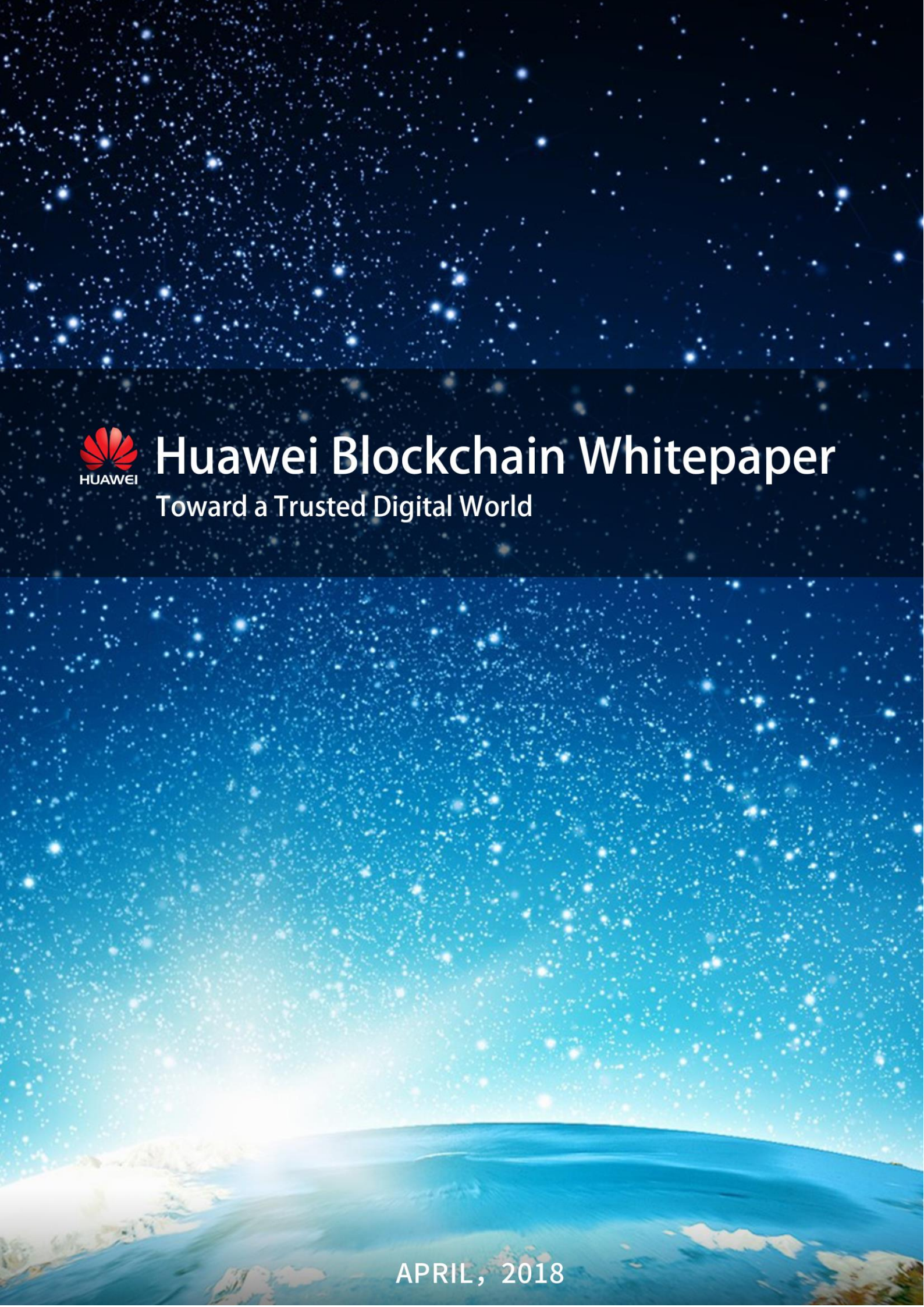

HUAWEI
Huawei Blockchain Whitepaper
Toward a Trusted Digital World
APRIL, 2018

Foreword

Blockchain has been a hotly discussed field for the past two years. At its core, blockchain is a method of distributed data storage enabling peer-to-peer transmission and consensus-building. It utilizes cryptographic protocols, consensus algorithms and a number of other technologies. These features help eliminate the possibility of fraudulent data flows that are common in traditional transaction systems, fostering a trusted environment both in transactions and in society more generally.

Preparations are now underway in a number of national governments, international organizations (such as the International Monetary Fund) and standard and open source organizations and industrial alliances to accelerate the application of blockchain. As a manifestation of the value of this new technology, countries are now devoting themselves to the global blockchain "arms race": China, for example, is now working on a nationwide blockchain development strategy. (For example, The National Development and Reform Commission (NDRC) has asked the China Academy of Information and Communications Technology (CAICT) to organize the blockchain discussion among industrial players, in order to decide upon an appropriate path forward for blockchain development. The Information and Software Service Division under the Ministry of Industry and Information Technology is also in the process of choosing an agency that will be responsible for the development of blockchain technologies in China). Having seen the rapid development of blockchain technologies and related industries in 2018, we are confident that China will be one of the first countries to truly make a trusted digital and economic society a reality, enabled by blockchain technologies. It is our belief that the industrial opportunities presented by blockchain will be significant.

Blockchain technologies have wider applications beyond the finance industry. Now, it can be applied to IoT, smart manufacturing, supply chain management, data storage, and transactions. This will bring new opportunities for next-generation information technologies such as cloud computing, big data, and carrier networks. The trusted environment created by blockchain will change the

current social and business model, and set off another round of technological innovation and industrial transformations.

Contributors

Advisors:

Zhang Wenlin, Gong Ti, Xiao Ran, Liao Zhenqin, Wan Hanyang, Chu Qing, Zhang Hui, Pan Qiuling, Qi Feng, Yi Zhiquan, Zhu Peiying, Liu Pei, Wang Wei, Wang Xiaowei, Liao Heng.

Researchers and drafters:

Zhou Yingda, Chris Pereira, Pan Qiuling, Zhang Xiaojun, Cao Chao, Hu Ruifeng, Liu Zaiyao, Wu Shuang,Zhang Liangliang, Guo Xingmin, Wu Yizhen, Du Wei, Gan Jiadong, Jiang Yaoguo, Stephen McNamara,William Michael Genovese, Zhu Zhaohui, Liu Jian.

Art Designer:

Yang Shaoqing

Proofreaders:

Pan Qiuling, Zhang Xiaojun, Hu Ruifeng, Liu Zaiyao, Zhou Yinda, Cao Zhao.

Contents

1 The Emergence of Blockchain

1.1 Origin of Blockchain

To understand the mechanisms behind blockchain and its development, a discussion of Bitcoin is inevitable. Blockchain first appeared in the Bitcoin system as an independent technology. In 2008, a person using the pseudonym of Satoshi Nakamoto (or his team) published a white paper on Bitcoin, titled *Bitcoin: A Peer-to-Peer Electronic Cash System.* In the following year, the original source code of Bitcoin system was published. This marked the birth of Bitcoin.

Setting aside the roller coaster ride of Bitcoin prices, the system design of Bitcoin itself merits attention. The system can be seen as a concept and technology experiment for a type of digital currency: In the traditional electronic payment system (such as bank transfer or third party payment), transactions are verified and recorded by the bank or a payment service provider, and the ledger is kept by centralized institutions. Bitcoin, however, has enabled the decentralized issuance and transfer of digital currencies. For the first time in history, a centralized third party agency or accounting management system is no longer needed to verify or record transactions — the public ledger is maintained and updated across the internet. Bitcoin promises a future in which digital transactions will move from a "centralized ledger + agent" model to "public ledger + consensus". This transformation is inseparable from blockchain technologies.

The concept of blockchain is not directly mentioned in the Bitcoin whitepaper, but the whitepaper did put forward a mechanism to assure the authenticity and tamper proof nature of transaction records, which can be seen as a prototype of the blockchain system. Here is how the protocol works: After initiating a transaction, the client will broadcast to the rest of the network, and await confirmation. Bitcoin nodes on the network then verify the transaction. If the transaction is valid,

the system will then pack the to-be-confirmed transactions and the hash value of the previous block into a new block. Then, the system will seek a random number to ensure that the hash value of the new block is smaller than a specific amount. Once the number is found, the node confirms that the new block is valid. The node will then broadcast the block to the entire network for verification. After the block is determined to be valid by the other nodes, the new block will be added to the chain, and all transactions in the block will be regarded as valid. Likewise, any valid transactions that happen after will be added to a subsequent block, creating a longer and longer chain-like ledger containing all historical transaction records. Any change to a block will result in a change to the hash value of the block. As a result, the hash value changes of the subsequent blocks will be inconsistent with the ledger, making it very hard to tamper with the blockchain.

This mechanism is one of the basis for Bitcoin. Using this mechanism, thousands of distributed nodes have been running around the clock for nearly 10 years. During this time, no major vulnerabilities have ever emerged. People have come to realize that the blockchain has exciting prospects in many ways and should in no way be limited to only money transfer.

1.2 Development of Blockchain

In essence, digital currency transactions are the value transfer of money (or money-like) assets. In fact, the concept of distributed ledger can be applied to many other fields in addition to digital currency transactions, including value transfers in a broader sense. In principle, the ownership and circulation of tangible and intangible assets can all be recorded and tracked using blockchain technologies, enabling peer-to-peer value transfer. This new method of value transfer will greatly change the way information and assets are managed in society.

However, the non-Turing complete nature of the Bitcoin system has made it hard to process more complex business scenarios. Inspired by Bitcoin, Ethereum has taken the technology a step further. It created a public blockchain platform, developed and launched in 2015. The platform aims at expanding the use cases of blockchain to more complex business scenarios. It allows developers to deploy smart contracts on the platform, under which code is written in advance that defines each type of business scenario. The business is then processed automatically in the platform if pre-set criteria are satisfied. Smart contracts are deployed transparently along the blockchain. With this platform, blockchain technologies can be applied to a wider range of business scenarios involving

contract processing, data exchange, ownership transfer, Internet of Things (IoT), logistics, and the shared economy.

Blockchain technology is now in its tenth year of development if the emergence of Bitcoin is counted. At present, blockchain can be divided into two categories: public chain and consortium chain. Public chain is best represented by Bitcoin and Ethereum. Anyone can be part of it and any records are open to the public. Consortium chains refer to a number of blockchain alliances created by a specific group of people. Likewise, the transaction records are kept in the blockchain, but they are only available to consortium members. Therefore, the consortium chain is not as open nor as large as a public chain. This type of blockchain is best represented by the Hyperledger, the open source blockchain project under Linux Foundation.

Table 1-1 Development of Blockchain

Development Timeline of Blockchain	Major Events	Impacts
2009–2014 (blockchain 1.0)	Announcement of Bitcoin system	Emergence of blockchain technologies
2014–2017 (blockchain 2.0)	Open source blockchain projects such as Ethereum and Hyperledger announced	Blockchain protocol layer and framework layer optimized; emergence of smart contracts, public chain, and consortium chain.
2017–?	Commercial deployment projects of blockchain spring up, but only a few implemented.	Blockchain may evolve into V 3.0 and its use cases will be explored in various industries.

Blockchain has been a very widely discussed field recently. But the technology itself has not been deployed on a large scale commercially. More often than not, we are seeing limited pilot use cases in finance, logistics, and charity. There are still a number of challenges to overcome in blockchain, including performance, access, privacy protection, and inter-chain communication. The technology is still in development. According to some consulting and analysis reports, commercial use of blockchain is expected to occur in the next three to five years. However, blockchain solutions still need to be improved in multiple respects in order to become commercially viable.

1.3 Two Current Misconceptions about Blockchain

There are many voices in the industry talking about blockchain. The various voices are mainly from two groups: one group is extremely exaggerating the functions of blockchain, and the other group is attacking the drawbacks of blockchain. However, we need to be more tolerant and objective towards new technology.

Misconception 1

Blockchain is Bitcoin. Currently, blockchain is "the" thing to talk about – and almost everyone is talking about it. However, when referring to blockchain, people are more passionate about its economic value, and tend to simply regard blockchain as being equivalent to Bitcoin or other cryptocurrencies. In fact, cryptocurrencies are only one application of blockchain and should not be viewed as one and the same as blockchain. Cryptocurrencies (e.g. Bitcoin) are primarily a means of investment. At present, there are more than 1,000 types of cryptocurrencies in the world, and the number is increasing. Enterprises or governments are focusing on how to utilize the reliability of the blockchain from the technical perspective, so as to ensure the security of transactions involving many enterprises, create more business value, and aim to release the technological potential of smart contracts and the distributed ledgers in more scenarios.

Misconception 2

The blockchain is an all-powerful technology that can replace databases, the Internet, and other foundational technology infrastructure. Some people believe that the blockchain will transform databases, replacing centralized traditional databases (Oracle, IBM DB2) with distributed databases. In fact, this view deifies the blockchain to an exaggerated extent. Blockchain is mainly based on

cryptography and consensus algorithms; most of the technologies used in the blockchain are rooted in the integration of existing technologies. Blockchain has not developed new technological systems. As a supplement to the existing technologies, the blockchain adopts distributed ledger technology and consensus mechanisms to form a tamper-proof method of transferring data based on existing encryption technologies. The distributed ledgers used in the blockchain cannot replace existing databases as they will not be used as standalone databases. Therefore, independent data storage is still necessary and will not be replaced. The blockchain cannot exist and form any technology system without the Internet, database, and other technologies. Therefore, the blockchain utilizes the "X technology + blockchain technology" model.

