NKN: A Scalable Self-Evolutionary And Self-Incentivized Decentralized Network

NKN Lab
www.nkn.org
(Dated: February 16, 2018)

NKN (New Kind of Network) is a new generation of highly scalable, self-evolving and self-incentivized blockchain network infrastructure. NKN addresses the network decentralization and self-evolution by introducing Cellular Automata (CA) methodology [1, 2] for both dynamism and efficiency. NKN tokenizes network connectivity and data transmission capacity by a novel and useful Proof of Work. NKN focuses on decentralizing network resource, similar to how Bitcoin [3] or Ethereum [4] decentralize computing power as well as how IPFS/Filecoin[5, 6] decentralize storage. Together, they form the three pillars of the Internet infrastructure for next generation blockchain systems. NKN ultimately makes the network more decentralized, efficient, equalized, robust and secure, thus enabling healthier, safer, and more open Internet.

CONTENTS

1. CHALLENGES

After years of transmutation, Internet is in danger of losing its original vision and spirit. For example, Network Neutrality is overturned [7]; spectrum and bandwidth are not efficiently utilized; information is fragmented and can be censored; privacy protection is limited. These signal that the network needs a reform.

Existing solutions are not suitable for next generation blockchain systems due to the following reasons:

- Utilize a centralized approach to improve efficiency.
- Sacrifice the scalability of the network to speed up consensus.
- Limit participation rate of nodes or require authorization to increase "security".
- Use purely financial motivations or trusted third-parties to solve problems which should be solved by mathematical/technical methods.

1.1. Limitations of P2P Networks

Peer-to-peer (P2P) networks currently face several major challenges, which are the opportunities for NKN. First static network topology is vulnerable to faulty and malicious attack. Second, there is no economic self-incentive scheme for network connectivity and data transmission. Finally, network scalability is widely sacrificed to enhance controllability. These are all to be solved by the NKN as shown in Fig. 1.

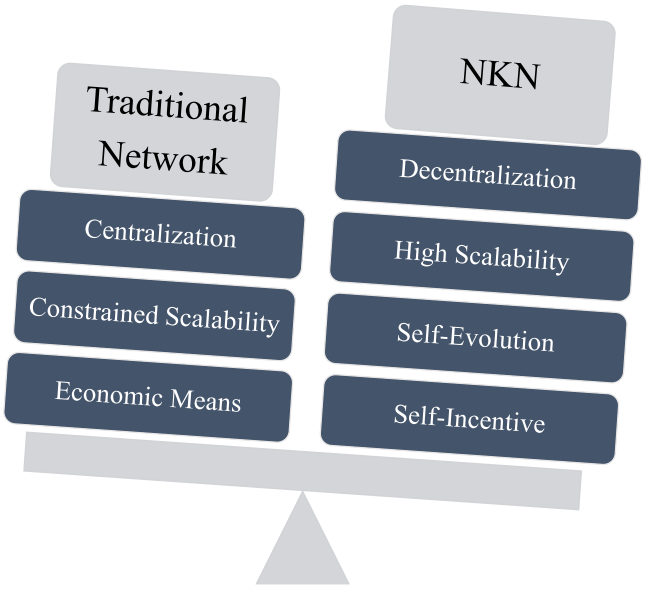

FIG. 1. Illustration of feature comparisons between existing solutions and NKN layers

1.2. Resource Utilization

A highly reliable, secure and diverse Internet is essential to everyone. Yet, huge inefficiency exists in the current network when providing global connectivity and information transmission. It's time to rebuild the network we want, not just patch the network we have. A fully decentralized and anonymous peer-to-peer system offers huge potential in terms of improved efficiency, sustainability and safety for industry and society.

1.3. Net Neutrality & Fragmentation

When the Federal Communications Commission (FCC) approved a measure to remove the net neutrality rules by the end of 2017 [7], a demand of ending our reliance on big telecom monopolies and building decentralized, affordable, locally owned Internet infrastructure becomes ever stronger. Unrestricted, non-surveilled Internet access environment has becoming unsustainable under an endless stream of attacks and blockage, leading to selective and biased information propagation. Without a proper incentivizing engagement scheme, it is almost impossible to maintain a constant and secured information propagation channel.

Furthermore, Internet has become fragmented due to various reasons. This not only exacerbates separation but also negatively impacts innovation of science, technology and economy.

2. VISION

NKN intends to truly revolutionize the entire networking technology and business.NKN want to be the protocol equivalent of TCP/IP for Internet in the blockchain era. NKN wants to be the Uber or Airbnb of the 1 Trillion dollar communication service business, but without a central entity. NKN aspires to Free the bits, and build the Internet we always wanted.

2.1. NKNs objectives

NKN sets the following objectives:

- anyone and any node can connect to this fully open network from any place at any time
- Promote network sharing
- Secure net neutrality from network layer innovations
- Always keep network open and scalable
- Perform efficient and dynamic routing

- Tokenize network connectivity and data transmission assets and incentivize participating nodes
- Design and build the next generation of blockchain network

2.2. The third pillar: Networking

By blockchainizing the third and probably the last pillar of Internet infrastructure, NKN will revolutionize the blockchain ecosystem by innovating on the network layer, after Bitcoin/Ethereum blockchainized computing power and IPFS/Filecoin blockchainized storage. The next generation blockchains based on NKN are capable of supporting new kind of decentralized applications (DApp) which have much more powerful connectivity and transmission capability. The vision of NKN is not only to revolutionize the decentralized network layers itself, but also to develop core technologies for the next generation blockchain itself.

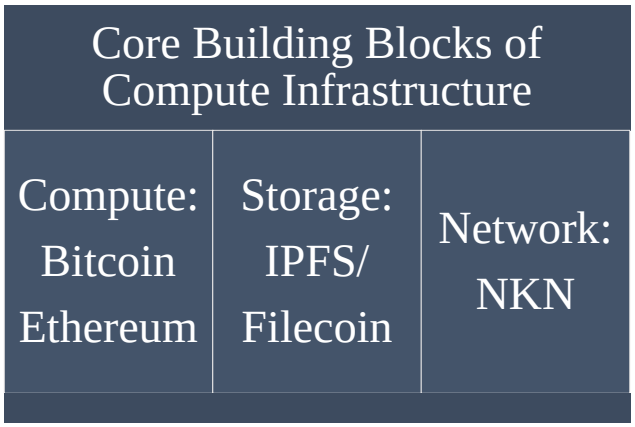

FIG. 2. NKN as the 3rd pillar of blockchainized Internet infrastructure.

2.3. Elementary components

NKN builds upon several innovative elementary components that are different from existing solutions, as shown in Fig. 3.

1. **Blockchainizing the remaining core building blocks of computing infrastructure**: NKN introduces the concept of decentralized data transmission network (DDTN) scheme and utilizes truly decentralized blockchain to provide network connectivity and data transmission capability by using massive independent relay nodes to solve the problem of precipitation of redundant data on the network.

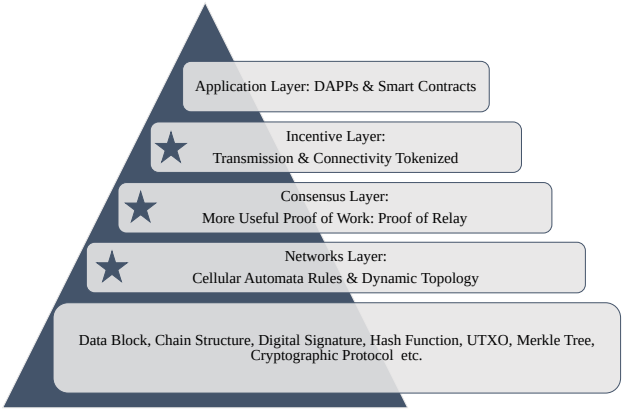

FIG. 3. Illustration of NKN elementary components.

2. **Cellular Automata powered DDTN**: NKN introduces the idea of using Cellular Automata to reconstruct the network layer. The intrinsic characteristics of Cellular Automata such as decentralization, peer equivalence and concurrency enable us to build a truly decentralized blockchain network.
3. **Cellular Automata driven consensus**: NKN achieves consensus efficiently with high fault tolerance in large scale distributed systems based on Cellular Automata, which is essential for decentralized systems without trusted third parties.
4. **Proof-of-Relay, A Useful Proof-of-Work**: NKN proposes Proof-of-Relay (PoR), a mechanism that encourages participants to contribute to blockchain by sharing their bandwidth to get rewards, enhancing network connectivity and data transmission capacity. PoR is a useful Proof-of-Work (PoW).
5. **Novel token mechanism for tokenization of network connectivity and data transmission capability**: NKN tokenizes network connectivity and data transmission capability by encouraging participants to share their bandwidth and connectivity in exchange for NNC (New Network Coin) and Qi (Gas equivalence). Idle network resources can be better used through such sharing mechanism. NKN improves the utilization of network resources and the efficiency of data transmission.
6. **Complete Toolbox for fast and painless DApp development**: With NKN, DApp developers now have a complete toolbox for building truly decentralized applications quickly and easily. DApp developers can focus entirely on creativity, innovation, user interface / user experience and business logic. Developers no longer need to go through wild jungles of blockchain, cryptography, consensus mechanisms, identity and security before starting to work on the products.

