WHITEPAPER

THINGSCHAIN

step out line - step in chain

Blockchain for the Internet of Things

Contents

Abstract 4
1. Introduction 5
Blockchain 9
How Blockchain is relevant for IoT applications? 11
Why are current blockchain solutions not suitable for IoT? 13

2. Overview and Vision of ThingsChain 14
How ThingsChain can solve the problem? 14
Some projects working in related domains 15

3. ThingsChain: Design and Architecture overview 16
pBFT (Practical Byzantine Fault Tolerance) 17
DAG (Directed Acyclic Graphs) 17
Introducing Radiating Block Graphs 18
Multi-layer blockchain 19
WebChain & NestChain 20
Cross Chain Communication 21

4. ThingsChain Network 23
Proof of Work (PoW) 24
Proof of Stake (PoS) 24
Delegated Proof of Stake (DPoS) 24

5. Security 28
Elliptic Curve Cryptograph 28
Multi-signature accounts 29
Storing data in encrypted form on the blockchain 29

6. Summary 30

Abstract

IoT devices are becoming increasingly more important in our digitized society. It is estimated that there will be 20 billion connected IoT devices in the world by 2023. Despite their growing prominence, IoT devices are hindered by the issues of lack of interoperability, poor security, and increased centralization. Blockchains are a possible solution to these problems, but current blockchain designs are not suited for application in IoT.

Our team has designed a solution which attacks these problems of interoperability and scalability by creating a new multi-layered blockchain architecture specifically for IoT application. ThingsChain is a multi-layered blockchain which solves the problem of scalability and low transaction throughput faced by current blockchains. The protocol design uses a multi-layer architecture with cross chain communication and added security protocols to ensure the safety of IoT data on the blockchain.

Introduction

Internet of Things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with software and sensors which enables these things to connect and exchange data[1]. IoT enables physical objects to get smarter and connect with the Internet to provide new capabilities.

For example, Nest thermostats allow one to remotely monitor the room temperature and automatically adjust it based on intelligent algorithms. IoT enables better monitoring of machines and equipment by having multiple sensors to capture data points like temperature, pressure, etc. and continuously relay it to servers where they can be analyzed and acted upon. This enables prediction of imminent breakdown and pre-emptive measures which significantly improve uptime and productivity of the machines. Enabling devices to communicate with each other and with the Internet enables many use cases which were not possible without IoT. This opens a plethora of new opportunities which are yet to be fully explored.

It is estimated that by 2023, there will be around 20 billion connected IoT devices in the world. Connected IoT devices include connected cars, machines, meters, sensors, point-of-sale terminals, consumer electronics, and wearables. Between 2017 and 2023, connected IoT devices are expected to increase at a CAGR of 19 percent, driven by new use cases and affordability. The major growth in connected devices will primarily come from wide-area and short-range IoT, as shown in Fig.1 below.

It is estimated that by 2023, there will be around 20 billion connected IoT devices in the world. Connected IoT devices include connected cars, machines, meters, sensors, point-of-sale terminals, consumer electronics, and wearables. Between 2017 and 2023, connected IoT devices are expected to increase at a CAGR of 19 percent, driven by new use cases and affordability[2]. The major growth in connected devices will primarily come from wide-area and short-range IoT, as shown in Fig.1 below.

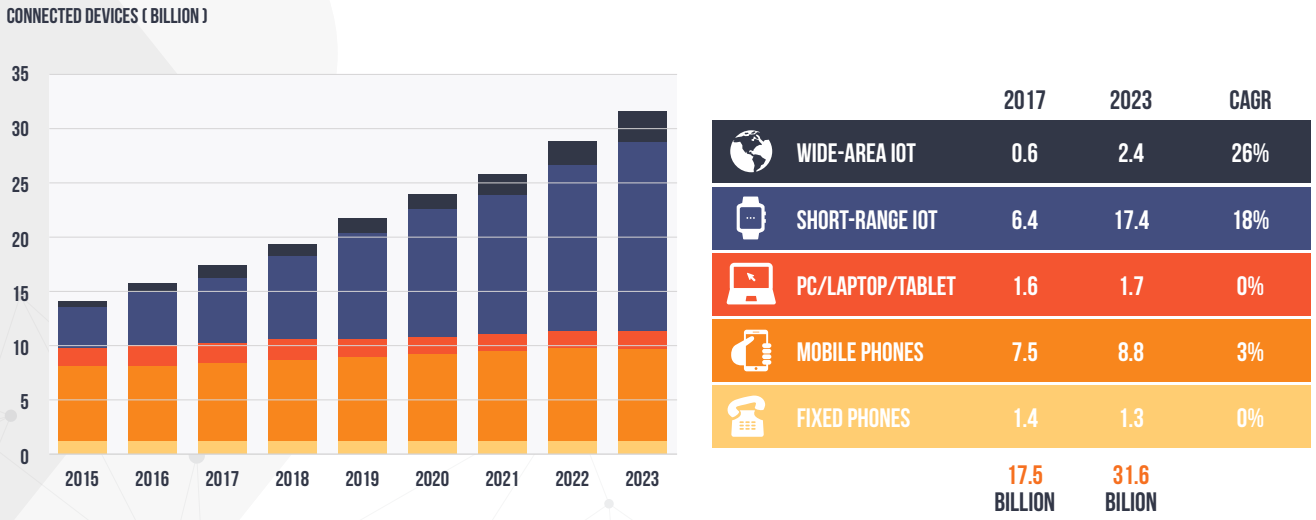


Fig 1. Number of connected IoT devices (Ericsson Mobility Report, 2017)