2 Core Technologies and Principle Mechanisms of Blockchain

2.1 Definition and Features of Blockchain

Blockchain is an organic combination of a series of existing mature technologies. It effectively records the ledgers in a distributed manner and provides a complete script to support various service logic. In a typical blockchain system, the data is generated and stored in blocks, and forms a chain of data in chronological order. All nodes of the blockchain are referred to in the data verification, storage, and maintenance. The creation of a new block usually requires the validation of the majority of nodes (the number differs according to the consensus mechanisms) in the entire network. The data will be broadcasted to all nodes to achieve network-wide synchronization, and cannot be revised or deleted afterwards.

Externally, a blockchain system has the following features:

- **Peer-to-peer recording of transactions and maintaining ledgers by multiple participants**

  The multiple participants here refer to the participants of the ledgers and exclude the blockchain end users. The ledger participants of a blockchain are composed of multiple entities with differing interests, and different participants initiate a ledger within different periods (the rotation differs according to the consensus mechanisms). Other participants will jointly verify the ledger information initiated by the dominant participant.

- **Public ledger**

  All participants have access to the ledger for recording transactions in a blockchain, because they need to access historical information and content to validate the information recorded in the blockchain. However, the public ledger refers to openness and accessibility, not disclosure

of information. Therefore, the industry expects to apply many privacy protection technologies, such as zero-knowledge proof, homomorphic encryption, and threshold encryption to the blockchain to solve the problem of validating information through operations using cipher texts.

- **Decentralized**

  The blockchain is a system that does not rely on a single trusted center. The blockchain can build trust between participants when dealing with data in a closed blockchain system. However, under certain circumstances, such as in identity management, it is unavoidable to introduce external data that needs to be endorsed by a trusted third party. For different types of data, the trust should be endorsed by different sources, instead of relying on a single trust center. In this case, the blockchain itself does not build trust, but acts as a carrier of trust.

- **Tamper proof**

  As the most significant feature of the blockchain, the feature of being tamper proof is a necessary condition for a blockchain system, but not a sufficient condition. Many technologies based on hardware can also read the data multiple times and prevent data tampering after recording data for once. A typical example is the Compact Disc-Recordable (CD-R). The blockchain cannot be tampered with because it adopts cryptographic hash algorithms and is collectively maintained by multiple parties. However, because of this, the nature of the blockchain is not in a strict sense completely tamper-proof. It is more appropriate to say that it is hard to tamper with the blockchain.

2.2 Core Technologies of Blockchain

2.2.1 Distributed ledger

Distributed Ledger Technology (DLT) is essentially a decentralized data storage technology that enables users to share, synchronize, and replicate data in multiple network nodes, multiple physical addresses, or multiple organizations. Compared to traditional distributed storage systems, DLT has two distinct features:

- The data in traditional distributed storage systems is managed and controlled by a central node or an authoritative organization. On the other hand, with DLT, based on certain consensus rules,

the blockchain adopts the multiple decision-making and common maintenance method for data storage, replication, and other operations. Faced with the explosive growth of Internet data, more challenges are being faced when establishing a data management system through a single central organization, which has to continuously invest to build large-scale data centers. This leads to the problem of efficiency of huge resource pools in computing, network, storage, and so on. Meanwhile, the ever-increasing size and complexity of the systems have also brought about increasingly challenging reliability issues. In response, blockchain adopts a decentralized data maintenance strategy via DLT, and can effectively reduce the burden carried by systems. In some scenarios, blockchain can even use the enormous resources that precipitate in a large quantity of scattered nodes across the Internet.

- In the traditional distributed storage system, data is divided into many parts and stored. While in the distributed ledger, every node has an independent, complete copy of data. It ensures that all copies are always in sync and contain the exact same information by periodical or event-driven consensus of all nodes. In the past few decades, there has been a growing concern over the weaknesses of the traditional service systems in terms of data reliability and cyber security.

  A common user cannot tell if the data has been stolen or tampered with by the service provider, let alone deal with cyber-attacks and data leakage. To deal with such challenges, industry has adopted additional management systems or technologies, which, however, increases maintenance cost of the system and reduce the operational efficiency of the system. In the distributed ledger, every node maintains a complete copy of the data. Therefore, the modification made by one node or a small number of nodes cannot affect the majority of data copies.

  In other words, be it deliberate, unauthorized tampering by service providers or malicious attacks launched by hackers, the data in the system could only be tampered with when the majority of the copies in the distributed ledger are modified at the same time. Otherwise, the unaffected nodes will soon detect and trace the malicious activity. This characteristic of the distributed ledger will significantly improve the reliability and security of the data in the service system.

These two characteristics of the distributed ledger have made it a fundamental, disruptive, and revolutionary innovation for the current service system.

2.2.2 Consensus

Blockchain is a traceable, tamper-proof, distributed (decentralized) system that can build trust between different parties. Inevitably, the distributed system must face the challenge of consistency, and the settlement process is how consensus is achieved.

The traditional distributed system and the blockchain are fundamentally different in terms of trust. The traditional distributed system often achieves disaster recovery, capacity and throughput expansion, and higher computational efficiency by adding nodes. They are managed uniformly as a cluster, so as not to give rise to trust issues. The blockchain has many participants who manage their own node(s) but have no control over other nodes in the system. Therefore, there is a need to build trust among all participants of the blockchain.

The agreement in the distributed system is reached via consensus algorithms, which aim to help other nodes in the system reach an agreement with each node's proposals. Based on the fundamental difference between traditional distributed system and blockchain, consensus algorithms are divided into consensus algorithms among reliable nodes and unreliable nodes. The former, such as the well-known Paxos and Raft and their variants, have been researched thoroughly and are widely applied to popular distributed systems. As for the latter, they were not widely applied until robust development of blockchain technology, despite being researched for a long time. Based on different scenarios, consensus algorithms among unreliable nodes are represented by Proof of Work (PoW) and Proof of Stake (PoS) for public blockchain, and Practical Byzantine Fault Tolerance (PBFT) and its variants for consortium and private blockchain.

PoW is an algorithm adopted by the Bitcoin system. The algorithm was proposed by W. Dai in the design of B-money in 1998. Ethereum also uses PoW to reach consensus. However, as Ethereum's block time is faster (about 15 seconds) and it is more likely to generate blocks, the system uses so-called "Uncle" as a reward mechanism to avoid the wasting of computer power of nodes. PoS algorithm was first realized by Sunny King with PPCoin (Peer-to-peer coin) in August 2012. Ethereum developers favor PoS more than PoW and plan to replace PoW with PoS as the foundation for consensus. PBFT was first put forward by Miguel Castro and Barbara Liskov during the OSDI99 Conference in 1999. This algorithm's operational efficiency is higher than that of the traditional BFT (Byzantine fault-tolerant). PBFT behaves correctly when no more than F out of 3F + 1 replicas fail. As the number of nodes increases in the system, PBFT can tolerate more Byzantine

nodes, yet its consensus efficiency drops significantly. That is the reason that the number of nodes in systems that use consensus algorithms is usually no more than 100.

The first principle of both PoW and PoS is to leverage financial incentives to encourage nodes to contribute to the system and punish malicious activities with financial penalties. In a Bitcoin style system there are two economic incentives to be a good actor: 1) miners that solve the block puzzle are rewarded with newly mined coins (until the fully supply has been issued) and 2) miners also receive a fee for each transaction in the new block. There are two differences between consortium/private blockchain and public blockchain. First, the nodes in consortium/private blockchain are fewer than those in the public blockchain. Therefore, it is more suitable to use PBFT and its variants. Second, the aim of nodes in a consortium/private blockchain is to obtain trusted data from the chain, and so to them, the incentives for ledger keeping pales in comparison with obtaining trusted data. As a result, the nodes in consortium/private blockchain are more likely to maintain the stable operation of the system.

2.2.3 Smart contracts

- **What are smart contracts?**

  Smart contracts are computer protocols intended to digitally facilitate, verify, or enforce the performance of a contract. Smart contracts allow the performance of trusted transactions without third parties. These transactions are trackable and irreversible. The aim of smart contracts is to provide security that is superior to traditional contract law and to reduce other transaction costs associated with contracting.

  Smart contracts were first proposed by Nick Szabo, a computer scientist, legal scholar, and cryptographer who coined the term in the 1990s. His definition of smart contract is as follows: A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises.

  Researchers like Nick Szabo hoped to use computer technology to develop the contract clauses and perform the contract with the help of cryptology and other digital security mechanisms. However, the theory of smart contract was not concretized at that time, as many technologies were still in the preliminary stages and there were no digital systems or technologies that supported programmable contracts.

The concept of smart contracts is quickly going mainstream as blockchain technology matures. Smart contracts are a key research area and are likely to be the future of Internet contracts. Here is how smart contracts on the blockchain work: There is an event processing and storage system and a completed finite state machine in place to receive and process multiple smart contracts, including processing status data. Once an event information unit is received by a smart contract, the finite state machine starts to work and automatically executes the contract as was previously agreed if a condition or several conditions are met. Smart contracts not only empower us to process information more efficiently but also prevent breach of contract as the contract is executed automatically without involving a third party, such as an authoritative organization.

- **Pros and Cons**

  The advantages of smart contracts are being recognized by an increasing number of researchers and technical personnel as they are extensively deployed onto the blockchain. In general, smart contracts feature:

  a. Efficient contract development

     Smart contracts are developed by digitizing and automating the execution of contract terms signed by both parties based on computing technologies, without the need to involve a third party, such as an authoritative organization or a centralized agency. This therefore simplifies the process of formulating an agreement.

  b. Low maintenance costs

     Smart contracts are monitored and executed automatically as agreed upon, preventing breaches of contract and significantly reducing the costs associated with human supervision and execution.

  c. Accurate contract execution

     Smart contracts are executed by computer systems without human intervention, and are therefore more accurate.

  Despite its many obvious advantages over traditional contracts, we should not lose sight of the potential risks of this emerging technology as we move forward.

  In 2017, a major vulnerability that could cause smart contract failures was discovered in Parity, the Multi-signature Ethereum Wallet, resulting in about US$150 million in assets being frozen. In February 2018, researchers from the National University of Singapore, Yale-NUS College,

and University College London claimed in a report that 34,200 of the nearly 1 million smart contracts on Ethererum were found to have vulnerabilities, leaving these individuals prone to hacker attacks, such as theft of ether, asset freezing, and contract deletion.

Although blockchain technology and smart contracts face cyber security risks, it is still widely recognized by industry insiders that they will be a major trend in information technology, and that the risks we are facing are inevitable in the course of technology development.

- **Application**

  So far, smart contracts have been deployed extensively onto Ethereum and Hyperledger Fabric blockchain as a core technology.

  a. Ethereum smart contracts

     Ethereum smart contracts are pieces of code that can be executed by the Ethereum Virtual Machine. Ethereum supports Turing-complete scripting language and is open to developers. Ethereum smart contracts can be written in advanced languages (Solidity, Serpent, LLL) and stored on the blockchain as code, but can't be modified once deployed. Smart contracts allow users to transact, manage, and run an account, such as managing money and account status.

  b. Hyperledger Fabric smart contracts

     Smart contracts are deployed more extensively on Hyperledger Fabric as stateless, event-driven, and auto-enforceable codes that can be written in Turing-complete languages. These contracts play a crucial role on the blockchain and can interact with ledgers directly. Unlike Ethereum, Hyperledger Fabric smart contracts are separate from the underlying ledgers, meaning that we don't need to migrate ledger data into a new smart contract when updating the old one. This way, data and logic are separated.

     Smart contracts on Hyperledger Fabric include system chaincodes and user chaincodes. System chaincodes take care of the processing of Hyperledger Fabric nodes, such as system configuration, endorsement, and verification. User chaincodes that run in a separate chaincode container are customer facing and charge the processing of distributed ledger status on the blockchain. Developers are responsible for writing algorithms to support higher-level services. User chaincodes operate in isolated chaincode containers.

2.2.4 Cryptography

Information security and cryptographic technologies are fundamental to information technology, and are widely used in blockchain. These include Hash algorithms, symmetric encryption, asymmetric cryptography, digital signatures, digital certificates, homomorphic encryption, and zero-knowledge proof. We will go over these concepts in this section from the perspective of integrity, confidentiality, and identity authentication.

- **Integrity (protected against tampering)**

  Hash algorithms are used to protect the integrity of ledgers on the blockchain. A hash function is any function that can be used to map data of arbitrary size to data of fixed size. In addition, a good hash function is collision resistant, that is, it is impossible to produce the same hash value (string) for differing input data.

  The hash of a block (n) of transactions (t) contains the hash of the previous block (n-1), with those validated transactions (t) being linked together via a Merkle root. Changing any record that has previously occurred on a blockchain would change all the hashes. This can help us quickly detect the presence of tampering.

- **Confidentiality**

  Encryption technologies can be divided into two broad categories: symmetric encryption or asymmetric encryption. Symmetric encryption uses the same key for encryption and decryption, while asymmetric encryption use different keys: a public key and a private key. Data encrypted using the public key can only be decrypted using the corresponding private key, and vice versa.