NKN utilizes Cellular Automata methodologies to achieve full decentralization. All nodes are equal, truly peer to peer, and each is capable of both consuming as well as relaying data. Cellular Automata makes it possible to have simple local rules that can generate highly dynamic and highly scalable global network overlay topology, that is independent of the underlying physical and logical infrastructure. The simplicity and locality of rules make it possible to have cost effective implementation on all type of network devices, from IoT, smart phones, all the way to edge and core routers. Despite its seemingly simplicity, Cellular Automata enabled routing can be highly random and unpredictable, thus providing superior security and privacy.

NKN nodes get rewarded for providing connectivity and transmission power, resulting in a fully competitive marketplace optimized for maximizing the entire network capacity. For existing networks, NKN will increase the utilization of capacity by sharing the unused bandwidth of participating nodes. More and more new nodes will join the network to earn reward, thus quickly bootstrapping and expanding the NKN network. Existing nodes are incentivized to upgrade and increase capacity. All of above will further boost overall network capacity, as well as improve the dynamic topology since the network has much more degrees of freedom in choosing the route.

In addition, NKN proposes a novel and more useful proof of work. Unlike traditional hashing computation type Proof of Work that converts electricity into heat, NKN introduces Proof of Relay based on many useful activities including staying online for extended period, expanding amount of peer connection, providing high speed and low latency relay, and etc. Even the consensus algorithm is designed from ground up to improve efficiency and fairness, while converge deterministically and globally based on local knowledge.

Furthermore, NKN intends to promote network sharing and network ownership by its users. NKNs economic model and governance model will reflect this in design and in implementation. Therefore, all these technology and economic model innovations truly complement each other and together will amplify the power of NKN network.

2.4. Complete platform for fast and painless DApp development

With NKN, DApp developers now have a complete toolbox to build truly distributed applications rapidly and painlessly. DApp developers can focus entirely on the ideas and innovation, UI (user interface) /UX (user experience), and business logic that make their product successful to the end users. They no longer need to wade through the wild jungle of blockchain, cryptography, consensus mechanism, identity and security before they even write one line of code for their users.

For example, in traditional app development with centralized SaaS (Software as a Service) offerings, you can run your app on cloud computing platforms, store your data on cloud storage, use web services for text message, phone call and payment. In the decentralized blockchain world, it is already conceivable today to build a new kind of Facebook by using Ethereum [4] /NEO [8] for computing, IPFS [5] for storage, and NKN for networking. The beauty of this new paradigm is that users will own their identity and data, and can be both consumer and provider of the entire system as well. On top of that, at each layer there are built-in self-incentive mechanism to maximize the network effect and bootstrap the entire community. NKN will be one of the three foundational elements and play a critical role in this decentralized paradigm.

3. TECHNOLOGY FOUNDATIONS

In this whitepaper, we take selective elements of the NKS (New Kind of Science) [2] as inspiration. NKN utilizes microscopic rules based on Cellular Automata to define network topology, achieve self-evolution behaviors, explore Cellular Automata driven consensus, which is fundamentally different from existing blockchain network layer.

As a powerful tool to study complex systems, Cellular Automaton is closely linked to philosophical categories such as simple and complex, micro and macro, local and global, finite and infinite, discrete and continuous, etc.

3.1. Cellular Automata

Cellular Automata (CA) is a state machine with a collection of nodes, each changing its state following a local rule that only depends on its neighbors. Each node only has a few neighbor nodes. Propagating through local interactions, local states will eventually affect the global behavior of CA. The desired openness of network is determined by the homogeneity of Cellular Automata where all the nodes are identical, forming a fully decentralized P2P (peer-to-peer) network. Each node in the NKN network is constantly updated based on its current state as well as the states of neighbors. The neighbors of each node are also dynamically changing so that the network topology is also dynamical without changing its underlying infrastructure and protocols.

3.2. Rules as Formulas

The Cellular Automata programming formula is called "local rule", which is an indispensable rule for next generation network of NKN and has an important influence on the network topology [2, 9–12].

A local rule is a Cellular Automaton with complex but organized behaviors on the boundary between stability

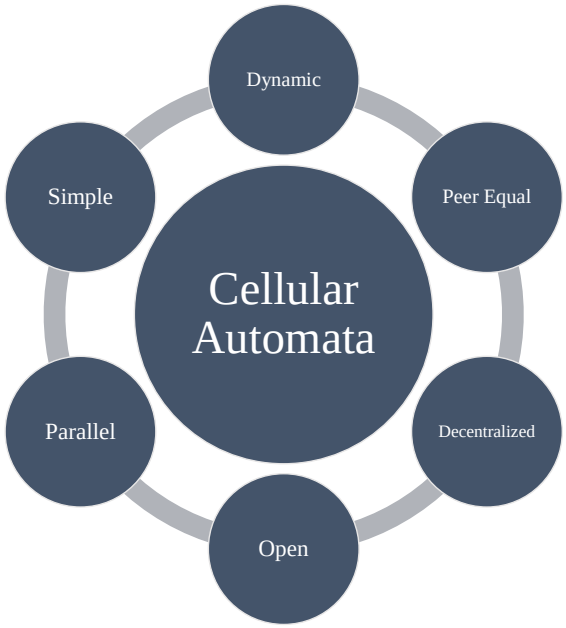

FIG. 4. Illustration of properties of Cellular Automata.

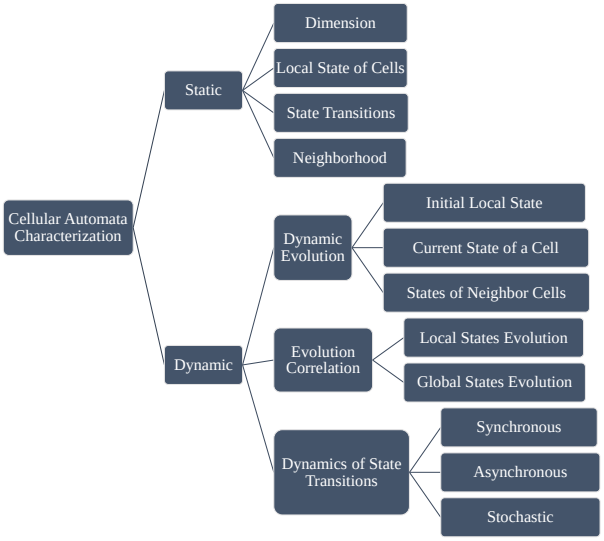

FIG. 5. Characteristics of Cellular Automata, the basis of NKN, enabling networks of decentralization, dynamics and self-evolution.

and chaos. Rules are essential because they are formulas to program Cellular Automata and Automata Networks. The static characteristics of a Cellular Automaton is a discrete dynamic system defined as

$$\mathrm{CA} = (S, d, N, f) \tag{1}$$

Finite number of nodes interact in a regular network. d denotes network dimension. S represents states of nodes, where each node has a local state. The state of all nodes determines the global state. f denotes a state transition function, which has a dramatic impact on the global evolution of the system. N denotes neighbor set, i.e. which neighbor nodes are taken into account in local state transitions.

The dynamic characteristics of a Cellular Automaton is illustrated in Fig. 5. Dynamic evolution starts from an initial state. Nodes change their states based on their current states and the states of their neighbor nodes. The global state is fully determined by local states of all nodes and evolves accordingly.

We believe CA-based or CA-derived systems are more natural and organic than current approaches. Complex systems with such a simple structure are closer to natural systems, thus enabling self-evolution.

4. NEW KIND OF NETWORK

NKN is the next generation of peer to peer network infrastructure built upon blockchain technology backed by Cellular Automata theory aiming at revolutionizing the Internet with true decentralization and native token incentive mechanism.

4.1. Next Generation Decentralized Network

Current leaders in blockchain area, Bitcoin/Ethereum, tokenize computational power through Proof of Work (PoW). IPFS/Filecoin [5, 6], Sia [13] and Storj [14], on the other hand, tokenize storage power through PoW. Yet, few system blockchainizes network connectivity and data transmission power, the third essential building block in the Internet. NKN is designed to tokenize network connectivity and data transmission capability as a useful PoW.

