Alila Tech: intelligent wearable IoT terminal application chain

Abstract:The era of big data has come. With the gradual maturity of 5G, AI, IOT and other technologies, the magnitude and capacity of human society to generate, obtain and process data will usher in a new leap, and the data economy will also come to a brand new stage of development. Through a rational application of data, our level of cognition to the world, the speed of response to demand, and our planning ability for commercial and social activities.

1. Introduction.

Alila Tech is an application chain for the intelligent wearable IoT terminal data service. Its algorithm technology is a program protocol to serve the wearable IoT terminal chip. By combining the advanced algorithm technology with the cost-effective IoT terminal chip, the data generated for the chain, desensitization analysis, data rights confirmation and other services. Realize the return of personal health data equity, and provide early warning for personal health through pathological database comparison, and also providing data support for scientific research in health care.

The combination of the blockchain and the wearable IoT terminal is undoubtedly a great potential application scenario. Alila Tech will provide users with effective data storage, analysis, and early warning solutions and connect to a wider range of older groups. Blockchain technology and encryption economy will open up new areas for its development, including data privacy, trust data sharing, scientific research, etc.

2. Alila Tech's solution

Alila Tech implanted the algorithm into the chip of IOT terminals such as smart watches, smart glasses and collected valuable privacy data (including real-time location, health data, etc.), through the characteristic sensors, so the advantage implanted with Alila tech algorithm device is that the privacy data will not be collected by centralized subjects or unrelated third parties; through the privacy protection technology, the privacy data can be safely transmitted to the trusted party. Alila Tech can fully protect user privacy.

Trust Data Sharing: The data stored on the blockchain is unalterable and traceable. If the data is verified as trusted (if the data is sent from a specific source / device), the original data is verifiable. Today, untrusted IoT data is everywhere and cannot be used in formal research, third-party sales, or other non-data owners. The data generated by Alila Tech is verifiable and fully trusted, making each Alila Tech user a "trusted data provider" and thus opening many potential areas of data applications: providing trusted data for research: Alila Tech's long-term goal is to provide data for research institutions to make pre-diagnosis of health risks possible. Research institutions can independently verify the data sources to ensure the data accuracy.

Create a platform for data sharing: Personal health data is extremely important for insurance companies, private health care institutions, or other healthcare institutions. Alila Tech users can choose whether to sell the data to the above subjects, making the profits available to fund the relevant research, or to reduce user costs.

Provide incentives for users to use equipment: Since continuous complete data is more valuable than dispersed data, data buyers (such as insurance companies) can reduce user costs by motivate Alila Tech users to wear devices to provide more complete data. Users can even make profits by wearing their devices.

Inter-machine communication: As devices connected to Alila Tech constantly increase, Alila Tech can connect with more and more devices. In case of emergency, Alila Tech products send emergency distress signals and real-time location information to the user guardian. With the support of the blockchain, this distress signal can be broadcast not only to the user's family members, but also to the equipment that can assist those in an emergency (such as turning the nearest monitoring equipment to the user position, opening the nearest lighting equipment or starting the alarm device, etc.

3. Identity management system

Alila Tech is essentially a chip program protocol solution for smart wearable terminals generated by the high combination of IoT technology and blockchain technology.

The development of the Internet of Things has had an impact on how the Identity and Access Control Services (Identity and Access Management,IAM) operates. In terms of identity authentication of things, the IAM must be able to run a user-to-device, device-to-device, and / or device-to-device service / system. Thanks to the imtamper ability of Alila Tech, a direct way to implement authentication management is to use Alila Tech as a decentralized public key infrastructure (PKI) in which each entity is assigned to encrypted authentication in the form of a Alila Tech certificate for privacy protection. This short life certificate is issued by long life certificates in built-in dry devices and issued on Alila Tech. Users or other entities can access and trust this short life certificate anchored on the blockchain, and then verify the objects connected to the online, ensure safe communication between equipment, services and users, and ensure its integrity.

In addition, the long life certificates embedded in the equipment can establish a cascading structure as the traditional PKI, and the upper equipment can issue certificates to the lower equipment. In a hierarchical structure, revocation and transfer of credentials will become possible. For example, if a device has a problem, its upper device or re-upper device can issue a cancellation assignment to the blockchain, which can in turn invalidate the credentials of the device.