As of now, most of these IoT devices are connected to centralized services where they constantly log the data generated by their sensors and get commands from monitoring and control. These backend devices could be servers hosted on-premises or cloud storage solutions like AWS S3, Google Cloud, etc. This introduces a degree of centralization in IoT devices, which were actually designed to operate in a decentralized fashion. IoT devices are limited by the scalability issues of the centralized servers they are connected to and thus, can't act in a completely decentralized manner.

Security and privacy of data generated by IoT devices is another area of concern. The data generated by IoT devices are stored in centralized servers and often very little thought is given to the security and privacy of data so stored. The issue can be in multiple domains:

1. Lack of security in data transmitted from device to the central server.

2. Lack of privacy protection of data stored on servers e.g. anonymizing data, etc.

3. No proper protocols for ensuring data security in centralized servers.

This often leads to a scenario where the servers storing IoT data act as a honeypot for hackers. Some examples of hacks which used IoT devices as their vector are.

1. The Mirai Botnet attack - In October 2016, the largest DDoS attack ever was launched on service provider Dyn using an IoT botnet. This lead to huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN[3].

2. Later, a variant of Mirai Botnet was used to attack the financial sector in 2018[4]. The IoT botnet primarily comprised of compromised home routers, TVs, DVRs, and IP cameras exploiting vulnerabilities in products from major vendors including MikroTik, Ubiquiti, and GoAhead.

A recent report by Symantec found that the number of IoT attacks increased from about 6,000 in 2016 to 50,000 in 2017 - a 600% rise in just one year[5].

Interoperability of IoT devices

Another key issue is the lack of interoperability between IoT devices. Even though a large number of IoT devices have been deployed, businesses have been unable to reap many benefits from them. Most of these IoT devices communicate using different protocols and making them communicate with each other as part of a network is non-trivial. Multi-vendor interoperability and security concerns are the two key obstacles preventing IoT devices from generating value for businesses today[6]. A greater portion of the value that IoT produces comes from interaction, cooperation, and eventually autonomous coordination of heterogeneous entities, which is missing today.

(1) : *Internet of Things - Wikipedia*

(2) : *Ericsson Mobility Report, 2017*

(3) : *5 Worst IoT Hacking Vulnerabilities*

(4) : *Mirai Botnet*

(5) : *600% increase in IoT attacks*

(6) : *Interoperability is the key for IoT*

Blockchain

Blockchain technology was first introduced by Satoshi Nakamoto in 2008. In 2009, he released an implementation of Bitcoin which was envisaged to be a peer to peer electronic cash system. Bitcoin was the first protocol which used blockchain technology as we understand it today.

The key idea behind blockchain is that the transactions in the network are included in blocks and each of these blocks refers to a previous block, creating a chain-like structure. Thus, blockchain is a singly linked list of blocks, with each block containing a number of transactions. It provides a decentralized and immutable data store that can be used across a network of users. It also creates assets and acts as a shared ledger that records all transactions. Each transaction can be easily queried, affording greater transparency and trust to all parties involved[7].

Ethereum is the next step in the blockchain evolution. Created in 2013, it is considered to be Blockchain 2.0 and allows for the running of arbitrary code to complete computational processes, rather than just record transactions. It is a Turing-complete virtual machine and runs as a public blockchain.

(7) : *Introduction to blockchain technology, Hackernoon*

Blockchain Operational Models

Blockchains can have different operational models based on the amount of trust required between nodes. There are two primary modes of operation of blockchains - permissionless and permissioned. In permissionless blockchains, anyone can start a node and verify blocks on the blockchain to contribute to the consensus. There is no permission needed to join a blockchain network. Hence, anybody can start interacting with a permissionless network. Bitcoin and Ethereum are examples of permissionless blockchains. Such blockchains need consensus mechanisms which are resistant to Sybil attack to prevent random actors joining the network and breaking its consensus. For example, Bitcoin uses PoW consensus which prevents Sybil attack by asking nodes solve cryptographic puzzles before adding a node.

Permissioned blockchains, in contrast, are closed and monitored ecosystems where access and capabilities of each node in the network are based on the roles assigned to them. Only a restricted set of actors have the right to validate block transactions and interact with smart contracts in such networks. E.g. Hyperledger Fabric is a permissioned blockchain where all nodes are considered as trusted and have cryptographic identities, e.g., issued by member services like Public Key Infrastructure (PKI), which makes them highly scalable with low computation and a relatively straightforward consensus mechanism.

