International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Y

Supplement 62
(07/2020)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Overview of blockchain for supporting Internet of things and smart cities and communities in data processing and management aspects

ITU-T Y-series Recommendations – Supplement 62

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Supplement 62 to ITU-T Y-series Recommendations

Overview of blockchain for supporting Internet of things and smart cities and communities in data processing and management aspects

Summary

Supplement 62 to ITU-T Y-series Recommendations provides an overview of blockchain aspects related to data processing and management (DPM) for the Internet of things (IoT) and smart cities and communities (SC&C). There are many benefits and challenges to addressing blockchain, IoT and sustainable SC&C together.

Blockchain presents opportunities for disruptive innovations, which enables global businesses to conduct transactions with less friction and more trust and efficiency. Blockchain shows great promise across a wide range of business applications in many fields, including IoT and SC&C.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y Suppl. 62	2020-07-16	20	11.1002/1000/14369

Keywords

Blockchain, DPM, Internet of things.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 62 to ITU-T Y.4000-series

Overview of blockchain for supporting Internet of things and smart cities and communities in data processing and management aspects

1 Scope

This Supplement provides an overview of blockchain related to data processing and management (DPM) for supporting Internet of things (IoT) and sustainable smart cities and communities (SC&C).

The scope of this Supplement includes analysis of:

– the advantages, challenges, key features and a common reference model of blockchain from the DPM perspective for supporting IoT and SC&C;

– key issues for blockchain to support IoT and SC&C from the DPM perspectives;

– the effects when using blockchain to support IoT and SC&C from the DPM perspective.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 application [b-ITU-T Y.2091]: A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface.

3.1.2 blockchain [b-ITU-T FG-DPM TR D3.5]: A peer to peer distributed ledger based on a group of technologies for a new generation of transactional applications which may maintain a continuously growing list of cryptographically secured data records hardened against tampering and revision.

NOTE 1 – Blockchains can help establish trust, accountability and transparency while streamlining business processes.

NOTE 2 – Blockchains can be classified as three types (i.e., public, consortium and private) based on the relationship of the participants and the way to provide services.

NOTE 3 – Definition compatible with [b-ISO 22739].

3.1.3 blockchain data [b-ITU-T FG-DPM TR D3.5]: The data in a blockchain, such as distributed append-only ledgers, state information, permission policies etc.

NOTE – Blockchain data may be distributed and be stored in blockchain peers. A blockchain peer may store whole or part of the data in a blockchain.

3.1.4 blockchain peer [b-ITU-T FG-DPM TR D3.5]: A functional entity or physical entity (e.g., device, gateway and system) which utilizes blockchain-related functionalities (e.g., executing transactions, and maintaining the blockchain data) in peer to peer communications.

3.1.5 blockchain transaction [b-ITU-T FG-DPM TR D3.5]: An operation (e.g., deploying, invoking and querying results of blockchain contracts) in a blockchain in which an authorized end user performs operations (e.g. reading/writing blockchain data, invoking a blockchain contract).

NOTE – Definition compatible with [b-ISO 22739].

3.1.6 consensus [b-ITU-T FG-DPM TR D3.5]: Agreements to confirm the correctness of the blockchain transaction.

3.1.7 Internet of things (IoT) [b-ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.8 service [b-ITU-T Y.2091]: A set of functions and facilities offered to a user by a provider.

3.1.9 smart contract [b- ITU-T FG-DPM TR D3.5]: Embedded logic that encodes the rules for specific types of blockchain transactions. A smart contract can be stored in the blockchain and can be invoked by specific blockchain applications.

NOTE – Definition compatible with [b-ISO 22739].

3.1.10 smart sustainable city [b-ITU-T Y.4900]: A smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social, environmental, as well as cultural aspects.

NOTE – City competitiveness refers to policies, institutions, strategies and processes that determine the city's sustainable productivity.

3.1.11 thing [b-ITU-T Y.4000]: With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks.