NKN solves the "efficiency" problem of blockchain by equalizing all nodes in the network. Each node follows a rule of Cellular Automaton and updates its state based on local rules. Proposed by "Father of Computers" John Von Neumann in the 1940s, Cellular Automaton (CA) is a generic term for a type of model, a framework characterized by discrete time, space, state, spatial interaction, and time causality [15, 16]. It is a discrete system that evolves locally according to specific rules and is proved to be able to emulate the evolution of complex systems. Cellular Automaton has the characteristics of decentralization, peer equality and concurrency. For the first time, NKN proposed Cellular Automata as the fundamental element of the network layer for blockchain, so as to ensure that the entire network layer can benefit from the advantages of it.

Updating formulas in Cellular Automata are called "local rules", which are found to be the critical factor that controls the transition of Cellular Automaton between stability and chaos [2]. As an indispensable part of NKN, rules are one of the main factors impacting the network topology.

NKN introduced the concept of Decentralized Data Transmission Network (DDTN). DDTN combines mul-

tiple independent and self-organized relay nodes to provide clients with connectivity and data transmission capability. This coordination is decentralized and does not require trust of any involved parties. The secure operation of NKN is achieved through a consensus mechanism that coordinates and validates the operations performed by each party. DDTN provides a variety of strategies for the decentralized application (DAPP).

In contrast to the centralized network connectivity and data transmission, due to the decentralization characteristics of blockchain, there are multiple channels between nodes to select. Also, all transmission nodes are utilized for data transmission to prevent data traffic congestion. Native tokens can incentivize the sharing of network connectivity and transmission capability and eventually minimize wasted bandwidth and connectivity. We call such property self-incentive.

We can conclude that the key characteristics of NKN are: decentralization, scalability, self-evolution, and self-incentive.

4.2. A useful Proof of Work

To understand this section, let's first have a primer on the blockchain technology pioneer Bitcoin and its operating mechanism, especially the generation and measure of Bitcoin.

We all know that Bitcoin [3] network generates new Bitcoin by "mining." The so-called "mining" is actually a Proof of Work mechanism that rewards Bitcoin and transaction fees to "miners", which are in proportion to completing the work of designated difficulty and competition with other nodes for Bitcoin blocks to record transactions. However, the "mining" process requires specialized and expensive hardware and consumes a lot of energy.

According to data from Dgiconomist and RIA Novosti, Bitcoin's proof of work mechanism consumed more than 40 terawatt hours of electricity in 2017. As of December 2017, Ethereum [4] consumed more than 10 terawatt hours of electricity during its operation history. Electricity consumed by these two cryptocurrencies combined has surpassed Jordan, Iceland, Libya and other countries.

A way to prove the work and avoid wasting resources is highly desired across the industry. NKN has invented an alternative to the traditional proof of work, by providing a more decentralized, dynamically evolving, self-organizing and self-evolving network infrastructure and designing a whole new set of consensus mechanisms.

This innovation based on network transmission and connectivity capability, or proof of work does not result in a waste of resources. Instead, it is a peer-to-peer sharing mechanism at blockchain level. In other words, all developers involved in the NKN community receive the rewards by contributing more network traffic than they consume. Unlike well-known bitcoin, NKN provides more of a "network-sharing" capability for connectivity and data transmission. The consensus algorithm uses Proof of Relay mechanism to guarantee network data transmission. Each node in the network has adjacent nodes for connectivity and data transmission. The development and expansion of the network transmission capabilities rely entirely on the participants contribution. At the same time, participants will receive rewards when sharing the bandwidth and connectivity capability.

Through the construction of a novel consensus mechanism based on Cellular Automata theory, NKN will achieve a more useful and practical proof of work to solve the problems caused by the widely criticized Bitcoin traditional proof of work.

4.3. Network topology and routing

In the network concept, the interacting elements are depicted as nodes and the interactions between the nodes are represented by edges/links connecting the corresponding nodes. The strength of the complex network paradigm lies in its ability to capture essential topological properties of interacting schemes while cutting down the specifics of both the nodes and interactions. In NKN, Cellular Automata is introduced to power the network. Therefore, Cellular Automata on Networks (CAoN) was seen as a natural extension of the Cellular Automata [9, 10, 17]. We use CAoN as an architecture which bridges the topological evolution of a network to its upper layers of a blockchain system. It is useful for dealing with a network in which the topology evolves according to predefined microscopic rules. Meanwhile, there is a dynamic process taking place on the network due to the inherent nature of Cellular Automata. We build it as a network infrastructure of blockchain, seeking true decentralization. Therefore,the network dynamic topology is interrelated with upper layers of a blockchain system. In practice, the CAoN allows for easy technical implementation of the microscopic rule involved in blockchain network layer.

To use a CAoN model a network behavior, we consider a mesh/P2P network at certain time t which is to be grown to a dimension of M nodes. As nodes can be added to the system at each time step, the overall network layer would be considered to own capability of self-growth/self-evolution. A representation is to consider the blockchain network layer as being of size M at all times where at certain time t many of the nodes have no links. Messages Regarding the network topology is entirely incorporated within an adjacency matrix $A(t)$ which is of dimension $M \times M$. The matrix holds information about which edges/links exist, their degree, direction and weights.The evolution of the network then is a process that alters the elements within this adjacency matrix, updating the attributes of any of the possible links which exist in the blockchain network layer. If the microscopic rule governing the evolution process is solely related to quantities which can be derived from the

current network topology then the evolution can be expressed in terms of an interaction function f acting upon the adjacency matrix as

$$A(t+1) = f[A(t)]. \tag{2}$$

The rules used correspond to any property of the nodes or the links upon designing a proper blockchain network mechanism. Be achieved in practice by visiting all possible links within the adjacency matrix $A(t)$ for a blockchain network containing M nodes once every time step. The update as to the nature of the link at the next time step is then prescribed by the microscopic rules. The rules can take the form of a lookup table in which the state of links are evaluated and the states are prescribed for the next time step in which is similar to the update of a cell within a classic Cellular Automaton except that it acts upon the connectivity of a node, thereby generating $A(t+1)$. This link-orientated update is a generic description of a dynamic network. The essential features of that evolution of blockchain network are then contained within the exhaustive rules.

On the other hand, the dynamical process influences the subsequent network topological evolution, so that topological properties are bridged to the upper layer functions of a blockchain system and vice versa. The governance of the topological update process by microscopic rules relates not only to network related quantities but also blockchain functional aspects of the nodes or links. Since the blockchain functional process requires a network on which to perform, NKN separates the network evolution into two phases. Define writing the blockchain functional message set relating to nodes or links at some time t as some matrix $S(t)$, the formal description of the evolution can be expressed in terms of the interaction function f and g as

$$A(t+1) = f[A(t), S(t)] \tag{3}$$

$$S(t+1) = g[A(t+1), S(t)] \tag{4}$$

Eq. 4 states that the network evolves according to certain process, which is determined by its own current topology $A(t)$, and also by certain attributes of its nodes and links that includes blockchain function-based message set $S(t)$. The blockchain functional process then occurs on the network layer to generate the new set of message $S(t+1)$. The global state of the blockchain is incorporated by the matrices A and S.

Each time the block is received, the neighbor updates its own node status and broadcasts its state and height with digital signature. These states will affect whether these nodes will be forwarded at the time of data packet transmission, indirectly affecting the topology of the entire network without changing the physical layer or the underlying protocol.

Furthermore, each block generation resembles the system's clock or the entire network's metronome, and the state of all nodes changes or remains the same regardless of the surrounding conditions, depending on the rules and node's current state

As an example to illustrate how we model the network, in ideal case, a general Network Automaton rule setup that allows an arbitrary number of neighbors with no set orientation. In this way, any network topology can be pre-constructed for use with any one of these Cellular Automaton rules. For simplicity, we adopt a minimalist approach to emulate blockchain expanding and data relay from a small set of microscopic rules. Provided that blockchain system at initial state is a cube connectivity with each node in a three dimensional (3D) space. The data transmission and connectivity between nodes are X, Y and Z, reflecting possible data transmission and connectivity of three, forming a cube at time step index zero, as shown in Fig. 6.

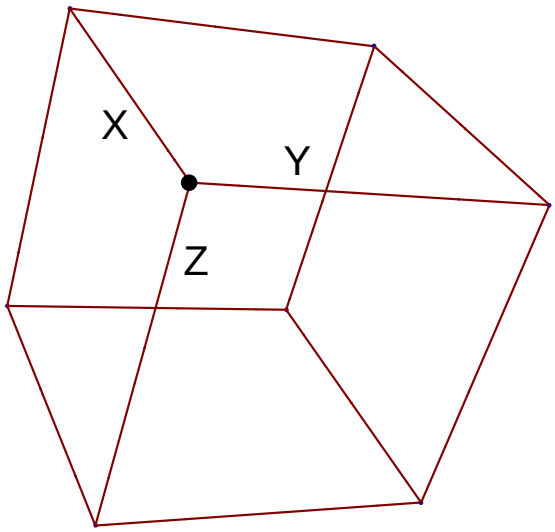

FIG. 6. Illustration of an exemplary blockchain node and link connections as a cube network in 3D space at time step zero.

