Beacon: A Peer-to-Peer Data Stream Grid

Danny Tan

September 27, 2019

Chinese Version 1.0

This White Paper is for reference only and does not constitute an offer or any form of investment advice.

Abstract.

Beacon is a kind of large-scale decentralized data stream service grid, and can be called the global "super computer bus" based on the publish/subscribe model. It provide a secure and universal way for data transmission and control logic for a large variety of and large-scale devices, machines, applications, services, and systems. It consists of cloud nodes and fog nodes that are scattered in different regions of the world which can join or withdraw freely. It is based on the highly-extended delegated equity consensus mechanism and a distributed ledger technology without permission thresholds, is a new economic operation mode providing various incentives (Such as node operation, data block exchange, proof of forwarding work, network expansion, etc.) for the participating parties. It is also a kind of secure global basic public service facility facing the future pervasive computing environment. Unlike the static paradigm that focuses on fragmentation results (essentially a snapshot mechanism, such as a database that provides addition, deletion, and modification functions), it is a low-latency quasi-real-time system of dynamic paradigm that focuses on the complete process (timeline mechanism, such as blockchain that only provides additional functions).

1. Background

In 2008, Satoshi Nakamoto published the Bitcoin White Paper [1], which proposed an electronic transaction system that does not rely on trust. This invention brought: ① a solution that does not rely on trusted third parties to solve the problem of double payments; ② A hash-based Proof-of-Work PoW [23] chain, that is, the consensus mechanism of "the longest chain competition" [25]; ③ A distributed public ledger technology that is called "blockchain" by the world after unchangeable records; ④ "Make nothing out of nothing", the economic incentive/mint mechanism called mining; ⑤ Based on the minimalist architecture, nodes can freely participate in a peer-to-peer network without authorization.

In 2014, IPFS [15], an InterPlanetary File System originally designed by Juan Benet, was: ① A Bittorrent cluster using Git warehouse distributed storage; ② A distributed hash table, a block exchange BitSwap protocol with an incentive mechanism, and Self-authentication namespace, a content-addressable, versioned, peer-to-peer hypermedia protocol built using the generalized Merkle DAG data structure; ③ Looking forward to making WEB faster, more secure, and more open without single point failure, without trust, decentralized storage, and permanent peer-to-peer file sharing network.

Cryptocurrencies based on Bitcoin, such as Dash [2], in addition to adding anonymous payments to improve interchangeability, do not rely on the authority of the center's instant payment function, the biggest highlight is that it is different from Bitcoin which only rewards miners for Proof-of Work hash calculation, it adds a two-layer incentive secondary network --- also known as the master node network. The master node is a high availability server with significant traffic bandwidth and large storage space running full node services. Based on the mortgage of a certain amount of coins, it provides certain services to clients on the entire network, which can greatly shorten the time of network broadcasting,
improve the health of the network, and the network will reward coins accordingly. It can be said that Bitcoin has introduced the "mining" industry and Dash has introduced the "node operation" industry, both of which are major innovations in the new economic ecological model. (Here it is emphasized that some altcoin projects known as "master nodes" may be scams.)

The ZEN coin [3] based on zero Proof-of-Work proposes basic and super main node incentives, the latter needs to ensure that all network communications between nodes are encrypted and provide certificate-based encrypted connections, thereby further expanding the types and usage of main node.

ZEL Coin [4], which is also based on zero-knowledge Proof-of-Work, its ZelNode [5] is based on different benchmark requirements in terms of server CPU, memory, storage, network bandwidth, service availability, and three types of different collateral Node [6], which leads to a new model of investment in computing resources. These nodes are not only used in the blockchain ledger, but also provide various decentralized services, such as decentralized identity and decentralized transaction services.

Different from the above-mentioned Proof-of-Work (PoW) -based master node coin [2] [3] [4], PIVX [7] is a master node coin that adopts the zero coin Proof-of-Stake (zPoS) consensus. One of the differences between coins is that under the constraints of transaction costs, the supply of coins can be dynamically calibrated.

Ethereum [8], as a smart contract and decentralized application platform, has triggered a wave of tokenized services. Some projects believe that centralized cloud services will gradually be replaced by tokenized and decentralized solutions. For example: Golem [9] is based on the utilization of users' idle machine resources to build a decentralized cheap computing power market, providing computing services such as CGI rendering, scientific computing, machine learning, etc., while using Ethereum's payment transfer system for direct payments between buyers (demanders), sellers (suppliers), and software developers; SONM [10] uses Docker container technology to provide IaaS/PaaS stack services, and uses its tokens to implement smart contract-based decentralized computing leasing market; Streamr [11] is based on the Ethereum platform [8], it is possible to use IPFS [15], BigChainDB [16], etc. as its event storage components, and with the help of Golem [9] as its computing power resources Providers, combined with Streamr's own technology stack (smart contracts, peer-to-peer networks, data markets, event processing and analysis engines, editors), provide a decentralized solution for messaging and event processing, and look forward to reaching Golem instead of Azure Virtual Machine, IPFS replaces Azure Blob Storage, Streamr replaces Azure Event Hub, Azure Stream Analytics and other platforms.