4. The ecological evolutionary direction of the Alila Tech

The Alila Tech team is currently committed to the following research directions:

1. Privacy-oriented computing

Here are several areas ： we are actively exploring in this technical direction

How a set of nodes on the ● blockchain perform privacy-oriented computing

● performs privacy-oriented smart contracts by virtual machines with contract content encryption. Although holohomomorphism encryption as well as indistinguishable code confusion techniques are theoretically able to achieve privacy-oriented

● further reduces the computing and storage requirements required for Alila Tech's blockchain privacy protection technology.

● studies post-quantum versions of the privacy protection technology currently used by Alila Tech, such as state-cutting and transfer of post-quantum ring signature techniques.

2. blockchain governance and self-correction

While proponents of Alila Tech maintaining its ledger consensus offer rewards, there is no chain mechanism to accurately correct the rules of governance agreements and reward the development of the agreement. We will further study blockchain governance and self-correction mechanisms to address this problem.

3. can expand and focus on privacy protection

Alila Tech will focus on scalable, privacy-focused and ductionable smart wearable applications

● uses an in-chain connectivity architecture to maximize scalability and privacy

● protects transaction privacy with lightweight secret addresses, a fixed-length ring signature (no "trusted startup"), and LFT mechanisms related to the public chain

● achieves a high-speed consensus mechanism using verifiable random functions and equity proof

● builds a flexible, lightweight Alila Tech system architecture

5. Alila Tech's technical system

1. design principles

Alila Tech is to become a central and nervous system focused on privacy protection and scalability within the field of intelligent wearable devices. To achieve this and to address a range of challenges mentioned above, our architectural design follows the following principles.

2. separation of responsibilities

Known as a typical representative of the Internet of Things, it is unrealistic to connect all smart wearable nodes directly into a separate blockchain. In addition to different IoT applications requiring different blockchain attribute settings, the requirements of carrying too many IoT nodes for their size and computing power in a single blockchain rise up in order of magnitude for IoT devices.

Instead, the separation of responsibilities ensures that each blockchain interacts with the IoT nodes of a particular group, and with the other blockchain when required. This is similar to the architecture of the Internet — heterogeneous devices first form an internally connected group, the internal network. Smaller internal networks in turn constitute a larger internal network, eventually connected to the Internet center and communicating with each other. Separation of Duty usually creates a balanced system to maximize efficiency and privacy protection.

3. Orkham razor principle

Each blockchain has different uses and applications and should be designed and optimized. For example, blockchain dedicated for transaction delivery does not subject to Turing complete smart contracts; blockchain running in trust areas does not need to pay too much attention to transaction privacy.

4. is friendly to the Internet of Things

As previously earlier, the IoThings world is full of heterogeneous systems and nodes that vary in computing power, storage capacity, and power consumption. Because strong nodes can easily complete the operation completed by weak node Nengji, the blockchain operation should be optimized with weak nodes as the design target. For example, operations is lightweight, saving resources like computing power, storage space and energy.

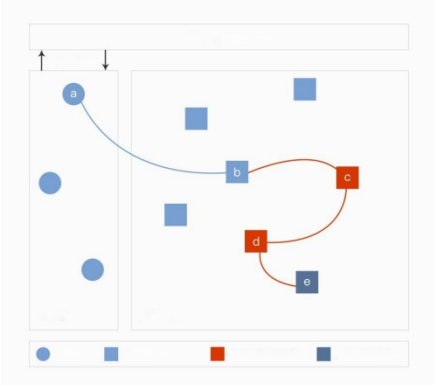
6. Anonymous communication technology based on P2P

The Alila Tech underlying communication network employs the P2P architecture and then incorporates an internode anonymous access mechanism to ensure the privacy protection of the information services. Alila Tech's P2P network anonymous communication is mainly achieved by:

1) runs a proxy server that periodically communicates with other Alila Tech applications, maintaining a TLS link to forming a virtual link in the Alila Tech network. Specifically, each user runs its own agent: get a directory, establish a path, and process connections. These agents accept TCP data streams and reuse them on the same line.