  The blockchain, in particular consortium blockchain, needs to use the Transport Layer Security (TLS) encrypted communication technology to ensure the security of data transmission throughout the network. TLS encrypted communication is the ideal combination of symmetric and asymmetric encryption technologies: The two communicating peers use asymmetric encryption technology to generate a symmetric key, and then use the key as the working key to encrypt and decrypt data. In this way, TLS encrypted communication takes advantage of both technologies: asymmetric encryption does not require a shared key and symmetric encryption operates fast.

- **Authentication**

TLS encrypted communication alone can only ensure confidentiality and integrity during data transmission, but cannot ensure that the peer on either end of the communication is trustworthy (due to the risk of man-in-the-middle attacks). Therefore, a digital certificate mechanism must be introduced to verify the peer identity and ensure the peer public key is correct. Typically, digital certificates are issued by a certificate authority (CA). The peer on one end of the communication holds the root CA's public key with which to verify the peer certificate is trusted (i.e. the certificate is issued by the holder of the root CA's public key), and authenticate the peer based on the content of the certificate. With the peer authenticated, the holder of the root CA's public key retrieves the public key in the peer certificate and hence completes the asymmetric encryption.

Furthermore, the blockchain applies the latest research of modern cryptography, such as homomorphic encryption and zero-knowledge proof, to maximize the privacy protection capabilities of the blockchain with its distributed and open ledger. The technologies in this area are still evolving and being optimized.

Blockchain security involves a system of numerous parts — the security and reliability of the blockchain system will be ultimately affected by a series of factors including system configuration, user access, component security, user interface, network intrusion detection, and attack defense capability. A blockchain system should be built on an appropriate balance of security, system building cost, and ease of use, all while meeting user requirements.

2.3 Huawei's Technological Innovation in Blockchain Evolution

2.3.1 Innovation on consensus

The Practical Byzantine Fault Tolerance (PBFT) algorithm addresses the low efficiency of the original Byzantine fault tolerance algorithm by reducing its complexity from exponential to polynomial. Thus it becomes practical to systematically use the Byzantine fault tolerance algorithm.

PBFT supports the Byzantine fault tolerance of "f" nodes in a cluster of 3f+1 nodes. In other words, any node can reach the correct conclusion with 2f+1 correct messages received (a maximum of "f

"nodes are tolerated to send malicious faulty messages). It is clear that consensus efficiency is the fundamental capability for the blockchain to practically provide services.

Despite its extensive use, PBFT is not free of shortcomings. To overcome the problem of a primary node, PBFT uses the complicated full point-to-point communication to monitor abnormal behavior. The communication becomes highly complex ($O*n^2$) and a large amount of signatures need to be verified. The ensuing heavy system overhead thus lowers the consensus efficiency and node expandability. In addition, once a masternode selection occurs, PBFT will fail to support consensus. If the new masternode cheats or malfunctions, repeated masternode selection will occur, during which the blockchain's serviceability could be significantly lowered or even fail.

Huawei's blockchain uses an efficient, proprietary, and Byzantine-fault-tolerating algorithm, effectively addressing the above-mentioned PBFT defect. It eliminates unnecessary signature verifications, simplifies the consensus process, and reduces the communication complexity from $O*n^2$ to $O*n$, resulting in higher consensus efficiency and expandability. An improved consensus process also secures stable serviceability of the blockchain in case of a node malfunction or masternode switchover.

2.3.2 Security and privacy protection

Huawei's blockchain offers stronger security and privacy protection.

- **Chinese standardized ciphers algorithm: Chinese standardized ciphers** is a series of algorithms developed by the Office of the State Commercial Cryptography Administration (OSCCA). As financial security becomes an increasingly important part of national security **Chinese standardized ciphers** are becoming more widely adopted. In November 2017, SM2/9 was officially accepted as an ISO/IEC standard. Huawei blockchain supports SM2/3/4 and can provide users with multiple encryption algorithms that meet compliance requirements.
- **Using homomorphic encryption to ensure privacy-proof transaction:** The blockchain is tamper-proof, decentralized, and can operate on an untrusted network. However, under the current blockchain mechanism, user ledgers are transparent to all participants; that is, the same user data can be accessed by anyone. Placing users' private data on the chain may increase the risk of data leakage. Currently, all public chain systems, including Bitcoin, display the full transaction information (including transaction amount). This means that most blockchains are not privacy-proof and may raise privacy issues in certain business scenarios, especially in the

financial sector. Financial transaction information is highly sensitive data and should never be open to non-related parties. Data keeping should also be in line with regulatory requirements.

Huawei's blockchain transaction solution encrypts users' transaction data, using the public keys of a homomorphic encryption library. As the transactions are processed and stored in the ledger in an encrypted form, the ledger information will remain intact even if the nodes are hacked. Huawei's solution also offers range proof verification. Without decryption, the endorsement node can endorse the ciphertext and verify the transaction, avoiding malicious transactions that endanger smart contracts. Huawei has developed a confidential transaction system specifically for the Hyperledger Fabric platform. Using an improved algorithm, the system features several times faster performance than the traditional additive homomorphic encryption and ring-signature based range zero-knowledge proof.

- **Zero knowledge proof:** a method in which the prover can prove to the verifier that his/her statement is correct without conveying any information about the statement itself. Huawei's blockchain will provide zero knowledge proof to protect users' private data and reduce users' data from leakage.
- **Smart contract security**: When a smart contract runs into trouble or a programming error occurs, a DOA attack may find its way into the system, causing huge losses to users. Huawei's blockchain provides a smart contract detection tool that aims to prevent the vulnerabilities from being exploited by hackers, therefore stopping them from breaking into smart contracts and accessing user data. In addition, Huawei's blockchain provides a security container, the operation of which is closely monitored. If a vulnerability is detected, the container will be isolated and the access of the container will be strictly controlled to ensure that the contract will be carried out under all conditions.
- **Consensus security:** Huawei blockchain provides a hardware-based consensus algorithm. The standardized verification procedures will protect consensus mechanism from attacks, improve consensus efficiency, and increase network stability.
- **Ledger security:** The local ledger of nodes is susceptible to tampering. If most of the nodes' local ledgers are tampered with, a 51% attack may occur. Huawei blockchain provides a hardware-based protection mechanism to protect the confidentiality and integrity of local ledgers and prevent ledgers from tampering.

- **End-to-end communication security:** Normally, the TLS protocol only serves to ensure the security of communication between applications. If the TLS is attacked before it even starts up, protection will be compromised. In response to this, Huawei blockchain provides a hardware-based solution to improve communication security between each node.

2.3.3 Off-chain channel

Transaction processing time is still one of the main barriers to the large-scale application of blockchain. Distributed architecture, varying computing capabilities of nodes, and changing network conditions make it hard to promptly achieve consensus on the entire network, resulting in very limited transaction speed. Currently, the Bitcoin network can process only about seven transactions per second, and the figure for Ethereum (supporting smart contracts) is about fifteen. In contrast, the Visa system, with its central server, supports up to 56,000 transactions per second. Alipay's transactions peaked at 256,000 units per second during the "double eleven" (China's version of Black Friday) period of 2017. Congested transaction channels have greatly restricted the wide-scale application of blockchain.

The blockchain community has long discussed and worked on solutions to expand transaction capacity. The existing mainstream solutions include block expansion, consensus algorithm improvement, adding security hardware (TEE), isolation witness, lightning network, transaction/status fragmentation, and multi-layer sub-chain. However, even with these abundant solutions, the give-and-take between decentralization, scalability, and security is still inevitable. It should be noted that the blockchain is application-based, and a balance among those factors can certainly be achieved as long as application requirements are met.

In large-scale DAPP (Decentralized APP) applications, micro transactions account for the majority of activity, but do not need to be verified overly quickly by the parent blockchain. Micro payments are very common in the shared economy. To effectively alleviate the processing pressure on the parent chain, most micro transactions can be processed in the off-chain channel. This means they do not interact with the parent chain during the transaction; instead, they only post a transaction to the parent chain after the child transactions complete, or when the parties exit the channel. This is exactly the design concept of the off-chain micro-payment channel, and its applications include the Lightning Network for Bitcoin and the Raiden Network for Ethereum smart contracts. The off-chain channel undertakes a series of procedures from chain locking to off-chain execution, and the status

changes of the transaction parties (fund allocation ratio), as well as the transaction itself, are monitored by the contract on the chain.

Huawei have developed an off-chain channel transaction system specifically for the Hyperledger Fabric platform. With handshake agreement of the transaction parties at its core, the transaction performance of dual user channel can be as high as 2,000 transactions per second. As the number of off-chain transaction channels increases, the transaction processing capability of the system in a unit time will be taken to a new level.

3 Current State of Blockchain Development

3.1 Current Industry Policies towards Blockchain

China and Europe are gradually seizing a leading position in the formulation of blockchain industry policies. The European Union (EU) has established the European Blockchain Observatory and Forum on February 1, 2018. Its main responsibilities are as follows: policy formulation, research, production, and academic society coordination, cross-country BaaS (Blockchain as a Service) development, and open-source, standard development. EU Horizon 2020 will also invest 5 million euros into the regional blockchain R&D fund (before December 19, 2018). It is estimated that the EU's investment in blockchain will reach 340 million euros in the period of 2018–2020. In the US, different policies between states make it hard to formulate a standardized industrial policy, despite the upsurge in blockchain startups. In the Middle East, Dubai has been hoping to have a say in the first wave of this new technology and has gained a leading position in what can be seen as government-led efforts (with necessary help from businesses) across the region to explore new blockchain technologies and their applications. In the Asia-Pacific region, Japan and South Korea are quite active in terms of blockchain. Japan's main player is NTT with government providing necessary support. South Korea is now exploring the application of blockchain in the finance sector.

The State Council of China has issued *the 13th Five-Year Plan on China's national informatization*. New technologies such as blockchain, big data, artificial intelligence, and deep machine learning are the focus of this national initiative. The People's Bank of China has issued the *13th Five-Year Plan for the Development of Information Technology in China's Financial Sector*, which explicitly states China's ambition to promote the research and application of new technologies such as blockchain and artificial intelligence. It also indicates that China will pilot a national digital currency. In October 2017, the Ministry of Industry and Information Technology released the

Blockchain Technology and Application Development Whitepaper, the first ever publicly released official guide to the blockchain in China.

Local governments, especially those in China's coastal areas are rushing to set up district-level blockchain laboratories and research institutes. Shenzhen, Hangzhou, Guangzhou, Guiyang, and a number of other municipal governments are now setting up blockchain development zones, and are providing those zones with favorable policies. In December 2017, Guangzhou issued the *Ten-part Blockchain Strategy*, under which blockchain innovation areas in Huangpu District and Guangzhou Economic and Technological Development Zone will be set up. In March 2018, Economic, Trade and Information Commission of Shenzhen Municipality released the *Notice on the Second Batch of Supporting Plan for Information Security Transformation of New Information Technology of Shenzhen Strategic Emerging Industries (2018)*. Blockchain will be the direction of support under the notice, making Shenzhen the fifth Chinese city to introduce blockchain supporting policies after Guangzhou, Guiyang, Qingdao, and Hangzhou.

3.2 Current Blockchain Development in Main Opensource Communities

Hyperledger

Hyperledger is an open source project launched by the Linux Foundation in 2015 to promote blockchain technology adoption, and advance cross-industry collaboration. It has the support of many international companies including IBM, Intel, Fujitsu, Cisco, Huawei, Redhat, Oracle, Samsung, Tencent Cloud, and Baidu Finance. At present, there are more than 200 members. The founder of the Apache Foundation, Brian Behlendorf, is the executive director of the Hyperledger project.

The goal of the Hyperledger project is to allow members to work together to build an open platform that supports different use cases in multiple industries and simplifies business processes. Hyperledger has multiple blockchain platform projects, including the Fabric projects (supported by IBM), Sawtooth project (supported by Intel), and Iroha, Burrow, and Indy.

As an important member of Hyperledger, Huawei has contributed a significant amount of code to the Fabric and Sawtooth Lake projects and also contributes two maintainers to the projects. . In

addition Huawei also developed Caliper (blockchain performance assessment tool) which was recently approved as a new Hyperledger project.

Enterprise Ethereum Alliance (EEA)

In February 2017, the Enterprise Ethereum Alliance (EEA) was formally established. The founding members of its rotating board include Accenture, Bank Santander, BlockApps, BNY Mellon, Chicago Mercantile Exchange (CME), ConsenSys, Intel, JP Morgan, Microsoft, Nuco, and the Initiative for CryptoCurrencies and Contracts (IC3). As of February 2018, the alliance had more than 150 members.

EEA aims to develop standards and technologies that will facilitate enterprises to develop blockchain applications based on Ethereum. It focuses on promoting the privacy, confidentiality, scalability and security of the Ethereum blockchain. It will also explore hybrid architectures covering the licensed Ethereum network, public Ethereum network, and industry-specific application layer.

Developed by Vitalik Buterin, Ethereum is a popular public chain technology that can deploy decentralized applications. However, it does not meet the needs of enterprises to develop consortium blockchain applications. Based on the Ethereum technology, many enterprises have explored the consortium blockchain applications and improved relevant technologies. EEA combines various interest groups, enterprises, and users to jointly work to build an Ethereum blockchain which meets the requirements of enterprise-grade applications and promotes the development of the Ethereum ecosystem.