Blockstack [12], as a decentralized computing network and App ecosystem, believes that stronger client devices, edge computing and global connections will reduce dependence on centralized platforms, and cloud computing will move towards decentralized computing. Evolution is the most significant technological change in the computer industry since the mainframe switched to desktop computers. It uses the Stacks blockchain to expand security and privacy decentralized applications on the one hand. They run most of the business logic and data processing at the client, unlike traditional Web applications in a centralized server. Blockstack hopes to push complexity to the system boundary (user equipment and user-controlled storage) through this end-to-end design, and on the other hand, inspire developers to develop various applications on the network.

The Internet of Things is a USD800 billion industry with more than 8.4 billion connected devices online. It is estimated that by 2021, the expenditure budget will reach USD1.4 trillion [13]. The combination of Internet of Things and blockchain has led to some interesting projects. For example, Helium [14] is positioned in a decentralized wireless network. It hopes that devices anywhere in the world can wirelessly connect to the Internet and perform geolocation by themselves, without power-hungry satellite positioning hardware or expensive cellular plans. The Helium hotspots provide wireless coverage services and act as the miner to
produce Helium tokens. It provides connectivity for low-power IoT devices through setting hotspots. It adopts blockchain to incentivize a bilateral market covering suppliers and consumers.

Since the birth of Bitcoin, it has inspired latecomers from different perspectives, and has spawned more and more new technologies and applications. These angles can be roughly divided into: ① Cryptocurrency-based electronic trading or decentralized financial systems; ② Encryption algorithms and privacy protection technologies that are continuously improved or innovated; ③ New consensus mechanisms or algorithms being developed; ④ Non-tamperable distributed Ledger technology; ⑤ Technology different from chain structure, such as DAG; ⑥ Various commercial projects based on the concept of blockchain; ⑦ New economic incentive mechanism or investment model; ⑧ Decentralized peer-to-peer network without authorization ⑨ Decentralized applications/systems/platforms, etc.; ⑩ The integration of blockchain with other fields such as the Internet of Things, edge computing, machine learning, etc.

The fact that the standard HTTP protocol for transferring files on the Internet now has huge technical and social influence due to its integration with browsers, but it does not adopt dozens of advanced file distribution technologies invented in the last 15 years. In some fields, IPFS [15], which aims to improve the Web, is constantly improving its influence, and it is also inspiring newcomers to continue innovating.

2. Rethinking

As new technology waves or changes come, on the one hand, we believe that decentralized network services or computing paradigms with built-in incentive mechanisms will be powerful competitors of traditional centralized network services or computing paradigms, and will definitely play an increasingly important role in the future. The more important influence; on the other hand, we believe that "time" is the core element in the physical world, and the data stream grid (DSG) service based on the time sequence mechanism will more easily become a core support in the pervasive computing [22] environment.

We observe the data stream network (DSN) services based on centralized traditional, such as the online services provided by PubNub [17], the services have played a huge role in many scenarios: ① Chat and socialization; ② Real-time online message push; ③ Remote System log collection; ④ Financial market data stream; ⑤ Multiplayer game communication and collaboration; ⑥ Health and safety field; ⑦ Home automation; ⑧ Supply chain applications; ⑨ Real-time collaboration, auditing, tracking, etc. across organizations; ⑩ IoT/IoV/IoE equipment monitoring, message control, continuous testing, etc. In addition, it is shown in the website PubNub.com that the monthly active single devices 330 million sets and the transactions reaches 2 trillion times per month, and its corresponding market potential is evident.

When we rethink the DSN of the data stream network, a new idea: "Beacon Grid" was born from this. It is a consensus mechanism [24] that can join and withdraw at any time without additional authorization. Relying on PoS [24] in an untrusted environment, it provides multi-directional economic incentives, especially cloud and edge node rewards, thus achieving the decentralized peer-to-peer data stream grid for the publish/subscribe model of topics. It is essentially an overlay network based on the Internet, and has a variety of features of grid computing technologies such as peer-to-peer networks, open heterogeneity, virtual resource (such as data stream) sharing, multi-link redundant transfer, and storage [18], therefore, we classify it as a kind of data stream grid service.(Please refer to Figure 1)
This White Paper does not describe the complete details, and some contents will change with the progress of related compilation or R&D.

As a latecomer, we think it is possible to redefine the data stream network DSN:

❖ By incentivizing "miners", Bitcoin injects the cost of electricity from the physical world into the cryptocurrency network, forming a credit endorsement of "value storage" behind it. Adopting the "node operation" mode, the server computing power, network bandwidth, power and other visible costs can be injected into the network to provide the starting source power for the network. A successful network can gather global investment/speculative resources, expedite an industry such as mining, and form a network with tens of thousands of nodes, whose number is much larger than that of the traditional centralized organization. This is difficult to imagine for a small start-up team in the traditional model. Whether to make full use of this new investment and operation ecology will be a major factor in the success of the peer-to-peer data stream network/grid.