2) Alila Tech is encrypted at the application layer, and the transmission between each relay node is encrypted by a point-to-point key, forming a hierarchical structure. The nodes it passes through package the client so that communication security between the relay nodes. Specifically, each Alila Tech relay node maintains a 长 period verification key and a short-term session key, the verification key to sign the TLS certificate, the descriptor of the relay node, and is also used by the directory server to sign the directory. The session key is used to decode requests from the user to establish a path while negotiating a temporary key. The TLS protocol also uses a short-term connection key between the relay nodes of the communication, changing periodically independently to reduce the impact of key leakage.

3) Alila Tech network use random paths to mask the footprint so that observers at some point do not know where the data really comes from and where the real destination is. The client incrementally establishes an encrypted line in the Alila Tech network. The line only extends one jump at a time, and each extended relay node only knows where the data comes from The relay nodes to which the data will be sent. No one of the relay nodes knows the entire line. The client negotiated a separate set of keys with each hop to ensure that each hop cannot track the passing relay points. Once a line is established, it can be used for data interaction.

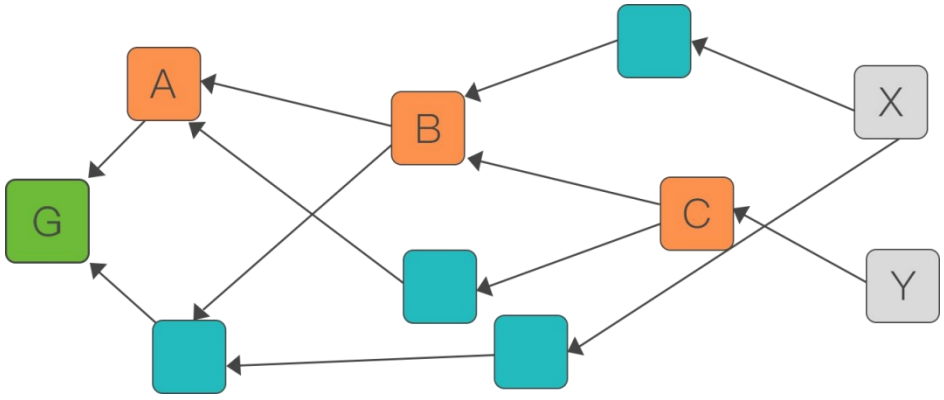


The rationale of Alila Tech's anonymous communication network is shown in the figure above. The directory server is the core of its network, responsible for collecting relay node information in Alila Tech network and publishing it to Alila Tech agent in the form of node snapshot and node description; the relay node is the basis of the Alila Tech network, the anonymous communication traffic in the network is forwarded through anonymous communication link composed of multiple relay nodes; the agent runs on Alila Tech client, it is responsible for establishing anonymous links and transferring network traffic between the user's network application and Alila Tech anonymous link. In the figure, an anonymous communication link of Alila Tech is composed of three relay nodes, which are successively the entrance, middle and exit positions depending on their positions.

7. Data structure

1. base DAG data structure

Alila Tech uses the underlying DAG structure to store transaction data in the first phase. At present, several projects such as IOTA and Byteball have successfully built public chains capable of the stable operation of the 长 phase, demonstrating the technological advancement and performance of the DAG chain. In the Alila Tech, the transaction information is encapsulated into one unit (Unit), and the units are linked together into a DAG diagram. Since units can be linked to any one or more previous units, they do not need to pay more computing cost and time cost for the consensus problem, nor to wait for strong data synchronization between nodes, or even the concept of multiple data unit assembly blocks, so it can greatly improve the concurrency of the transaction, and minimize the confirmation time.



The DAG data structure of Alila Tech is shown in the figure. The directed edge between the units indicates a reference relationship between two units, a directed side pointing to A by B, indicating the B reference A,A, B is a parent unit of A, the unit C; the unit G has no parent unit, called the creation unit, the creation unit is unique; the unit X,Y has no subunit, which is called the top unit.