In this simple and exemplary model to illustrate how NKN works, the network layer is superimposed on the data layer. The rules of the blockchain network layer are very simple. If a node is picking up a data package, it relays that data at some rate. The objectives of each node are to expand into available route in the search for more data, and to relay data to support further expansion. Each node can expand at least one new neighbor in a random direction at a particular time, but only if the node has data to do so. To model active data transmission and connectivity to the expanding tip, and node passes data to its neighbor node if the neighbor does not pass data to it. We are endeavoring to categorize the blockchain system in the CAoN architecture. This serves not only to clarify any ambiguity that arise in the programming of a blockchain network layer, but also as a potential aid to improving efficiency in that the required

iteration, data transmission and connectivity aspects are clearly defined by the rules imposed.

In detailed process, the topological expanding starts that data is transmitted by a link between two adjacent nodes of a blockchain. Consider that the message set on which the network topological rules will act to update the attributes of a link in the network is simply the amount of data that each of the two nodes has at each end of the link and their in-routes and out-routes. By writing the functional message set as a dataset such that $Si(t)$ refers to the data that node i has at time t. It is possible to expand the CAoN in an adjacency matrix A so that if $A_{i,j} = 1$ the link exists and is directed from i to j, whereas if $A_{j,i} = 1$ the link exists and is directed from j to i. If neither $A_{i,j} = 1$ nor $A_{j,i} = 1$ then the link does not exist. Here $A_{i,j}$ and if $A_{j,i}$ are mutual repulsive. As each node has limited possible connectivity which is three in this example but not limited to this number in practical implementation, we only consider the subset of links in the blockchain network which could possibly exist. The topological update process runs through all of these possible links and each pair of nodes which could be connected is considered once. The link attributes $A_{i,j}$ and $A_{j,i}$ are then updated simultaneously. Therefore, the network topological update process as rules could be found by an thorough truth table. data transmission and connectivity starts by mapping the adjacency matrix $A(t+1)$ to a normalized transition matrix $T(t+1)$ describing the flow of data between adjacent nodes. Through this process, a node relays data equally among those neighbors which are not forwarding resource to it. For example the amount of data a link transmits is indicated by its states ranging from X state (small amount) to Z state (large amount) as a network configuration.

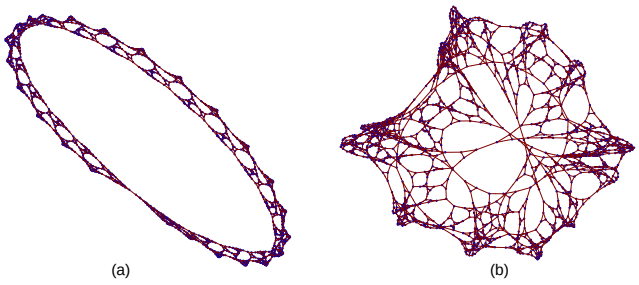

FIG. 7. Illustration of various complex blockchain network topologies with various simple rule sets (a) ring topology, rule 1655146, time step 1573; (b) pseudo-random topology,rule 1655185, time step 1573.

NKN will use similar network model to bridge between network evolution and function of blockchain by using simple microscopic rules at the level of nodes and links. The well-defined and simple rules not only make replication straightforward but also aid technical implementation at the programming level as shown in Fig. 7. The rule set determines the blockchain network topology. Therefore, a proper CAoN model enables simple and distinct establishment of microscopic rules. NKN encourages members of NKN developer community to create more complex but powerful rules to more accurately model a blockchain network, such as adding data transmission and connectivity costs at consensus layer or finite data transmission and connectivity limit, or a time dependent rule which is corresponding to the time of block generation in the blockchain.

4.3.1. Dynamics

Asynchronous CAoN are not globally synchronized for state transitions. Each node evaluates the state transition function independently of other nodes and then change its state immediately, that is what we called dynamics [18]. Two possible conditions of a node to change its state as shown in Fig. 8.

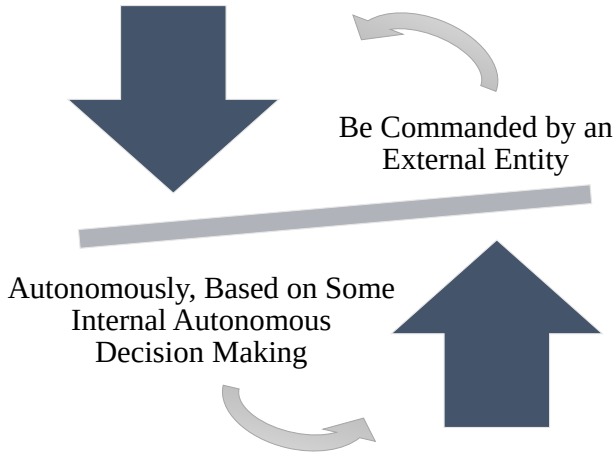

FIG. 8. Illustration of possible conditions that a node to change its state in CAoN.

As shown in Fig. 8, when dynamics are commanded by an external entity, the environment forcing some change of state or rule in a node. For example, the topologies of CAoN could be changed by rewriting various rule sets as shown in Fig. 9.

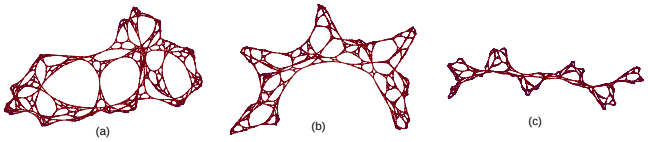

FIG. 9. Dynamics of network topology by rewriting rules of Cellular Automata at the same time step index, (a) rule 1655163, time step 1573; (b) rule 1655175, time step 1573; (c) rule 1655176, time step 1573.

On the other hand, autonomously, based on some internal autonomous decision making are changing randomly

from time to time based on an internal clock. Therefore, asynchronous CAoN provides for a more continuous notion of time. That is the time is no longer a sequence of time frame but it is a continuum, in which nodes acts independently of each other.

We conclude that asynchronous CAoN somewhat appears to be more realistic which could be deployed into a blockchain network that such a complex distributed system is asynchronous [18]. At the same time, they exhibit simple self-organization topologies. Based on NKS in literature [2], a simple node model is used to reproduce complex network phenomena with random and dynamic network connections.

4.3.2. Self-Organization

The global dynamics of Cellular Automata can be classified into 4 types [2]: steady, periodic, chaotic, and complex. Our focus is in the complex type (Class 4), also known as the edge of chaos, where all initial patterns evolve into structures that interact in complex ways, with the formation of local structures that can survive for long periods of time. Wolfram speculates that even if not all of the Class 4 Cellular Automata are capable of universal computation, many of them are Turing-complete. This view has been successfully proven by the Rules 110 [2, 19] and Conway's Game of Life [20]. Complex, self-organizing and dynamical structures emerge spontaneous in Class 4 CA, providing us a perfect candidate for the basis of decentralized systems.

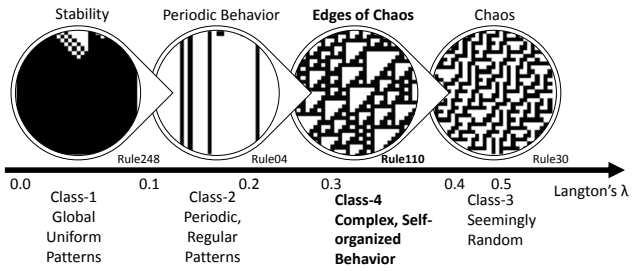

FIG. 10. Wolframs 4 Classes of Behaviors versus Langtons λ parameter on 1D Cellular Automata.

A quantitative measure of the rule that can explain and predict the behavior type of the CA is the Langtons λ parameter defined by the fraction of rule table entries that results in active state. As λ increases from 0, the system will transit from steady state to periodic state, then to complex state, and finally to chaos state, as shown in Fig. 10. In the classic 1D CA with nearest neighbor interaction, Class 4 behavior emerges as λ is around 0.3. Langtons λ parameter provides us a theoretical guide on how to find the desired updating rules, which is essential for high dimensional systems.

4.3.3. Self-Evolution

The self-evolution characteristics of NKN stems from its autonomous dynamics. Although it starts from an initial local state, nodes change their state based on their current state and of the states of neighbor nodes based on internal autonomous decision making as the networks topology changes pseudo-randomly from time to time. During the self-evolution process, the state transition function clearly has a dramatic impact on the global evolution of the network [21].

