InfiniteChain

Technical White Paper 2017/9/17

A blockchain implementation that has no transaction speed limit, protects privacy, and supports multi-chain operations

TIDETIME SUN LIMITED

Table of contents

InfiniteChain

Technical White Paper 2017/9/17

InfiniteChain

A diversified industry application that overcomes restrictions in blockchain processing and realizes truly decentralized transactions

Ever since Bitcoin implemented a cryptocurrency with decentralized controls in 2009, people have been waiting eagerly for the transformation of social values that decentralization might bring. The industry has been in a rush to explore how the blockchain technology that Bitcoin is based on might be used to realize even greater business efficiency.

InfiniteChain proposes an all-new type of distributed auditing as well as a method for multi-chain operation that overcomes bottlenecks encountered thus far by blockchain technology and its implementation in commercial applications. Its advantages include:

- No transaction speed limit: The main and sidechains can operate together to achieve over 15 million transactions per second (TPS)
- Protection of transaction privacy: The privacies of both the consumer and the provider of digital assets are assured during the transaction process
- Fusion with existing centralized commercial scenarios: Integration of agent mode while maintaining the parity of decentralized data

Finally, this white paper gives examples of potential value and business opportunities from the use of blockchain in financial, legal, medical, and supply chain scenarios. For share trading and asset transactions, the multi-chain structure of InfiniteChain can not only realize even faster transactions but also superior privacy protection, thus truly offering a transaction ecosystem with mutual trust.

1. Introduction

This white paper begins by introducing the problems and bottlenecks currently facing blockchains before explaining the origin, planning, structure, and ecology of the InfiniteChain (IFC) next-generation blockchain structure. As the name suggests, IFC is a decentralized system structure with no limits on speed and number: A multi-chain model where a main chain and multiple sidechains are running concurrently is used to solve the problems of inadequate transaction bandwidth, excessive data volumes, and the lack of privacy protection in conventional blockchains. IFC creates a completely new and fully-featured blockchain structure that can be trusted.

1.1. Background

Bitcoin is a cryptocurrency with decentralized controls that was created in 2009. The blockchain technology it is based on is now widely accepted and used in many industries. Apart from becoming an internationally recognized currency, people are now hoping that this shared value system will enable the development of decentralized applications (Dapp) in each industry based on blockchain technology.

In addition to its use in cryptocurrency transactions, the advantages of blockchains have been noted by various fields, advantages such as decentralized information verification and resistance to tampering. Key applications include value registry[1], value web[2], and value ecosystem[3]. Industries with related applications include logistics, financial systems, medical records, the collection and verification of data in the Internet of Things (IoT), supply chain management, stocks or options trading, social networking software, electronic patient records, micropayment/mobile payment systems, asset transactions, and distribution of digital products. People are hoping that blockchains will be able to play the role of a trusted machine in the operation of such systems. Keeping a detailed record of related information and solving information asymmetry problems will enable a trusted record to be established. In the use scenarios mentioned above, large amounts of information will need to be recorded on the blockchain.

Nevertheless, blockchain technology has encountered bottlenecks in the course of its development. If these cannot be overcome, it will be difficult for the blockchain to be fully implemented in the different application scenarios mentioned above. Each of these problems will be explained below.

[1] Application of distributed ledger to Proof of Existence and Possession (PoEaP).
[2] Value registry, smart contract, domestic payment, international payment, trade finance and capital market.
[3] Applications for non-financial services such as public ledgers where it can provide many kinds of commercial applications.

1.2. Problem 1: Insufficient blockchain bandwidth

Blockchain's decentralized operation is dependent on Internet users worldwide for its maintenance and use. Any user can therefore use block transactions to exchange cryptocurrency, write smart contracts, or record information. Bitcoin and Ethereum are, however, limited to no more than 7 and 25 TPS[4], respectively. If no technology available can place large numbers of transactions on the blockchain, it will simply not be practical to solve information asymmetry by storing transactions on blockchains.

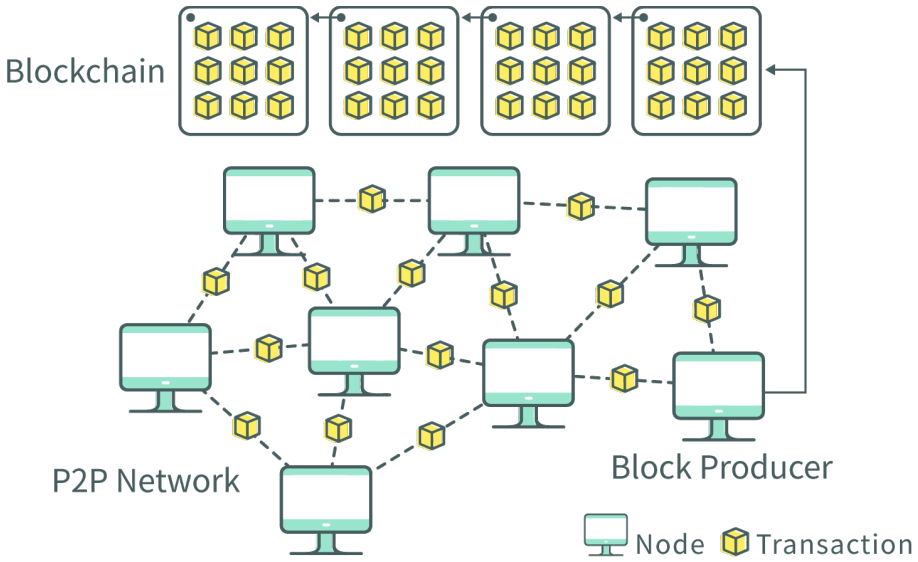

Figure 1. Public Blockchain Consensus Algorithm

As shown in Figure 1, the decentralized operation of the blockchain basically uses a consensus protocol such as Proof of Work (PoW) or Proof of Stake (PoS) to obtain or select a Block Producer[5] from participating nodes. The Block Producer then collects transactions through a Peer-to-Peer (P2P[6]) network and records these transactions in a single block within the blockchain using electronic signatures and a hash function[7]. All nodes in the public blockchain participating in the consensus protocol must continuously update any changes to the data in the blockchain as well as obtain transactions that ordinary users want to place on the blockchain. Large amounts of information must therefore be exchanged[8] over P2P networks, thus making it impossible to increase transaction bandwidth. Public blockchains are generally considered to have global consensus[9]. A detailed explanation is given in Appendix A.