The unit consists of the unit head and the unit message. The unit head mainly contains the following fields:

Unit version;

Token token;

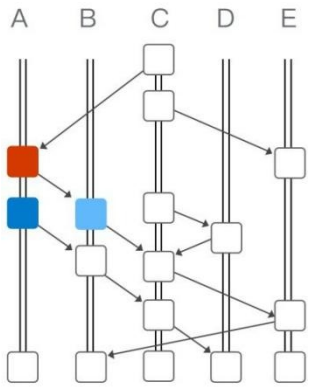
Unit Creator signature: a single signature or multiple creators sign together;

The hash; of a single or more parent units referenced by the parent unit hash:

List of witnesses: hash. with other units (usually the parent or ancestor unit) of the same witness

2. is based on an enhanced HashNet data structure for DAG

HashNet is a directed acyclic graph (DAG) consisting of countless vertices and directed edges of connecting vertices. As shown here.



The graph records what kind of data is sent in what order by all nodes across the network, and each node has a copy of such a HashNet 贝 in memory.

There are 5 computer nodes in the figure above A,B,C,D,E, each node has a column placing the vertex vertex (also called event). The latest event will be placed on top of the graph, HashNet is over time.

8. Advantages in wearable device applications

Alila Tech will connect with a large number of smart wearable devices to realize the superposition of digital assets, so as to solve the existing related practical problems. Alila Tech wants to build a set of bridging applications that connect physical world assets. To realize this vision, Alila Tech will expand based on LFT's underlying technology.

1) seconds-level fast transaction authentication

By optimizing the key links, etc., including signature algorithm, ledger structure, data operation, serialization, consensus mechanism, message diffusion, Alila Tech aims to achieve rapid transaction verification. Meet the scene needs of most users.

The storage of 2) massive data

The bookkeeping mode of blockchain duplex is constantly used in the system and has accumulated a large amount of data, resulting in a decline in operation speed. Alila Tech will realize the separation storage and table storage mechanism, and realize data mass storage.

3) node data fast synchronization

Alila Tech will develop a mirror mechanism, which can regularly mirror the local ledger to achieve a convenient roll-back mechanism, and under a unified consensus, the mirror label can be designated for roll-back. At the same time, shorten the operation cycle of the new node addition, you only need to synchronize the latest mirror images and a small number of recent transaction sets, you can integrate into the network and participate in consensus verification.

The 4) data permission control policy

Alila Tech provides two types of permission control policies for data information writing and reading. Data information writing permission, multiple users are set under the same account, and corresponding permissions are set for different operations to meet the use scene of multi-party signature control. Data information read permission, the user can grant and withdraw the single user or user group on the data operation permission, the user group can be flexibly configured by the user. Data includes user account information, transaction information, etc., and the granularity can be refined to the transaction or account Each property field.

5) multiple privacy protection

To facilitate the use of Alila Tech product services, in addition to traditional client generation and storage mechanisms, Alila Tech provides both web hosting access and private key hardware generation (U-key) schemes. Web managed access, in which the user name and password are mapped into private keys via a specific algorithm and stored on the service side. The private keys stored on the server side are encrypted data that can only be decrypted on the user side; the hardware private key is designed to meet the needs of the user.

9. Release of the Alila Tech Pass

In order to realize the value shaping of Alila Tech in the global smart wearable device application scenario, the joint agency is issued on the autonomous tokens of the wave field ecological community, the code ALT. Giving raw tokens to participants through liquidity mining, the value of ALT will increase with the continuous destruction of ALT digital assets and the scale realization of Alila Tech application value.

The total circulation of ALT is 1 million, including 57% mining, agency 15%, foundation 10%, team 8%, incentive 6%, private placement 4%

Of these, 10% of funds and 8% of teams were locked up for three years, 15% of institutions were released on average for three years, 6% incentive and 4% of private placement belong to the original circulation.

10. Excavation mechanism for the ALT

Alila Tech through consensus algorithms, encryption, peer-to-peer networks and reward mechanisms, forms an autonomous community, forming a mining mechanism to achieve a trust not achieved through the central mechanism, and finally achieve point-to-point Value circulation.

Alila Tech mining selection PoS mechanism, to achieve the characteristics of small energy consumption, fast speed, low threshold, good preservation and other characteristics.

Under the PoS mechanism, the algorithm requires the system to do three things:
1. randomly specifies the appearance sequence of producers;
2. is not block blocks block blocks;
3. shuffles each cycle to disrupt the original order;

Through the mechanism of P o S computing force synthesis, ALT digital assets are excavated in three years (150,000 in the first year, 260,000 and 160,000 in the third year); the same, the total destruction of 670,000, the destruction address can be checked in real time, and the whereabouts of each digital asset can be inquired through the block browser.