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

API	Application Programming Interface
DPM	Data Processing and Management
DPoS	Delegated Proof of Stake
FBA	Federated Byzantine Agreement
ICT	Information and Communication Technology
IoT	Internet of Things
IT	Information Technology
NFV	Network Functions Virtualization
P2P	Peer to Peer
PBFT	Practical Byzantine Fault Tolerant
PoS	Proof of Stake
PoW	Proof of Work
SC&C	Smart Cities and Communities
SDN	Software-Defined Network

SQL Structured Query Language

VM Virtual Machine

5 Conventions

None.

6 Overview of convergence of blockchain and IoT and SC&C from the DPM perspective

Blockchain is a type of peer to peer (P2P) distributed ledger based on a group of technologies, e.g., P2P communication, distributed ledger and crowding consensus, which maintains a continuously growing list of cryptographically secured data records as hardened against tampering and revision.

NOTE – Blockchain is also to be seen as a decentralized system which supports P2P distributed ledgers. If not otherwise specified in this Supplement, the keyword "blockchain" refers to a P2P distributed ledger, and also refers to a decentralized system which supports a P2P distributed ledger.

Some blockchains are reliant on the exchange of cryptocurrencies with anonymous users on a public network (e.g., Bitcoin [b-Bitcoin], Ethereum [b-Ethereum]); and others are for business working on a permissioned network (e.g., Hyperledger [b-Hyperledger], Enterprise Ethereum [b-Enterprise Ethereum]), with known identities and without the need for cryptocurrencies.

Blockchains show great promise across a wide range of business applications in many fields, e.g., IoT and SC&C, finance, accounting, banking, healthcare, government, manufacturing, insurance, retail, legal, media and entertainment, and supply chain and logistics.

6.1 Main advantages and challenges of blockchain from the DPM perspective

It is a distinct characteristic of blockchain to process data by a decentralized mechanism. Some or all participants in a blockchain can store and maintain data in the blockchain in whole or in part. This decentralized processing has the advantage that IoT data can be managed by the blockchain. However, processing the data stored in a blockchain can be challenging.

The main advantages of blockchain from the DPM perspective include the following.

– In a blockchain, there is no single authority that can approve the transactions or set specific rules to have transactions accepted. This allows the blockchain to be trusted to process and manage data.

– The participants in a blockchain can jointly cooperate to create, store and maintain their data by themselves. The algorithms of crowding consensus and decentralized storage of the blockchain allow the participants to fully trust the transactions and relevant data.

– In a blockchain, data are secure and immutable to change, although the blockchain works in an untrusted environment. The data in a blockchain can only be extended and previous records cannot be changed. The participants can thus trust the blockchain to store their data.

– In a blockchain, the transaction processes are transparent to the participants. This can also provide a certain amount of privacy protection for the participants. Every participant involved in a transaction can contribute to the transaction and access the transaction record. If the actual content of a transaction record is encrypted, the privacy of the originator of a transaction and the counterparties to the transaction can be protected, although other participants can access the transaction record.

– In a blockchain, it is not easy for data to be lost. The data may be stored by some or all the participants in the blockchain.

– In a blockchain, the participants can deploy or invoke smart contracts to make transactions and to store data in decentralized mode automatically.

With the rapid growth of the number of participants in a blockchain, the blockchain will face some key challenges when it processes and manages data, including the following.

– How many of the participants can participate in a transaction? As the number of participants grows, the speed and efficiency of establishing consensus and making transactions may decrease rapidly and become more and more unacceptable.

– How much of the data should be duplicated and stored in the blockchain? Too much data duplication wastes storage resources and network bandwidth, and slows the blockchain transaction process.

– Which data should be stored in the blockchain? The participants may not provide enough storage volume to store all the data of a blockchain.

– How could changes be made to improve the speed and efficiency to find and access data of a blockchain? It is not easy to search and access data that are stored in huge numbers of blocks in a blockchain.