❖ As an overlay network built in the Internet [34], a kind of data stream grid and efficient productivity tool, its true value is reflected in the significant reduction in its use cost and the demand for a large number of application scenarios (such as several DSN application scenarios mentioned above), higher security guarantees, better privacy protection measures, return of data ownership, more efficient cross-organizational collaboration, optimization of resource allocation based on globalization, super large scale service capabilities, and ultra-fine service operations. The core elements for realizing these values are cloud nodes scattered in different computing centers all around the world, edge nodes located in every corner of the world, terminal devices and applications everywhere, support different levels of channel design, and achieve high performance and scalable distributed ledger of nano payment and micro payment, green and eco-friendly consensus mechanism and minimal network architecture, super flexible and free competitive market (such as node operation) and ecosystem.

❖ Although the code of Bitcoin has been optimized and upgraded, in general, it is a system that can run on its own without external intervention, basically complying with the first-principle of physics: simple, beautiful, and pervasive. This is the core philosophy that should be upheld. Therefore, we advocate that Beacon Grid adopts the simple and lightweight architecture design concept that is integrated rather than supported by complicated components, such as simplification and integration of interfaces, encryption, consensus, routing, distribution, storage, channels, protocols, etc., fully focusing on the most core pervasive functions (for the aggregation, storage, and distribution of data streams such as messages and control) to meet the needs of various scenarios, making it a key component of pervasive computing [22]. If the prototype is compared to a huge "super server", then the beacon grid will be the key existence of a huge "secure super bus". In the concept of the Internet of Everything (IoE [19]), it will play the role of a lightweight component of minimalism. We expect this large-scale lightweight component, which relies on open protocols (such as CoAP [20], MQTT [21]), can achieve its specific pervasive computing functions.

3. Brief introduction
Unlike decentralized computing networks such as Golem [9], SONM [10], and Blockstack [12], Beacon is a decentralized network with specific goals, therefore, it does not adopt the technologies which can expand the programmability and application flexibility of container/virtual machine, viewing technically, it is the high-performance, highly scalable, and pervasive vertical lightweight fusion system that can provide large-scale service capabilities, rather than the pervasive computing/service platform.

3.1. Distributed ledger

- Adopting the highly scalable distributed ledger technology based on PoS [24], which is responsible for: ① Forging new coins; ② Operational rewards of the Beacon cloud node or Beacon edge node; ③ Beacon Agent Proof-of-Forward (PoF:) rewards; ④ Such as provider/consumer/referrer/forerunner rewards; ⑤ Various types of Beacon coin payments, including nano payment, micro payment, small payment, etc.;

Note: Please refer to paragraph below for relevant details

- Beacon Proof-of-Staking PoS [24] ledger adopts graph technology instead of chain technology, which makes it have high expansion and high throughput capabilities, and it also forms the underlying support of the Beacon network. Whether it is the data stream forwarding mechanism in the node agent or the data block exchange involved in the time series data stream storage mechanism, such as the "transaction" behavior between nodes, depends on the support of the distributed ledger mechanism.( Please refer to Figure 4)

- The use of PoS instead of PoW is based on two considerations: ① Emphasize on the cost injection of computer service computing power instead of Hash computing power; ② Avoid the influence of hash computing power cost on the price of coins, thus highlighting the value of grid services Influence of the price of coins; ③ Encourage large-scale expansion of nodes rather than mining machines;

- Beacon Grid is a universal basic application project. It is not a publicly available blockchain platform, nor is it a trading system focusing on cryptocurrency. Therefore, the PoS [24] ledger is mainly based on nano payment, micro payment, small payment, and adopts fast confirmation mechanism, while sets a large transfer mechanism.

- Adhering to the design concept of minimalist and lightweight architecture, unlike most blockchain projects, Beacon will not support Turing-complete smart contract (virtual machine and contract language), and choose to use hard-code methods to implement the built-in contract logic related to payments. Note: Only consider adding smart contract as a required feature option according to the project progress

3.2. Core mechanism of data stream agent

Figure 2: Schematic diagram of publish/subscribe model

- Using the topic-based publish/subscribe mechanism and supporting open protocols (MQTT, CoAP, etc.), so that programming languages, development kits, applications, micro services, devices and systems that support such protocols can be connected to the "super bus" service, which is similar to accessing the traditional message broker service or computer cluster system.(Please refer to Figure 2)
Publish/subscribe mechanism can support one-to-one (such as private chat, analysis channels), one-to-multiple (such as news channels, stock quotes, news push), multiple-to-one (data acquisition, log monitoring, voting), multiple-to-multiple (group chat, multiplayer game) usage scenarios [11].