3.3 Development of Blockchain Standards

International Telecommunication Union – Telecommunication Standardization Sector (ITU-T)

From 2016 to early 2017, the International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) Study Group 16 (SG16), SG17, and SG20 respectively launched DLT research on the overall requirements, security and IoT applications. ITU-T set up three focus groups, namely, the Focus Group on Application of Distributed Ledger Technology (FG DLT), Focus Group on Data Processing and Management (FG DPM), and Focus Group on Digital

Currency including Digital Fiat Currency (FG DFC) to carry out research on DLT applications and services in blockchain, build a trusted IoT and smart city data management framework based on the blockchain, and develop standards for digital currency in the blockchain. Huawei serves as Chairman of the FG DLT architecture group and Chairman of the FG DPM blockchain group.

China Communications Standards Association (CCSA)

The following two committees of China Communications Standards Association (CCSA) have established working groups and projects respectively.

CCSA Ubiquitous Network Technical Committee 10 (TC 10) established an IoT blockchain working group in October 2017. The working group is responsible for the application and standardization of blockchain technologies in the fields of IoT, IoT-covered smart city, Internet of Vehicles (IoV), edge computing, big data, logistics, and smart manufacturing. The group chairman is from China Unicom and vice chair is from Huawei.

The Blockchain and Big Data Working Group under the CCSA IP and Multimedia Communication Technical Committee (TC1) has proposed two blockchain industry standards: "Blockchain: Part 1 General Technical Requirement" and "Blockchain: Part 2 Evaluation Indicators and Methods".

Joint Photographic Experts Group (JPEG)

At the 78th meeting of the Joint Photographic Experts Group (JPEG) committee in February 2018, the JPEG committee organized a special session on blockchain and DLT, and discussed impact of these technologies on the JPEG standards. Given the potential impact of technologies such as blockchain and DLT on future multimedia, a special group is to be established to develop standards for interoperability between different systems and imaging services that rely on blockchain and DLT.

Internet Engineering Task Force (IETF)

The Decentralized Internet Infrastructure Proposed Research Group (DINRG) was established at the IETF 99 conference in June 2017 to study the blockchain architecture and corresponding standards. In 2018, the IETF will devote more effort to the promotion of the interoperability of standards in blockchain.

Institute of Electrical and Electronics Engineers (IEEE)

The Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) set up the P2418 Blockchain Working Group (Standard for the Framework of Blockchain Use in IoT). The working group focuses on the research of the application of blockchain technologies in IoT scenarios, and standard development for the future standard interoperability of the blockchain in IoT scenarios.

International Organization of Standardization (ISO)

ISO TC 307 "Blockchain and distributed ledger technologies " committee established five study groups (SG 01 "Reference architecture, taxonomy and ontology", SG 02 "Use cases", SG 03 "Security and privacy", SG 04 "Identity", and SG 05 "Smart contracts") to develop global blockchain standards and related supporting agreements.

World Wide Web Consortium (W3C)

W3C launched the following three Community Groups (CG). First, the Blockchain CG aims to study and evaluate new technologies related to blockchain and use cases such as interbank communication, to generate message format standards of blockchain based on ISO20022.The community group launched the Flex Ledger project, focusing on the data interactivity between blockchains. Second, the Blockchain Digital Assets CG is committed to discussing Web specifications for creating and using digital assets on blockchain. Third, the Interledger Payments CG focuses on connecting multiple payment networks (ledgers) worldwide.

3.4 Development of Blockchain Industry Alliances

R3

In September 2015, the Blockchain consortium, R3, was initiated by R3 CEV （R3 Crypto Exchange Venture） and has since attracted many financial institutions such as Wells Fargo, Bank of America, Deutsche Bank, HSBC, Morgan Stanley, and Citibank. Currently, R3 has more than 60 members. R3 is committed to providing blockchain technologies to banks and offering blockchain conceptual products. In 2016, Corda, a blockchain technology platform tailored for financial institutions, was introduced by R3 and opensourced in 2017.

Carrier Blockchain Study Group (CBSG)

In February 2017, the US telecommunications carrier Sprint, the California blockchain startup TBCASoft, and the Japan-based Softbank Group formed the Carrier Blockchain Study Group (CBSG), integrating the systems of Sprint together over a platform developed by TBCASoft. Based on Sprint's underlying core network, CBSG has constructed the blockchain platform (TBCSoft) layer which can be accessed by multiple base station subsystems to share ledgers of multiple applications.

Mobile wallet roaming, international remittances, recharging and IoT payments can be carried out on the cross-carrier payment platform system. CBSG has successfully tested the mobile payment system, which can be used to recharge prepaid phones of different carriers. In the future, the organization will launch applications to integrate computing, identify authentication, and clearing. At the 2018 Mobile World Congress (MWC), CBSG announced its five new members: KT, LG U+, Telefonica, FLDT, and Etisalat. Its list of members has grown from four to nine. Huawei has maintained in-depth discussion with CBSG.

Trusted IoT Alliance (TITA)

In September 2017, Cisco, Bosch, ConsenSys and IOTA jointly established the Trusted IoT Alliance (TITA). Its members also include BNY Mellon, U.S. Bank, BigchainDB, and others. TITA aims to establish a reliable, blockchain-based IoT ecosystem to enhance the security and reliability of IoT. The alliance will also develop standards for open source blockchain protocols to enhance IoT security. According to its roadmap, TITA will support blockchain implementations based on Hyperledger, Bitcoin, and Ethereum technologies.

Blockchain in Transport Alliance (BiTA)

Established in August 2017, Blockchain in Transport Alliance (BiTA) has attracted more than 100 companies as members, including FedEx, UPS, Penske, GE Transportation, SAP, Salesforce, and JD Logistics. BiTA gathers various parties involved in the freight and logistics industries to discuss the application of blockchain in the freight industry and develop relevant standards, thereby increasing the transparency and efficiency of the freight process and promoting the development of the industry.

Blockchain Insurance Industry Initiative (B3I)

In October 2016, the Blockchain Insurance Industry Initiative (B3I) was jointly launched by the top five insurance giants of Aegon (Netherlands), Allianz (Germany), Munich Re (Germany), Swiss Re,

and Zurich Insurance Group (Switzerland) to study the application feasibility of blockchain in the insurance industry and develop blockchain-based proofs of concept for insurance.

China Blockchain Technology and Industry Development Forum

On October 18, 2016, the China Blockchain Technology and Industry Development Forum was established in Beijing by the Information and Software Services Division of the Ministry of Industry and Information Technology and the Industrial Standards Department II of the Standardization Administration of China. The forum pools the resources of all parties from the government, industry, university, and research sectors to track the development trends of blockchain technologies and applications, develop relevant standards, build a roadmap for the development of China's blockchain, and organize exchanges with overseas partners.

Financial Blockchain Shenzhen Consortium

In May 2016, more than 20 financial institutions and technology companies including the Shenzhen FinTech Association jointly established the Financial Blockchain Shenzhen Consortium with the goal of developing one or more financial blockchains within 3 to 5 years. At present, Huawei, Huaxia Bank, China Guangfa Bank and other financial companies have participated in the consortium and are committed to research on the application of blockchain in the financial sector and the establishment of industrial consensus.

Trusted Blockchain Alliance

Under the guidance and support of the Ministry of Industry and Information Technology, China Academy of Information and Communications Technology proposed to establish the Trusted Blockchain Alliance, a cooperation platform for the government, industry, universities, and research sectors, to implement the 13th Five-Year Plan for Informatization Development and to promote deep integration of blockchain technologies with the real economy. At present, it is expected that over 150 companies, including Huawei, JD Finance, Chainnova, Tencent, China Mobile, and China Telecom will participate in the alliance. Huawei will serve as the vice president of the alliance to support China's top-level design in the blockchain and help build a harmonious and win-win industry environment.

4 Typical Blockchain Application Scenarios

For now, Huawei is mainly (but not solely) focusing on the following scenarios:

-	Scenarios	Description
Data	Data storage/exchange	Build reliable data exchange platforms to record the registration and transactions of data assets, realizing the traceability of data assets, and help enterprises create commercial value via data assets.
	Identity verification	ID management, for example, realize the access verification and firmware management of IoT devices/users and improve system security.
Applications in different industries		
IoT	New energy	Build a new energy peer-to-peer (p2p) trading system, enabling reliable transactions and value transfer.
	Supply chain traceability	Share data, streamline all processes, and improve data transparency and traceability.
	Internet of Vehicles (IoV)	Share information such as mileage and speed of vehicles with interested parties such as insurance companies and vehicle

-	Scenarios	Description
		manufacturers.
Telecom	Multi-cloud and multi-network synergy	With trusted access to multiple clouds and networks, realize global seamless roaming of cloud services based on "multi-cloud and multi-network" synergy.
Finance	Supply chain finance	The financial system is connected to business systems of companies, enabling easy loads to upstream and downstream companies in the supply chain.
	Inclusive finance	Record personal credit information to reduce the cost of auditing, increase the usage of financial service, thus drive greater economic development.

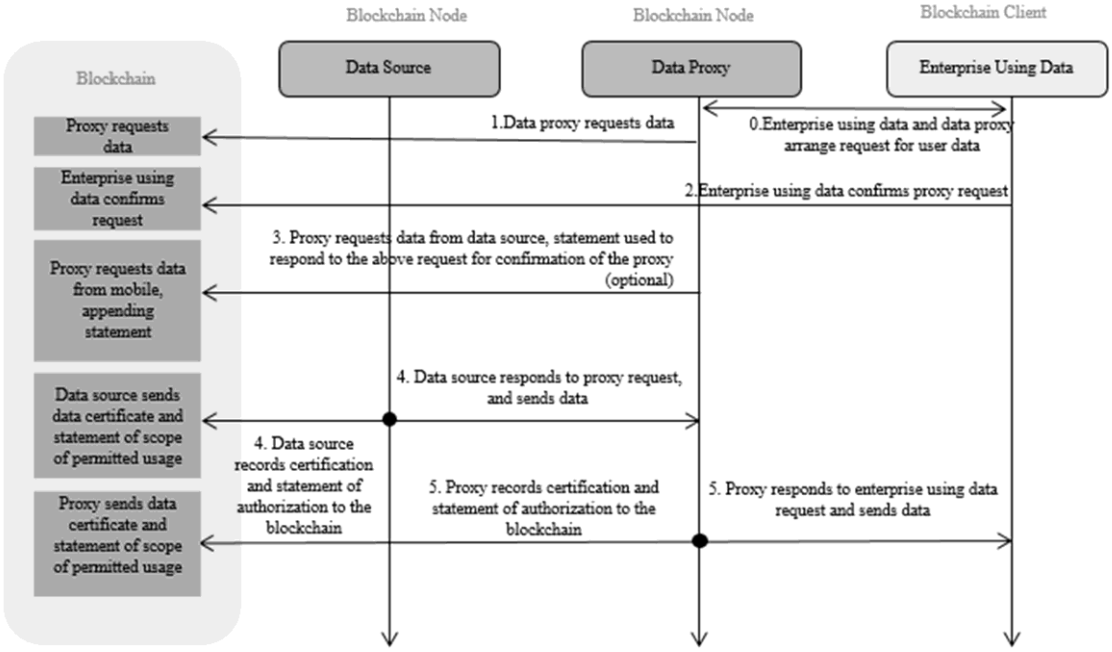
4.1 Data Exchange: Transparent and auditable processes, building up trust in society

Data will be the most important component of the future economy, which will be dominated by interconnectivity and machine learning. Applying AI algorithms to analyze data could lead to numerous discoveries that may greatly change the world. Data exchange will benefit companies with limited data collection capabilities, promoting companies' innovation and creating new sources of revenue. However, because data exchange is often illegal currently, and because of the low transparency of information and ease of data tampering, data exchange remains limited.

Because it is decentralized, secure, tamper-proof, and traceable, the blockchain can help to build trust among participants and promote the sustainable and substantial growth of data exchange. With information on data ownership, exchange and verification scope recorded in the blockchain, the data ownership can be confirmed, and a clearly defined scope of verification can also regulate the

use of data. Each step from data collection to distribution is also recorded in the blockchain. Therefore, data is traceable, and the quality of the data can be enhanced by limiting data sources. Decentralized data exchange platforms based on the blockchain can promote global large-scale data exchange.

Figure 4-1 Data Exchange Authentication based on Blockchain



A typical example is in IoT where a wide range of IoT devices and sensors collect a large amount of data. Serving as a medium for data exchange, decentralized data exchange networks can support the distribution of data and record real-time detailed data exchange. They can also build trust, maintain transparency, and support IoT participants in the data exchange ecosystem during the processes of data collection, storage, exchange, distribution, and data services. However, breakthroughs are still needed in scalability, exchange cost, and exchange speed in the decentralized data exchange networks to accelerate the commercialization of the IoT data market.

4.2 Identity Verification: Verify the identity and accelerate the development of digital society

Identity and access management (IAM) services can also adopt blockchain technology. Moreover, as it is highly reliable, traceable, and collaborative, the blockchain may serve as a basic technology in the application areas of IAM services.