How Blockchain is relevant for IoT applications

Blockchain technology is suited for application with IoT devices as it provides the much-needed properties of decentralization, transparency, and immutability. With different devices being part of the same blockchain protocol, it also tackles the problem of interoperability. We explore these topics in more detail below.

1. Decentralization

Decentralization frees data generated by IoT devices from the control of centralized agencies. As we discussed earlier, if IoT devices are controlled by centralized entities there is a risk of these entities trying to use this data for their own benefit. For example, using sensor data to show specifically targeted advertisements to individuals. Also, all data being stored on centralized servers make them target for attacks. Use of blockchain provides decentralization which makes IoT devices and their data more secure from attacks.

2. Transparency

By their very design, blockchains are distributed public ledgers. If IoT device data is stored in blockchains, then anybody can audit it and verify the stored data. This gives a degree of transparency which is seldom seen in centralized entities. Centralised entities often try to hide their transactions and data, and details are only revealed to entities with authority or power.

3. Immutability

Since transactions stored in a blockchain is immutable, the data stored in blockchains can be used for auditing purposes. If IoT device data is continuously stored in blockchains, then it can easily be audited anytime by using blockchain specific APIs.

4. Interoperability

One key issue with IoT devices is that of interoperability. IoT sensors from different vendors often don't follow the same communication protocol and it is difficult to make them talk to each other. But if blockchain is used as the underlying layer, then each IoT device can save transactions in the blockchain and thus one device can communicate with the other as all the device save data and transactions to the same underlying blockchain.

5. Automatic interactions with smart contracts

Some blockchains like Ethereum provide a platform for executing 'smart contracts'. Smart contracts are programmable logic or contracts which can be coded and deployed in public blockchains. Users or entities can interact with these smart contracts by paying some gas fees. These smart contracts thus enable automated contract execution on the blockchain.

Use cases which combine smart contracts with IoT devices open many new possibilities. For example, an IoT temperature sensor can be attached to a box containing fresh fruits which is being transported. The IoT sensor would periodically send its temperature reading to a smart contract. As long as the temperature is below a certain threshold, there is no action. But as soon as it crosses the threshold, the smart contract penalizes the deposit made by transporter for inability to maintain agreed temperature while transporting the product.

This process is completely automated and there is no human involved. The smart contract being deployed on blockchain ensures that there is no problem of trust, and if some party tries to tamper this process, the same will be captured immutably on the blockchain.

Why are current blockchain solutions not suitable for IoT?

Though blockchains provide properties which are beneficial for IoT ecosystem, it doesn't mean that every blockchain is suitable for IoT. Below are some potential issues with the applicability of current blockchain solutions for IoT.

1. Problems with scalability

Current popular blockchain platforms like Bitcoin and Ethereum are not suited for IoT transactions as the number of transactions supported on these blockchains is very small. IoT devices, on the other hand, need a very high number of transactions, as thousands of sensors can be used for capturing different data points for an entity, e.g. factory.
There are few specialized IoT solutions which use distributed ledger technology but are designed specifically for IoT devices. IoTA, for example, uses DAGs to enable decentralized ledger and high transaction throughput rate. But the current design of IoTA introduces some degree of centralization because of use of Coordinator nodes run by the IoTA foundation.

2. IoT nodes are lightweight and can't do mining, storing blockchain, etc.

A. IoT devices are generally small sensor devices and are not equipped to do heavy computations like proof-of-work mining, etc.

B. IoT devices don't have space for storing complete blockchains and independently verifying them. For example, Bitcoin and Ethereum chain size are currently more than 100 GB. No IoT devices have that much storage capacity.

C. IoT devices are not able to connect with peers all the time. Their connection to peers depends upon their connectivity and uptime. Though, most current blockchains need constant connectivity to get newer blocks and be updated.

Because of the above-mentioned limitations, most blockchains today are too heavyweight for IoT devices.

Overview and Vision of ThingsChain

ThingsChain: Blockchain 4.0

ThingsChain is a next-generation platform for IoT devices based on blockchain technology. It uses a multilayered architecture which provides a solution to the issues faced by current blockchains like lack of scalability and low transaction throughput rate.

How ThingsChain can solve the problem?

ThingsChain uses a multi-layered approach to store IoT device data. The main layer is called Webchain and the secondary layer is called NestChains. Nest Service Chains are the layers which would interact with services and have a high throughput. Only the changes in the state every 10 minutes are updated on the NestChain. Thus the NestChain acts as the final source of truth, while WebChains store transitory information.

The WebChain could potentially be a private blockchain and would rely on the NestChain for relaying transactions between secondary layers. The secondary layer provides flexibility and extensibility to adapt to diversified requirements of different IoT applications. Thus, this architecture enables high scalability which is needed for handling transactions from IoT devices.