6.2 Main challenges of DPM in IoT and SC&C

There have been many visible successes in many fields for IoT and SC&C, especially for high-value applications, e.g., smart meters and e-health. However, there are some key challenges for DPM that IoT and SC&C must face, especially in the forthcoming era of internet of everything, e.g:

– high cost of connectivity and low scalability, if using current centralized connection solutions, to connect the huge number of things (both physical and virtual) (see [b-ITU-T Y.4000]);

– huge numbers of IoT devices means huge volumes of IoT data, presenting problems in maintaining a balance between data storage and accessibility;

– unease about building trust in the untrusted Internet for diverse IoT devices, many of which, and their data, are too vulnerable to be trusted;

– lack of solutions to meet the need to maintain long life-cycle IoT devices and IoT data;

– lack of standards for authentication and authorization of IoT devices and IoT data.

6.3 Main benefits and challenges of blockchain for supporting IoT and SC&C in DPM

There are many benefits from making blockchain, IoT and SC&C work together. Some key benefits, including building trust, reducing costs, accelerating transactions and increasing security, are described as follows.

– Blockchain offers new ways for IoT and SC&C to automate business and data processes among participants, without previously setting up a complex and expensive centralized information technology (IT) infrastructure. Data protection of blockchain fosters stronger working relationship among participants and provides greater efficiency as the participants take advantage of the protected data.

– Making IoT, SC&C and blockchain work together enables IoT devices to participate in blockchain transactions. Specifically, IoT devices can send data to a public, consortium or private blockchain for inclusion in shared transactions with distributed records that are maintained by consensus and cryptographically hashed. The distributed replication in blockchain allows business partners to access and supply IoT and SC&C data without the need for central control and management.

– The distributed ledger in a blockchain makes it easier to create cost-efficient business networks for IoT and SC&C where virtually anything of value can be tracked and traced, without requiring a central point of control.

– Blockchain is good at data privacy protection. All data in a blockchain can be encrypted, which thus restricts access to authorized stakeholders only. Blockchain with IoT and SC&C

together becomes a potential game changer by enabling the ability to invent new styles of digital interaction, enabling IoT devices to participate in blockchain transactions, as well as creating opportunities to reduce the cost and complexity of operating and sustaining business.

In spite of all the benefits mentioned in the previous paragraph, there are some key challenges to blockchain supporting IoT and SC&C from the DPM perspective. Some of these mainly involve aspects like scalability, privacy protection and data exchangeability, described as follows.

– Scalability: In the era of Internet of everything, there will be huge numbers of IoT devices connected and IoT data collected. It is difficult for current blockchains to meet those needs, how, for instance, to establish consensus among the huge number of IoT devices, and to store and manage data for them. Almost all current blockchains are built for humans, not for IoT devices, much less for huge numbers of IoT devices.

– Privacy protection: Current blockchains provide some data privacy protection solutions. Although data privacy is protected, the transactions themselves can be traced in public or in special stakeholder cycles. This has hindered both deployment of and businesses migration to blockchains.

– Data exchangeability: There are many types of blockchains that store different kinds of IoT data. Currently, there are no standards or systems to facilitate exchanges of IoT data among the various types of blockchains.

7 Analysis of key features of and a common reference model for blockchain from the DPM perspective when supporting IoT and SC&C

7.1 Key features of blockchain for DPM

Blockchain has some key technical features, including, but not limited to, the following.

– P2P communication: Blockchain peers interact using P2P communication technologies, and the underlying communication networks are transparent to blockchain peers.

NOTE – Blockchain peers can also utilize other types of communication technologies to participate in blockchain activities, although P2P communication technologies are used commonly.

– Distributed and sustainable services: A blockchain is a decentralized system whose use has the benefits of distributed systems. Further, blockchain is more sustainable because blockchain peers can easily participate in the blockchain and its functionalities can be extensible through the deployment of diverse smart contracts.

– Transparent and auditable procedures: Blockchain peers participate in blockchain activities that are transparent and auditable, e.g., establishing blockchain consensus, making blockchain transactions and storing blockchain data.