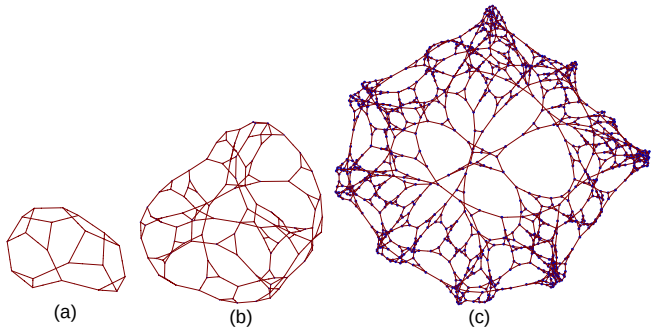

FIG. 11. The self-evolution process of the 3D CAoN model example on rule 1655185 at various time step index (a) 100; (b) 1000; (c) 10000.

As shown in Fig. 11, during self-evolution, only more and more global equilibrium situations survive until self-organization patterns becomes global [21].

4.4. Efficient Decentralization

Due to the dynamical nature of NKN, network topology between nodes is constantly updating. Proper updating mechanism is critical to achieve decentralization of the resulting topology. If, for example, the updating mechanism is chosen so that a newly joined node has higher chance to choose nodes with more neighbors to be its neighbor, and the probability is proportional to the degree of the node, then the resulting network will be scale-free [22]: the degree distribution follows a power law form. Such networks have centralized hubs defined by nodes with huge degree. Although hubs could potentially increase efficiency, they make network less robust as the failure of hubs will have much larger impact than the failure of other nodes.

One of the NKNs goals is to design and build networks that are decentralized while still being efficient in information transmission. This should be done by using a proper topology updating mechanism that considers both algorithm and incentive. On the algorithm side, neighbors should be sampled and chosen randomly; on the incentive side, reward for data transmission should be sublinear so that hubs are discouraged. Sparse random network is one possible topology that could be generated

from such mechanism. It is decentralized and thus robust to the failure of any node, while still being efficient in routing due to its small network diameter [11].

5. CELLULAR AUTOMATA POWERED CONSENSUS

Since blockchain is inherently open and decentralized, the nodes in the network are peers. The inherent lack of trust in blockchain systems is particularly noteworthy because any node can send any information to the blockchain. Blockchain's distributed peers must evaluate and make agreement on all information and decision before they are permanently integrated into the blockchain [23].

In addition, NKN is focusing on the networking applications, which requires high speed, low latency, low cost of reaching consensus, and extremely high scalability. Just take the example of cost to reach consensus. In a typical financial transaction type of application, the value of the transaction can be high enough to afford relatively expensive consensus mechanism. For NKN to support real time communication dApp, we do not want to spend thousands of CPU cycles for consensus on a hundred byte data packet a node need to relay.

Therefore, we need to invent entirely new consensus algorithms for NKN. Lets start with a quick survey of existing mainstream consensus.

5.1. Mainstream Consensus

Currently there are several approaches to reach consensus in blockchain: Byzantine fault tolerance algorithm (BFT) [24], practical Byzantine fault tolerance algorithm (PBFT) [25], proof-of-work algorithm (PoW) [3], proof-of-stake algorithm (PoS) [26, 27], and delegated proof-of-stake algorithm (DPoS) [28].

1. **Byzantine Fault Tolerant (BFT)**: Byzantine fault tolerance is a model that Leslie Lamport proposed in 1982 to explain the issue of consensus. It discusses the consensus under the scenario where some nodes could be evil (the message may be forged) and provides a worst-case guarantee [24]. In Byzantine fault tolerance, let the total number of nodes be N and the number of bad nodes be F, If $N \geq 3F+1$, then the problem can be solved by the Byzantine Fault Tolerant (BFT) algorithm. Leslie Lamport proved that there is a valid algorithm when the fraction of bad nodes does not exceed one-third, good nodes could always reach consensus no matter what messages bad nodes send. Consensus is not guaranteed when the number of bad nodes exceeds the threshold.The Byzantine fault tolerant algorithm solves the problem of reliable network communications and the consensus of nodes in the case of faulty condition.

2. **Practical Byzantine Fault Tolerant (PBFT)**: Practical Byzantine Fault Tolerant (PBFT), first proposed by Castro and Liskov in 1999, was the first BFT algorithm to be widely used in practice [25]. PBFT is much more efficient and works in an asynchronized way, while it can still tolerate same number of faulty nodes as BFT, making it more practical to use in real systems.

3. **Proof-of-Work (PoW)**: Bitcoin blockchain network introduced an innovative Proof-of-Work (PoW) algorithm [3]. The algorithm limits the number of proposals by increasing the cost of them, and relax the need for final confirmation of conformity by agreeing that everyone will accept the longest-known chain. In this way, anyone who tries to vandalism will pay a great economic cost. That is, to pay more than half the system computing power. Later, various PoX series algorithms are proposed following this thought, using economic penalties to restrict the spoilers. PoW is the consensus used by Bitcoin and is also the earliest used in blockchain system. In brief, PoW means how much work a miner pays and how much it gains. The work here is the computing power and time which a miner provides contribute to the blockchain system. The process of providing such services is "mining." In PoW, the mechanism to allocate reward is that the mining income is proportional to the computing power. The more powerful mining machine used, the more expected reward miners will get.

4. **Proof-of-Stake (PoS)**: Initially, POS (Proof-of-Stake) reduces the difficulty of calculating hash according to the amount of tokens held, i.e. there is an inverse relationship between the number of tokens and the difficulty of mining to calculate the hash. Said vividly, PoS is similar to financial assets in bank, which distribute financial return proportional to the amount of assets that stakeholder holds in a given period. Similarly in PoS, the blockchain system allocates interests according to stakeholder's token amount and hold time. Each stakeholder has one vote [26, 27].

5. **Delegated Proof-of-Stake (DPoS)**: DPoSDelegated Proof-of-Stakeis similar to PoS, except for that not every stakeholder is able to create block. Instead, nodes vote for trustees that represent them to enter the parliament and perform a regular PoS. Users who would like to become trustees need to go through community canvassing in order to gain trust of the community [28].

5.2. Cellular Automata Powered Consensus

5.2.1. Scalability Issue of BFT and PBFT

Its challenging to get consensus in large distributed system using BFT and PBFT algorithm. In BFT algorithm, the total number of messages to be sent in the system is $O(N!)$[24], making it not practical when for small N. PBFT algorithm reduced the total message count to $O(N^2)$[25], which is tractable but not scalable when N is large. In addition, both BFT and PBFT requires every node to have a list of all other nodes in the network, which is hard for dynamical network.

5.2.2. Consensus in Cellular Automata Described by Ising Model

Cellular Automata (CA) is naturally a large distributed system with only local connections. The asymptotic behavior of the system is controlled by its updating rule. It is possible to achieve guaranteed global consensus in CA using message passing algorithm based only on sparse local neighbors for a set of updating rules.

Using the mathematical framework originally developed for Ising model [29] in physics, we found and proved that a class of CA rules will guarantee to reach consensus in at most $O(N)$ iterations using only sparse neighbors' states by an exact map from CA to zero temperature Ising model. Some studies investigated the fault tolerance of Cellular Automata and how to increase robustness in Cellular Automata-Based systems [30–32]. We further showed that the result is robust to random and malicious faulty nodes and compute the threshold when desired consensus cannot be made.

5.2.3. Ising Model

Ising model is a model of spin systems with pairwise interaction under external magnetic field[29]. The Hamiltonian (energy) of the system without external magnetic field can be written as

$$H(s) = -\sum_{i,j} J_{ij} s_i s_j, \tag{5}$$

where $s_i = \pm 1$ is the spin of node i, and J_{ij} is the interaction between node i and node j. We consider the case where J_{ij} can only be 1 (ferromagnetic interaction) or 0 (no interaction). The probability that the system will be in state s under equilibrium follows the Boltzmann distribution

$$p(s) = \frac{1}{Z} e^{-\beta H(s)} = \frac{1}{Z} e^{\beta \sum_{i,j} J_{ij} s_i s_j}, \tag{6}$$

where $Z = \sum_s e^{-\beta H(s)}$ is the partition function, $\beta = \frac{1}{k_B T}$ with k_B being Boltzmann constant and T being the temperature, representing noise level of the system. We will use the units where $k_B = 1$ for simplicity.

Ising model on lattice has been extensively studied[29, 33]. For the Ising model on a D dimensional lattice with nearest neighbor interaction, a phase transition occurs at finite critical temperature T_c except for $D = 1$ where the critical temperature $T_c = 0$. When $T < T_c$, the system collapse into one of the two states where nodes have a preferred spin (spontaneous magnetization), while the system does not have a preferred spin when $T > T_c$.

For example, for a 2D square lattice with nearest neighbor interaction, we can obtain the exact solution of the Ising model. The critical temperature is

$$T_c = \frac{2}{\ln(1+\sqrt{2})} \approx 2.27, \tag{7}$$

and the spontaneous magnetization is

$$\langle s \rangle = \pm \left[1 - (\sinh 2\beta)^{-4}\right]^{\frac{1}{8}}. \tag{8}$$

All of the spins will become the same (either 1 or -1) when $T \to 0$.