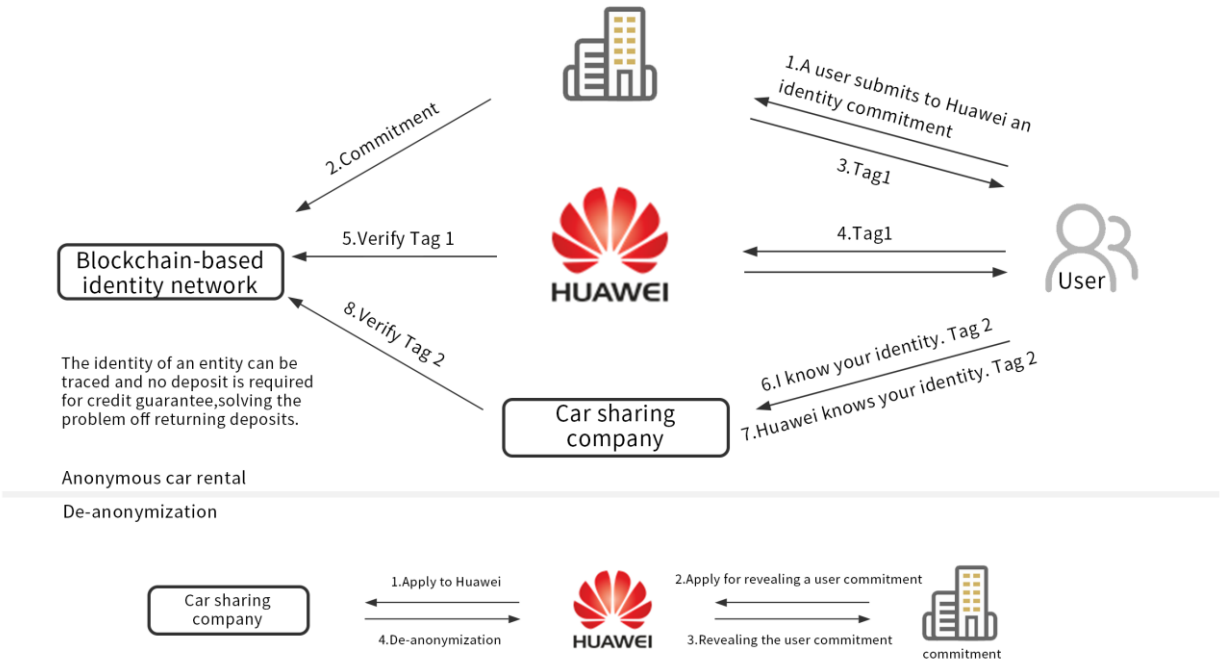
With the acceleration of the digitization process, the application areas of IAM services are expanding to include the Internet, IoT, and society more generally. In these applications, the typical role of IAM services is to ensure that legitimate users or devices can access and enjoy services safely and efficiently.

IAM services play an important role in various areas, but at present, the services also face problems such as privacy disclosure, identity fraud, and fragmentation which pose great challenges to users, devices and systems.

The introduction and development of blockchain technology provide new ideas aimed at addressing the above challenges. Applying blockchain technology to IAM services could lead to a collaborative and transparent identity management solution that will help enterprises and organizations better perform identity management and access verification.

Huawei's application in IAM services based on the blockchain technology relies on new supporting hardware, software, and blockchain platforms to provide enterprises, organizations with professional, secure and efficient IAM services. Here is how Huawei's blockchain technology is used in IAM.

Figure 4-2 Huawei's Blockchain-based Autonomous Identity Verification Solution



4.3 New Energy: Lay a foundation of trust for clean energy claim

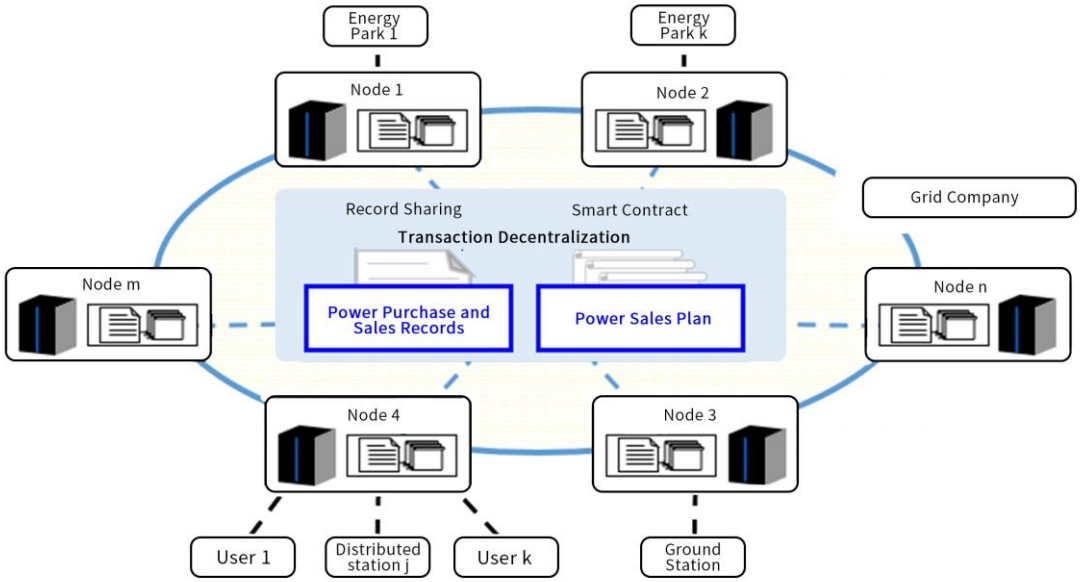
In the area of new energy, blockchain technology is changing the existing industry structure, reducing exchange costs, and retaining records more effectively. As a result, it helps promote the Internet of Energy to go digital, then to informationize and ultimately become intelligent. As an example, photovoltaic power supply is generally distributed in nature, and power plants and users can both use solar panels to store energy, using blockchain and smart metering to measure and record power generation. This enables the generation of a tamper-proof ledger of how much power has been generated.

Smart contracts can also be used to facilitate point-to-point purchase and trading of excess power. Future use of new energy for power generation will bring enormous benefits and environmental savings to society. When users purchase clean energy from a given supplier through the use of a smart contract and the contract is concluded, relevant environmental protection and charity

organizations will be able to issue certificates to users and power plants to recognize their use of clean energy, with these certifications verified and trusted thanks to blockchain.

In one new energy project, Huawei has applied blockchain technology and provides users with a clear record of each transaction and photovoltaic panels and power stations that generate the electricity they use. Users can choose their power supply sources based on the power price and the remaining available power of power stations. Meanwhile, the power generation companies can dynamically calculate the power supply and demand of each power station according to the power supply application submitted by users, and adjust the power generation strategy and price in a timely manner.

Figure 4-3 Huawei Blockchain New Energy Solution



4.4 Internet of Vehicles: Blockchain enables precise sharing of information, building a new approach to business

The Internet of Vehicles (IoV) is supported by a wide range of technologies. It is based on network connections and data collected from on-board sensors. It also requires the integrated technologies of device management and big data analytics in the cloud, plus a lot of innovative applications. In return, the increasingly integrated and accumulated technologies and applications have led to a gradual but dramatic transformation of business and maintenance models in the automobile industry. The automobile business has developed from providing single-product services to currently offering multi-party coordinated maintenance services. It can be foreseen that the value chain will develop into a complete ecosystem in the future.

In the transformation process, more and more business entities have joined the chain along the complete lifecycle of cars, and they will have increasingly close relationships with each other. The

cooperation between insurance companies and 4S stores is a typical example. But currently in the cooperation process, information is scattered across various links and in different forms. In addition, information transmission only depends on the credit and guarantees of both parties. This means that integrity, consistency, and reliability of information and efficiency of cooperation are restrained to some extent. This also increases the threshold for more business entities and third-party applications to join the value chain. Specifically, the Internet of Vehicles has the following characteristics:

- **Wide range of data**

  A large number of on-board sensors, network connections, and cloud services enable automatic and distributed data acquisition and analysis.

- **Involvement of multiple parties**

  Users/enterprises, car manufacturers, 4S stores, insurance companies, car sharing companies, second-hand markets, vehicle management departments, law enforcement agencies, innovative application developers, and more.

- **Inconsistent interests and no single trusted party**

  For example, there are conflicting interests between users, insurance companies, and 4S stores, and processes for authoritative arbitration are often ex post facto and lengthy.

- **Objective evidence needed**

  Objective evidence, such as accident records, is used by all related parties.

- **A large number of process interactions**

  For example, a traffic accident, a car transaction, and a user's service request often involve process interactions among several parties. A unified method to interconnect data can greatly increase efficiency.

It can be seen that blockchain's target problem scenarios and advantages coincide with the characteristics of the Internet of Vehicles. With blockchain technology, we can use tamper-proof data and a unified and traceable ledger to record the information of a car's entire lifecycle. The ledger can be shared among all related parties (both information providers and users), achieving decentralized information exchange. By combining more advanced technologies such as smart contracts and data interoperability on the chain, processes along the entire value chain can be automated, further improving efficiency. For example, based on a car's lifecycle information, the

blockchain can be used for scenarios such as delivery/repair/modification/maintenance, defining fault liabilities, insurance claims, and collecting proof regarding the condition of used cars.

Data privacy is the key challenge for applying blockchain to IoV, in both technical and non-technical aspects, because the IoV involves various players including users, enterprises, and regulatory authorities. Technically, it is necessary to use certain mechanisms, such as encryption and authorization, to ensure that the data related to a process can be accessed only by process participants, rather than offering unrestricted access to any data on the chain. On the non-technical side, the problem lies in whether users agree to share the data of their cars with multiple entities, such as sharing maintenance records with insurance companies. Given these problems, priority can be given to low privacy-sensitive scenarios, such as fleet management, car sharing, and process interoperability in car companies, at the initial stage.

4.5 Supply Chain Source Tracing: Blockchain helps build credibility by ensuring honest transactions

The annual crackdown on fake products on March 15 (World Consumer Rights Day) is only a tiny part of anti-counterfeiting efforts. Product traceability and anti-counterfeiting are still major problems confronting society and companies. For example, although labeled green food is supposed to be wholly organic, people still doubt the data of intermediaries as too many human factors are involved across the supply chain. This undermines credibility of the society and company. Society still faces many credibility problems, like whether food is truly organic, or whether high-end art and luxury items are genuine.

Tamper-proof data, transaction traceability, timestamp existence proof, and other features of blockchain can ensure effective accountability and prevention of counterfeiting, helping to effectively resolve disputes over tampered data between related parties of the supply chain.

Three categories of products require traceability of the supply chain: first, edible products (meat, vegetables, fish products, baby formula, Chinese herbal medicines, etc.); second, high-end consumer goods (premium wine) and high-end art (relics, jewels, etc.); third, documents and certificates (property ownership certificates, academic certificates, etc.). Blockchain can support a

source-tracing system that involves all upstream and downstream companies of the entire supply chain, so that the source, trajectory, and accountability of products can all be traced.

Taking milk as an example: At present, the source-tracing system of milk mainly includes cow owners, feed suppliers, filling equipment manufacturers, logistics companies, regulators, and sellers (stores or supermarkets). First, cow owners obtain data on daily feeding and milk tests through third-party sensors and record the data in the ledger. Based on that data, regulation or epidemic prevention teams then provide needed support to farm businesses and supplement the distributed ledger. In this way, once the data on feed provided to farmers is uploaded, it will be much more efficient to track illegal feed and determine liabilities.

Data from filling processes at equipment manufacturers and data from logistics companies can provide insights into the freshness of milk throughout the process of transportation. Data from sellers can enable ordinary users to acquire the information of all production and sales processes of the milk powder they want to buy via an app. This system of traceability eliminates the existence of illegal products in the supply chain and effectively builds the government's public credibility. Based on shared data, parties can also learn about each other's needs and cooperate more effectively for mutual wins.

In the production process, if the data of a product fails to meet the standards, a warning that requires rectification will be given immediately. In addition, the quality confirmation signature will not be generated for the failed product, so it will not be recognized by the platform. As a result, the corresponding milk product will not be sold. If the data shows that standards have not been met, then the product will be promptly disposed of to guarantee the quality of the milk. At the same time, regulators will issue certain penalties to owners who fail to guarantee the quality of the milk. The penalties could include revocation of certification or being added to supplier black lists. These measures aim to monitor operations and form a virtuous cycle, avoiding intentional counterfeiting.

4.6 Cloud-network Synergy for Carriers: Building a new business model to integrate carrier networks

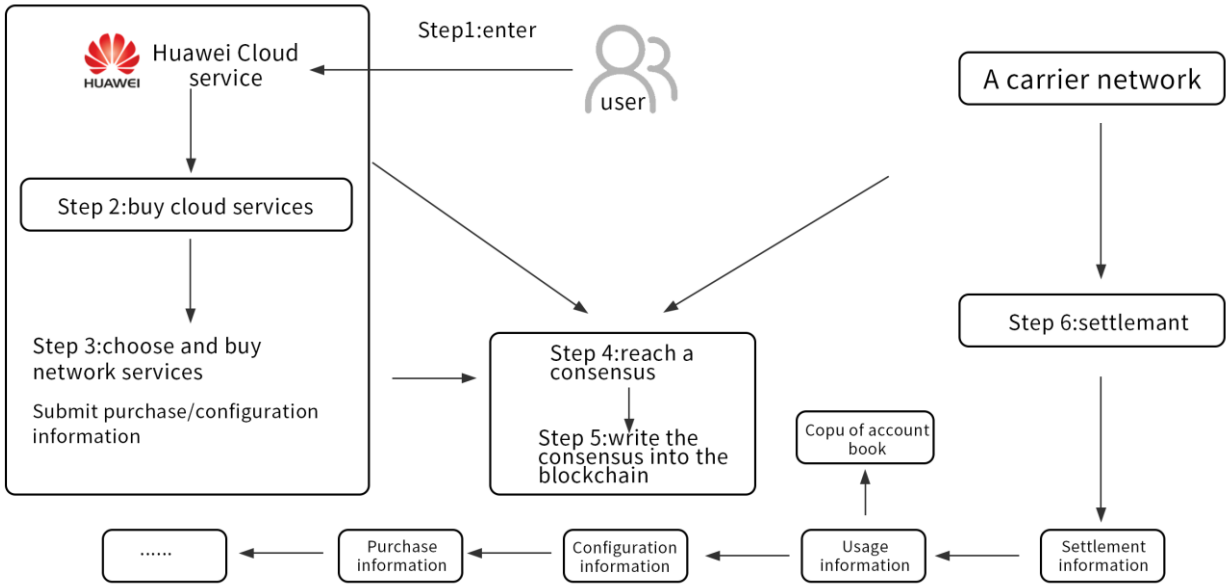
Traditionally, both networks and services are provided by carriers on the basis of "silo NaaS (network-as-a-service)" architecture. In this architecture, networks provide a supportive system, and

the cost of networks and services is settled internally. However, with the integration of ICT companies, the communications industry is opening up. In addition to carriers, a large number of OTT cloud service providers and virtual service providers can also provide telecom services. In order to meet the needs of the new business ecosystem, carrier networks need to be restructured to provide NaaS capability, which is as flexible, resilient and automated as IaaS and PaaS. These paid services can be provided to cloud service providers and virtual service providers so as to monetize network technology. For blockchain, trust can be established at a number of touch points. As the carrier network service transforms from internal settlement to external monetization, it is possible to introduce blockchain technology to multiple clouds, networks and devices and build a new business model with mutual trust.