Some projects working in related domains

1. IoTA - IoTA focuses on enabling IoT device communication through a distributed ledger technology called Tangle. It is unique in the sense that it gets rid of concepts like blocks and miners. In IoTA, each transaction needs to approve two previous transactions. This mechanism thus prevents the inherent issues with blockchain technology like poor scalability and low transaction throughput rate.

2. Iotex - IoTeX aims to become the privacy-centric and scalable nervous system for IoT. It uses a unique architecture of blockchain within blockchain to counter the scalability issues faced by traditional blockchains like Bitcoin and Ethereum. It also gives lots of emphasis on privacy of the data stored on the blockchain and uses ring signature technology to enable this.

3. Iotchain - Iotchain is a blockchain project from China which also enables IoT devices to interact with each other. They use DAG technology, similar to IoTA.

4. HDAC - HDAC is a blockchain project which is working on creating a highly reliable blockchain network that can conveniently utilize the services of the world's numerous IoT devices. They focus on specific fields in IoT like M2M (machine to machine) transactions and device authentication. They are based out of Korea and have partnered with Hyundai.

Design & Architecture Overview

The goal of ThingsChain is to create a trustless and decentralized system in which transactions are similar to real-world transactions. ThingsChain accomplishes it by designing its network as a multi-layer blockchain with double consensus algorithm to allow transactions to be linked with additional information on-chain. Users, developers, node operators, organizations, enterprises, crypto-exchanges, partners and other blockchains & cryptos can take part in the development of ThingsChain as described above. In this paper, we will discuss the components of the network and the roles of each participant in the whole ecosystem of ThingsChain.

As discussed above, ThingsChain blockchain will have a multi-layered structure. The main layer will be called Webchain and the secondary layer will be called Nestchain. Every 10 minutes, the real transactions or important information will be stored in Nest chain.
DAG (Directed Acyclic Graphs).

pBFT (Practical Byzantine Fault Tolerance)

pBFT is a replication algorithm which was designed to tolerate Byzantine faults. The objective of Byzantine fault tolerance is to be able to defend against failures of system components with or without symptoms that prevent other components of the system from reaching an agreement among themselves, where such an agreement is needed for the correct operation of the system. pBFT algorithm provides high-performance Byzantine state machine replication, processing thousands of requests per second with sub-millisecond increases in latency[8].
DAG (Directed Acyclic Graphs).

As discussed earlier, blockchains effectively have a linked list like structure. The blocks in a blockchain need to be added one after the other like a list. This structure leads to issues of scalability and a low number of transactions per second which inhibit mainstream adoption of blockchains. Bitcoin and Ethereum, both suffer from these issues.

This inherent handicap of blockchain has led to an exploration of alternate ways of maintaining decentralized databases. Directed Acyclic Graph (DAG) is one such alternative. A Directed Acyclic Graph is an implementation of a graph, and it allows the networks using it to circumvent some of the blockchain's most daunting limitations.

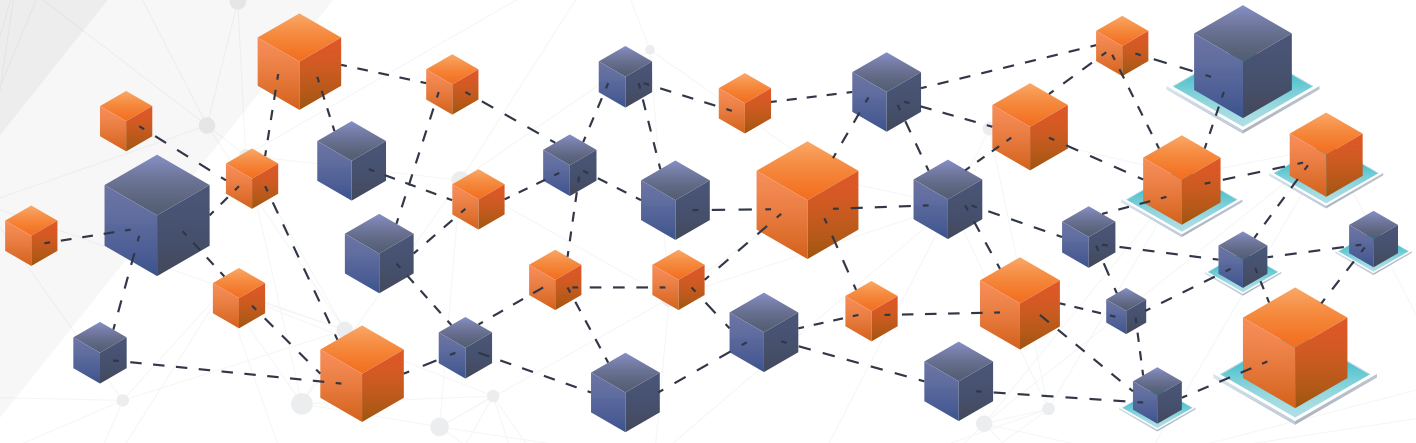


Fig 2. The "Tangle" in DAG: Each node represents a new transaction[9].