---

[4] Yo Banjo, "Ethereum won't scale like you've been told," https://medium.com/@yobanjo/ethereum-wont-scale-like-you-ve-been-told-cae445bef539.

[5] It is also referred to as a “Miner.”

[6] A Peer-to-Peer (P2P) network is an Internet networking system with no central servers, and depends on the exchange of information between peers. It reduces the number of unnecessary nodes in network transmissions and thereby lowers the risk of data loss. Unlike centralized networks with a central server, in a P2P network every peer is a node that also functions as a server. One single node cannot find another node directly; instead, all data must be exchanged through peers.

[7] The hash function is a method for generating a small digital “fingerprint” for any data type. A hash function compresses the message or information, reducing its size and fixing its format. The information is completely re-combined by the function to create a new fingerprint called a "hash value."

[8] Propagating.

[9] Bitcoin and Ethereum have between 8,000 – 10,000 participating nodes at any given time, many of which are also mining pool nodes with massive processing power.

A “private blockchain” or “consortium blockchain[10]” are methods that attempts to solve the problem of insufficient transaction bandwidth. The number of participating blockchain nodes is limited to facilitate rapid propagation and the use of special consensus protocols (e.g., all types of PoS, BFT, and PoA[11]), which contribute to speeding up the selection of block producers. There is obviously a big credibility gap between private blockchains and public blockchains. The core philosophy of a decentralized system is to reduce the access threshold and remove restrictions on participating nodes so that no monopoly on trust machines can be formed. In a private chain, the smaller number of nodes increases vulnerability to 51% attacks[12] and prevents global consensus.

1.3. Problem 2: Insufficient blockchain payload space

As described in the previous section, in each type of system the public blockchain plays the role of the trust machine. As large amounts of transaction records are pushed onto the blockchain, the amount of data on the blockchain will rapidly increase within a short amount of time. Depending on the consensus model, full nodes of the blockchain must store every block on the blockchain and the transactions they contain. The consensus protocol of Bitcoin, for example, restricts the growth in blockchain capacity to around 70 GB[13] per year. In the absence of such restrictions, the propagation and storage of blocks becomes a major problem. This situation is also known as “blockchain bloat[14].” VISA reported that it generated a total of 92.064 million payment transactions in 2015. If translated into the data structure used for Bitcoin transactions, it would amount to around 2,900 transactions per second and 47TB of storage space. This already far exceeds the hard drive space on an ordinary computer[15].

1.4. Problem 3: Lack of Privacy Protection

At the moment, privacy protection in blockchains consists mainly of using a mechanism similar to money-laundering to conceal information about cryptocurrency transactions. There are two main methods: (1) Cryptography accumulator: Used by Zerocoin; (2) CoinJoin: Used by SharedCoins, Dark Wallet, CoinShuffle, the PrivateSend feature of Dash, and JoinMarket. Cryptocurrency transaction information recorded on the blockchain gives no indication of the sender.

The two methods above can only be used for cryptocurrency transactions and so cannot be used for other general transactions or contracts. The popularity of Ethereum’s smart contract is due to its ability to handle general transactions or contracts, not just cryptocurrency transactions. These include asset transactions and patent licensing as well as contract, document, and information records. Smart contracts for non-cryptocurrency transactions cannot make use of cryptocurrency's privacy protection technology, thus limiting the system’s scope of application.

---

[10] Examples includes the Coco architecture proposed by Microsoft and Intel and the hyperledger.

[11] In PoS, representatives are usually chosen to compete for block producer status; since in all types of BFT point to point communication between all nodes is required, it can only have between 20 - 30 nodes; in PoA (Proof of Authority), authority nodes designated in advance are responsible for producing blocks.

[12] A 51% Attack is where control over more than 51% of the nodes gives the controllers the ability to modify blocks or control their production.

[13] Around 300,000 transactions a day with each transaction taking up 700 Bytes. The amount of memory added per year would be 300,000*365*700 Bytes ≒ 70GB.

[14] Some experts warn that Ethereum will soon be hit by this problem（https://read01.com/zh-tw/aKE6A7.html#.WcBzIdv3U0o）。

[15] https://www.zhihu.com/question/39067000.

1.5. Problem 4: Limited application scenarios

The decentralization concept has gained acceptance in some circles. The forging and trading of cryptocurrencies, for example, can now be completely implemented using a decentralized model. Nevertheless, human economic activities are influenced by law, habit, legacy systems, and interpersonal relationships. Dispensing completely with centralized operations is impossible. Industries with related applications, as mentioned in Section 1.1, such as: logistics, financial systems, medical records, the collection and verification of data in the Internet of Things (IoT), supply chain management, share or rights transactions, social networking software, electronic patient records, micropayment/mobile payment systems, asset transactions, and distribution of digital products—nearly all of these applications still require a centralized agent or intermediary. If the public blockchain cannot be integrated with industries that have similar centralized operations, the use of the blockchain as the trust machine will be greatly limited.

The following example uses digital product distribution to explain why that is the case. For digital products such as e-books, music, movie rentals, and electronic tickets, the widespread use of the Internet and larger bandwidth has popularized sales over online platforms. To expand their sales channels, the rights-holder will usually commission agents to make sales over the agent's network platform. The agent collects payments from users and maintains a record of accounts. The accounts are then provided to the rights-holder at fixed intervals with details on downloads and corresponding royalties. However, since the accounts are recorded and maintained by the agent, the rights-holder is unable to verify their authenticity. For example, the agent's records may contain accidental omissions or other errors due to bugs in the system. Or the agent may deliberately forge or modify the records to reduce the amount of royalties payable to the rights-holder.

In other words, even if the agent placed the account ledgers on the blockchain, the rights-holder would still be unable to verify their authenticity. In scenarios like that above, the blockchain is unable to play the role of the trust machine. It has been suggested that all related transactions should be conducted through cryptocurrency. This method, however, encounters too many limitations: First, such purchases are often micropayments, but with blockchain's overly high transaction costs, there is not enough transaction bandwidth to handle large volumes of micropayments; second, consumers usually pay by ordinary currency or credit card; third, no space is available for some records that are not related to currency transactions. If there is a way to overcome this limitation while also achieving "information symmetry," the goal of decentralization, it will greatly increase the versatility of the blockchain.