Data stream publishing does not mean that client subscriptions are necessarily required, that is to say, there is a demand on scenarios with delayed multiple backups [11]. When the node accepts a published data stream, unlike the traditional single point message broker service or a cluster that is only responsible for message distribution, it first saves the data stream to this node, and then waits for the opportunity to distribute the data block to other nodes for backup, which is the natural and intimate option for this grid. This is determined by the nature of immediate saving, which is less expensive than real-time distribution. Real-time distribution of message consumes more computing and bandwidth resources, therefore, such requests will be processed with priority, and redundant backups without subscriptions will be delayed. (Please refer to Figure 3)

Figure 3: Schematic diagram of delayed subscription and data block distribution

Data stream publishing does not mean that client subscriptions are necessarily required, that is to say, there is a demand on scenarios with delayed multiple backups [11]. When the node accepts a published data stream, unlike the traditional single point message broker service or a cluster that is only responsible for message distribution, it first saves the data stream to this node, and then waits for the opportunity to distribute the data block to other nodes for backup, which is the natural and intimate option for this grid. This is determined by the nature of immediate saving, which is less expensive than real-time distribution. Real-time distribution of message consumes more computing and bandwidth resources, therefore, such requests will be processed with priority, and redundant backups without subscriptions will be delayed. (Please refer to Figure 3)

Figure 4: Schematic diagram of the time sequence data stream storage structure

Light-weight data stream storage model based on time sequence, which: ① Using a design principle similar to IPFS [15], data blocks of a certain time interval or capacity are dispersed in different nodes (as opposed to direct data stream forwarding, which is a delayed data block distribution mechanism), but The implementation needs to take into account lightweight design requirements; ② It has a default expiration time, a part of a data retention strategy, similar to the Retention Policy (RP) of InfluxDB [52], but by paying a certain amount of coins as the price Prolong the expiration time of related storage; ③ adopt the TSM engine mechanism similar to InfluxDB [52] as the storage engine implementation design; ④ The non-public payload in the stream data will first be encrypted and signed with the private key of the data source owner, and then stored with Forwarding, the grid system cannot sense the specific load content, but the meta-information of the data stream can be queried and downloaded according to the timestamp; ⑤ Unlike centralized services, using encryption technology, the publisher has complete data ownership; ⑥ Streaming data storage will retain some metadata, such as distribution duration, network delay, packet size, etc., which is helpful for further optimization or analysis of network performance. Analysis; ⑦ The cold and hot data classification mechanism is adopted, and the cold
data will be distributed and propagated through the data block exchange protocol; (please refer to Figure 3 and Figure 4)

- Beacon grid core message propagation will be completed through mechanisms such as gRPC. However, the stream data of business layer, such as the log stream of the Beacon node, running data stream such as CPU of Beacon node, are the publishers and consumers of one sequence $SYS$ theme. Node operators can observe and analyze the operating status of related nodes. Developers can also analyze data related to system performance and resource consumption. Future machine learning algorithms can be used as consumers, these data can also be used to detect anomalies and find out network attacks timely. (Please refer to Figure 5)

![Figure 5: $SYS$ theme diagram](image)

- Beacon agent has built-in channels of three levels: emergency/important, common, public/reward, respectively, occupying the CPU and memory resources of the static part according to a certain proportion, and the CPU and memory resources of the dynamic part will be adjusted basing on the dynamic threshold (similar to the difficulty factor in Bitcoin mining), thus allocating to channels of different levels. For the distribution of these three levels of channels, consumers and suppliers need to pay different amounts of Beacon coins. However, the public level can use nano-level payment, and its cost is close to zero, which is equivalent to the "free" model in Internet public services. Other levels, whether it is publishers or subscribers, are the payable model. The subscribers will pay to the Beacon participant (such as beacon node) according to the proportion as a forwarding reward and publisher. The purpose of the three-channel separation design is to ensure that the channels can operate independently without interfering with each other. Different from the design method of determining the service priority according to the payment level, it can guarantee that various payment costs can have the opportunity to get the corresponding level of service response.

- For emergency/important and common level channels, it is difficult for malicious publishers to launch attacks and try to consume node resources, because the other party needs to pay the cost of use (pay at market price). For Beacon grid, it is the normal data stream publisher. (Please refer to Figure 6)

![Figure 6: Schematic diagram of independent classification channels](image)

- The level of public/reward, based on the situation of ultra-low prices or extra rewards, there will be malicious publishers and malicious subscribers using non-valued payloads to consume the resources of the Beacon node (CPU, memory, traffic, storage, etc.) or gain rewards by cheating.

  1. It can delay the issuance of rewards or set up a time lock mechanism, or the subscribers can issue or unlock after the consumption payment is generated;
  2. Set a dynamic limit threshold based
on the publisher/subscriber's address to limit the number of connections, number of devices, data stream duration and capacity of the same public address.

3.3 Node service

○ Beacon node refers to the type similar to ZelNode or Dash master node that can obtain additional rewards through node operations, instead of the beacon PoS node, the former has specific specifications limit and online availability requirements, but the latter does not have such rigid rules.