– Crowding consensus and transaction: A blockchain is decentralized and not dependent on centralized entities. Some or all blockchain peers participate in establishing consensus and making transactions subject to the deployment and policy of the blockchain.

– Flexibility and pluggability: Blockchains are usually pluggable on permission management, consensus mechanism, transaction approach, contract management and storage policy.

Clauses 7.1.1 to 7.1.2 introduce two key technologies, crowding consensus and smart contract, of blockchains related to aspects of DPM.

7.1.1 Crowding consensus

One of the main features of blockchains, crowding consensus allows blockchain data to be distributed, maintained and processed among participants according to specific transition rules. The participants are given the right to collectively perform transitions through a consensus algorithm. Additionally,

participants should be securely decentralized, which ensures that no single participant or a set of colluding participants can take up a majority of the set.

There are some common crowding consensus models used in different types of blockchain. Each model has features to process and manage blockchain data.

7.1.1.1 Proof of work

The proof of work (PoW) [b-PoW] is currently the most common consensus for public blockchain systems, e.g., in Bitcoin and Ethereum. In a PoW consensus, many participants (or named miners) compete at the same time to solve a computationally intensive puzzle to gain the right to publish the next block (and a financial award if applicable). The winner in a PoW consensus for a blockchain transaction has the right to record and write the blockchain data into the blockchain.

The PoW is applicable to some applications and services for IoT and SC&C. Currently, in the markets, there are some blockchains for IoT and SC&C derived from the public platforms, e.g., Bitcoin and Ethereum.

The PoW has some inherent disadvantages that limit its applicability to applications and services for IoT and SC&C. First, PoW is resource exhaustive. Due to the computational resources needed, the miners in PoW consensus-based blockchains (e.g., Bitcoin and parts of Ethereum) consume huge quantities of electrical energy each year. Second, secure transaction settlements in those types of blockchain suffer from expected latencies measured in minutes or 10s of minutes that affect scalability.

7.1.1.2 Proof of stake and delegated proof of stake

In proof of stake (PoS) [b-PoS] consensus, the mining is done by stakeholders in the financial sector who have strong incentives to have good control of blockchains. The purest form of PoS is to make mining easier for those who can show they control a large amount of cryptocurrency. PoS starts by owner consuming their coins, thereby giving them a pre-determined privilege to generate a block for the network.

The generation of block in PoS is similar to PoW. The difference is that the hashing operation is done through a limited search space, unlike PoW where it is unlimited. In PoS, mining is eliminated and computing power consumption is reduced.

One of the disadvantages of PoS is the "nothing at stake" problem, where block generators have nothing to lose by voting for multiple blockchain histories, which leads to consensus never resolving. Another disadvantage is that the "richest" participants are always given the easiest mining puzzle.

Delegated proof of stake (DPoS) [b-DPoS] is the fastest, most efficient, most decentralized and most flexible consensus model available. DPoS leverages the power of stakeholder approval voting to resolve consensus issues in a fair and democratic way. All network parameters, from fee schedules to block intervals and transaction sizes, can be tuned via elected delegates.

PoW is hungry for computational resources and PoS (including DPoS) is hungry for "currency" resources which affects their scalability and makes them unsuitable for scaled applications and services for IoT and SC&C.

7.1.1.3 Practical byzantine fault tolerant

Practical byzantine fault tolerant (PBFT) consensus [b-PBFT] could be used in distributed systems. A participant in a PBFT-based blockchain system supports asymmetric encryption and has a couple of keys (one public, the other private). The participant publishes the public key and can verify and sign passing messages with the private key. Once enough identical responses are reached, then a consensus is met that the message is a valid transaction. Consequently, hashing power is not required in the process. PBFT is a system devised for low-latency storage system. This is applicable to digital

asset-based platforms that do not require a large amount of throughput, yet demand many transactions. Consensus can be reached fast and efficiently.

Secondly, trust is entirely decoupled from resource ownership, which makes it possible for a small non-profit to keep powerful organizations honest. PBFT is used by some consortium blockchains, e.g., Hyperledger.