1.6. Summary of Problems

Based on the explanations above, we can now give a summary of the current problems to be solved:

Problem P1 :

Blockchain transaction speeds are too slow. How can it handle a large number of transactions in a short period of time?

Problem P2 :

How can blockchain bloat be avoided when storing large numbers of transaction records on the blockchain?

Problem P3：

How can the privacy of involved parties be protected when records for transactions other than cryptocurrencies are written to the blockchain?

Problem P4：

In the real world, the division of labor in the commercial environment means that intermediaries (or agents) cannot be easily replaced. They may also form a wall between digital asset publishers and consumers. So how can intermediaries be retained while providing transparent, reliable, and verifiable consumption records?

These four problems are tightly interrelated. For example, if **Problem P1** is solved and blockchain's transaction bandwidth is greatly expanded, then **Problem P2** seems inevitable. Large numbers of transaction records on the blockchain will lead to excessive data storage. If **Problem P3** is solved, the privacy of the transaction parties will be protected and third parties will not be able to obtain the transaction details. But then **Problem P4**, that it, dishonest agents, may become even worse. The IFC multi-chain architecture proposed in this white paper will completely solve these problems. Please refer to Section 2.

2. Explanation of IFC Technology

In this section, we will first explain the workings of the IFC multi-chain blockchain, then look at how it solves **Problems P1** - **P4** from Section1.6.

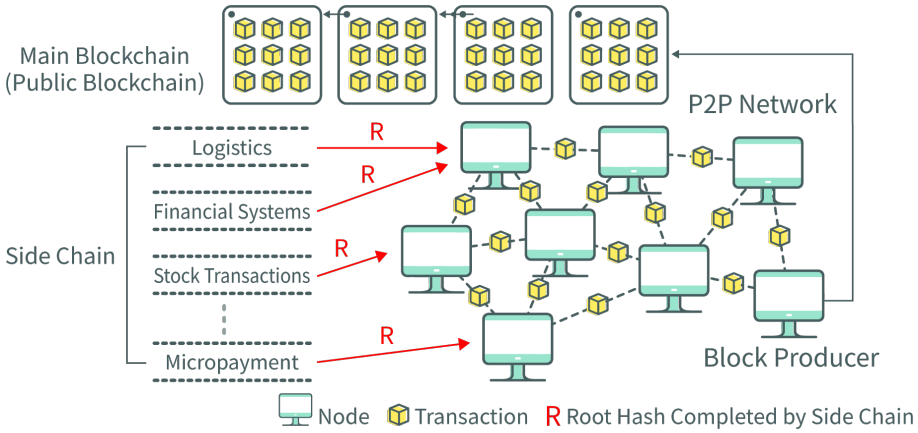

Figure 2. The Multiple-Chain Architecture of InfiniteChain

2.1.IFC Multi-chain Blockchain Architecture

The architecture of the IFC multi-chain blockchain is shown in Figure 2. A multi-chain is a joint operating model consisting of the main blockchain and several sidechains. Generally speaking, transactions such as cryptocurrency transactions or individual contract records that do not need to be processed quickly are sent directly into the P2P network and finally linked to the main chain by nodes that have become block producers.

High-volume transactions, or those that require centralized matchmaking, however, are first processed on a sidechain. A hash value is then generated for the transactions, which is then sent to a node in the P2P network and linked to the main chain. The sidechain runs at a high speed and accumulates a large number of transactions after a certain amount of time. A hash value and corresponding identification code is then generated by the auditing node responsible for the decentralized operation of the sidechain and then sent to to the main chain. The entire IFC multi-chain blockchain architecture is made up of “ordinary nodes” (referred to as nodes) and “audit ing nodes.” These are responsible for the decentralized operation of the main chain and sidechains.

There are several techniques for running transactions outside of the main chain before adding them to the main chain. After explaining each of these techniques, we will look at how IFC sidechains are different. The first type is “relay-based.” Assets are transferred between the main chain and sidechain before the transaction is conducted on the sidechain[16、17]. The assets are transferred back to the main chain after a certain time. This reduces the number of transactions that take place on the main blockchain. Implementations of this system include BTC-Relay and Rootstock. The problem is

[16] A SIMPLE EXPLANATION OF BITCOIN “SIDECHAINS” https://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/

[17] How Two New Sidechains Proposals Could Change Bitcoin's DNA https://www.coindesk.com/two-new-sidechains-proposals-change-bitcoins-dna/

how to implement a 2-way peg protocol. For example, the blockchain of Bitcoin is impossible to establish such a relayer.

Another type is “channel-based” and usually referred to as “off-chain.” Lightning-network and Raiden, for example, use off-chain transactions to increase their TPS. In this method there is no need to use nodes to obtain consensus about transactions produced in sidechains. A payment channel is created in advance on the main chain and all the participants to the transactions made over this channel exchange electronically signed information outside of the main chain to indicate that transactions have taken place. A summary of these transactions are then written back to the main chain. Both of the above methods only offer a solution for high-frequency transfer of cryptocurrency or tokens and cannot be applied directly to contract records and other non-cryptocurrency transactions. In addition, these off-chain transactions cannot be audited. Only related participants can have these off-chain data.