○ Beacon node has a complete set of ledger records, and also provides external ledger data synchronization services, especially block binary ledger data, which shortens the synchronization time and required network traffic of the ledger record set of newly added nodes.

○ Beacon node Proof-of-Forward (PoF) is on the data stream routing path, which does not include the nodes of the publishing node and the consuming node. It is passively selected (similar to random and not affected by the publisher and consumer) to avoid malicious nodes, malicious publishers and subscribers. Unlike Proof-of-Work PoW, this type of node does not participate in the consensus mechanism, and is mainly used as a component of the Beacon node reward. Of course, it is not excluded as a weighting factor in the random sampling process, which reduces the probability of new nodes being drawn and delays new node attacks. This situation only occurs when the consensus node and the serving node are integrated. (Please refer to Figure 7)

![Figure 7: Schematic diagram of data stream forwarding path](image)

○ Publishing and subscribing based on the same Beacon node will be given priority. This is especially true for edge nodes or nodes with large communication delays with other nodes, and the performance is obvious. (Please refer to Figure 8)

![Figure 8: Schematic diagram of the priority mechanism](image)

○ Various Beacon grid nodes need to report validity, a special ping mechanism, corresponding rewards can be obtained only if it meets the sampling condition threshold setting. And this operation status data, after being anonymized, will be saved in the grid to provide data support for grid performance improvement.

○ Beacon cloud nodes refer to the network, which can provide proxy access, storage, and
distribution services. These nodes are mainly deployed on the cloud, such as cloud hosts provided by cloud service providers, which can meet specific specifications such as the number of CPU cores, memory size, disk capacity, network bandwidth requirements, and continuous online service requirements, etc., these nodes form the main backbone of Beacon grid services.

- Beacon fog/edge node special network, ordinary enterprises or home users, using the enterprise or home bandwidth, on the ordinary computers or single board computers, or renting virtual host of decentralized fog services such as Golem [9], SONM [10], can provide services such as proxy access, storage and distribution (connecting to cloud nodes) for peripheral devices and applications. After these nodes have mortgaged a certain amount of coins, they participate in the node incentive plan together with Beacon cloud node. The applications and devices connected to these nodes form a micro-centralized client/server network at the edge, so that the browser and client applications transparently access the Beacon decentralized network, which are realized through the specific gateway services (such as Proxy, DNS service, etc.) deployed in fog/edge nodes.

3.4. Core technologies forming peer-to-peer network

- Confidentiality and security mechanism
  - Adopting Ed25519, this signature scheme using SHA-512 and Curve25519 [46] Edwards Curve Digital Signature Algorithm (EdDSA [47]). In cryptography, Curve25519 is an elliptic curve, provides 128-bit security, and is designed for elliptic curve Diffie-Herman (ECDH) key agreement schemes. It is one of the fastest ECC curves not covered by any known patents [48]. In public key cryptography, EdDSA is a digital signature scheme using a Schnorr signature variant based on a twisted Edwardian curve, which is designed to be faster than existing digital signature schemes without sacrificing the security [49].
  - Beacon grid will strictly abide by the data confidentiality mechanism, and the event payload of non-public streams which are data sources such as end users/devices/applications will be strongly encrypted using asymmetric keys, and only the party with authorized private key is able to read the data.
  - Construct Beacon peer virtual private network which runs the encrypted communication packets between Beacon nodes on the bearer network, and prevents behaviors such as network sniffing.
  - S/Kademlia method with secure key routing
    - S/Kademlia [33], as a distributed hashtable DHT, can be used to coordinate and maintain the metadata of peer-to-peer systems.
    - S/Kademlia [33] protocol uses parallel queries on several disjoint paths to resist common attacks, and uses implicit passwords to restrict the free generation of node IDs. Its static and dynamic cryptography puzzles force all node IDs to be evenly distributed. The routing table maintained by each node is evenly partitioned, and communication across honest subnets can also continue. Even if there are more than half of dishonest nodes in the network, the success rate of 85% can also be achieved. In addition, the uniformity of such node IDs only requires a reliable boot node, and new users can easily join as network members.
    - S/Kademlia [33] bearer network [34] has the De-Brujin network topology [35], which can efficiently send messages to specified receivers. It not only plays a role in the ledger communication, but also establishes a reliable distributed route between the beacon nodes and efficiently transmits messages containing data stream loads.
    - The network topology of S/Kademlia [33] determines that it will not treat nodes differently, and when combined with reward distribution and message forwarding, it will not cause the Matthew effect dilemma [43].
    - This kind of ledger node and service node adopts the same routing method, which also adheres
to the concept of integrated design and also constitutes one of the core technologies of Beacon network.