IOTA is the most talked about cryptocurrency using DAG. Use of DAGs has completely removed the need of miners and transaction fees to maintain a distributed consensus.

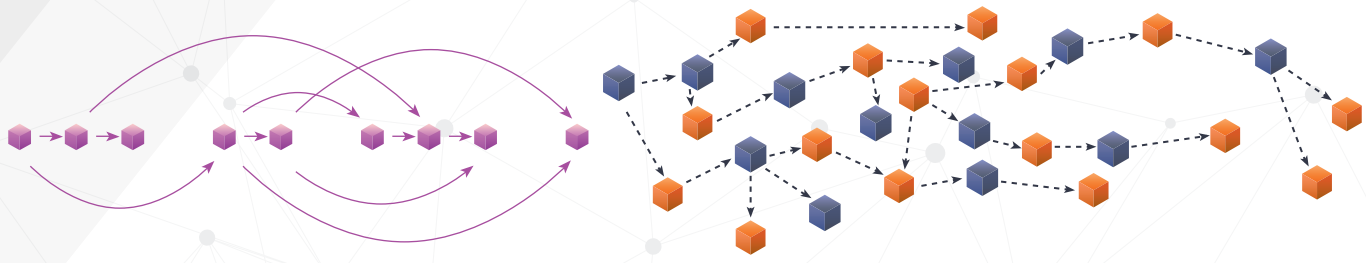
On Bitcoin, miners compete in solving a mathematical puzzle for the opportunity to write to the blockchain's history. On IOTA, however, everyone's a miner; everyone is responsible for both issuing and validating transactions[10].

Introducing Radiating Block Graphs

Radiating block graphs are similar to DAGs. A DAG is a finite directed graph with no directed cycles. It consists of finitely many vertices and edges, with each edge directed from one vertex to another[11].

The key structure which makes DAGs work is a Tangle. The Tangle is a particular kind of directed graph, which holds transactions. Each transaction is represented as a vertex in the graph. When a new transaction joins the tangle, it chooses two previous transactions to approve, adding two new edges to the graph[12].

Radiating Block graphs also work on a similar concept with multiple nodes and directed connections between them.



DAG ***Radiating Blocks Graph***

Fig 3. Illustration of DAG and Radiating Blocks Graph

Multi-layer blockchain

ThingsChain proposes to have a multi-layer blockchain structure. The main layer will be called WebChain and the secondary layer will be called as NestChain. This structure will increase the storage capacity, process more transaction confirmations per second and provide more security. A two-layer structure will also decrease the size of the blockchain which nodes are needed to store.

Only the final transactions will be stored in the secondary chain which is the NestChain. The transitory transactions will be stored on the WebChain and once a set of transactions is finalized, the net effect of those transactions on the state of the blockchain will be updated on the NestChain.

The use of a DAG like Radiating Block also makes the system more secure as there is no issue of attack by miners with a concentration of hashing power. Since each new transaction which joins the tangle approves two other previous transactions, there are no miners needed to verify the transactions in the system.

(8) : *Byzantine Fault Tolerance, Wikipedia*

(9) : *IoTA Whitepaper*

(10) : *Introduction to DAG and cryptocurrencies*

(11) : *Directed Acyclic Graphs - Wikipedia*

(12) : *The Tangle - An Illustrated Introduction*

WebChain and NestChain

WebChain

WebChain is the main layer of ThingsChain which uses Radiating Blocks Graph. The new concept of Radiating Blocks Graph will increase the transaction rate as compared to current blockchain technology. It is considered a big improvement for IOT industry.

WebChain uses delegated proof of stake model as a consensus mechanism. Nodes can vote on who would be the block validators. The amount of votes each node has depends upon the number of tokens they have staked in the network.

NestChain

This is a brand-new technology idea in which blocks are controlled by Supernode. In Webchain, the number of blocks is high and those do not follow any certain order hence necessary storage and redundant data could be enormous. Therefore, the main purpose of Nestchain is to filter important and necessary data and then store it in the WebChain every 10 minutes. With this technology, user data will be more secure, transaction rate would increase and 51% attack could be avoided.

NestChain uses Proof of Truth consensus mechanism. It's the consensus that only real transactions or confirmed information are confirmed by supernodes and stored in the NestChain.

There could be different NestChain for different purposes. These would be called as Service Nestchains. There could be separate NestChains for different sectors. One example is for the government. Civilian's IDs could be stored into the NestChains, but the government can control which civilian IDs are added to the main layer, WebChain. Only those IDs which are verified by government agencies could be stored in the main layer, which is the WebChain. Similar service NestChains could be deployed for Medical, Real Estate or Banking use cases but only verified data is allowed to be updated on the main layer.

