus rights, eliminating cases where miners or other parties solely control confirmation power. A verifiable random function is used to

select who confirms the next block, every confirmation receiving a Skyrim seed directing to the next confirmation.

Pluggable verifiers and online protocol recovery and upgrade are also supported. Meanwhile, in order to meet needs from different chains in Skyrim, the distributed ledger framework also supports pluggable consensus mechanisms including DBFT, RBFT, PoS, DPoS and custom PoW.

Skyrim's storage system works on the distributed ledger. The key feature of the completely decentralized, tamper-proof ledger is that trust is shared amongst multiple parties through use of smart contracts, distributed networks, distributed storage, distributed authority, distributed security, and a variety of modules.

Skyrim's protocols are carried out with distributed ledger technology, cross-chain entities, cross-system privacy, and cross-chain protocols. The distributed ledger system does not only store data but also records its use. Each data request, data matching, data transfer, and data usage is attested to the ledger, forming a complete private record of the data use.

3. Skyrim Network Data Protocols

3.1 Distributed Identifications

Organizational networks can be established using information such as student IDs for academic institutions or employee IDs for businesses. All entities can select a range of identity verification methods in order to create systems free from third party interference. Private information is securely stored in decentralized databases.

Our identity system is backed by an user system and a global identity system.

- User system is supported by the following components:
- User Register/Login,
- User Info Storage,
- User Profile Analysis,
- User Chain Data.
- Global identify system is supported by
- Data unique Identity,
- User unique Identity,
- Identity Relation

3.2 Data Protection

Skyrim's tamper-proof identification system can function with legal validity. Since blockchain is an open source third-party technology, users can carry out IP legal right authentication, payments, and transfers worldwide. The reputation system helps build a reputation-based protection for content that adds another layer of security to the content exchange system.

3.3 Data Value Ranking

An open sourced ranking algorithm is used to measure the influence of relationships between addresses, smart contracts and distributed applications (DApps). It helps both users utilize information among the ever-increasing amount of data on all blockchains & developers to use our search framework directly in their own applications.

3.4 Storage & Content Delivery

This system is stored in IPFS which uses all spared resources on the net to contribute storage spaces together. The storage space is unlimited and extendable with multiple copies to store, which means there is no need to worry unusual data's missing. It also uses the P2P acceleration to achieve high speed document visiting.

A distributed data storage layer supports decentralized storage for different types of data. Skyrim stores, manages, and attests data throughout its life cycle. A digital identity is created for each copy of data from registration, request, authorization, to exchange. Copyright protection is also recorded to each copy on the blockchain.

3.5 Smart Contracts

Businesses can grow by implementing smart contracts and trust networks through new procedure protocols, controls, and exchanges of data. Smart contract programs may call functions offered by the host system and/or third-party libraries. Also, programs running on different computers in a distributed framework do not provide any guarantee for execution time. Such openness and decentralization are the reflection of the essential spirit of blockchains but give birth to various sources of security threats. In fact, the lack of security is plaguing the smart contracts. The Skyrim Network blockchain is equipped with a power security engine consisting of two major components, a rule-based semantic and syntactic analysis engine for smart contracts; a formal verification toolkit to prove the security properties of smart contracts.

3.6 Metadata Protocols

Metadata annotations can be used to define additional characteristics or capabilities of a metadata element, such as a service, entity type, property, function, action or parameter. For example, a metadata annotation could define ranges of valid values for a particular property. Instance annotations can be used to define additional information associated with a particular result, entity, property, or error; for example, whether a property is read-only for a particular instance. Where annotations apply across all instances of a type, services are encouraged to specify the annotation in metadata rather than repeating in each instance of the payload. Where the same annotation is defined at both the metadata and instance level, the instance-level annotation overrides the one specified at the metadata level.

3.7 Data Protocols

This section provides a high-level description of the Entity Data Model (EDM): the abstract data model that is used to describe the data exposed by a Skyrim service. The Skyrim Metadata Document is a representation of a service's data model exposed for client consumption.

The central concepts in the EDM are entities, relationships, entity sets, actions, and functions. Entities are instances of entity types. Entity types are named structured types with a key. They define the named properties and relationships of an entity. Entity types may derive by single inheritance from other entity types.