- Adopting Coral [51] distributed sparse hashtable DSHT
  - In the block data exchange mechanism, when adopting Kademlia distributed hashtable DHT, there will be a phenomenon of ignoring "far" nodes that may own data and forcing "near" nodes to save data, which wastes storage and bandwidth. However, Coral stores the address, and the peer node can provide the corresponding data block through the address.
  - Coral users only need a working peer instead of a complete list. This can only assign the subset to the "nearest" nodes, thus avoiding hotspots (reloading all the nearest nodes when the key becomes popular).
  - Coral organizes an independent DSHT hierarchical structure that becomes a cluster according to region and size. This allows nodes to first query the peers in the region, that is, "search nearby data without querying remote nodes", which greatly reduces the delay of the query.
- By constructing a MerkleDAG object, a directed acyclic graph, it provides useful attributes for data stream storage, including ① Content addressable: all content is uniquely identified by multiple hash checks and ② Prevention of tampering: all content Use its checksum to verify; ③ Repeated data deletion: all objects have the same content and are stored only once, which is very useful for the public part of the data;
  - The distributed Byzantine fault-tolerant protocol Snowball [31] based on the metastable mechanism that combines the advantages of the classic consensus protocol (strong consistency, high efficiency) and the Nakamoto protocol (openness, no authority), the use of probabilistic security assurance and adjustable security parameters make the probability of consensus failure arbitrarily small.

In addition, BFT attributes are added to increase system efficiency and security.
  - It has the characteristics of static green, low communication cost and high scalability. This method of multiple repeated sampling (the inspiration is from Snowball sampling in 1961 [38]) allows the nodes to reach a consensus, and will also play a role in the data stream proxy in message forwarding and data synchronization, which also reflects the benefits of integrated design.
  - Due to the Proof-of-Work PoW consensus, on the one hand, it does not have scalability, on the other hand, we hope to inject the cost into the nodes, not the hash mining. Proof-of-Staking PoS [24] or Delegate Proof-of-Staking DPoS [28] based on the longest also does not have scalability. In view of the vision of Beacon network, which is a network with a very large number of nodes, scalability is its core element.

4. Scalability dilemma

Ledger technology that adopts the longest chain rule, such as Proof-of-Work, resolves transaction conflicts through competition, and the increase in the number of nodes, coordinated network of nodes to maintain distributed ledger, will bring additional communication and processing expenditure. And it leads to exponential processing time complexity, so there is a scalability dilemma, which requires a balance between performance, consistency and availability. Ledger technologies that use the Delegate Proof-of-Staking mode, such as typical representatives Algorand [29], Tendermint, Ouro-boros Praos, Dfinity [39], and EOS, through PoS, can verify the verification function [29], or decentralized voting [30], but when the number of nodes is very small, the security of the network is reduced. If the number of nodes is increased, the performance will be reduced, and it will face the scalability dilemma. It is worth noting that the longest chain competitive iChing [45] protocol, a kind of PoS consensus protocol based on probabilistic competition, has extremely high scalability, and the consensus nodes can easily join and exit it.
Based on the directed acyclic graph DAG, Avalanche [31], a consensus protocol family that replicates transactions between nodes, has excellent scalability and can be applied to large-scale node networks. In addition, it cited its Snowball protocol [31] and made related improvements to the Wavelet consensus [32], which can guarantee the irreversible and globally consistent order of transactions without any impact on security, performance or activity.

5. The "chicken and egg" dilemma

From the evolution history of the Internet, we can find that centralized Internet service companies such as Google provide a common universal service adopting the client/server model. The client is mainly browser, such as E-mail, instant messaging, and document processing, file storage, etc., and these past paid software often run on the computer of customer. Adopting a "three-party payment" business model such as advertising, it is different from the traditional economic model of supply/consumption. When Google provides free search service, it must include a large number of web pages on the Internet, which requires the development of web page ranking algorithms, providing super huge Internet access and a large number of servers, and setting up many large data centers in different regions of the world. This requires early stage capital investment which is much higher than the traditional companies before generating significant revenue. In the period of the Internet bubble, this kind of venture capital-driven deficit-operation phenomenon was called the "burning money campaign", but it greatly eased the "chicken and eggs" dilemma [26]. However, small Internet companies are not so lucky and are stuck in it. Only after reaching a certain scale, they can achieve profitability, otherwise, they will either be acquired or closed down.

The "free" [40] business model that alleviates this dilemma to some extent makes the phenomenon of "winner-take-all" more obvious than that of traditional industries, and on the other hand data leakage of large-scale centralized Internet services, such as the hacking incident of Yahoo affected nearly 3 billion user accounts worldwide [41]. For users, this is some kind of evidence in exchange for "free" services at the expense of data ownership and privacy.

To provide a large-scale secure public "data stream bus" grid service that focuses on user privacy and digital property rights, like other general Internet services, there is still a cold start process from zero to one, that is, "chicken and eggs" dilemma [26], which is the first strategic factor. In addition to software code R&D, an important area of capital investment is infrastructure investments in various cloud servers, edge servers, and network bandwidth. Vertical business companies like PubNub [17] also need continuous investment of hundreds of millions of dollars in order to maintain their corresponding market position. In addition, the problem of converting target users to seed users is particularly obvious and acute for the bilateral market that connects supply and consumption, such as Golem [9], SONM [10], and Streamr [11].