This means that there is no contention between producers and no missing blocks and there is one block every 3 seconds. One of the greatest advantages over the POW and POS,PoS mechanisms is that the consensus cycle is much shorter. At the same time, PoS also distributes part of the reward to network maintenance nodes and voters as a reward for community maintenance.

11. Governance system

Divalization is the cornerstone of blockchain technology, but there are obvious defects in its pure form, leading to inefficiency and poor rapid iterability. We argue that the scalability issues related to blockchain and the continuous updating and addition of functions and functions is a natural product of technology evolution, use cases and their applications are irrelevant but rather consensus concerns on governance. An appropriate governance system with attrition and business efficiency will achieve continuous and rapid innovation.

In order to achieve the main goal of decentralized public blockchain operation, its scale ability, meets the requirements of regulatory agencies and government, and the needs of large enterprises, the next step of Alila Tech is to improve its governance mode and make it have the ability to continuously iterate while the rapid development of ecosystem. In order to reach this new governance consensus, we aim to identify the right stakeholders and to determine how these stakeholders categories are represented and how decision-making rights can be distributed. It is important that this governance model is effective and cost-effective, with consensus and decisions to balance all the interests of blockchain Opinion of those concerned. Alila Tech sets a flexible framework that assists with on-and under-chain governance

12. Disclaimer

The documentation is used only for the delivery of information and does not constitute any advice, solicitation or invitation for investment in the sale of stocks or securities in Alila Tech Ecology and its related agencies. Such invitations must be made by a confidential memorandum and must comply with relevant securities and other laws.

The contents of this document shall not be construed as forcing participation in the Alila Tech autonomous community, including requesting a copy of this white paper or sharing this white paper with others.

Participating in the Alila Tech autonomous community represents participants who have reached age standards and have full civil capacity.

The Alila Tech team will continue to try reasonably to ensure that the information in this white paper is true and accurate. During the development process, the platform may be updated, including but not limited to the platform mechanisms, tokens and their mechanisms, and token allocation. Some of the document may be adjusted in the new white paper as the project progresses, and the team will make the update public by publishing a notice or a new white paper on the website. Participants are sure to get the latest white paper timely, and adjust their decisions according to the updates. Alila Tech Ecology clearly states that it is not liable for losses caused by participants' (a) reliance on the content of this document, (b) inaccuracies of information in this article, and any behavior that GiD causes in this article.

The team will spare no effort to achieve the goals mentioned in the document, but based on the presence of force majeure, the team cannot fully make complete commitments. Alila Tech's token ALT in the Bofield eco-autonomous community is an important tool for the efficiency of the platform and is not an investment. Having ALT does not grant ownership, control, decision-making to the platform. ALT, as a value medium used in the Alila Tech ecosystem, is not a currency of any kind: (a) securities; (b) equity of a legal entity; (c) stocks, bonds, notes, warrants, certificates or other instruments conferred with any rights.

The value appreciation of ALT depends on the market law and the demand after the application. It may have no value, the team does not commit to its value, and is not responsible for the consequences caused by the increase or decrease in value. To the maximum extent permitted by applicable law, the Team shall not be liable for damages and risks arising in the autonomous

communities of Alila Tech, including, without limitation, personal damage, loss of business profit, loss of business information, or any other economic loss.

Alila Tech Ecology complies with any regulatory regulations conducive to the healthy development of the industry and the self-discipline declaration of the industry. Participants participation means the representative will fully accept and comply with such inspections. Also, all information disclosed by the participants to complete such inspections must be complete and accurate.

References.

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998..

[2] *H. Massias,X.S. Avila,and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux,May 1999..*

[3] S. Haber,W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology,vol 3,no 2,pages 99-111,1991..

[4] *D. Bayer,S. Haber,W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication,Security and Computer Science,pages 329-334,1993..*

[5] *S. Haber,W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security,pages 28-35,April 1997..*

[6] A. Back, "Hashcash-a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002..

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy,IEEE Computer Society,pages 122-133,April 1980..