If the distributed system we are interested in can be mathematically described by an Ising model, then the system is guaranteed to achieve consensus (all nodes have the same states) when temperature is zero. Finite temperature plays the role of failure by adding randomness to state transition, and finite critical temperature leads to robustness to such failure.

5.2.4. Link Between Cellular Automata and Ising Model

Cellular Automata (CA) is closely related to Ising Model. A CA is characterized by its updating rule

$$p(s^{t+1}|s^t) = \prod_i p(s_i^{t+1}|s^t) \tag{9}$$

that represents the probability of the system to transfer to state s^{t+1} at time $t+1$ given system state s^t at time t. The transfer probability is conditional independent because every node in CA updates its state solely depending on the previous system state. For deterministic CA, the transfer probability $p(s^{t+1}|s^t)$ is a delta function. If a Hamiltonian of the form $H(s) = -\sum_{i,j} J_{ij} s_i s_j$ can be defined for a CA such that

$$p(s_i^{t+1}|s^t) \propto e^{-\beta H(s_i^{t+1}|s^t)} = e^{\beta \sum_j J_{ij} s_i^{t+1} s_j^t}, \tag{10}$$

where $H(s_i^{t+1}|s^t)$ is the Hamiltonian of the system given state $s_j = s_j^t, \forall j \neq i$ and $s_i = s_i^{t+1}$. The transfer probability becomes

$$p(s^{t+1}|s^t) \propto e^{\beta \sum_{i,j} J_{ij} s_i^{t+1} s_j^t}. \tag{11}$$

We now define a new state S^t which is a joint state of s^{t-1} and s^t such that $p(S^t) \equiv p(s^{t-1}, s^t)$. The transfer

probability of S^t is now proportional to the Boltzmann distribution

$$p(S^{t+1}|S^t) = p(s^{t+1}|s^t) \propto e^{\beta \sum_{i,j} J_{ij} s_i^{t+1} s_j^t} = e^{-\beta H(S^{t+1})}, \tag{12}$$

with Hamiltonian $H(S^t) \equiv -\sum_{i,j} J_{ij} s_i^{t-1} s_j^t$ where the interaction within s^t and within s^{t-1} is zero. Thus, the CA is mapped to an Ising model with state S. The stationary distribution of S follows the Boltzmann distribution

$$p(S) = \frac{1}{Z} e^{-\beta H(S)}, \tag{13}$$

while the stationary distribution of s is given by

$$p(s) = \frac{1}{Z} \sum_{s^*} e^{\beta \sum_{i,j} J_{ij} s_i s_j^*} \tag{14}$$

Deterministic CA can be mapped to Ising model at zero temperature, where $T \to 0$, $\beta \to \infty$, $p(S)$ and $p(s)$ is nonzero only at state(s) with lowest energy. In the case of $J_{ij} = 1$ which we are interested in, only two states ($s_i = 1, \forall i$ or $s_i = -1, \forall i$) are allowed at zero temperature.

5.2.5. Majority Vote Cellular Automata as a Consensus Algorithm

Majority Vote Cellular Automata (MVCA) is a Cellular Automata using majority vote as updating rule. It can be formalized as

$$s_i^{t+1} = \text{sign}\left(\sum_j J_{ij} s_j^t \right), \tag{15}$$

where $J_{ij} = 1$ if node i and j are connected, otherwise 0. $\text{sign}(x) = 1$ if $x > 0$, or -1 if $x < 0$. $\text{sign}(0) = 1$ or -1 with equal probability. The definition of sign(0) does not have any impact if each node has odd number (k) of connections, which is true for D dimensional Cellular Automata with nearest neighbor connections and self connection. We will assume k is odd for simplicity.

We can define the Hamiltonian as $H = -\sum_{i,j} J_{ij} s_i s_j$. One can check that the majority vote rule satisfies the mapping condition $p(s_i^{t+1}|s^t) \propto e^{\beta \sum_j J_{ij} s_i^{t+1} s_j^t}$ with zero temperature ($\beta \to \infty$). From the previous section we know that when MVCA reaches equilibrium, all nodes will have the same state which depends on initial condition.

To show that MVCA will converge to its equilibrium, we use the equation derived in previous section $p(S^{t+1}|S^t) \propto e^{-\beta H(S^{t+1})}$. Since $\beta \to \infty$, $p(S^{t+1}|S^t)$ is nonzero only when $H(S^{t+1})$ is minimized. From the definition of $H(S)$ we get $-\sum_{i,j} J_{ij} s_i^{t+1} s_j^t \leq -\sum_{i,j} J_{ij} s_i s_j^t, \forall s_i$, where equal is possible only when $s^{t+1} = s$ since s^{t+1} is uniquely determined by s^t when every node has odd number of connections. Specifically, for $s = s^{t-1}$ we have $H(S^{t+1}) \leq H(S^t)$, where equal holds only when $s^{t+1} = s^{t-1}$, i.e. system in equilibrium or two state oscillation. The latter one can be avoided when J is dynamic so we ignore it for now. So $H(S^{t+1}) < H(S^t)$ before MVCA reaches its equilibrium. On the other hand, we note that $H(S)$ can only be integers that change in step of 2 and $-kN \leq H(S) \leq kN$, where N is the total number of nodes in the system and k is the number of connections each node has. Thus MVCA guarantees to converge to consensus state in at most kN iterations for any initial state. Similarly, if the initial state has m "incorrect" values, it takes at most km iterations to correct those "incorrect" values.

Although in the derivation above we use CA as the model, we did not assume local connectivity. In fact, the results are valid for any network topology with symmetric connectivity matrix J.

5.2.6. Randomized Neighbors

Cellular Automata and Ising model are both lattice based system with interaction strength mostly depends on Euclidean distance. Such kind of models are mathematically easier to solve, while not practical to implement in distributed systems, especially when nodes are dynamical, unreliable, and uncontrollable. Here we propose that random network should be a better topology for consensus in distributed system with dynamical nodes. The consensus algorithm we proposed works in random networks without any modification so that every node does not need to maintain a specific connectivity. We should mention that the random network we discuss here is purely an overlay network, regardless of how the nodes are physically connected. In a distributed systems where node does not have a list of other nodes, one can use algorithms like peer sampling to achieve random connectivity.

A critical parameter that controls how fast information propagate and thus consensus could be made is the network diameter which is defined as the shortest distance between the two most distant nodes in the network. For a random network where each node has k neighbors and k is $O(logN)$, the diameter of the network is at most $O(logN)$ [11], much smaller than a lattice based system. This is expected since random network could have long range connections, which is not possible in lattice systems. As a result, random networks convergence faster to consensus states. It is also shown that increase k leads to smaller diameter [11], as one may expect.

Wolfram Class 4 Cellular Automata is ideal to construct the randomized network for superior consensus performance. In Class 4 CA, the connectivity is effectively unpredictable, self-organized and self-evolved.

5.2.7. Simulations of CA Consensus Algorithm

To show the performance of our consensus algorithm, we apply it to a simulated network with $N = 1,000,000$ nodes. Each node has k neighbors randomly selected from the network. At each iteration, its state is updated based on the states of its k neighbors plus its own state using MVCA rule as proposed above. Neighbors are one-directional so that J is not guaranteed to be symmetric. Initially (iteration 0), the state of each node is independently chosen to be 1 or -1 with some probability. We run the simulation for several iterations with different k, as shown in Fig. 12. One can see that the MVCA converges to global consensus state in just a few steps even with $k = 10$, much faster than the theoretical upper bound kN. Note that consensus will be reached even when the initial state contains equal number of 1 and -1 nodes. Larger k leads to faster convergence.

We should mention that when N is large, the topology of the random network will be closer to its typical case as the probability to have any specific connectivity decreases exponentially as N increases. Thus, one should look at mean convergence time rather than worst case when (and only when) N is large, as in our simulations.

We further simulate the scenario where a fraction of nodes are malicious. In this case correct nodes have initial state 1, while malicious nodes have initial state -1 and does not update their states regardless of the states of their neighbors. The goal of the correct nodes is to reach consensus on state 1, while the malicious nodes try to reach consensus on state -1. From the results (Fig. 13) we can see that there is a transition between collapsing to the wrong state (-1) and keeping most correct nodes at the correct state (1). For $N = 1,000,000$ and $k = 10$, the critical fraction of the malicious nodes is around 30%, which is significant considering the size of N. The critical fraction also depends on k, as shown in Fig. 13. Larger k has two effects: more malicious nodes can be tolerated, and less correct nodes will be affected by malicious nodes.

Results in Fig. 12 and Fig. 13 show the upper bound and lower bound of the network dynamics with faulty initial states: the former one simulates the case where nodes with incorrect initial state are not malicious, while the latter one simulates the case where nodes with incorrect initial state are all malicious and want the rest of the network to agree on the incorrect state. Network dynamics fall between these two curves with the same initial states whatever strategy faulty nodes (the ones with faulty initial state) take.