The key of an entity type is formed from a subset of the primitive properties of the entity type. Complex types are keyless named structured types consisting of a set of properties. These are value types whose instances cannot be referenced outside of their containing entity. Complex types are commonly used as property values in an entity or as parameters to operations.

Properties declared as part of a structured type's definition are called declared properties. Instances of structured types may contain additional undeclared dynamic properties. A dynamic property cannot have the same name as a declared property. Entity or complex types which allow clients to persist additional undeclared properties are called open types.

Relationships from one entity to another are represented as navigation properties. Navigation properties are generally defined as part of an entity type, but can also appear on entity instances as undeclared dynamic navigation properties. Each relationship has a cardinality. Enumeration types are named primitive types whose values are named constants with underlying integer values.

3.8 Data Operation Protocols

Operations allow the execution of custom logic on parts of a data model. Functions are operations that do not have side effects and may support further composition, for example, with additional filter operations, functions or an action. Actions are operations that allow side effects, such as data modification, and cannot be further composed in order to avoid non-deterministic behavior. Actions and functions are either bound to a type, enabling them to be called as members of an instance of that type, or unbound, in which case they are called as static operations. Action imports and function imports enable unbound actions and functions to be called from the service root.

4. Skyrim Network Trusted Platform

Skyrim Network will build its own trusted platform to provide useful services for data assets industry. Basically, its platform is designed for data asset transactions in application level. Skyrim Network Trusted Platform has its own key trusted network service, toolkits and other decentralized services to facility its platforms. This platform is friendly to developers, data asset holders and traders, especially for decentralized asset-related service provides.

4.1 Standard APIs & Application SDKs

Skyrim’s Standard API for developers is a comprehensive blockchain platform offering diverse services including: data deposit, data certification, and process certification. With Skyrim’s Standard API, any sized business, no matter how large or small, can utilize blockchain technology to further enhance brand perception and value as well as to expand into new business models using immutable data.

Developers can use Skyrim SDK to develop various applications based on Skyrim, for example, wallet client, DApps, etc. With use of NEO SDK, project can work in the existing environment without needing to move to Skyrim VM.

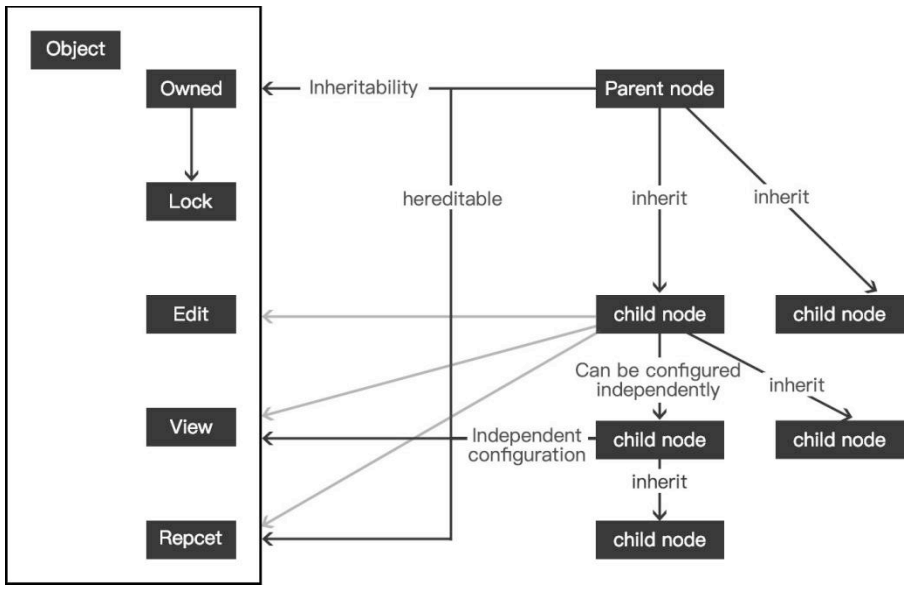
4.2 Data Service Modules

4.2.1 Data Transaction Module

Skyrim Marketplace is a distributed data exchange complete with data sets, algorithms, and models. It acts as an extension to Skyrim, providing data products, data predictions, and data computing resources. At the same time, it maintains compatibility with other major cross-chain systems to create a large data exchange platform. The native DApp lets providers across industries implement the data trading market.