According to a study on enterprise customers by British Telecom (BT), 90% of companies hope for "Cloud Network Automation" services, so as to ensure security and the compliance of E2E Service Level Agreement (SLA). They are also looking for E2E performance reports and E2E management and troubleshooting. The Cloud Network Automation system needs to enable customers to enter from any sales point on the cloud or network service, and to purchase services from any cloud or network service provider without the need to switch between points of access.

In response to the needs above, one possible solution is a cloud-chain business based on the consortium chain. For companies within the consortium, Huawei designs a system to authorize the sale of "multiple clouds and networks", and records and tracks their sales and configuration information. For example, if a cloud service provider needs to purchase network services, the cloud service provider can submit a request for purchase or information configuration to the blockchain, the network service provider checks and confirms the request, then both sides reach a consensus and write it into the blockchain, and thus the purchase is completed. The settlement can be made based on the information of purchase, configuration changes and usage recorded in the blockchain. The blockchain can then ensure the consistency of the ledger and support real-time settlement.

Figure 4-4 Blockchain solution with Cloud-Network Synergy



4.7 Supply Chain Finance: Mitigating financial risks and expanding financial services

Huawei focuses its efforts in blockchain applicationin on the financial industry, because this fits Huawei's core strategy of promoting digital transformation and maturation of financial services through "cloud, pipe and device", and also because blockchain facilitates the safe distribution, display, transmission and treatment of information. Generally, industries that benefit the most from blockchain are those with low trust among parties to a transaction and those with high requirements for secure and complete transaction records. One such domain is the financial industry. According to relevant consulting reports, blockchain or distributed leger technology (DLT) can save the financial industry between US$500 million and US$700 million per year. This cost reduction is mainly realized by blockchain through optimizing existing processes, such as the value chain for cross-border payments, account checking, user identity verification and anti-money laundering. It is also achieved by facilitating information sharing in supply chain finance and inclusive finance.

"Blockchain + supply chain" finance is one of the best application scenarios of blockchain in the financial industry, and represents a huge market. Supply chain finance can provide services in a systematic and structural manner. The flow of information is the key to risk control in supply chain finance. To obtain accurate, comprehensive, and effective data is the foundation as well as the difficulty of risk control in supply chain finance. Through DLT and other technologies, blockchain can build a reliable information network between companies and financial institutions in the supply chain, enabling entities to obtain information from the sources of corporate management, and ensure that E2E information is transparent and tamper-proof. In this way, all participants can share data on business flows, material flows, and capital flows through a decentralized record-keeping system.

By virtue of blockchain, banks can grant credit based on a company's actual circumstances and real-time operational data, thereby shortening the time required to collect, verify, and evaluate data. Risks are reduced, and the accuracy and efficiency of decision-making is significantly improved. Meanwhile, companies can get loans with lower costs and receive faster financial services through the supply chain finance, which promotes the smooth development and expansion of their services.

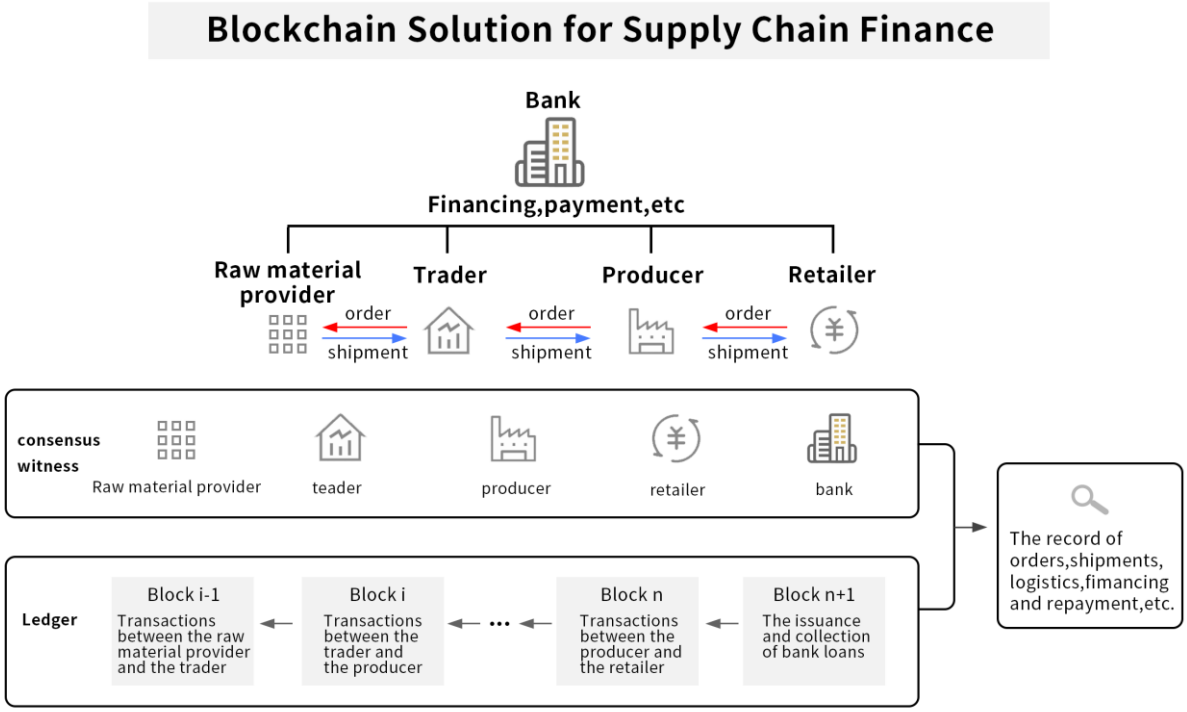
Specifically, blockchain technology can strongly support supply chain finance in the following areas:

- Because blockchain is tamper-proof, it can reliably record capital flows, material flows and business flows of upstream and downstream companies as well as the surrounding companies, making it easier for supply chain finance participants to collect and transmit reliable data, and facilitating financial institutions to access first-hand supply chain information. If IoT devices are widely deployed by companies, it's possible to outline their real operating conditions and assets on the basis of the purchase-sell-stock information system. Through their online banking system and the direct link with banks, companies can carry out capital transactions with upstream and downstream companies and provide accurate information on financial funds. This information can help financial institutions greatly simplify the credit assessment process while addressing trade financing, warehouse financing and accounts receivable financing, thereby accelerating the whole process and reducing financing costs.
- Through smart contract technology, blockchain can further secure company cooperation on top of "contractual trust", simplifying the process of business operations such as mutual guarantee, risk sharing, repurchase, and contract performance, and reduce the cost of time and money

spent in addressing potential disputes relating to breach of contract. Taking contract financing as an example, as the buyer and seller establish a medium-to-long-term supply relationship, the procurement demand for raw materials can be estimated on the basis of sales data, giving insights into supply and demand and providing an important guarantee for loan recovery. Even if the procuring company agrees to take measures to mitigate risk, financing loans could still turn into non-performing assets if risk compensation measures like repurchase and refund are not pursued. In the current practice, compliance is mainly ensured by way of contractual trust, but there may be legal disputes in the process of performance, increasing the cost of time and money afterwards. With smart contracts, when the contract content is written in the blockchain, the contract can take effect and operate automatically. This means that technology can help avoid intentional or unintentional breach of contract, thus ensuring the effectiveness of risk control and the security of financing.

The following is a depiction of how blockchain technology is applied in supply chain finance:

Figure 4-5 Blockchain Solution for Supply Chain Finance



5 Huawei Blockchain Solutions

5.1 Blockchain Service (BCS) on Huawei Cloud

The blockchain service (BCS) on Huawei Cloud is designed for enterprises, supported by open-source blockchain technologies and our rich experience in distributed parallel computing, PaaS, data management, and encryption.

The BCS is a general basic technology that is open, user-friendly, flexible, and efficient. Centering on the blockchain cloud platform, the BCS can support enterprises quickly and flexibly develop blockchain solutions and applications on Huawei Cloud. Huawei works with enterprise customers to promote the deployment of blockchain solutions and applications and to build reliable, public infrastructure and an ecosystem based on blockchain and shared success.

The BCS is delivered on Huawei Cloud, which is reliable and open, serving global customers. Huawei Cloud delivers diverse cloud computing products and customized industry solutions to enterprises. These products and services are supported by our unique technologies, low cost, flexibility, telecom-level security, and efficient, on-demand management. The BCS can be integrated with existing Huawei Cloud products and solutions to support enterprises move towards the era of cloud in a secure, efficient, and tamper-proof approach, and quickly deploy new solutions and applications.

5.1.1 Design principles and positioning of BCS

Design principles

- **User-friendly**

It's not an easy task to deploy an enterprise-level distributed blockchain system based on open-source components. It requires professional blockchain knowledge, and the design and configuration are complex and error-prone. The BCS can help enterprises solve these challenges through automated configuration and deployment of blockchain applications and blockchain life-cycle management. This makes the blockchain system easy to use for customers, allowing them to focus on innovation and development of applications.

- **High openness**

  The BCS is built on open-source tools such as Hyperledger, Kubernetes, and Docker to support users in the deployment of a sophisticated blockchain system. We use open-source resources to develop better products and services, and contribute to open source communities by investing in and leading relevant projects.

- **Security and reliability**

  A focus needs to be on independent innovation based on open-source technologies. We hold patents and have technical experience in fields like consensus algorithms, homomorphic encryption, zero-knowledge proof, telecom-level cloud security, high-speed network connectivity, and mass storage. The BCS is delivered based on the strong competence of Huawei Cloud – complete capabilities of management of users, keys, and permissions; isolation management; reliable fundamental cyber security; and operational security.

- **Cloud-blockchain integration**

  Blockchain can show its real value when it is adopted in specific enterprise applications or solutions for specific industry cases. Huawei Cloud provides the resources required for the development of blockchain, diverse cloud computing products, and customized industry solutions. The integration of BCS and Huawei Cloud can bring more convenience, value, and possibilities to enterprises.

- **Collaboration and cooperation**

  Huawei Cloud is focused on the building of fundamental blockchain technologies and platform capabilities. We are committed to the collaboration with industry partners on reliable blockchain solutions and the ecosystem. Huawei aims to help customers deploy blockchain solutions and achieve greater business success.

Product purpose

The BCS is positioned as a technology enabler for the growth and innovation of enterprises. Huawei provides enterprises and developers with one-stop blockchain platform services including planning, purchase, configuration, development, product launch, and O&M. Leveraging the BCS, enterprises can quickly build a secure, reliable, high-performance blockchain system based on their services. The blockchain system is cloud-based with features of on-demand charging, flexibility, and visualized data management, leading to a significant increase in usability and reduction in initial and ongoing usage costs.

5.1.2 Logic architecture of BCS

The BCS is designed based on the principles mentioned above to solve enterprises' challenges of blockchain system in terms of performance, function completeness, scalability, and usability. It is supported by innovative technologies like layer-specific architecture design, cloud-blockchain integration, optimized consensus algorithms, containers, micro-service architecture, and scalable distributed cloud storage.