The PBFT has two common features. First, all parties have to agree on the exact list of participants. Second, membership in a byzantine agreement system is set by a central authority or closed negotiations. These factors might adversely affect a cryptocurrency, but may be useful in a digital asset holdings platform.

The characteristics of PBFT (e.g., permission management, efficiency and low energy consumption) make it applicable to scaled applications and services for IoT and SC&C.

7.1.1.4 Federated byzantine agreement

In federated byzantine agreement (FBA) consensus [b-FBA], it is assumed that participants know each other and can distinguish which are considered important. The participant in question then waits for the vast majority of the others to agree on a transaction before they themselves consider it settled. In turn, the important participants mentioned do not agree to the transaction until the participants they consider important agree as well, and so on. Eventually, enough participants will accept the transaction.

FBA relies on small sets of trusted participants. These sets are from participants that trust each other's information. When enough sets of trusted participants are formed, the rest of the blockchain will reach consensus, based on the fact that some of the trusted participants did. Good behaviour among participants will result in the formation of small sets of trusted participants, with the level of trust built over time.

FBA is applicable to private and consortium blockchains. The FBA is not suitable for scaled applications and services for IoT and SC&C.

7.1.1.5 Round robin

If there are some levels of trust between participants in a blockchain, especially permission blockchain, it can use round robin consensus. Round robin consensus [b-Round Robin] is often used for private blockchains or consortium blockchains, where some or all participants take turns in creating block. This model ensures that no single node either creates the majority of the blocks or causes a halt in block production.

Round robin consensus usually uses a straightforward approach with no cryptographic puzzles and has low energy requirements. Due to the need for some level of trust among participants, round robin is not applicable to permissionless applications and services for IoT and SC&C.

7.1.2 Smart contract

Some of the blockchain systems, e.g., Ethereum and Hyperledger, support smart contract, which allows participants to deploy smart contracts on the blockchains and allows smart contracts to be triggered and executed automatically.

A smart contract is a collection of code and data. The code of a smart contract provides the appropriate method to process the data and make transactions.

A smart contract can perform calculations, store data and automatically send funds to other accounts. In practice, all mining blockchain peers execute the smart contract code simultaneously when mining new blocks. Usually, the participant issuing a transaction to a smart contract will have to pay for the cost of the code execution in addition to the normal transaction fees. There is a limit on how much execution time can be consumed by a call to a smart contract. If this limit is exceeded, execution stops and the transaction is discarded. This mechanism not only rewards miners for executing the smart

contract code, but also prevents malicious users from deploying and then accessing smart contracts that will perform a denial of service on the mining participants by consuming all resources (e.g., using infinite loops).

Smart contract is useful to some applications and services for IoT and SC&C. When IoT devices are connected to a blockchain through smart contracts, they can exchange data with each other, without human intervention.

7.2 Abstract common reference model of blockchain and capabilities for DPM

There are several types of representative blockchain, e.g., Bitcoin, Ethereum and Hyperledger, that have features to process and manage data (see Appendix I). This clause provides an abstract common reference model of blockchain to illustrate its common features.

Without loss of generality, a blockchain commonly consists of a group of logical functional components that can be divided into five layers, namely: fundamental; core; service supporting; application; and cross, as illustrated in Figure 7-1. In a blockchain, the functional components in the lower layers provide supports to that in the upper layer.

NOTE 1 – This does not mean that every blockchain uses this abstract common reference model and supports the same functionalities.