Cross Chain Communication

Cross Chain communication is very important for a multi-layered network especially when it is designed for IoT devices. IoT devices produce data at a very high rate as they are sensors which capture data all the time. This could be every second or every millisecond. There is always a need for an IoT device in one secondary layer to communicate with an IoT device in another secondary layer. To enable this Nestchains have been designed such that they can exchange data and transactions with other NestChains via WebChain. Since IoT devices have low computation and storage capabilities, it is imperative that communication between them be made light-weight so that it doesn't constrain their resources.

Cross chain communication can be achieved by using sidechain pegging technology proposed by Adam Back[13]. This works as follows: to transfer parent chain coins into sidechain coins, the parent chain coins are sent to a special output on the parent chain that can only be unlocked by an SPV proof of possession on the sidechain.

(13) : *Enabling Blockchain Innovations with Pegged Sidechains*

To synchronize the two chains, the following two waiting periods need to be defined:

1. The confirmation period of a transfer between sidechains is a duration for which a coin must be locked on the parent chain before it can be transferred to the sidechain. The purpose of this confirmation period is to allow for sufficient work to be created such that a denial of service attack in the next waiting period becomes more difficult.

2. The user must then wait for the contest period. This is a duration in which a newly-transferred coin may not be spent on the sidechain. The purpose of a contest period is to prevent double spending by transferring previously-locked coins during a reorganization.

While locked on the parent chain, the coin can be freely transferred within the sidechain without further interaction with the parent chain. However, it retains its identity as a parent chain coin, and can only be transferred back to the same chain that it came from.

Thus, sidechain pegging can be effectively used to achieve cross-blockchain communication similar to how we have described above.

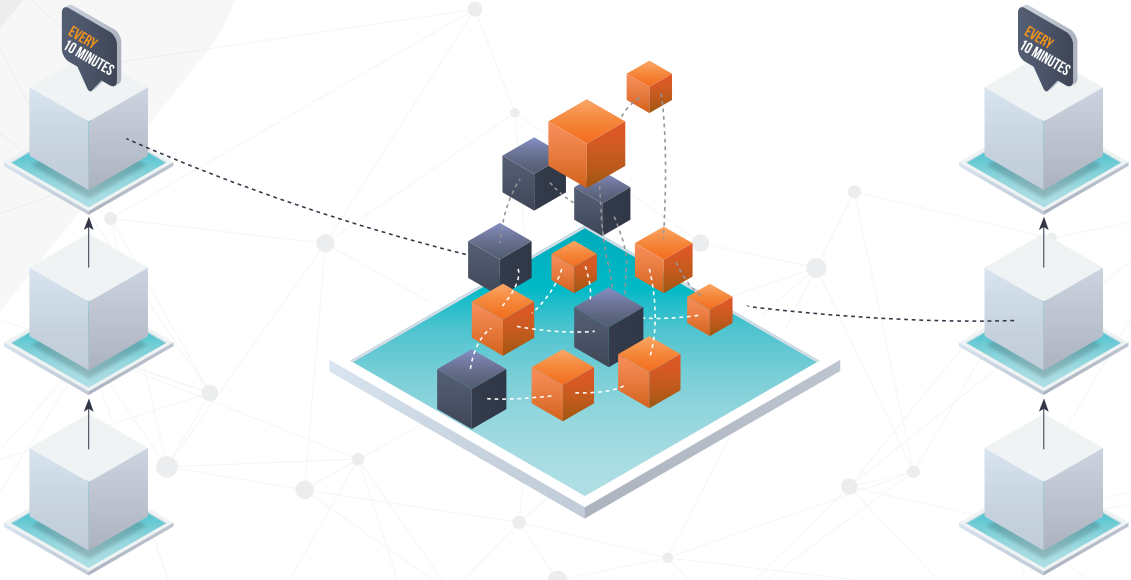


Fig 4. Communication between 2 NestChains

ThingsChain Network

Consensus mechanisms are an important aspect of the design of any blockchain based system. It defines how the nodes in the network interact with each other and how they should act to contribute to the trust in the network. Some of the popular consensus mechanisms used in blockchains today are Proof of Work, Proof of Stake, and Delegated Proof of Stake. In ThingsChain network, WebChain will use a Delegated Proof of Stake (DPoS) consensus mechanism while NestChain will use Proof of Truth as the consensus mechanism. Below we give a brief description of these consensus mechanisms.

Proof of Work (PoW)

Proof of Work consensus mechanism is used to confirm new transactions and produce new blocks in the blockchain. The miners solve a cryptographic puzzle related to the transactions included in the block. If they are able to find a correct solution, they are said to have "mined" a block and this block is then sent to other nodes in the network for validation and inclusion in the blockchain. Proof of work thus acts as a "Sybil attack" prevention mechanism, as anybody who wants to add a block to the blockchain has to solve a cryptographic puzzle before his block can be added to the blockchain. Blockchains based on this consensus mechanism are Bitcoin, Litecoin, etc.