Beacon adopts the "node operation" model to stimulate its infrastructure investment. Adopt the coinage method to allow future-oriented faithful investors to realize future value realization in the future (different from other tokens, the emphasis of Beacon is that it can provide basic pervasive services instead of providing the transferable cryptocurrency. Currently, there are a lot of funds in the cryptocurrency circle for speculation or investment. This is a free and open market. We think it is an era opportunity for some initial projects, investing a lot of funds to operate decentralized peer-to-peer network nodes (cloud nodes and fog nodes). It can be seen from Metcalfe's law [37] that when the number and scale of nodes exceed a certain threshold, and even reach an order of magnitude that cannot be reached by traditional industry organizations, it will explode great effects like the current Internet service.

As Satoshi Nakamoto said, by injecting valuable computing power/electricity in the physical world, on the one hand, it provides value support for the Beacon economy (although large-scale cost investment does not necessarily mean that it can create value, it can indeed help the project to pass the critical point), on the other
hand, it can solve the cold start dilemma from "zero to one" (that is, infrastructure investment of large-scale network).

6. "Group gap"

We see that in a lot of ICO projects based on the Ethereum protocol, most of the people who buy tokens are for speculation or investment, not the project users or customers. As a result, the users of the project are only a small number of people. The application status of the project is incomparable with the early Internet projects. Very few users will greatly limit the development of the project. In this way, ICO is only a new financing method, and does not give play to the core existence of the token, that is, the use of token. This phenomenon is also reflected in Bitcoin. It has not become a cryptocurrency. It is used as a large-scale transfer of payment currency among different users. At the same time, a reasonable balance between payment fees and new minting is achieved, and it becomes a This kind of "digital gold" serves as a type of stored value tool for investors, thus far from Satoshi Nakamoto's original cryptocurrency vision. Subsequent projects that are determined to become electronic cash also face this challenge. As time goes by, perhaps twenty years later, if more and more people begin to accept cryptocurrencies, crypto assets and their underlying technologies, the situation may become even more brilliant.

We can observe that in the cryptocurrency field, cryptocurrency wallet services, centralized exchanges or decentralized exchanges, and financial services for crypto assets already exist, which are very active because they target a specific user group. However, those which have introduced the "blockchain" technology and focused on the field of application production, are just in another group. The broader general public and enterprises are far from the majority of the above two groups, which confirms the social phenomenon of "group gap" from one aspect.

Just like the common win-win cooperation in the industry chain, due to the general group cognitive consensus in the cryptocurrency field, various cooperations between each other are abound, which forms a small ecology, but it will take time to break through this "group gap" and expand beyond existing groups.

To mitigate the above challenges, it is necessary to introduce early users as much as possible, and it is necessary to give appropriate incentives to such pioneer users. This has also shown a good momentum in some pilot projects, such as PI coin [27]. But excessive incentives also bring negative effects, such as malicious spam users, therefore, incentive balance is very important. It can not adopt the completely free model like the Internet service. It can only learn from the mixed model of free and charge in the Internet service, that is, the three types of hybrids of nano payment (infinitely close to free), micro payment (small payment), and emergency payment. This method also refers on the conventional marketing methods such as recommendation reward, use reward, senior user reward which are commonly in the existing economic model, (making nano payment and micro payment methods reach the "equivalent to free" fact in the early development process). With the increasing awareness of new-generation users in terms of paid use, data property rights, privacy protection, etc., the success rate of converting seed users will also continue to increase. In addition, it is necessary to wait for appropriate third-party services (such as legal currency conversion, service replacement), so that more outsiders can easily use or consume related public services.

It is because of the above-mentioned challenges that we are forced to think about how to make Beacon lighter, simpler, and more pervasive, so that it can continue to operate like Bitcoin, without the need for more function iterations. With continuous increase of users and continuous expansion of network scale until it breaks through the critical point, it can have characteristics that traditional centralized systems or services do not have, and become a preferred solution for many third-party applications or equipment, manufacturers, and organizations.

Through the provision of large-scale infrastructure
by a speculative/investment group, it provides individuals, companies, and organizations outside the group the replaceable production tool/production material with a greater focus on security and privacy, more emphasis on digital property rights, more decentralization, more scale and cost-effectiveness, thus gradually bridging this "group gap" and realizing an evolutionary case from "credit endorsement" to "value production".

7. Value consensus

For those who are new to cryptocurrency, they confused about: "Open source Bitcoin code can be copied to create a cloned coin. Then it can be copied at no cost, contrarily, it means that Bitcoin is not worth investing in. "In fact, there're various alternative coins in the market, as well as various junk coins and scam coins. But the end result is that after the core part of Bitcoin or other cloned code is stripped, only those varieties with independent innovation and intrinsic value will be recognized and accepted by the market, and they will have a chance to survive. This can also be a preliminary proof of the free market [42], which itself has a consensus mechanism of certain value determination.