4.2.2 Data Privacy Module

Based on the access control contract, we manage data privacy in the following model:



4.2.3 Data Operation Module

Skyrim provides a series of cryptography and data operation module support in areas including multi-factor entity authentication, distributed data exchange, and distributed procedure protocols. This includes encrypted data transfer, key sharing protocols, multi-party key management, ring signature modules, blind signature modules, and secret sharing mechanisms. In identity and data validation zero-knowledge proof and homomorphic encryption schemes are used, and in a collaborative application two records are kept. Other multi-party technology schemes are being explored for the future.

4.2.4 Data Verification Module

As a truly decentralized protocol, Skyrim entitles its users to consensus rights, eliminating cases where miners or other parties solely control confirmation power. Skyrim selects who confirms the blockchain using a verifiable random function, every confirmation receiving a Skyrim seed directing to the next confirmation. Skyrim also supports pluggable verifiers and online protocol recovery and upgrade. Meanwhile, in order to meet needs from different chains in Skyrim, the distributed ledger framework also supports pluggable consensus mechanisms.

4.3 Skyrim Network DApp Platform

- Developers

Skyrim Network DApp platform is friendly to all developers in sectors such as social, gaming, tools, financial services, and entertainment. This platform extends all convenient developer tools to developers, and provides incentives and rewards to keep it robust and fast growing. With its huge traffic, this platform will convey more benefits to developers in marketing and data sharing.

- Data Assets Holders

Data assets holders will be critical participants in the community, as they may receive information, insights, and services on the platform. They will be positively involved in information exchange, asset investment, asset management, and more customized services provided by decentralized financial services providers.

- Community Super Representatives

The Skyrim Network community will elect super representatives in the standard of platform credits and multiple actions. This team will help manage the platform community. Super representative will make decisions on the adjusting of system parameters, which may include transaction fees, ratings and reviews, new services, arrange contents, user authorizations and creation of new representative.
Super representative will upkeep the decentralized community and support data system for further development.

4.3.1 Decentralized Asset Services

The goal of Skyrim Network would be establishing a transparent, secure, decentralized and incentives driven framework for the open creation of creators and data asset. In the trading and asset management sector, we need to connect individual's values and credibility with assets more efficiently.

The platform will provide a fair and transparent platform with a self-governing ecosystem and on which news content value is determined by community consensus. This will be achieved by using blockchain technology to record and reward value-added actions by platform. These actions include content creation, content curation, validating transactions, providing data storage and so on.

It also provides a fair and transparent standard to highlight KOLs and publishers with more credibility, which may lead followers to get insights and implement trading actions. Users' trading actions and preferences in reading news, presenting real assets and trading actions, will all become critical data assets, which are going to be securely stored by the Skyrim Network.

All asset services on this platform will be provided by institutions on Skyrim Network platform, which mainly operate their services in trading, listing, issuing, mortgage, lending, etc. by protocols developed by Skyrim. All financial data will be stored distributedly in this system.

4.3.2 Skyrim Network Built-in DApp Platform

A DApp, called UNI, will be developed to provide a single entrance to any cryptocurrency related activities. It combines the standard services described in Section 5.3, i.e. providing the Skyrim Wallet, news feeding service, community service, a decentralized exchange, token sale, and online brokerage in many services. This fully functionalized App is favorable for any people who are interested in cryptocurrency industry. In particular, UNI provides a seamless user experience that users can discuss or trade directly in UNI when news of cryptocurrency is fed to them. Besides, UNI protects users from censorship and data privacy violation. UNI offers a better user experience in digital currency payment and peer-to-peer exchange compared to existing apps.

Here we present how UNI is designed.

With its innovative functions in friendly interactive user face, large groups, news feed with token incentives, wallet managements, and platform credits exchangeable in many crypto assets, this UNI DApp shows its huge potential in acquiring news users and retaining loyal ones. Since its first launch, UNI has kept a high weekly growth and acquired more than 200,000 active users. In near future, it is going to efficiently expand in Korea, Russia, and Southeast Asia as a critical player.