5.2.8. Extension to Asynchronous and Unreliable Networks

One advantage of using Ising model to describe the system is the natural extension to noisy and unreliable communication channels. The temperature parameter in Ising model controls the amount of noise in the system, and in our case is the noise in the updating rule. By including a default state, probabilistic failure of message delivery can be modeled by finite temperature in Ising model. Thus, consensus can still be made as long as noise is under the threshold, as discussed above. The threshold can be computed numerically given the statistics of network connectivity. Asynchronous state update can also be modeled by such noise when communication timeout is added, making it practical for implementation.

5.3. Proof-of-Relay

Proof-of-Relay is a useful Proof-of-Work.

Consensus of Qi token is achieved through a useful proof of work (PoW) ,which can be understood as more likely to choose nodes of high performance of computing, network connectivity and data transmission capability. The node verifies the relay workload by adding the digital signature when forwarding data. Then nodes pass the information by consensus algorithm. However, the verification of the transaction requires the election of a small number of nodes or the competition of a large number of nodes and finally they need to reach a consensus on the entire network.

The whole network competition in proof of relay (PoR) is not a waste of resources. In contrast, full network competition in PoR can effectively improve network performance. The escalation of resources is not necessarily wasteful. It is beneficial because the NKN system mechanisms make them all workable. Although NKN does not set a threshold for participation in mining, the entire network of competition mechanisms potentially drives participants to upgrade equipment performance to obtain ledger status. The advantage is that no matter if the final formation of a massive mining pool, mad rush, or a personal upgrade, for the entire network, especially the experience of clients using NKN are improved. The upgrade of network infrastructure is crucial. Driving infrastructure upgrades through PoR mechanisms are beneficial to system participants, regardless of the outcome of PoR competition. In addition, we have several options, such as selecting a node according to its transmission capability, sending out packets forwarded by the node within a certain period of time, and forwarding more packets to people who are more likely to verify the transaction. PoR and PoW actually similar, the disadvantage is that the bad guys motivated PoS weak, the benefits are very fit with NKN purpose.

Another consensus mechanism is to validate the transaction by selecting one or more verification nodes in NNC using Cellular Automata driven consensus. The other nodes are only responsible for verifying and agreeing on the validity of his verification. Election verification node needs to reach a consensus, the final verification block is valid also need consensus.

NKN will create a Proof-of-Relay reward that encourages nodes to share idle data transmission and connectivity resource. This idle resource will be converted into

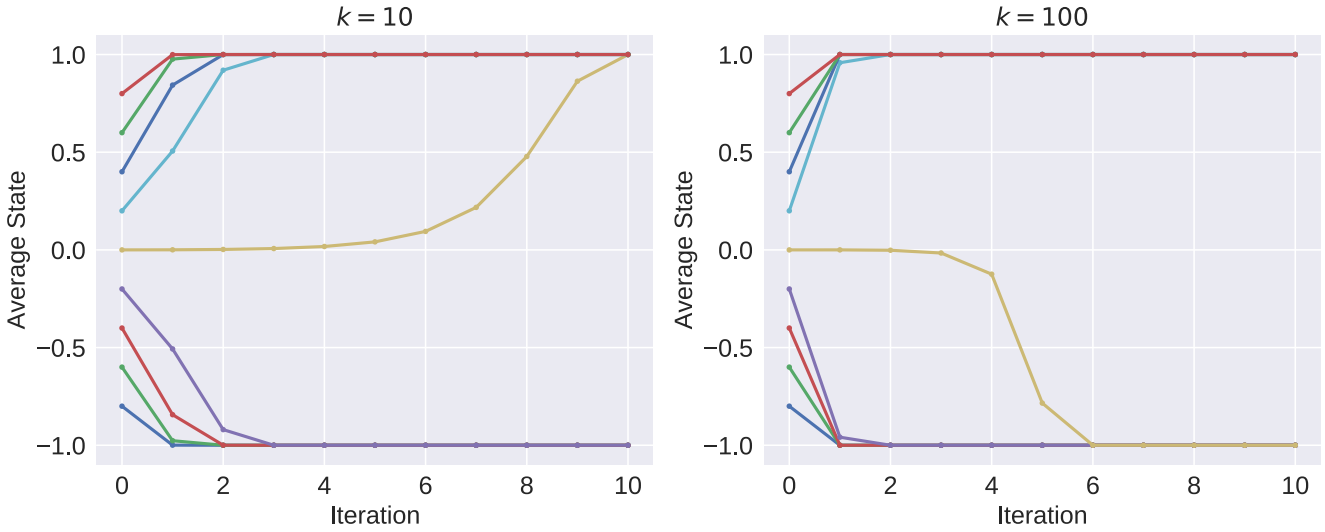

FIG. 12. Average state of the system converges to either 1 or -1, both representing global consensus. MVCA converges to consensus state which is the state of the majority nodes in just a few steps even with only 10 neighbors in a 1,000,000 nodes network. Increasing the number of neighbors accelerates convergence. Note that when exactly half of the nodes are in one state while the other half in the other state, the converged state could be either one.

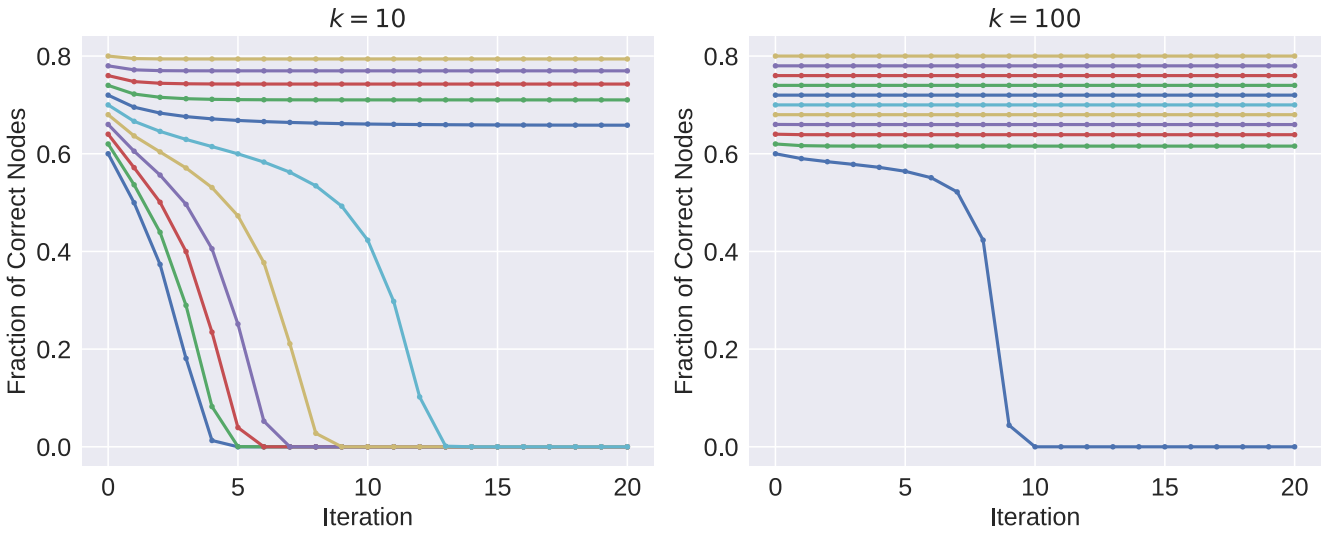

FIG. 13. Fraction of correct nodes (state 1) under the attack of malicious nodes (state -1) that does not update their states. There is a transition between whether the system will collapse to the wrong state when the initial fraction of malicious nodes changes.

shared network transmission assets through NKN's innovative technology. Thus it effectively solves the problems of high tension of network data transmission and connectivity resources, promote the full potential of network connectivity and data transmission capability in society.

Miner nodes can provide their idle network connectivity and data transmission capability to the NKN blockchain, and miners can benefit from mining operations. Miners upstream bandwidth and online duration two data determine the mining points, according to the score of the total network weight to distribute Qi generated on a certain period to the bookkeeper and token holders.

5.4. Potential Attacks

Since NKN is designed with attack prevention in mind, it is necessary to review the related types of attacks ac-

cordingly. Attack analysis and mitigation will be one of the important aspects of NKN development and future work, which will be included in the yellow paper.

1. **Double-spending attack** refers to the same digital currency can spend more than once. This is due to the reproducibility and counterfeiting of digital currencies. In classic blockchain systems, nodes prevent double-spending attack by consensus to confirm the transaction sequence.

2. **Sybil Attacks**: malicious behavior pretended to be multiple users is called a Sybil attack. Malicious miners can pretend to deliver more copies and get paid. Physical forwarding is done by creating multiple Sybil identities, but only transmitting data once.