Proof of Stake (PoS)

Proof of Stake systems have the same purpose of validating transactions and achieving consensus, however, the process is quite different than in Proof of Work systems. With Proof of Stake, there is no mathematical puzzle, instead, the creator of a new block is chosen in a deterministic way based on their stake. The stake is how many coins/tokens one possesses. For example, if one person were to stake 10 coins and another person staked 50 coins, the person staking 50 coins would be 5 times more likely to be chosen as the next block validator[14]. Casper (Ethereum's PoS protocol), TON (Telegram Open Network), etc. are based on Proof of Stake consensus mechanism.

Delegated Proof of Stake (DPoS)

Delegated proof of stake as the name suggests is a variant of PoS consensus mechanism. The only difference is that in DPoS systems, users 'vote' to select 'witnesses' (other users they trust to validate transactions), and the top tier of witnesses (who have collected the most votes) earn the right to validate transactions. Users can even delegate their voting power to other users, whom they trust to vote for witnesses on their behalf.

Votes are weighted according to the size of each voter's stake. A user need not have a large stake to enter the top tier of witnesses. Rather, votes from users with large stakes can result in users with relatively small stakes being elevated to the top tier of witnesses[15].

(14) : *Consensus Mechanism - PoW vs PoS*

(15) : *What is Delegated Proof of Stake*

Proof of Truth

ThingsChain will use a proof of truth consensus mechanism which will ensure that only correct data is stored in the NestChain. It's a consensus mechanism which allows only real transactions or information confirmed by supernode to be stored in Nestchain.

ThingsChain network consists of 3 types of Nodes:

1. Full Node - This node is part of WebChain. Full Node is a computer who participates in WebChain network and has connections with other Full Nodes. The Full Node makes sure of the correctness and integrity of the NestChain layer. They can also provide additional services on the network and ensure that the network is running correctly. This ensures that most of the high throughput transactions are handled on the WebChain itself and only once in every 10 minutes the changes in the states are updated on the NestChain.

Transactions will be sent to Full Nodes and forwarded to Delegates. A Delegate is a Full Node who has been voted by other Full Nodes (Voters) to be the validator for the next block. Voters are Full Nodes who stake their TIC (ThingsChain token) to get the votes. To vote for a Delegate, a Full Node must create a transaction called Vote Transaction and the total Votes will be counted with weights are the current staking balance of the Voters. Full Nodes can be run by any computers and they play a vital role in the sustainability of the Thingschain network. To promote Full Nodes to stake TIC and join in the voting process, Thingschain has the Block reward system for Delegates and its Voters. Thingschain rewards the block generators a fixed amount of TIC per block.

2. Super Node - This node is part of Main NestChain. The main objective of Super Nodes is to make transactions in ThingsChain information-rich. NestChain layer in ThingsChain will be run by SuperNodes. Super Nodes will approve NestChain Blocks that contains transactions and propagate the NestChain transactions to other Super Nodes and Full Nodes across the ThingsChain network.

A Super Node deposits a large amount of tokens as stakes to support its commitment to the network. To incentivize Super Nodes to participate in the ThingsChain network, the network rewards them with the fees given by the users for processing the attached information. This acts as an earned interest for Super Nodes for depositing a large amount of tokens as stakes in the network.

3. Service Node - This node is part of Service NestChains like government service chain, medical service chain, real estate service chain, etc. Service nodes make up the Service NestChains which are developed for specific use cases. All data transacted in the service nodes need not be updated in the NestChain, only the trusted and verified changes in state are updated in the NestChain. ThingsChain is decentralized at the Full Node and SuperNode layer but not at the service node layer. If a particular service NestChain run by Service Nodes is disrupted then the network fails to provide the service. This also models real-life scenario where if a particular government agency pulls out from a platform, then the data about that government agency is not available on the common platform.

Advanced Service Nodes provide services like Verification of Nestchain, Instant Payment System or Private Payment System. Service Nodes must be trusted by the network. After completing the process to prove the identities and authorities, Service Nodes become trusted Nodes and can start providing their services to the network. Service Nodes work together following the Proof of Truth mechanism to maintain the consensus of the network.

Service Nodes can be run by Governments, Hospitals, Universities, Banks, and Enterprises. The services on Thingschain network are provided by certain Service Nodes and they are not decentralized. For instance, only China Government can provide Verification service to Chinese Passports. Thingschain is designed to be decentralized on the Web-chain and the Nest-chain and not for the extra services. Whenever a Full Node, a Delegate or a Super Node gets out of the network, Thingschain is still run by other Nodes. However, if a Service Nodes gets out of the network, the service provided by that Service Nodes will be suspended. That is the reality of the real world and ThingsChain's design is to bring it to the network, not to break it.

As shown in Fig. 5, every 10 minutes, the real transactions or important information will be stored in Nest chain. That's why the transitory transactions will not be stored in the NestChain. Only the necessary information will be selected depending on the purpose of each industry like KYC (Know Your Customer) service for government, information of patients for medical health records, etc.