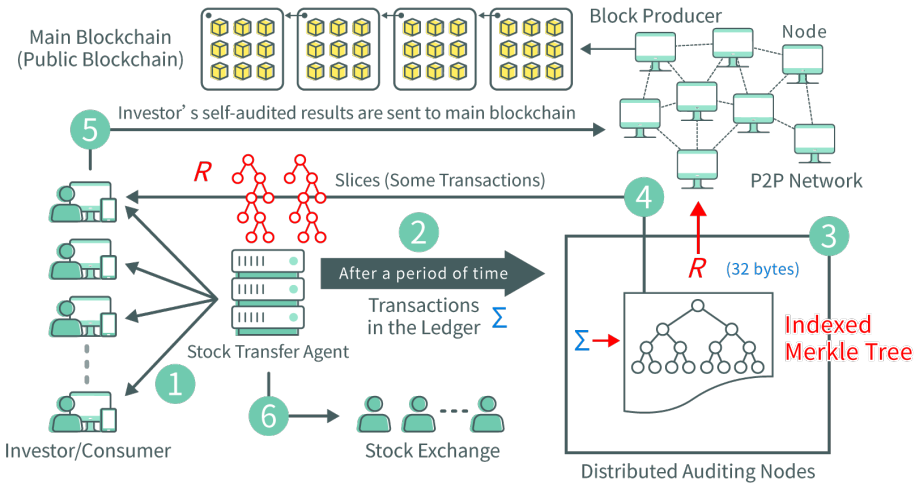

Figure 3. How InfiniteChain’s side chain operates

IFC sidechains are “hierachy-based”, which are adopted by Plasma and PokaDot. The consensus of transactions is obtained by the higher level main chain and the validity of transactions are obtained by any kinds of data structures in the lower level side chains. There are no restrictions on the number of sidechains, so it is very suitable for connecting real-world scenarios to blockchains. IFC's features include increased bandwidth, overcoming information bloating, and providing privacy protection, while also solving the problem of integrating existing application systems with decentralized systems.

In the multi-chain operation of the IFC, the main chain is a public blockchain so that it can obtain global consensus. The sidechain operation of the IFC incorporates our company’s own patented “Distributed Auditing Function[18].” It provides an effective scheme to valid the operating of agents which manifest the transactions in sidechains. The multi-chain blockchain of the IFC can therefore solve all of the problems outlined in Section 1.6.

The maintenance and operation of the main chain is the same as the operation and management of ordinary public blockchains. Sidechain operations are initiated by industry applications (e.g., transaction agent platforms, professional brokers, investment banks, securities companies, auditors,

[18] Invention name: Distributed Auditing Method, Device and System. This is an international patent owned by the IFC research team.

appraisers, lawyers, toolkit developers). For market and business development, different sidechains are managed and operated for individual business types. Sidechains must regularly synchronize their information with the main chain to avoid the counterfeiting or tampering of data. The main chain can operate in parallel with multiple sidechains to achieve transaction speeds in excess of 15 million TPS (Transactions per Second).

The operation of a single sidechain is shown in Figure 3. The operation of a single sidechain is shown in the following steps:

Step (1) : The agent responsible for initiating the sidechain operation starts by conducting a series of transactions with participants (or consumers).

Step (2) : After a certain period of time, the agent sends transactions ∑ from Step (1), the distributed auditing fee, and the bond Token $[19] to the auditing node. Token $ is the cryptocurrency transmitted via the main chain.

Step (3) : The audit node uses transactions ∑ to generate an Indexed Merkle Tree (MT). MT is also used to generate a root hash value R[20]. R and the corresponding identification tag are sent to the main chain for storing. All participants can use the identification tag from the main chain to obtain R.

Step (4) : Participants are responsible for auditing their own transactions to see if they were correctly placed in the MT :

- The given root hash value R is used to ask the auditing node to return slices[21] of the participant's own transactions, with each slice representing one such transaction. Since R is anchored to the main chain, an audit[22] of the slice that does not turn up a particular transaction is electronic evidence that the agent did not put their own transaction in the MT.

Step (5) : Participants send their own audit results to a node within the P2P network:

- Audit passed: The audit results which have been electronically signed by the participant are packaged and compressed by the block producer before being placed on the main chain. This process takes up only a small amount of the main chain's transaction bandwidth.
- Audit failed: If the participant's audit finds that the agent provided missing or incorrect data, the associated information is signed and then sent to a node for arbitration by block producers. If arbitration finds that the agent made an error, then the participant receives a share of the bond.

Step (6) : The agent pays royalties to the rights-holder. A rights-holder can use R and MT to verify that a royalty payment is free from error.

---

[19] The bond can also be stored in main chain.

[20] Bottom-up recursive hashing of the MT leaf nodes all the way up to root node gives a root hash 32 bytes in length. Addition of the agent's electronic signature (128 bytes) brings the total length to just 160 bytes.

[21] A slice is a small part of the MT. An MT ledger that holds 500,000 transactions takes up at least 300 MB. If other tags are added, then several GB of storage may be needed. A slice contains just 1/100,000th of a full ledger's data. It can be used to audit an MT ledger to see if it contains a transaction located within the slice node.

[22] Each transaction can be audited within 1 ms.

The integrity of transactions generated by sidechain operations are maintained by all participants. A bond is deposited in advance on the main chain by the agent. Participants and agents both electronically sign their transaction information to realize mutual non-repudiation. In Step (4), multiple participants are involved in auditing the existence and integrity of transactions on this sidechain. Any omissions or errors found in an agent's transactions are arbitrated by nodes on the main chain. If arbitration is passed then the bond is automatically shared among the participants who issued the arbitration; if not, it is refunded to the agent. This boosts the incentive for participants to take part in the audit.

2.2.Why IFC is Far Faster than Conventional Blockchains

An IFC system will contain many sidechains. Transactions are conducted in different sidechains. A single transaction agent is usually responsible for all transactions from a matchmaking service[23]. Transactions processed by a sidechain agent do not need to be immediately placed on the blockchain. The hash value for a ledger containing N transactions is eventually placed on the blockchain, the equivalent of placing N transactions on the blockchain all at once. In practice, placing the hash value of a transaction ledger on the blockchain only takes up the bandwidth of a single transaction. In this manner, the transaction bandwidth of the blockchain can therefore be expanded almost indefinitely. The number of transactions per second is no longer constrained by the limitations of the blockchain. Not having a speed limit means that fast speeds can be attained.

Our company's implementation of the system allows a million transactions to be easily placed on one ledger and distributed audits for individual transactions to be completed within one millisecond[24]. And distributed auditing can be carried out completely in parallel. Since public blockchains can currently handle dozens of transactions per second, the speed of a blockchain can now be easily increased to tens of millions of transactions per second. As shown in the following formula

> Transactions per second = (Average number of blocks generated per second) × (Average number of transactions per block) × (Average number of transactions per IFC ledger)

If we set the IFC main chain's transactions per second to 10, then the entire blockchain's transactions per second $=10\times1{,}000{,}000=10{,}000{,}000$ TPS. 10 million TPS can therefore be achieved with ease. This technique elevates the practicality of the blockchain to a whole new level. This means that Section 1.6's **Problem P1** has now been solved.