Every service on UNI has a market size of enormous potential. Taking the social media business as an example: according to Statista, there are 2.46 billion social media users in 2017, and this number is ever growing. It is predicted that there will be more than three billion social media users in 2021. Regarding with online brokerage services, newly emerging China based online brokerage providers like Tiger and Futu both have achieved more than 50 million USD annual profits and market capital of more than 1 billion USD.

4.3.3 Decentralized Data Asset Exchange

Skyrim Network has its own financing mechanism and product structure. This financing system has rules to follow, well documented and protect the absolute security of assets while benefiting users.

For digital assets, there is a great risk in the secondary market exchange. Risk-sensitive users shall choose the financial function on the Skyrim Network platform and invest in a higher-rated digital asset foundation. Skyrim Network will determine the ranking of the foundations by voting, thus the quality foundations will be displayed at the traffic portal, which on the

one hand, expand the foundation traffic, and on the other hand, recommend the excellent foundations to more users to ensure the user's revenue. Users can choose to use the appropriate amount of digital currency to invite people with expertise in one aspect answering some difficult questions. If the onlookers want to view, they must pay certain amount of digital currency. The answerer, the questioner and the viewer have benefited from such a win-win solution. This set of mechanisms will facilitate the generation of quality Q&A. These Q&A will also be kept on the blockchain for permanent benefits.

On this platform, we categorize individuals and institutions' information in 5 categories, such as ID certification, history background, consuming capability, behaviors, and social networks. This data stream will make a price of asset transactions in a fair and transparent way. The financial system connects individuals and institutions, and bridges information flow and capital flow.

4.3.4 Decentralized Stable Coin

We wanted a simple decentralized stablecoin, without the need to trust some company's hidden bank account or special algorithm. Services on our platform can be paid by stable coins, with framework that enables you to exchange fiat directly with an escrow account.

We welcome decentralized stable coin to be developed by ecosystem participants on our platform, which may support financial services, exchange, crypto traders, and commerce. This stable coin will bridge real world assets and blockchains, enabling trustworthy asset tokenization.

4.3.5 Decentralized Payment

Skyrim Network's foundation is going to operate a decentralized payment system with two digital currencies, SNS token and a stablecoin, which will be used to purchase offline and online products without geographical restrictions in the future.

To effectively motivate Skyrim Network users and realize the ecological growth of the platform, Skyrim Network has issued the platform's encrypted digital currency-Skyrim Network System Token (SNS). Platform vendors in various sectors such as releasing, loan, asset management, trading, insurance, sales, etc. will all use SNS to acquire traffic and improve liquidity.

4.3.6 Decentralized Reputation System

Regarding with its aim to build the news and community platform connecting all crypto users, this UNI DApp is intended to building a trusted network, which allows users to build trusted brands, show real assets, and present real track records in trading and investing. UNI is going to establish the standard in credibility and empower all participants to protect their data assets related to financial data and trading actions. UNI also provides an array of tools to help institutions and individuals better collect information, rank reputations of partners , make decisions, and implement trading strategies.

The UNI platform performs like an open finance platform, integrating multiple financial services related to crypto and other sectors to serve individuals and institution. Based on a trusted network in data asset and transparent track records of all participants, UNI bridges

information flow and capital flow, which outperforms traditional online brokerage providers tremendously.

5. Skyrim Network Ecosystem & Governance

5.1 Ecosystem Participants

Skyrim Network has clear and sharp strategy to involve ecosystem participants, including communities, crypto investors, data asset providers, developers, blockchains and clouds. Basically, we have there three different kinds of participants: killer community DApps, platform service providers, blockchains and miners.

First, Skyrim Network Core has solid experiences in developing decentralized communities and asset platform in the crypto industry in investment, incubation, social media, chain services, and DApps. Skyrim Network Core has built its own decentralized trusted network application UNI to form its own trusted platform.

Also, Skyrim Network Core co-worked Conflux Team and develop the next generation infrastructure blockchain service in a strategic level. Based on the chain architecture developed together, Skyrim Network develops the layer 2 customization with huge potential to support a variety of protocols and multiple DApps services. Basically, we will provide solid data asset protocols for traditional finance and crypto industry together.