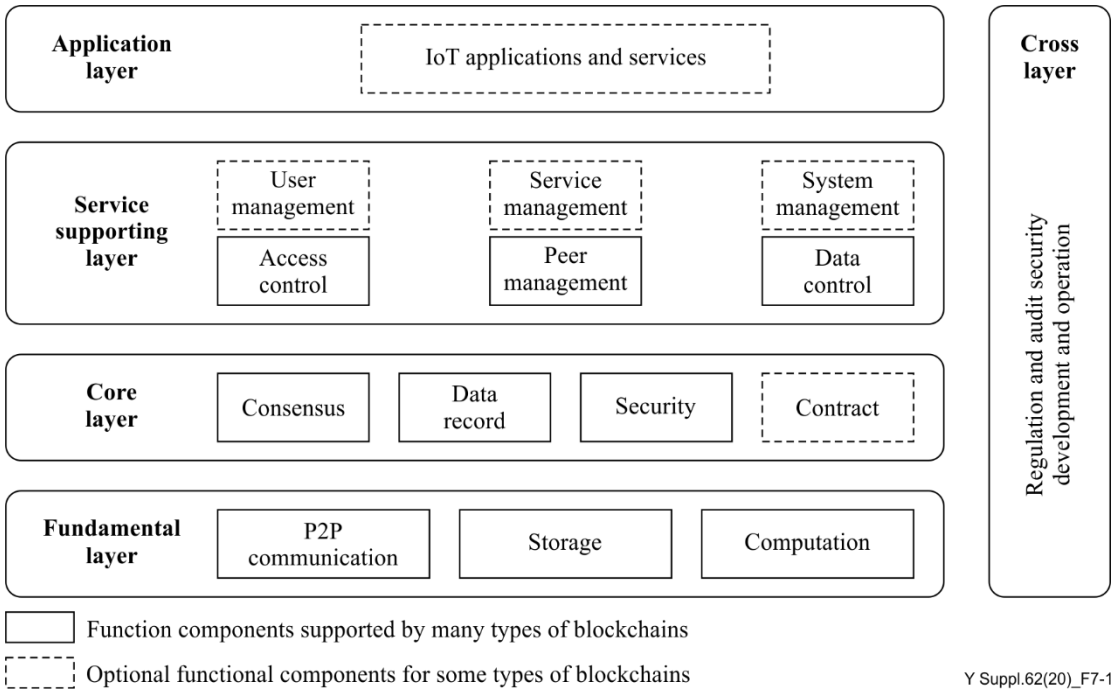

Figure 7-1 – An abstract common reference model of blockchain

NOTE 2 – In Figure 7-1, the logical functional units in dashed boxes are optional for some types of blockchain, especially for some public blockchains.

7.2.1 Fundamental layer

The fundamental layer provides the running environment and basic components for normal operation of the blockchain. The function components in this layer may include the following.

– A P2P communication functional component that supports blockchain peers to interact and to exchange blockchain data with P2P communication technologies. The underlying communication networks are transparent to the blockchain.

– A storage functional component that supports blockchain peers to store and query blockchain data in an effective, secure and steady way.

– A computation functional component that provides the running environment and computing capabilities including container, virtual machine (VM) and cloud technologies that can be applied by each blockchain peer.

In the fundamental layer, physical or virtual security infrastructures support to store, manage and control the access to participants' sensitive data, including their private keys (or identifiers).

7.2.2 Core layer

The core layer provides core capabilities based on the environment and capabilities provided by the fundamental layer. The core capabilities include consensus establishment, data recording, security protection and contract management.

The functional components in this layer include the following.

– A consensus functional component that supports the blockchain peers to make consensus, which usually provides the following capabilities, including:
  - support for multiple blockchain peers to participate in the consensus and confirmation process;
  - support for an independent blockchain peer to validate the relevant data transformed in a blockchain;
  - prevention of any independent blockchain peer to record or modify data without the confirmation of other blockchain peers involved;
  - possession of a certain fault tolerance capability, including non-malicious failure, e.g., blockchain peer physical failure or network malfunction, as well as malicious failure, e.g., a blockchain peer under illegal control.

  NOTE 1 – Clause 7.1.1 lists some consensus models. In most blockchains, consensus models are pluggable.

– A data record functional component that provides distributed storage for blockchain data, which provides the following capabilities, including:
  - support for the persistent storage of blockchain data;
  - support for a complete data record among multiple blockchain peers;
  - support for provision of a genuine data record to authorized users;
  - ensuring data consistency among the records of each blockchain peer.