2.3.Does IFC Suffer From Blockchain Bloat?

IFC's approach is to let the agent conduct transactions. We refer to this as a sidechain operation. After a certain amount of time, the root hash of this sidechain is placed on the main chain. Since the transaction ledger formed by the sidechain does not need to be stored on the main chain, Section 1.6's **Problem P2** namely information bloat, doesn't exist in the main chain. Nor does it fix **Problem P1** while creating **Problem P2**. The details of all sidechain transactions are in the safekeeping of the

[23] This can be applied to the e-book sales, music sales, video rentals, electronic ticket sales and currency transactions.

[24] See Table II in the paper "Efficient Real-time Auditing and Proof of Violation for Cloud Storage Systems. Gwan-Hwan Hwang and Hung-Fu Chen. Published in the 9th IEEE International Conference on Cloud Computing (IEEE Cloud 2016), June 27 - July 2, 2016, San Francisco, USA." Title of patent based on this paper: "Method for Auditing Cloud Access in Real Time." This is an international patent owned by the IFC research team.

responsible agent. Since its root hash and identification tag have already been placed on the main chain, they cannot be altered by the agent.

2.4.How the IFC Protects the Confidentiality of Transactions

During sidechain operations, all transactions are stored securely in the MT. Transaction details are also encrypted with the public keys of the participant and digital asset provider. Only the participant and digital asset provider can use their private keys to validate their own transactions. The privacies of the participant and digital asset provider are therefore protected. We have developed several privacy protection models to complement our distributed auditing technology. Please refer to Appendix B for more information.

2.5.How IFC Integrates with the Agent's Operating Model

The main problem facing a decentralized system that involves agent operations is ensuring that the transaction records placed by the agent on the blockchain are correct. The IFC's patented distributed auditing technology can solve this problem. Since the agent's sidechain operations are still audited in a distributed manner, the system remains true to the concept of decentralization. Several systems for letting agents process some transactions in advance before recording them on the blockchain were proposed when Bitcoin was still in the early stages of development. None of these systems were able to solve the problem of black-box operation by the agent, however. Since this ran counter to the blockchain philosophy of decentralization, those systems failed to gain widespread acceptance. The distributed auditing technology of the IFC solves this problem once and for all.

During sidechain operations, all transactions are securely stored in the MT and only their hash values are published. Participants and digital asset providers can use the indexing function to immediately pinpoint the leaf node for a particular transaction in the MT. When a participant wishes to audit their own transaction and see if it was correctly stored in the transaction ledger, the participant can submit a transaction audit request to the agent. As the participant already has the transaction serial number (the completed transaction is electronically signed by the agent and so cannot be repudiated by the agent), the agent must then present the slice for this transaction. The consumer can then use the root hash of this ledger and the slice for this transaction to verify the integrity of the transaction and whether it exists in this transaction ledger.

The integration of distributed auditing with sidechain operations with the overall blockchain ecosystem means that block producers are not only granted the power of arbitration but are also rewarded in cryptocurrency for block production and contribution. Consumers from the sidechain can also be rewarded with currency by the system for audit participation.

2.6.How the IFC Builds Off-chain Ledgers

The current trend is to exploit the immutability of blockchain-based distributed ledgers for Proof of Existence and Possession (PoEaP) applications and provide public ledgers for all kinds of commercial applications. A sample scenario is the placing of academic credentials in a blockchain. Such applications often need to place large amounts of data or large ledgers onto the blockchain in one batch. For example, a single university has tens of thousands of graduates in one particular year. At the end of the academic term, the university must place the degrees of all graduates onto the

blockchain all at once or within a short amount of time. Since a public blockchain has a limited transaction bandwidth, it would be impractical to place each and every graduate's degree onto the blockchain as a separate transaction. All degrees must first be packaged and compressed before storage. The usual method is to use a Merkle tree to compress the data and generate a root hash. The root hash is then stored on the blockchain. This can be considered an off-chain ledger: While most of the ledger's details are not located on the blockchain itself, the root hash can be used to verify whether the information being queried is located within the Merkle tree ledger. The complete MT is usually retained by the agent and presented only when information needs to be verified.

If the MT contains a huge amount of data, however, it can take a long time to download and search. Special techniques are therefore necessary to reduce the amount of data to be downloaded and speed up searching. The IFC team's patented technology[25] can meet this need: When one million records are placed in an off-chain ledger, the hash value can be used to verify any record in one millisecond. No more than 1KB of data needs to be downloaded. Standard SQL database query commands such as range selection operations are also supported.

2.7.Management Model of Main and Sidechains

For obtaining global consensus, the operation of main and sidechains in IFC should comply with the operating logic of a public blockchain. Our goal is to have the main chain be able to control the operating of sidechains. A management system should be established on a public blockchain. It should be able to initialize sidechains and set and change permissions for an agent to create, terminate, or control the operation of a sidechain. Besides, participant should be able to check the relationship between main and sidechains on the blockchain.

As for the access control or governance issues in private and consortium blockchains, they are usually implemented by binding different roles and permissions to nodes. However, it violates the basic idea of a public blockchain which is a decentralized autonomous organization for obtaining global consensus. In IFC, the management regulation of main and sidechains are enacted by announcing contacts[26] on a pubic blockchain. Note that contacts are stored on the blockchain and executed by nodes. Different applications have different regulations. Paticipants of an application obtain its associated contacts in main chain so that they can follow the announced regulation to perform related operations of the application.

The application manager announces some contacts which form a "contact network" which is consisted of a main contact and some subcontacts linked by addresses of contacts. Refer to Figure 4. The main contact with an unique entry address[27] which is the entry point of the application and actually the reference point of the associated contacts for the application on the blockchain. The address is immutable as it is published on the blockchain. Participants, agents, and managers recognize this unique address to know the operating protocol of an application.