Skyrim network protocols will also be plugged in different key blockchain. As a key contributor to Skyrim Network, Tron foundation provided the huge user base, strategic partnership and go-to-market support for this ecosystem. Also, its strategic partner DACC, invested by Tron, has developed more than 1 million global community users & 5,000 global KOLs. Not only with 3 AM & 499 decentralized community, the largest blockchain communities in Asia-Pacific regions with the formation of millions of user base.

In the business and economic side, Skyrim Network core will leverage blockchain ventures like BlockVC, DKB Fund and Roark Fund, key foundations like Tron, DACC & Conflux foundations and more than 100 institutions and top global exchanges to extend its service in the globe. Skyrim network core already invested and incubated in top tier wallets, exchanges, communities, crowdfunding platforms, intelligent protocol, security solutions, wallets, human capital management, intelligent hardware, etc. more than 100 DApps & services and 10million crypto users. Based on what we have now, we will get started from open finance industry and internet media to extend our global ecosystem.

5.2 Skyrim Network Core & Co-builders

Skyrim Network core includes a world-class globalized team of blockchain service developers, platfrom builders, and ecosystem designers & governers. To become part of the Skyrim Network core, each of its current members had either to win in the world's Skyrim

Network programming contests or to take the first place in one of the nationwide multi-level coding competitions or to pass the votes of the core governance. Skyrim network also involves the best ecosystem co-builders such as TRON, Conflux, DACC, 499, BlockVC and top exchanges. The verification of co-builders will be held by the governance.

Jason Chung –Core Protocol Developer

- 10 years cryptology expertee in building peer-peer protocols
- 8 years of platform and os development experiences
- Dedicated to building the next generation of safer and more expressive communication technology

Vincent- MD

Vincent has more than 10 years operation and management experiences in top Internet and blockchain companies. As an early believer in blockchain, Vincent has attended to operation and investment of several projects, such as Sopay, Delphy, etc.

Sergii Vernick- Global Market Head

- As Product Manager of Silicon Valley startup and in charge of bringing the product to the US market
- 9 years software development experience and 3 years financial services experience

Celine Yang- Asia-Pacific Operation Head

- A serial entrepreneur , with 8 years cross-border ecommerce experiences as an operation partner
- Lead global decentralized community

5.3 Decentralized Governance & Compliance

5.3.1 Decentralized Governance

Community management governed by super-representatives. Unlike the centralized online community, Skyrim network provides the purely decentralized management method for our ecosystem.

Skyrim Network super-representatives will come from community influencers, investors, miners and service & asset providers.

Skyrim Network core will verify the identification of authoritative candidates. According to the specific personal information, historical postings, and exchange of information records, the community participants can identify them in multiple ways. It will be determined and voted by many parties that a specific individual or institution can obtain certain credibility in the corresponding community and exist as an authoritative node. By selecting these super-representatives, Skyrim Network core will help to organize them for community management in accordance with their credibility level and offer corresponding rights in return.

5.3.2 Compliance

Identity verification and data systems of Skyrim network are compliant with the various legal frameworks in different countries and regions worldwide. Skyrim Network will build mechanisms to apply legal requirements into our roadmap to make sure that all sectors are compliant as the components of the trusted data asset network.

5.4 Skyrim Network Economic & Token Models

5.4.1 Skyrim Network Economic

To ensure the ecosystem prosperity in the long run, Skyrim Network will issue different tokens to facility the transactions of data assets, simplified the pricing model of organizations and storage the value of its whole ecosystem. Transactors, builders and miners are three key different parties in our ecosystem.

For the balance of a healthy & long-term ecosystem and encourage more creations of data assets, Skyrim Network economics is designed to issue its own Skyrim Network System tokens (SNS) to encourage the liquidity in platform level for investors, developers and asset providers, as builders party. Secondly, its Skyrim Network Gas (SGAS) will ensure the decentralization of the whole system, as the miners party. We will also integrate a decentralized stable coin to ensure the transactional system in our DApps.

As a decentralized economy, Skyrim Network realized the needs of different token models to ensure the governance, economic creations and transaction stability and our limit to reach the optimization of economic models as well. Skyrim Network Governance will hold the right to vote for innovations in economic designs in our ecosystem.