The BCS contains 4 layers and 2 stacks:

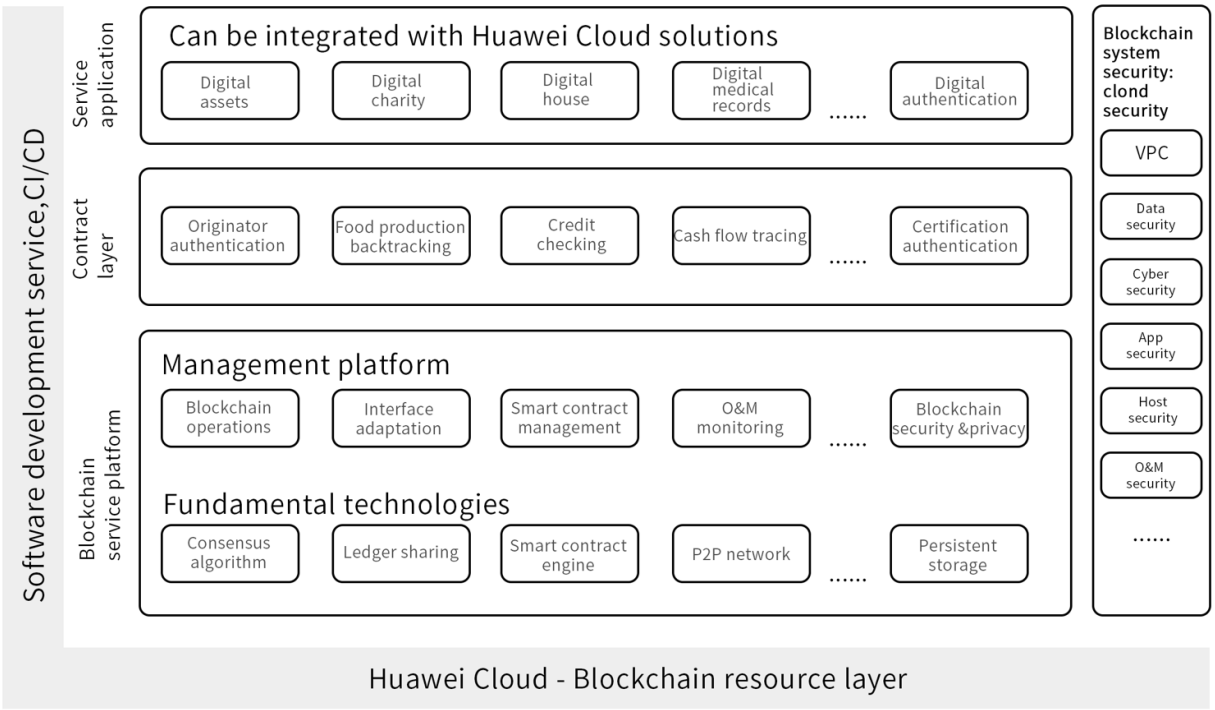
- Blockchain resource layer: Refers to the IaaS and PaaS of Huawei Cloud, which provide the scalable storage and high-speed network, and support on-demand purchase, flexible scalability, and self-healing nodes.
- Blockchain service platform: Extremely reliable and scalable. In order to meet market demand, it will gradually extend support to outstanding blockchain frameworks like Corda and Ethereum. It helps enterprises quickly build a secure, reliable, and high-performance blockchain system with low costs for upper-layer applications.
- Contract layer: Currently supports Hyperledger smart contracts. Users can create different smart contracts according to different use cases. Later we will work with partners to build a contract library for general use cases, such as supply chain management and backtracking, supply chain finance, digital assets, digital charity, and Internet insurance. Enterprises can leverage the library to quickly create contracts for specific use cases.
- Service application layer: Provides reliable, secure, and agile blockchain applications for end users. Users can leverage various Huawei Cloud solutions (e.g. supply chain finance solution,

game industry solution, supply chain backtracking solution, and new energy industry solution) to deploy applications with the contract layer together.

- Blockchain system security: Supported by Huawei Cloud Security. The most important features of consortium blockchain are the node controllability and ledger security. Huawei Cloud Security can provide comprehensive protection for blockchain nodes, ledgers, smart contracts, and upper-layer applications.
- Software development service: Supports users in end-to-end CI/ CD (Continuous Integration/Delivery) processes for service applications and smart contracts from development, testing, to deployment.

The layer-specific architecture design of Huawei Cloud blockchain services can help enterprises quickly and conveniently deploy blockchain solutions. See the figure below for the logic architecture framework:

Figure 5-1 BCS Logical Architecture Framework



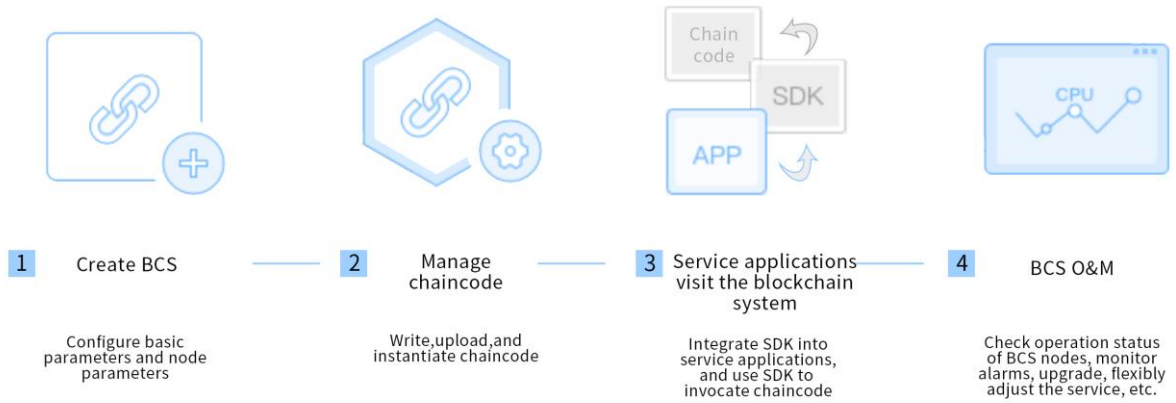
5.1.3 Functions of the BCS platform

The BCS platform is the main part of Huawei Cloud blockchain service, and is comprised of two parts: the BCS management platform and the underlying blockchain technology.

BCS management platform

Huawei provides enterprises with system-wide blockchain services, including fast creation, deployment, chaincode management, and monitoring, as illustrated below:

Figure 5-2 Life Cycle Management of Huawei BCS



The following modules are designed for the life cycle management of the BCS:

- **BCS operation modules**
  - BCS configuration

    Huawei BCS provides an interface for configuring a few simple parameters to complete BCS deployment, such as blockchain service name, Kubernetes cluster (deploy the blockchain service) name, flexible file name, consensus algorithm type, and node parameters.

  - BCS deployment

    After BCS parameters are configured, users can click the Confirm button to rapidly complete BCS deployment. Then, based on the configured BCS parameters and built-in best practices, the PaaS platform automatically deploys each node of the blockchain to the specified cluster through the Docker container in Kubernetes. Comparing to self-building blockchain system, it's

faster that only five minutes are taken to complete the deployment of an enterprise blockchain system on BCS.

- BCS status monitoring

From the BCS list, the administrator can check the type, number, and status of nodes in the BCS to easily learn about the status of BCS in real time.

- BCS node management

The administrator can purchase service resources on demand according to service requirements and loads, and dynamically adjust the number of peer nodes and order nodes when the system is running. This effectively lowers the initial and operation costs for enterprises. Additionally, when any node goes wrong, the system automatically restores the node to ensure that the blockchain applications are reliable.

- Management of BCS consortium members

Huawei Cloud BCS supports consortium blockchain. Members of the consortium are independent tenants of Huawei Cloud, and they manage their own node and ledger separately. Based on the unique tenant member invitation mechanism of Huawei BCS, the consortium initiation member can invite other Huawei Cloud tenants by their accounts to join the blockchain system, and increase the consortium members as needed. Subsequently, the BCS will add a consensus-algorithm-based mechanism through which nodes automatically join the consortium. In this way, the consortium members can be managed more dynamically.

- **BCS smart contract management**

The smart contract is also known as the chaincode. The chaincode encapsulates service network transactions in the code and runs in a Docker container. Tenants can develop and test software on Huawei DevCloud or offline. Huawei Cloud BCS currently supports the Go programming language and will support Java and more in the future.

a. Smart contract installation and instantiation

The chaincode must be uploaded and installed on the peer node and then instantiated on the channel. The instantiation process needs consensus of the participants and will be recorded in the blockchain. After the instantiation, the chaincode will run in the Docker container.

All channel members must install the chaincode on each peer node that runs the chaincode, but only need to instantiate the chaincode on one peer node. To use the same chaincode, channel members must provide the same chaincode name and version during installation.

b. Smart contract triggering

After the smart contract is instantiated, contract execution can be triggered by an external condition, e.g. by schedule, by event, by transaction, or by other means. Triggering by schedule refers to the process through which contract invocation is automatically triggered at the time specified in the contract after nodes reach a consensus on the triggering time. Contract invocation by event, by transaction, and by others means are processes of triggering contract execution during a new request for consensus.

c. Smart contract change and clearance

When contract terms need a change, all participants must sign and then execute the updated contract. Alternatively, they can relocate or clear the contracts that are no longer needed due to expiration or service requirement changes. The update and clearance can only be achieved with consensus of multiple nodes.

- **O&M monitoring**

For tenants to rapidly and correctly identify the system operation status and support their other O&M needs (e.g. application upgrade), Huawei BCS provides a complete, and visualized O&M monitoring system that offers functions such as monitoring and alarm.

Monitoring

The monitoring function supports collection and visualization of system status data. System status data includes information on system visits, duration, node health, and usage of underlying hardware resources (CPU, memory, storage). Through visualized monitoring, the status of the entire blockchain system can be monitored in real time.

Alarms

The alarm function keeps relevant personnel notified, via email or other means, of serious issues in the system, such as fraudulent nodes, ledger manipulation, and machine malfunction, so that they can be promptly dealt with.

Technologies that underlie blockchain

- **Consensus algorithm**

There are two types of consensus mechanisms distinguished by the consensus process: the first is probabilistic consensus, which is verified by the engineering science; and the other is absolute consensus, which verifies itself. Huawei Cloud BCS is enterprise-oriented, so it adopts the second type of consensus mechanism. The BCS provides several secure and efficient consensus algorithms for users to choose from for different scenarios and different security and performance requirements:

- Solo mode: Only one consensus node is required; it's easy and fast to use; it's suggested to be used for development and testing.
- Kafka/ZooKeeper-based fast consensus algorithm: no specific requirements for number of consensus nodes; crash of less than half of the nodes is tolerated.
- FBFT (fast Byzantine fault tolerance algorithm): 3f+1 nodes are used; Byzantine fault on a maximum of 1/3 of the nodes is tolerated.

Detailed comparison of the consensus algorithms are as follows (f refers to fault):

Table 5-1 Comparison of Consensus Algorithms

Consensus algorithm	Solo	Kafka (crash fault)	FBFT (byzantine fault)
Number of nodes	1	2f+1	3f+1
Faulty nodes tolerance	None	Crash of a maximum of 1/2 of the nodes	Byzantine fault on a maximum of 1/3 of the nodes
Transaction performance	Average	10000+ TPS	2000+ TPS

- **Shared ledger**

  Three types of ledger are involved:

  - Block ledger: records transactions of smart contracts, saved in a file.

- Status ledger: records the latest status of smart contract data, saved in the KV (Key-Value) database.
- Historical ledger: records all historical indexes of smart contract execution transactions, saved in the KV database.

- **Persistent storage**

  Huawei BCS stores the shared ledger to Huawei Scalable File Service (SFS). The SFS supports users' Elastic Cloud Server (ECS) with fully hosted shared file storage, which complies with the Networked File System (NFS) protocol; is scalable to the Petabyte (PB) level; offers expandable performance; and supports massive data and high-bandwidth applications.

- **P2P network**

  Gossip protocol, used for data dissemination and exchange among nodes, is a common protocol in the area of P2P. The nodes in a BCS network synchronize and disseminate data by gossip protocol. It is efficient, highly fault-tolerant, and has a convenient structure.

- **Smart contract engine**

  The smart contract engine is operated in the Docker used for network isolation and security. Through Huawei blockchain services (BCS) provided by Huawei Cloud, real-time monitoring of high risk function calls and Docker container escape is made possible, to mitigate the risk that smart contract present to the blockchain.

- **Blockchain security and privacy**

  Blockchain security and privacy are priorities of Huawei BCS. Apart from the security measures of Huawei Cloud and Hyperledger, Huawei BCS also supports the following security and privacy measures:

  - Encryption algorithms and diverse enterprise signature strategies: Such as SM2, SM3, and SM4, and many methods of authentication for enterprise users. BCS protects the key by providing a hardware-based, trusted computing environment. It is much more secure than common servicesHAdditive homomorphic encryption:used for protecting the privacy of transaction data.
  - Zero-knowledge proof: Used for protecting the privacy of transaction participants.

- Huawei BCS provides a full CA management system to every tenant to ensure the security of authentication and data transmission and to meet the privacy protection requirements of the transaction.

- **Access adaption**

  Huawei BCS currently supports business applications calling the smart contract via native Fabric SDK. Soon, SQL API access will be provided. Users can choose SDK or SQL API access to call the smart contract to access the blockchain.

5.1.4 BCS security advantanges

Consortium chain has a stricter access control than public chain and is in line with national security standards. These two characteristics ensure the access authentication and the regulatory rules of the chain can meet the requirements of relevant national regulations. Consortium chain can also improve the transaction speed while maintaining a trusted, secure environment. Based on cloud security, Huawei BCS provides a highly secure environment for blockchain services in the following areas:

- **A secure, trusted cloud platform: security and standards compliance**

  Huawei Cloud has obtained over 20 certifications globally, including for security protection for Grade III information system of the Ministry of Public Security of PRC, TRUCS certification and Gold O&M, CSA STAR Gold Certification and C-STAR, and PCI-DSS certification. We will continue to work to achieve compliance in different regions and different industries, aiming to ensure the security and standards compliance of Huawei Cloud.