3. **Denial-of-Service (DoS) Attacks**: an offline resource centric attack is known as a denial of service attack (DoS). The system's behavior in "unexpected" situations is often not well-specified and tested. Denial of service attacks are valid for denying anonymity in P2P networks. In denial-of-service attacks, attacks want to prevent a transaction from reaching a deal. For example, an attacker may want to target a specific account and prevent the account holder from posting the transaction.

4. **Quality-of-Service (QoS) Attacks**: some attackers want to slow down the system performance of NKN users, potentially reducing the amount of network connectivity and data transfer used.

5. **Eclipse attack**: the attacker's goal is to hide part of their system. The method used is usually the network equivalent of the privilege escalation attack: gain control over the network location that has more control over the network and then use that control to gain more control. Eclipse attack in essence is a kind of attack on the P2P network, this attack method has little to do with the consensus algorithm. In theory, Eclipse attack is valid for both PoW and PoS, but this attack method relies heavily on node's vulnerability in P2P network processing, so the implementation of attack is not universal.

6. **The 51% Attack**: different consensus algorithms will have a theoretical security value, the security value is what is the majority, if most nodes recognize a thing, then it will reach a consensus and become a reality. In the PoW consensus model, if an entity masters most of the power (51%) of the entire network, the entity can construct an active block with less time on average than all other miners. In the same time period, the entity can construct more blocks, making it the longest branch accepted by the network as the final confirmation block. Therefore, the entire blockchain will be under the entity's control. On the other hand, the larger the network size, the more difficult it is to control most of the computing power.

7. **Selfish-Mining Attacks**: in a selfish mining strategy, the selfish miners maintain two blockchains, one public and one private. Initially, the private blockchain is the same as the public blockchain, and each time the selfish miners dig out the blocks, they are added to the private blockchain, rather than broadcast to others. Then such selfish miners have the advantage of a block ahead of others, and then mining in the private chain, even if the public blockchain quickly catch up with the private blockchain, The selfish miners are still able to broadcast the block, the other nodes on the network, the two blocks are the same height, almost half the probability of selfish blocks will be recognized by other nodes. Such selfish miners have the advantage over others. The use of selfish mining strategy, selfish miners can get more than the proportion of their earnings in the whole network of the ratio of the amount of tokens.

8. **Fraud Attacks**: malicious miners can claim large amounts of data to be transmitted on but efficiently generate data on-demand using applets. If the applet is smaller than the actual amount of relay data, it increases the likelihood of malicious miners winning block bonuses from NKN. On the other hand, malicious miners may promise to transmit/relay more data, but not quantity of the actual relay, relying on fast forwarding data from other relay nodes.

6. CONCLUSIONS

This whitepaper presents a clear and cohesive path towards the construction of NKN blockchain. However, we also consider this work to be a starting point for future research on decentralized network connectivity and data transmission capability. The future work includes work that relates to Cellular-Automata-driven routing, Cellular-Automata-based consensus, proof of relay etc. When such a Cellular Automata based Blockchain is established, all kinds of DAPP will benefit from the true decentralization of the platform. NKN brings several economic highlights.

First, NKN is an ideal platform for developing decentralized data transfer sharing DApp. NKN accomplishes rapid and painless DApp development of the kit. DApp developers can be completely focused on the creative ideas and innovations that make their products successful for end users, as well as business logic. They no longer need to worry about details of network infrastructure.

Second, NKN incentive model encourages more people to join the network to share and enhance connectiv-

ity and data transmission, changing the entire network structure and creating a huge market. NKN is targeting the trillion dollar communications business, and aim to provide better connectivity to everyone by incentivize the sharing of unused networking resources, expanding and revolutionize the sharing network.

Compare to current systems, the NKN blockchain platform is more suitable for peer-to-peer data transmission and connectivity. In the meantime, this self-incentive model encourages more nodes to join the network, build a flat network structure, implement multipath routing, and create a new generation of network transmission economic structure.

From the perspectives of computing infrastructure innovation, NKN will revolutionize the blockchain ecosystem by blockchainizing the third and probably the last pillar of Internet infrastructure, after Bitcoin/Ethereum blockchainized computing power and IPFS/Filecoin blockchainized storage. Complementing the other two pillars of the blockchain revolution, NKN will be the next generation decentralized network that is self-evolutionary, self-incentive, and highly scalable.

NKN is a strategic exploration and innovation of the general network layer infrastructure delivering the next generation network to other fields. A highly reliable, secure and decentralized Internet is essential so that every individual and every industry can achieve their full potential in the digital world. NKN will offer tremendous potential for achieving a fully decentralized peer-to-peer system to make the Internet more efficient, sustainable and secure.

The current network has huge inefficiencies for providing universal connectivity and access for all information and applications. It's time to rebuild the network we really need instead of constantly patching the networks we already own. "Free the bits, rebuild the Internet we've always wanted" spirit will be the guiding beacon for NKN project, today and in the future.

[1] Stephen Wolfram. Statistical mechanics of cellular automata. *Reviews of modern physics*, 55(3):601, 1983.

[2] Stephen Wolfram. *A new kind of science*, volume 5. Wolfram media Champaign, 2002.

[3] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[4] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 2014.

[5] Juan Benet. Ipfs-content addressed, versioned, p2p file system. *arXiv preprint arXiv:1407.3561*, 2014.

[6] Protocol Labs. Filecoin: A decentralized storage network, 2017.

[7] Federal Communications Commission. Restoring internet freedom, 2017.

[8] NEO. Neo white paper: A distributed network for the smart economy, 2017.

[9] Xin-She Yang and Young ZL Yang. Cellular automata networks. *Proceedings of Unconventional Computing*, pages 280–302, 2007.

[10] Carsten Marr, Mark Müller-Linow, and Marc-Thorsten Hütt. Regularizing capacity of metabolic networks. *Physical Review E*, 75(4):041917, 2007.

[11] Fan Chung and Linyuan Lu. The diameter of sparse random graphs. *Advances in Applied Mathematics*, 26(4):257–279, 2001.

[12] Ali Mohammad Saghiri and Mohammad Reza Meybodi. A closed asynchronous dynamic model of cellular learning automata and its application to peer-to-peer networks. *Genetic Programming and Evolvable Machines*, 18(3):313–349, 2017.

[13] David Vorick and Luke Champine. Sia: simple decentralized storage, 2014.

[14] Shawn Wilkinson, Tome Boshevski, Josh Brandoff, and Vitalik Buterin. Storj a peer-to-peer cloud storage network. 2014.

[15] John Von Neumann. The general and logical theory of automata. *Cerebral mechanisms in behavior*, 1(41):1–2, 1951.

[16] John Von Neumann, Arthur W Burks, et al. Theory of self-reproducing automata. *IEEE Transactions on Neural Networks*, 5(1):3–14, 1966.

[17] David MD Smith, Jukka-Pekka Onnela, Chiu Fan Lee, Mark D Fricker, and Neil F Johnson. Network automata: Coupling structure and function in dynamic networks. *Advances in Complex Systems*, 14(03):317–339, 2011.

[18] B Chopard and M Droz. *Cellular automata*. Springer, 1998.

[19] Matthew Cook. Universality in elementary cellular automata. *Complex systems*, 15(1):1–40, 2004.

[20] John Conway. The game of life. *Scientific American*, 223(4):4, 1970.

[21] Benoit B Mandelbrot. *The fractal geometry of nature*, volume 173. WH freeman New York, 1983.

[22] Albert-László Barabási and Réka Albert. Emergence of scaling in random networks. *science*, 286(5439):509–512, 1999.

[23] Arati Baliga. Understanding blockchain consensus models. Technical report, Tech. rep., Persistent Systems Ltd, Tech. Rep, 2017.

[24] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.

[25] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)*, 20(4):398–461, 2002.

[26] Pavel Vasin. Blackcoins proof-of-stake protocol v2. *URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf*, 2014.

[27] Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, 19, 2012.

[28] BitShares. Delegated proof-of-stake consensus, 2013.

[29] Ernst Ising. Beitrag zur theorie des ferromagnetismus. *Zeitschrift für Physik*, 31(1):253–258, 1925.

[30] Mark McCann and Nicholas Pippenger. Fault tolerance

in cellular automata at high fault rates. *Journal of Computer and System Sciences*, 74(5):910–918, 2008.

[31] Luděk Žaloudek and Lukáš Sekanina. Increasing fault-tolerance in cellular automata-based systems. In *International Conference on Unconventional Computation*, pages 234–245. Springer, 2011.

[32] Ilir Çapuni and Peter Gács. A turing machine resisting isolated bursts of faults. In *International Conference on Current Trends in Theory and Practice of Computer Science*, pages 165–176. Springer, 2012.

[33] Lars Onsager. Crystal statistics. i. a two-dimensional model with an order-disorder transition. *Physical Review*, 65(3-4):117, 1944.