5.4.2 Token Models

Skyrim Network will issue a total supply of 499,900,000,000 Skyrim Network System tokens (SNS) as a contribution-mining-based utility token.

Firstly, supported by TRON blockchain with its TRC 10 protocol, SNS token will be available for major TRON wallets and can be re-issued to Skyrim Network chain after it launched.

SNS supply will reach its decentralization equilibrium point after 10 years and its reduction of output with production difficulty will happen every two years; And whereas SNS initially has no circulation in the market at the first beginning and is mainly used for building Skyrim Network ecosystem and motivating the entire community. All parties need to contribute for the asset ecosystem to get SNS tokens besides its trades on exchanges.

The Skyrim Network Foundation proposes to generate and issue SNSs soon after the creation of the Skyrim Network Foundation. Upon issuance and prior to the completion of the Skyrim Network platform, Tokens will be issued as tokens based on the Token Standard. SNS Token is the basic utility token applied for building our ecosystem and providing incentives for those who are willing to make contributions to the whole community, e.g. our guardians or super-representatives, investors, asset providers and team members as well. More importantly, cooperative partners are eligible to mortgage SNS for certain services provided by Skyrim core.

Its main functions are as follows:

- Compensation for platform services;
- Reward verification for certain contribution;
- Records medium of transmitting value;

There are several asset-related contributions incentives model for SNS holders:

- Data asset providers, including data contribution, storage and exchange;
- Early participants and super-representatives of Skyrim Network community;
- Developers of Skyrim Network ecosystem;
- Third-party developers on the Skyrim Network platform;
- Contributors of Skyrim Network Technology Community Code;

Skyrim Network designs a dual token model. Specifically, SGAS is the token used for incentives given to miners as Mining of SGAS to incentive miners and ensure our decentralization in infrastructure level.

5.4.3 Proof of Asset Mining

SNS can be used as a proof of Asset Mining including but not limited by:

- Mortgage to obtain customized services, e.g. asset transactions, or valuations;
- Compensation to ensure liquidity for data assets;
- Verification for digital assets on the Skyrim Network platform;
- Credibility and reputations for data assets and owners;
- Connection of Storage of value in crypto asset level such as Bitcoin and so on;

5.5 Partners

Strategic Partner

Partners

6. Disclaimer

SNS Foundation does not make, and hereby disclaims, any representation or warranty with respect to or SNS Tokens (such as merchantability or fitness for particular purposes), except those expressly specified in this White Paper. Each participant's decision to participate in the SNS Token sale and purchase any SNS Token shall be made based on his/her own knowledge of the SNS platform and SNS Tokens and the information disclosed in this White Paper. Without prejudice to the generality of the foregoing, each participant will, upon the launch of the platform, accept SNS Tokens on an "as is" basis, irrespective of the technical specifications, parameters, performance or function thereof. This Whitepaper may be amended from time to time and the Foundation and Distributor shall be under no obligation to inform you of such amendment. You should read carefully this Whitepaper, and any amended version thereto, including the final version of this Whitepaper, as may be published at http://SNS.co.

SNS Foundation hereby expressly disclaims its liability and refuse to be liable for the following liabilities:

(1) any person's purchase of SNS Tokens in violation of any anti-money laundering, counter-terrorism financing or other regulatory requirements that are imposed in any jurisdiction;
(2) any claims or breach of intellectual property rights as a result of any content shared by the content provider on the SNS platform;
(3) any person's purchase of SNS Tokens in violation of any representation, warranty, obligation, covenant or other provision under this White Paper, which results in the failure of paying and withdrawing SNS Tokens;
(3) termination of the SNS Token crowd-sale for any reason;
(4) failure or termination of the SNS platform's development which results in the failure to deliver SNS Tokens;
(5) delay or rescheduling of the SNS platform's development and resulting failure to meet any published schedules;
(6) any error, flaw, defect or other issues in the source code of the SNS platform;
(7) any malfunction, breakdown, collapse, rollback or hard forking of the original public chain the SNS platform replies on;
(9) utilization of the proceeds raised through the SNS Token sale;
(10) failure to promptly and completely disclose any information relating to the development of the SNS platform;
(11) any participant's divulgence, loss or destruction of the private key to his/her wallet for cryptocurrency or cryptographic (in particular the private key to the SNS Token wallet);
(12) any default, breach, infringement, breakdown, collapse, service suspension or interruption, fraud, mishandling, misconduct, malpractice, negligence, bankruptcy, insolvency, dissolution or winding-up of any third-party crowdfunding SNS platform or exchange for SNS Token;
(13) any difference, conflict or contradiction between this White Paper and the agreement between any participant and any third-party crowdfunding portal;
(14) trading or speculation of SNS Tokens by any person;
(15) listing or delisting of SNS Tokens on or from any exchange;
(16) SNS Tokens being classified or treated by any government, quasi-government, authority or public body as a type of currency, securities, commercial paper, negotiable instrument, investment instrument or otherwise that results in it being banned, regulated or subject to certain legal restrictions;
(17) any damage, loss, claim, liability, punishment, cost or other adverse impact that is caused by, or associated with, or connected with, even incidental to or relevant to the risk factors disclosed in this White Paper.

This is a conceptual white paper describing our proposed SNS. This whitepaper may be amended or replaced at any time. There are no obligations to update this whitepaper or to provide recipients with access to any information beyond what is provided in this whitepaper. Readers are notified as follows:
Not available to all persons. The SNS platform and SNS Tokens are not available to all persons. Participation may be subject to certain restrictions and requirements, including the need to provide certain information and documents.
No offer of regulated products in any jurisdiction. SNS Tokens are not intended to constitute securities or any other regulated product in any jurisdiction. This whitepaper does not constitute a prospectus nor offer document of any sort and is not intended to constitute an offer or solicitation of securities or any regulated product in any jurisdiction. This whitepaper has not been reviewed by any regulatory authority in any jurisdiction.
No advice. This whitepaper does not constitute advice in relation to whether you should participate in the SNS platform or acquire any SNS Tokens. Nor should this whitepaper be

relied upon with any contract or purchasing decision in relation to the SNS platform and SNS Tokens.

No representations or warranties. No representations or warranties are made as to the accuracy or completeness of the information, statements, opinions, or other matters described in this document or otherwise communicated in connection with the SNS Project. Without limitation, no representation or warranty is given as to the achievement or reasonableness of any forward-looking or conceptual statements. Nothing in this document is or should be relied upon as a promise or representation as to the future. To the fullest extent permitted under applicable law, all liability for any loss or damage whatsoever, whether foreseeable or not, arising from or in connection with any person acting on this White Paper or any aspect of it, notwithstanding any negligence, default, or lack of care, is disclaimed. To the extent liability may be restricted but not fully disclaimed, it is restricted to the maximum extent permitted by applicable law.

English version prevails. This whitepaper is provided in an official English version. Any translation is for reference purposes only and is not certified by any person. If there is any inconsistency between a translation and the English version of this White Paper, then the English version prevails.

The SNS Development Team and SNS Foundation will strive to make the SNS Project as successful as possible. However, digital assets and platforms involve risk, and success is not guaranteed. Prospective SNS users and SNS Token holders must assess their risks and their ability to bear those risks. In addition, all necessary professional advice, including in relation to tax and accounting treatment, must be taken prior to participating in the SNS platform.

NOTICE TO RESIDENTS OF THE UNITED STATES

The offer and sale of this token has not been registered under the U.S. Securities Act of 1933, as amended (the “Securities Act”), or under the laws of certain states as this token should not be taken as securities. This token may not be offered, sold or otherwise transferred, pledged or hypothecated except as permitted under the act and applicable state laws pursuant to an effective registration statement or an exemption therefrom.

NOTICE TO RESIDENTS OF CANADA

Unless permitted under legislation, the holder of this token must not trade the token before the date that the issuer becomes a reporting issuer in any province or territory of Canada.

NOTICE TO RESIDENTS OF CHINA

The tokens are not being offered or sold and may not be offered or sold, directly or indirectly, within the People’s Republic of China (for such purposes, not including the Hong Kong and Macau Special Administrative Regions or Taiwan), except as permitted by the laws and regulations of the People’s Republic of China.