8. Incentive mechanism

From the beginning, a clear incentive mechanism has been set up. It adopts the scheme of constant total amount, quarterly linear deflation within the time span of 36 years, and until it stops minting and becomes 100% consumption-driven by consumer.

In addition, the distribution mechanism of new coin rewards:

- Consistent node rewards across a complete cycle at a fixed ratio;
- Cloud/edge node rewards across a complete cycle at a fixed ratio;
- Proof-of-Forward rewards across a complete cycle at a fixed ratio;
- Startup incentive pool that is unlocked year by year in the first 4 years at a fixed ratio;
- Early bird user incentive pool that is unlocked year by year in the first 6 years at a fixed ratio;
- User recommendation incentive pool that is reduced year by year in the first 8 years at a fixed ratio;
- Development funds pool that is unlocked year by year in the first 10 years at a fixed ratio;
- Market funds pool that is unlocked year by year in the first 15 years at a fixed ratio;
- Node expansion dynamic incentive pool with single node reducing and total amount increasing in the first 20 years at a fixed ratio;

9. Machine and human

After the early users (incentive subjects) made consumption payments, the reward pool used machine algorithms to perform a certain amount of time-delayed feedback on the payer. This game mechanism replaces the free and cost-free model and is an interesting way while taking into account human psychology.

The phenomenon of Ponzi scheme [44] is common, first, it is the greed of human nature and the gamble of fluke gambling, and secondly, the overflow of decentralized individual capital. If this natural human demand can be channeled, it will become a risk investment force, thereby constructing a production tool and production relationship that create value and benefit humanity, and stimulate its inherent potential and explosive power.

In the future, with continuous progress of science and technology, the total value creation of machines will show an exponential growth and will surpass humans in many fields. This situation makes the role of machines more and more important in the entire conventional value creation system (excluding highly innovative human economic activities). When they become the subject of value creation, a new economic form integrating machines and humans will appear. Most ordinary people will play the new role of "investor", "employer", "manager", "manager", "planner", etc., and the "employees" who do the actual work will be machines. As "human-machine hybrid micro-commercial entities" continue to emerge, the decentralized model with lower entry barriers will play an important role.
By observing the business model of Uber [50], you will find this novel production relationship between "driver" and "car", and with the advent of intelligent driving technology, the above ideas will become increasingly possible.

10. Summary

In the computer architecture, the "bus" is a communication channel, which is a general way to provide data transfer and control logic for components inside or between computers. For example, if the motherboard is likened to a city, the "bus" is like the bus in the city, the passengers on the bus are data, and the passengers are transmitted according to various routes, so that they can reach their destinations quickly and smoothly [36].

Currently, various Apple devices, such as iPhone, iPad, and Mac, can interoperate, such as data synchronization, message reminders, screen display, answering calls, finding Apple devices, etc. Behind them, it is driven by such mechanisms. The user has not felt the existence of the computing service behind it. It is a very good example of pervasive computing at present [22], and has initially demonstrated its powerful interactive capabilities, representing a certain future trend.

It can be imagined that in the future, the large-scale peer-to-peer data stream grid of the role of "secure super bus" in this huge "supercomputer" is positioned in the pervasive computing model/new generation of value Internet, provide a secure, universal way of data transfer and control logic for the components, that is, a wide variety of devices, applications, systems, services, etc. Whether in encrypted communication, private social networking, Internet of Things, Internet of Vehicles, Industrial Internet, supply chain, inclusive finance, smart home, smart city, big data analysis, artificial intelligence, or other various cross-border service application scenarios, with the continuous emergence of 5G communication technology and more pervasive computing cases, such basic public service facilities around the world will play an increasingly important role. In other words, "ubiquitous computing" is inseparable from the service support of "ubiquitous and secure data stream channels".

11. Acknowledgments

Any innovative activity is inseparable from the situation created by the predecessors, without these, any idea of Beacon could not be realized. Satoshi Nakamoto not only invented Bitcoin, but also opened a brand new era. With the emergence of the InterPlanetary File System (IPFS), it also inspires the latecomers to re-examine the HTTP-based WEB system.

12. References

15. https://ipfs.io A peer-to-peer hypermedia protocol designed to make the web faster, safer, and more open.
17. https://www.pubnu.com/
26. https://en.wikipedia.org/wiki/Chicken_or_the_egg
27. https://minepi.com
37. https://en.wikipedia.org/wiki/Metcalfe%27s_law
39. Timo Hanke, Mahnush Movahed, Dominic Williams. DFINITY Consensus, DFINITY Technology Overview Series Consensus System Rev.1, 2018
42. https://en.wikipedia.org/wiki/Free_market
44. https://en.wikipedia.org/wiki/Matthew_effect
48. https://en.wikipedia.org/wiki/Chicken_or_the_egg