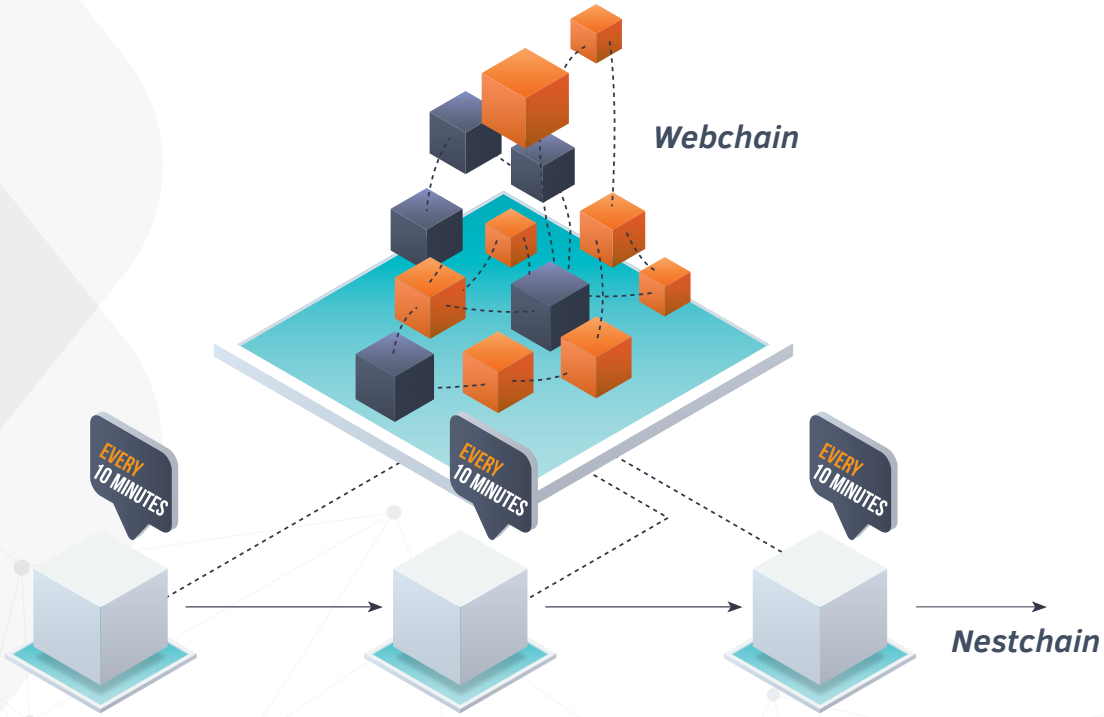


Fig 5. Interaction of WebChain and NestChain

Security

Security due to decentralization

Decentralized networks are much more secure as there is no centralized server where all the data and transactions are stored which can be attacked to steal the information. There is a risk of the client side or the cloud service being hacked causing user data to be stolen.

Along with decentralization, ThingsChain is using some of the latest technologies for enhanced security and performance. Few of them are mentioned below.

Elliptic Curve Cryptography

Elliptic Curve Cryptography(ECC) is used in public key cryptography for ThingsChain. ECC offers the same security level when you compare it with RSA. A few advantages of ECC are that it has much shorter operand size and more efficient implementations. Over the years, it has become a de-facto standard for protecting security and privacy for emerging IoT systems and cryptocurrency networks[16].

(16) : *Elliptic Curve Cryptography, IoT Security and Cryptocurrencies*

Multi-signature accounts

ThingsChain supports multi-signature accounts. A multi-signature account is an account that requires multiple signatures to sign for transactions. Users can specify the signers who will be needed for operating a particular account.

This provides better security as it protects against the scenario where the account operator goes rogue. Suppose there is an account which is used to push data on the blockchain by a government agency. If a single person has access to this account, then there is a risk of him going rogue and potentially entering incorrect data. Such situation is prevented by using multi-signature accounts as now consent of multiple people is needed to operate that account.

Storing data in encrypted form on the blockchain

Data on the ThingsChain blockchain will be stored in encrypted form by default. This will prevent attackers from just reading off the data stored in the blockchain by IoT devices. In a public blockchain, data stored is accessible by anyone. Hence, to protect privacy and provide confidentiality ThingsChain stores all sensitive data in encrypted form.

Summary

ThingsChain is an attempt to create a next-generation blockchain based platform for IoT applications which solves the current problems of scalability, low transaction throughput, and interoperability. We have designed a multi-layer blockchain based protocol where different layers can communicate with each other as needed. Different layers handle transactions for which they are designed and only the most important transactions are updated on the main chain. We also use advanced security protocols to ensure that the IoT data is securely stored on the blockchain. Our vision is to enable a future where IoT devices can interact with each other in an interoperable and trustless manner without any concerns about the security of the data stored.


THINGSCHAIN
step out line - step in chain
www.thingschain.network