NOTICE TO RESIDENTS OF THE UNITED KINGDOM

In the united Kingdom this document is being distributed only to, and is directed only at,: (i) investment professionals (within the meaning of article 19(5) of The Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 as amended (the “FPO”)); (ii) persons or entities of a kind described in article 49 of the FPO; (iii) certified sophisticated investors (within the meaning of article 50(1) of the FPO); and (iv) other persons to whom it may otherwise lawfully be communicated (all such persons together being referred to as “Relevant Persons”).

NOTICE TO RESIDENTS OF OTHER COUNTRIES

All participants must ensure that they are permitted by the laws of their countries to purchase SNS Tokens. SNS Foundation will only ensure that the SNS platform is legal and compliant with the law of the issuing country but will not ensure all other countries adopt or use similar laws, especially the event that the participant use other methods to avoid relevant

laws or intentionally hide from any relevant legislations. SNS Foundation will not be liable for this.
This document has not been approved by an authorized person. Any information to which this document relates is available only to a relevant person. This document is only for relevant persons and none relevant persons shall not take any action based on this document nor should he/she/they rely on it. It is a condition of you receiving and retaining this document that you warrant to the SNS Foundation, its directors, and its officers that you are a relevant person.

SNS Foundation's social media and email platform are places where we encourage interaction, discussion, organization and participation between users of the community, in fact anyone interested in the product of SNS Foundation.
Whilst we make reasonable efforts to monitor participation to ensure that discussions are related to products that are made available in the community, there may be situations where we are not in a position to monitor all statements, comments and views made by every user. We ask that you're respectful in your comments. We reserve the right to remove anything we deem to be abusive or personal attacks, material that is unlawful, obscene, defamatory, threatening, harassing, abusive, slanderous, hateful or embarrassing to any other entity or persons, third party advertising, chain letters or 'spams'. Please be aware that anything posted may potentially be read by thousands (or hundreds of thousands) even years from now. Therefore, users should exercise cautions when posting on any of our social media sites. We also reserve the right to terminate involvement by users who post such content.
The views and opinions expressed on any social media sites of ours do not necessarily represent those of SNS Foundation. Therefore, we cannot be held responsible for the accuracy or reliability of information posted by external parties. Any information posted on any of our social media platforms should not be considered as financial, legal, accounting or other professional advice.
For your safety, never include your phone number, email, address or other personal information in a post. Your comments are visible to all.
Certain information set forth in our website and other documents may contain "forward-looking information", including "future oriented financial information" and "financial outlook", under any applicable laws and regulations (collectively referred to herein as forward-looking statements). Except for statements of historical fact, information contained herein constitutes forward-looking statements and includes, but is not limited to, the (i) projected financial performance of SNS Token; (ii) completion of, and the use of proceeds from, the sale of SNS Token being offered during the token sale; (iii) the expected development of the business, projects and joint ventures; (iv) execution of SNS Token's vision and growth strategy, including with respect to future M&A activity and global growth; (v) sources and availability of third-party financing for SNS Foundation's projects; (vi) completion of the platform's projects that are currently underway, in development or otherwise under consideration; (vii) renewal of the platform's current customer, supplier and other material agreements; and (viii) future liquidity, working capital, and capital requirements. Forward-looking statements are provided to allow potential participants the opportunity to understand management's beliefs and opinions in respect of the future so that they may use such beliefs and opinions as one factor in evaluating an investment. These statements are not guarantees of future performance and undue reliance should not be placed on them. Such forward-looking statements necessarily involve known and unknown risks and uncertainties, which may cause actual performance and financial results in future periods to differ materially from any projections of future performance or result expressed or

implied by such forward-looking statements. For further explanation of the risk involved in the SNS platform's community please consult the documents as issued by SNS Foundation.

Although forward-looking statements contained in this presentation are based upon what management of SNS Foundation believes are reasonable assumptions, there can be no assurance that forward-looking statements will prove to be accurate, as actual results and future events could differ materially from those anticipated in such statements. The SNS platform undertakes no obligation to update forward-looking statements if circumstances or management's estimates or opinions should change except as required by applicable securities laws. The reader is cautioned not to place undue reliance on forward-looking statements.