Figure 4 demonstrates an example of an IFC contact network. The main contact (A) announces the protocol and operating status of the application. A subcontract could be used to (1) publish or define some administrative matters such as the permission and public key of participants and agents;

---

[25] See Table II in the paper "Efficient Real-time Auditing and Proof of Violation for Cloud Storage Systems. Gwan-Hwan Hwang and Hung-Fu Chen. Published in the 9th IEEE International Conference on Cloud Computing (IEEE Cloud 2016), June 27 - July 2, 2016, San Francisco, USA." Title of patent based on this paper: "Method for Auditing Cloud Access in Real Time." This is an international patent owned by the IFC research team.

[26] Such as the smart contact of Ethereum.

[27] The address of a contact in a blockchain.

(2) the history and current status of a sidechain; or (3) announce a ledger with a large amount of records. For example, R_x in subcontract (C) announces the root hash of a ledger which is off-chain. It surely can support the off-chain data certification as we mention in Section 2.6. Subcontact (B) is associated to a sidechain. Its definition and description contains related information such as ID and public key of its agent, URL address of the agent, type of the side chain, ID of the active sidechain. R1, R2, and R3 are previously recorded root hashes of this sidechain. Subcontact (D) is associated to another sidechain.

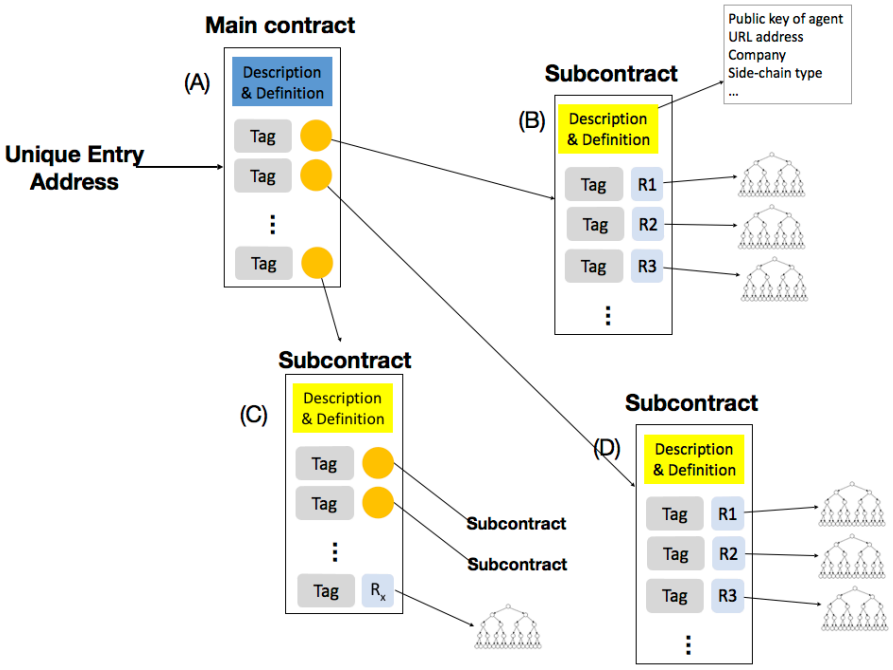

Figure 4 The contact network of IFC

The table below is an overall comparison between IFC and other public/private chains.

	Public blockchain		Private or consortium blockchain	InfiniteChain
	Bitcoin	Ethereum	POS, PBFT, or POA consensus	Public blockchain, Hierachy-based sidechains, distributed auditing
Node count	No limit Currently 8K~10K	No limit Currently 8K~10K	Limited	No limit
Has reach a global consensus	Yes	Yes	No	Yes (Main chain)
51% attack	Virtually impossible	Virtually impossible	Easy	Virtually impossible
TPS	≒7	≒25	1,000~2,000	>10,000,000
Blockchain bloat	None	Yes	Severe	None
Privacy protection	Limited	Limited	Limited	Complete
Integration with centralised scenarios	None	None	None	Yes
Fast off0chain ledger audit	None	None	None	Yes

3. IFC Application Scenarios

The popularity of the blockchain has led to widespread discussion in each industry on the potential value of its applications. The financial field is seeing ongoing developments in transactions and payment, while people in the social field are looking at using blockchains to record activities and build up their reputation; people in the medical field are looking at the advantages of using the blockchain for storing electronic patient records; and in the legal field, blockchain has huge potential in validation, auditing, and smart contract applications.

If implemented on existing trusted public blockchains, the following application scenarios will encounter **Problems P1**, **P2**, **P3**, and **P4** as mentioned in Section 1.6.

Share and rights transactions

In the share trading scenario, the need for buyers and sellers to track the transaction of share rights means that transactions will take longer. Companies must expend a great deal of resources on attorneys, auditors, and consultants to review the transactions among investors. With the blockchain acting as the trust mechanism, middlemen such as auditors can be taken out of share transactions. If transactions are linked to the blockchain, buyers can spend less time tracking share rights. However, the massive volume of share transactions is simply too large a load for the transaction bandwidth of current blockchains. IFC not only offers fast transaction speeds but also emphasizes privacy. Every participant to a transaction can only see the records relevant to them. Benefits include speed and confidentiality. A practical system can be implemented using the IFC multi-chain architecture.

Asset transactions

All assets can be digitized. Once an asset has been digitized, it can be quantified, circulated, bought and sold, and mortgaged to generate huge value. In the future, houses and cars may all become assets on a blockchain. Ownership will be decided using private keys, making the moment of all real estate far easier. The biggest advantage of applying the blockchain to digital assets is that circulation becomes far easier once assets are published to the blockchain.

The IFC offers many methods for converting digital assets; it also supports transaction applications. During a transaction, all participants receive suitable privacy protection. Non-reputability of the transaction is also guaranteed, allowing participants to trust and rely on one other.

Bank supervision/legal compliance

Banks can use the trust machines of public blockchains to satisfy requirements for internal controls and legal compliance. For example, each transaction or business activity made by a bank employee can be recorded immediately. The transaction serial number and the bank's electronic signature prevent the transaction from being repudiated by the bank. Once all records have been consolidated they are placed on the blockchain. The data is transparent and cannot be tampered with, making post auditing unnecessary.