- **Identity and access control**

  Users of Huawei BCS are public cloud tenants. Huawei gives tenants the capability of access control via Identity and Access Management (IAM). Enterprise tenants can manage users and security credentials (e.g. access keys) and control the rights of users and their rights to access cloud resources by using IAM. This enables system administrators to manage user accounts (e.g. employees, systems, and applications) and to control the rights of users to utilize resources. In the case of shared operative resources, IAM can give minimum privileges to users according to their needs to avoid sharing accounts and keys. It also ensures the security of user accounts and reduce information security risks of the enterprise through log-in verification, password policy, and access control lists.

- **Data isolation of the blockchain tenants**

  Huawei Cloud isolates data through Virtual Private Cloud (VPC). VPC helps to isolate the network of different tenants to avoid the unauthorized acquisition of data. Tenants can use VPC to fully manage its own visual networks and achieve the complete isolation of the layer 2 and 3 networks. Tenants can use CloudVPN or Direct Connect to connect VPCs and traditional data centers on their intranets to smoothly transfer applications and data from intranets to the cloud. In addition, tenants can use the security group function of VPC to develop more specific security and access rules so as to meet their specific requirements for data isolation.

  Members of blockchain alliances are treated as independent tenants in Huawei BCS and tenants are operated in VPCs respectively. The VPC isolation mechanism is used to ensure the data and right isolation of every blockchain alliance member and to facilitate the establishment of multicenters on the blockchain. It also helps to further boost the strengths of blockchain in having multiple stakeholders, enabling multilateral consensus, being tamper-proof, and being secure.

- **The security of ledger storage**

  Through Huawei BCS, tenants' scalable files in the ledger are stored on the cloud. A number of measures are taken to safeguard the security of the ledger while maintaining the scalability of the files.

  - **Key protection and management:** Key Management Service (KMS) is used in the management of the scalable file storage system. It is a secure, reliable, and easy-to-use key hosting service, which can help users manage keys and ensure their security. KMS develops and manages the key via Hardware Security Module (HSM), which keeps the key within hardware to avoid disclosure of the key and to ensure its security. It conducts access control and traces the log of every operation over the key. KMS also records every use of the key for auditing and compliance needs.
  - **Confidentiality of the data**: KMS is used for the development, management, and disposal of the Customer Master Key (CMK). Huawei Cloud provides full encryption service and generates three copies as a backup. As a result, the reliability of data can be ensured and data durability is as high as 99.99995%. Volume backup Service (VBS) also supports the backup and recovery of the elastic volume and generation of a new scalable file based on the copy of the original scalable file.

- **Deletion and disposal of data:** Huawei Cloud protects data from being leaked during and after the process of deletion, including the deletion of memory and disk data, soft delete, and the scrapping of physical disks.

- **A complete protection system provided by Huawei Cloud**

  The above security measures are the most important security measures provided by Huawei Cloud to the BCS. A complete protection system includes but is not limited to coverage of the following: cyber security, DDoS attack, application security (WAF and security scanning), and the security of virtual machines, containers, data, and operations. This system can protect the blockchain from all varieties of security risks.

5.1.5 The technical features and strengths of Huawei BCS

Huawei BCS is based on the secure, reliable, and high-performance Huawei Cloud. With the simplicity, usability, maturity, reliability, and integration of the cloud and blockchain, Huawei BCS provides enterprises and developers with enterprise-level blockchain services using its unique architecture. It has the following features and strengths:

High cost performance

- One-stop development and testing

  Huawei DevCloud solution can develop, test and deploy blockchain applications and code for smart contracts, simplify CI/CD procedures, and reduce development and integration costs for users. DevCloud is an R&D cloud platform that integrates Huawei's R&D practices, advanced R&D philosophies, and tools, providing R&D tools to developers and making software development simpler and more efficient.

- Fast deployment

  The deployment and operation of enterprise-level commercial blockchain services can be completed in as little as five minutes. Huawei BCS helps to cut 80% of the development and deployment cost of a blockchain developed by an enterprise itself.

- Pay as you go

  Users can adjust resources and pay according to their demand, which can help reduce 60% of the initial and operating cost.

- Whole-process O&M and monitoring

Huawei BCS and Huawei Cloud provide the customers with a whole-process monitoring service of the system status, functions, transactions, O&M, and warning, reducing O&M costs for users.

High performance

- Efficient access

  With its ability to access high-speed networks, and its high concurrency and fast access, Huawei Cloud can satisfy users' needs for efficient access to the blockchain.

- High-performance consensus

  Huawei BCS provides users with many high-performance consensus algorithms (Solo, the Kafka-based CFT, and FBFT). FBFT is a highly optimized version of BFT and is a balanced choice of security and efficiency. Users can choose from 2000+TPS and10000+TPS as required by business scenario.

- Second-level consensus

  Users can set the transaction speed to seconds or even lower to meet the performance requirements of the business.

- High-speed storage

  Through Huawei BCS, blockchain ledgers are stored in a highly scalable file on Huawei Cloud so that user requirements for massive and rapid-access storage can be met. Huawei will also gradually enhance the storage capability of blocks and relational DBs to meet user requirements for storage speed from various angles.

High security

Security requirements of the blockchain:

- The consortium blockchain should be controllable (e.g. nodes and ledgers) and meet regulatory and entry requirements.
- Using the distributed ledger technology to generate tamper-proof and encrypted transaction data.
- Transactions are traceable, and indisputable
- User privacy: Transactions are performed anonymously; connected transactions are forbidden.

- Transactions are visible and auditable.

Huawei BCS is able to protect the blockchain in three ways:

- Huawei's cloud-based security services ensure the blockchain system operates reliably.
- Hyperledger's security system is able to generate tamper-proof transaction data and protect user privacy with the certificate management function and a chained-block data structure.
- Huawei's BCS satisfies users' further security and privacy requirements with secret hardware protection key, homomorphic encryption, and zero-knowledge proof solutions.

High availability

- High-availability architecture

  The BCS is built on Kubernetes and Docker platforms and runs in Huawei's high-availability cloud. It can be initiated rapidly. It is scalable (e.g. nodes and members) and auto-recoverable (e.g. nodes). These properties ensure that the blockchain system is highly available.

- High-availability access and storage

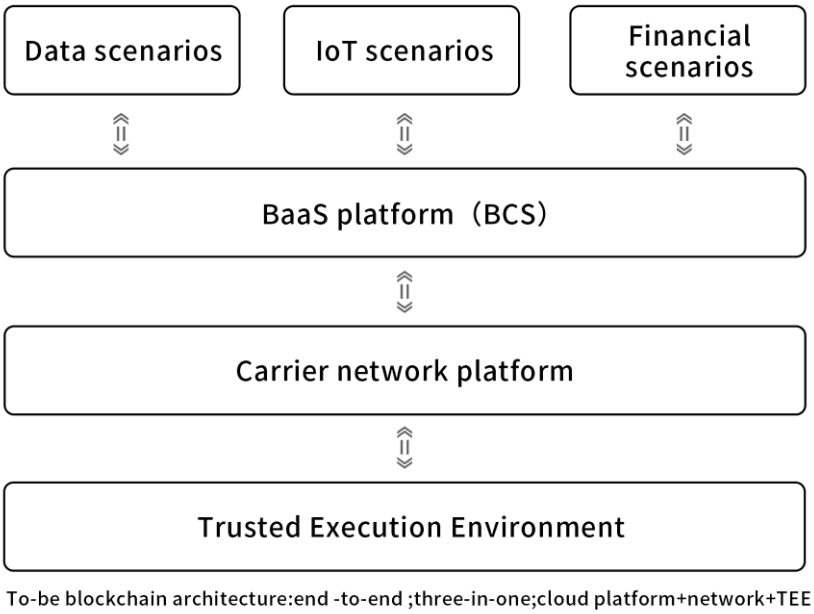
  The BCS supports software development kit (SDK) and SQL-API calls and can therefore meet user needs across a variety of scenarios. Ledgers on the blockchain are securely stored on the cloud-based elastic storage system. The system is secure, elastic, and scalable, has a large storage capacity and can back up files automatically. The BCS also offers two data storage options for users to choose from: the file storage and the relational database solutions. The high-availability relational database allows users to run their blockchain stably and smoothly.

- Supporting global deployment and multiple deployment methods

  Huawei's cloud-based blockchain services are being increasingly deployable across different management domains of Huawei's cloud as well as the joint cloud across the world. Its global deployment capability can make a multi-centered blockchain that is secure and highly available. Companies and users can either deploy their blockchain as a consortium-based or private system as needed.

5.2 The Blockchain System Architecture Proposed by Huawei

Figure 5-3 Blockchain System Architecture Proposed by Huawei



With the blockchain platform as the center ,Huawei has proposed an end-to-end blockchain system architecture that integrates network, TEE(devices+chips), and blockchain platforms. The end-to-end blockchain solutions that integrate software and hardware are more responsive and secure.

TEE: Hardware can be used to optimize the operation procedures of blockchain. This combination of hardware and software greatly improves the security and performance of blockchain.

The blockchain has not been commercially deployed on a large scale for security and performance reasons. All the blockchains deployed so far have balanced between these two and only issue security and performance alerts for software, such as the consensus algorithm and mechanism. However, future blockchains will see significant improvements in security and performance with the introduction of chips level TEE that are specially designed for the blockchain.

Embedding chips into the blockchain represents a great step forward. We are ready to work with industry partners to improve the security and operational efficiency of the blockchain.

Networks need to be incorporated into blockchain as an important role

Networks will face two major issues as blockchain develops: As technologies such as Hyperledger evolve, blockchain technology is being used in more and more scenarios. It is now able to accommodate demands for an increasing number of nodes. The current P2P network architecture might work well with a limited number of blockchain nodes. However, when these nodes reach into the hundreds, using P2P to send large numbers of broadcasts and messages is inefficient and causes a waste of ICT infrastructure and broadband resources.

In its early days, blockchain was decentralized by design to minimize unnecessary impacts from central crashes and to improve data reliability. As the consortium chain becomes more widely deployed, we are seeing a shift from decentralized blockchains to multi-centered blockchains. Blockchain only solves the problem of consistency of ledgers of data centers in distributed deployment. No consideration is given to the reliability of carrier networks.

Huawei believes that considerations of network equipment could be incorporated into blockchain technologies to increase network reliability. As edge computing becomes more prevalent, some current network equipment is gaining the ability to process data. With edge computing capabilities, networks can incorporate blockchain, thereby assuring equipment security. Network information will be made a link in the blockchain. This will alleviate processing and storage pressure faced by cloud platforms from a large number of nodes, while also enabling certification of IoT devices, to allow legitimate access to networks by large numbers of IoT devices in the future. An important consideration for the future is how the design of networks will evolve along with blockchain.

6 Summary: Huawei's Views and Recommendations

Blockchain is an open technology to support digital value transfer, enabling new types of networks powered by decentralized trust. We see the following:

- 2018 is the first year that will see the wider-scale deployment of blockchain. Before a complete set of blockchain standards are developed, piloting the blockchain in different industries is a top priority, such as in government data storage, IoT-based logistics, connected cars, carriers' cloud-network synergy, and supply chain finance. Blockchain can create a fair and trusted business environment for these industries.
- From a the technical perspective, security is an important issue when constructing blockchains. The Chinese national cryptographic algorithm standards will be used for the majority of blockchain applications in the Chinese market. Looking ahead, blockchain system architecture at Huawei will consist of three layers (cloud, pipe, and devices) and will provide a highly reliable and secure system by using the combination of hardware and software protection.
- For industry ecosystems, the blockchain is likely to be mainly deployed in China, the US, and Europe. It won't be a temporary technology. To truly lead the pack in the industry, we need the support of clear and favorable industry policies from the government. Now, central and local governments in China are actively creating a favorable technological and business environment for the blockchain industry to grow.

The following are some recommendations to facilitate the rapid development of the blockchain industry and build a trusted society:

- **Work with alliance and industry partners to facilitate the implementation of blockchain standards**

  Blockchain technology is still young. In 2017, progress has been seen but still slow in blockchain standards all over the world, posing a major obstacle for the blockchain to develop. Security is at the heart of blockchain technology, but problems in terms of algorithm and system standards still exist. We recommend that national organizations lead the development and implementation of blockchain standards in key areas (e.g. cross-chain blockchain, and encryption algorithm) with support from industry players, to accelerate the development of the global blockchain industry.

- **Create an incubation environment for the blockchain industry to grow**

  Create an incubation environment for the blockchain to grow by encouraging large enterprises as well as government to pilot the technology, discover problems, and make improvements. Today, some blockchain projects are still more talk than action, and are intended to attract investment funds through pure concept hype. This is not conducive to blockchain industry growth. Therefore, national governments and key enterprises should play an active role in driving the application and development of the blockchain technology and improving the industry environment.

- **Develop clear policies on the application of blockchain technology**

  In China, policies on the blockchain industry are being implemented on a small scale in several provinces and cities. With the development of Internet+ in mind, the government needs to develop clear policies to foster the growth of the blockchain industry, thereby supporting blockchain technology, shaping blockchain standards, developing blockchain solutions, and establishing showcase projects. In particular, the government should balance allocation of decision-making authority and exercise of oversight to support the positive development of blockchain.

- **Actively take part in open source communities to promote barrier-free exchange of blockchain technologies between businesses**

  We should engage in more activities in international blockchain communities and improve our blockchain capabilities, to bring enterprises in different sectors together to work on the blockchain technology and solutions. We also encourage enterprises to contribute more to

blockchain technology. Partnerships founded on cooperation and contribution will facilitate shared success across the global blockchain market.