  NOTE 2 – Blockchain data can be stored in or out of a blockchain (e.g., in a cloud). When the data is stored out of a blockchain, the blockchain can store relevant signature and addresses in order to keep the data consistent and accessible.

– A security functional component that guarantees underlying security for blockchain data and transactions, which generally includes mathematical processes, e.g., encryption and decryption, as well as digest and digital signature.

– A contract functional component that supports operations related to smart contract, including deployment, execution and search of the smart contract.

7.2.3 Service supporting layer

The service supporting layer provides reliable and efficient access and monitoring of blockchain. It provides unified access control, data control and management for peers, users, services and systems in blockchain.

The functional components in this layer include the following.

– An access control functional component that performs access control of blockchain data relating to user accounts, ledgers, transactions and interfaces.

NOTE 1 – In permissionless blockchain, there is no user management, every participant has the same rights to participate in the blockchain.

– A peer management functional component that supports a blockchain peer in information query and management, additionally including functions like peer configuration, monitoring and authorization.

NOTE 2 – Blockchain peers are usually divided into those for consensus and access. Consensus peers participate in a blockchain consensus process, while access peers support external application to synchronize blockchain data and submit the transaction.

– A data control functional component that supports the following capabilities:
  - data residence in the blockchain peer distribution and exchange;
  - logic validation before consensus and result calculation after consensus;
  - multiple signature permission control to specific transaction processing;
  - logical execution based on blockchain contracts.

– A user management functional component that supports user management and transaction making, which is optional for some public blockchains.

– A service management functional component that supports service selection and subscription, as well as cross-chain linkage and data exchange.

– A system management functional component that supports the management of monitoring, events and security.

7.2.4 Application layer

The application layer includes blockchain applications that utilize functionalities provided by the lower and cross-layers.

7.2.5 Cross-layer

The cross-layer is a vertical layer, which provides function support across multiple layers. Functional components in this layer include development and operation, security, regulation and audit.

8 Analysis of key issues for blockchain support of IoT and SC&C from the DPM perspective

8.1 Identification and authentication

In a blockchain, usually there are two types of identity, one for data and another for participants (IoT things, individuals and organizations). Identifiers for blockchain data, e.g., for transactions or blocks, are usually random hash strings, which are generated by hash algorithms like SHA-256 [b-SHA-256], and global unique.

Depending on the permission mechanisms of blockchains, permissioned or permissionless, the identifiers used for participants are varied and the corresponding authentication is varied accordingly.

8.1.1 Permissionless blockchain

In permissionless blockchain, the identifiers for the participants are random hash strings and global unique, like the identifiers for blockchain data. Additionally, permissionless blockchains can use passwords or other solutions (e.g., biometric solutions) to authenticate participants. There are some key issues for permissionless blockchains from the perspective of identification and authentication for blockchain participants as follows.

– The random identifiers are uneasy to be remembered and traced. If the identifiers are lost, then the corresponding resources in blockchains cannot be accessible again.

– Identifiers are random and the processes for identification and authentication are separated, which makes it difficult when supporting large-scale IoT devices to participate in blockchain.

8.1.2 Permissioned blockchain

There are many solutions for permissioned blockchains to identify and authenticate the participants, e.g., traditional identity and authentication, and decentralized self-sovereign identity.

Traditionally, identification and authentication are separated. The identities of the participants are created and managed by one or a group of organizations. The participants are identified by blockchain peers, after which they can be authenticated by the blockchain peers with passwords or other solutions (e.g., biometric solutions).

Decentralized self-sovereign identity combines identification and authentication in one procedure. A decentralized self-sovereign identity of a participant can include the identifier of the participant and relevant information to authenticate the participant. The participants can totally control their identities.

Some key issues for permissioned blockchains from the perspective of identification and authentication for blockchain participants include:

– if using traditional identity, how to support large-scale IoT devices to participate the blockchains;

– if using decentralized self-sovereign identity, how to authorize participants to create and manage their self-sovereign identities.