In comparison, existing internal controls and legal compliance depend on third-party audits. In addition, preliminary internal training, laws and regulations, as well as post audits/verification are

required. With the IFC and distributed auditing technology, a bank and its employees' business records are completely transparent. Bank employees can audit the accuracy of their own activity records or of a particular action raised by the bank. The forging of records is also impossible in this use scenario.

Micropayment/Mobile payment

In 2016 the scale of third-party mobile payments in China more than doubled, reaching 38 trillion RMB (equivalent to 5.5 trillion USD[28]). Data from Forrester Research showed that mobile payments in the US grew by 39% over the year, reaching 112 billion USD.

People are increasingly using micropayments for trivial everyday transactions, such as buying coffee and paying utility bills. The IFC's ability to store large numbers of records will allow more and broader micropayments to be recorded to the blockchain. The distributed auditing function of the IFC can also be used to protect the privacy of individual consumer transactions. The IFC platform can be used for more than recording cryptocurrency transactions. Conventional credit cards, wire transfers, checks, or other cryptocurrencies can be recorded on the IFC platform, allowing for easy integration with these existing systems.

Traceability in organic agriculture

The blockchain can be used to record the entire production history of organic agricultural products. At each stage, from the farmer, producer, purchaser, government inspection, and logistics/transportation, all the way to the sales channels, once each production record has been generated and verified it can be linked to the blockchain. Consumers as well as any member or node in the organization will be able to trace each record entry and use the trust machine to confirm that the production history has not been tampered with and thus can be trusted. This will effectively enhance the credibility of organic agricultural products. Distributed auditing technology can be used to guarantee the integrity of the recorded data.

Supply chain management

In the supply chain management field, upstream/downstream vendors, suppliers and manufacturers need to communicate with each other. They also need to use supply chain management to reduce business expenses. Supply chain management encompasses the flow of materials (products), flow of information, and the flow of money. The complexity and diversity of interests involved in global supply chains present a challenge that the IFC is well-equipped to handle.

In material flow management for maritime freight, for example, the top 30 container ports in the world processed 370 million TEU (20-foot standard containers[29]) in 2016. If each individual container must be tracked, the number of transactions and hardware payload space will be far more than the ordinary public blockchain can handle. One additional consideration is that business must keep their secrets out off competitors' hands, so not all information can be recorded on the blockchain. Here the IFC's advantages not only include product history tracking in the event of any production problems,

[28] https://www.read321.com/182130.html

[29] TOP 30 container ports in 2016. http://www.ship.sh/news_detail.php?nid=24840 。

but also built-in privacy protection, which prevents the disclosure of business information (including quotes for materials).

Social networks

Social media is now an indispensable part of everyday life. LINE, for example, has more than 1 billion subscribers worldwide and around 215 million active users each month. As of 2016, 1.5 trillion messages, 40 billion voice calls, and 14.6 billion dynamic messages have been sent or received over LINE. A large amount of data is generated daily on social networks by users.

The IFC can preserve a complete record of all social networking activity made by users. All texts, images, videos, and events will be recorded, making it difficult to use social networks for illegitimate purposes.

The decentralized nature of the IFC means that users can track and protect their own content without worrying about important and confidential data being illegally compromised. Privacy and trust is emphasized by the IFC.

Electronic patient records

In the past, patient records were controlled by each medical facility and not by the patients themselves. Patients were often unable to review or keep a detailed record of their own treatments and medical history. Such an arrangement often led to difficulties between patients and medical practitioners, because patients simply were not able to give their doctors a complete medical history.

Using the IFC, we can use the recorded data and content to generate a digital identity of the patient. The change history of the patient record can also be included to prevent forgery and illegal tampering of the records. The integrity of the data can be guaranteed from the moment the data is created to the time it is actually used, free of human interference at any juncture. The patient record can only be deciphered by people who have such authorization, providing patients with more effective and secure protection of their privacy.

Blockchain finance

VISA, for example, generates on average 2800 transactions per second worldwide (with up to 58,000 TPS). If VISA's transaction system is to be combined with the blockchain trust mechanism, linking the massive volume of transactions generated by VISA to a conventional blockchain in a short amount of time will be extremely difficult. If the IFC structure is used, we can use sidechains to record the tens of thousands of transactions generated every second and carry out distributed audits, which solves the transaction bandwidth problem. The IFC provides fast transaction services with distributed audits that ensure the integrity of transactions. This will be fundamental to application of blockchain to finance.

Social governance

In the past, personal identification, notarization, legal arbitration, voting, and credit systems all used centralized services for reading and writing data, and thus were vulnerable to forgery. The blockchain offers a very good way of solving such problems. The blockchain is public, transparent,

immutable, as well as being low-cost. So it is easy to predict that blockchain technology will be used in the future to prevent forgery in notarization applications.

The IFC compensates for the blockchain's weaknesses in privacy and speed, so large amounts of data can be processed simultaneously. When applied to electronic voting, it can be used to verify identity while recording votes. It therefore retains the advantages of blockchain, while making up for its weaknesses.

4. IFC Development Status and Partnership Plan

The IFC team has already filed two international patent applications in several countries:

(1) Distributed Auditing Method, Device, and System.

(2) Method for Auditing Cloud Access in Real Time.

In terms of system implementation, programming and testing have been carried out for proof of concept. The team is currently in partnership talks with several companies.

XPLAY[30] is an entertainment video media platform that has already successfully completed its first round of initial coin offering (ICO). XPLAY uses blockchain to pay content providers royalties in the form of cryptocurrency based on the actual amount of video content downloaded by its users. Consumers make payments to XPLAY through micropayments. If each payment must immediately be sent as cryptocurrency to the content provider, there will be excessive transaction costs. In addition, the blockchain lacks the transaction bandwidth to support large volumes of micropayments. Here XPLAY plays the role of the agent. They use IFC's multi-chain model and distributed auditing to record consumers' micropayments to the blockchain with privacy protection, no matter the volume. Content providers can also effectively audit the ledger, making such a partnership more financially attractive. This system will soon go live and begin serving consumers.

An internationally renowned securities and futures exchange also plans to record the transaction records for all share rights, shares, and futures on the blockchain to reduce buyer tracking time as well as increase the accuracy and reliability of related queries. The massive volume of transactions is, however, more than the blockchain's transaction bandwidth can handle. The IFC's multi-chain model is not only able to record large numbers of transactions, but it also emphasizes privacy. Each participant to a transaction can only see the records related to them. Benefits include speed and confidentiality. A useful system can therefore be implemented.

[30] http://xplay.fund/

5. Conclusion

Decentralized application systems based on blockchain technologies are just now beginning to enter our everyday lives. Experts have pointed out, however, some bottlenecks in the basic technology. As noted in Section1.6, these are **Problem P1** (insufficient bandwidth), **Problem P2** (blockchain bloat), **Problem P3** (difficulty protecting privacy), and **Problem P4** (difficulty integrating with centralized scenarios). If any one of these problems remains unsolved, then the dream of blockchains becoming trust machines will be just that, a dream. The blockchain will be limited to a platform for mining and trading cryptocurrency, or will only be used in a limited number of application scenarios.

The IFC team is certain that the future lies with decentralized systems that overcome information asymmetry to allow users to be engaged in trusted activities. They have also proposed practical technologies to solve such problems indefinitely. All of the related technologies have been prototyped to assess their performance and feasibility. The IFC team's contributions will undoubtedly make an impression on future developments in decentralized application systems and blockchain.

Appendix A:Reasons for Non-Scalability of Public Blockchain Transaction Bandwidth

The transaction speed of a blockchain is generally expressed as the number of transactions that can be stored to the block per second (Transactions per Second, or TPS). This can also be referred to as the "transaction bandwidth." It is basically the average number of blocks generated by the blockchain per second multiplied by the average number of transactions encapsulated per block. The formula is:

Transactions per Second = (average number of blocks generated per second) × (average number of transactions per block)

Bitcoin uses PoW to randomly select block producers, so the average number of blocks generated per second on the blockchain is quite small. In practice, a block is on average generated only once every 10 minutes. Bitcoin's blockchain is therefore throttled to around 7 TPS. Most of the later blockchain developments trying to overcome this speed constraint adopted a PoS consensus protocol to determine block producers. Basically, a node that wants to become the next producer must compare its stake against other competitors. According to the PoS consensus protocol, the node with the highest stake becomes the next block producer. Unlike PoW, there is no need to compete on the level of computing power, and thus PoS is faster. As shown in Figure 1, a node that wants to become the next block producer receives disseminated transaction data from the P2P network. Once it is selected by the consensus protocol, a block is generated and disseminated to other nodes over the P2P network.

For the PoS consensus protocol to work, all competitors must know the stake of all other competitors. These competitors are scattered all around the world and communicate with each other through the network. Even if they know who the competitors are, they usually have to query the stake of other competitors from the previous blocks on the blockchain. It usually takes several seconds to determine who the next block producer will be. In other words, the average number of blocks produced per second on the blockchain is less than 1. The average number of transactions encapsulated per block is also limited by the node's network bandwidth and the data transmission speed of the P2Pnetwork.

In addition, the block producer must verify[31] all of the transactions to be encapsulated in the block , which also takes time. Once a block producer has been decided through PoS consensus, the producer is usually given a time limit for generating a block, usually this amounts to several seconds. Ethereum is currently limited to around 25 TPS. Experts have already voiced their doubts over Ethereum's push to have more than 100 Dapps running online at full speed. Their reasoning is that they think this will overload the Ethereum blockchain[32]. From this we can conclude that if all web users are allowed to participate in a "public blockchain," speed constraint will remain a problem, since all participating net users must exchange information via P2P. However, the large number of participants and the open nature of public chains means that it is the most trusted.

[31] To prevent double spending or illegal transactions.
[32] Yo Banjo, "How Etheroll and other Dapps will kill Ethereum," https://medium.com/@yobanjo/how-etheroll-and-other-dapps-will-kill-ethereum-e973d8e1c465.

Appendix B: IFC Sidechain Privacy Protection Technology

The privacy of digital asset providers is protected in two ways. The first is that all transactions stored in the Indexed Merkle Tree (MT) are encrypted using the public key of the digital asset provider. When the consumer audits one of his or her transactions, they can use the public key of the digital asset provider to encrypt the transaction data, and then compare the encrypted data against the data stored in the MT. When the digital asset provider wishes to conduct an audit, the entire MT ledger can be presented to the digital asset provider. But the digital asset provider can only see and audit data that can be decrypted with their private key, so the privacy of the other data is protected. This method offers a sound security mechanism, but each asymmetric decryption operation is time consuming (approximately 22 ms). The digital asset provider must attempt to decrypt each transaction stored in the MT; only those that can be decrypted are transactions related to that digital asset provider[33]. If the MT contains a large number of transactions this becomes very time-consuming. For example, if there are 100,000 transactions in the MT, the audit will take more than 150 seconds to complete[34]. If there are 1,000,000 transactions, it will take more than one hour. It may then be a bad idea for the digital asset provider to use a device with low processing power, like a mobile phone, to conduct audits. Please note that this is not a problem for the consumer, since the consumer only audits the small number of transactions related to them.

The other way is to generate an indexed Merkle tree for each digital asset provider (referred to as the Digital Asset Provider Indexed Merkle Tree, or SubMT for short). All of a digital asset provider's transactions are stored in the SubMT without encryption. The root hash of all SubMTs are then used to generate another MT (referred to as the Main Indexed Merkle Tree, or MainMT for short). The root hash of the MainMT is announced on the blockchain by the validator node. When consumers verify the integrity or existence of one of their transactions: (1) The validator node first presents a slice from the SubMT of relevant digital asset providers to the consumers for verification; (2) The consumer then verifies whether the root hash for this SubMT exists in the MainMT.

When the digital asset provider wishes to audit his own transactions[35], the validator node presents the SubMT of the digital asset provider and the MainMT. The digital asset provider then confirms that his or her SubMT appears in the MainMT and is not duplicated. Then, all the digital asset provider has to do is check all of the transactions in his or her SubMT. Since the SubMT contains only his or her own transactions, the transaction details of other digital asset providers will not be visible. Privacy is therefore protected. Auditing only your own transactions means that even devices with low processing power, such as mobile phones, can be used for auditing with no problem.

---

[33] Transactions that cannot be decrypted are those related to other digital asset providers.

[34] This processing time does not include the traversal time for MT.

[35] Open source program for announcement.