8.2 Data generation and storage

Blockchain data is generated by blockchain peers under crowding consensus when they participate in transactions and is decentralized and stored by some or all blockchain peers that are involved in the transactions.

Some key issues for data generation and storage for IoT and SC&C include:

– when large-scale IoT devices are participating in a blockchain, how to establish consensus and how to decentralize and store blockchain data;

– because usually IoT devices have limited computation and storage capabilities, how they can participate in blockchains.

8.3 Data management

The operations of data management for blockchain data include addition, search and access. Blockchain data cannot be changed (deleted, inserted and updated), but can be set to expire or be updated through the addition of new blockchain data.

8.4 Data exchanging and sharing

The data exchanging and sharing for blockchain data usually occurs within a blockchain or between different blockchains.

8.5 Cross-chain interaction and data mitigation

There are many kinds of blockchains for IoT and SC&C, and these blockchains are independent of each other. The lack of standardization for cross-chain interactions among the different blockchains results in issues relating to data mitigation from one blockchain to another.

8.6 Data security and privacy

Blockchain can keep data security for blockchain data. Blockchain data are hard to change, and because of decentralized storage, difficult to lose.

In a blockchain, transaction progress is usually transparent to some or all blockchain peers, according to its policies. This means that almost every participant can access all blockchain data. Transaction contents can be encrypted, which provides privacy protection to a certain extent. However, there are some potential areas of difficulty to consider for blockchain to process blockchain data for IoT and SC&C.

Some key issues for data security and privacy for IoT and SC&C include the following.

– Because the capabilities of computation of the majority of IoT devices are limited, they usually use simple encryption solutions to protect their data. The strength of the encryption will be insufficient to resist attacks in the future.

– Because of the transparency of transactions among the blockchain peers involved, this solution may leak some sensitive information about the participants.

8.7 Data auditing, tracking and tracing

In permissionless blockchains, participants are anonymous and participate using random names (random hash strings), which makes it difficult or even impossible to audit the data in those types of blockchain.

In permissioned blockchains, participants have authorized identities that are suitable for audit, tracking and tracing.

8.8 Blockchain as a decentralized database

Blockchain can act as a decentralized database. According to the approaches and technologies for data storage and management, database management modes may be divided generally into three categories:

– centralized;

– distributed;

– decentralized.

In centralized mode, data are located, stored and maintained in a single location (e.g., in a single data centre). In this mode, databases are usually managed by one maintainer. In distributed mode, data are located, stored and maintained in a single location or spread across a network, in a similar way to the centralized mode, although the data are distributed for storage in different areas; distributed databases are usually managed by one maintainer. The centralized mode and distributed mode are usually used in traditional database management systems. Databases in distributed mode are widely used in applications and services for IoT and SC&C.

In decentralized mode, usually used in blockchain, the data are spread across a single or multiple network(s) and managed by different stakeholders (or all of the participants). Those stakeholders maintain the data in decentralized mode in some secure and transparent ways. Database in decentralized mode is applicable to untrusted environments. The maintainers (stakeholders) for a database in decentralized mode are independent and may neither know nor trust each other.

There are some key issues to be studied for DPM for IoT and SC&C when using blockchain technologies, including the following.

– Blockchain data are arranged in blocks and stored in databases on blockchain peers usually with simple key-value pairs. If a blockchain acts as a database, improvement in the efficiency of searching of and access to blockchain data is required.

– Blockchain data are decentralized and stored by the participants involved. When accessing blockchain data from one participant, although the blockchain data stored are trusted, the integrity of stored blockchain data by the participant should be validated.

– It is not easy for third-party applications to search and access blockchain data with structured query language (SQL) and interfaces in blockchains.

9 Analysis of the effects of using blockchain to support IoT and SC&C from the DPM perspective

9.1 Impact on IoT networks and service platforms for IoT and SC&C

With the rapid evolution of networks and services of IoT and SC&C, more and more things (both physical and virtual) are getting connected. The huge number of things connected will reshape networks and service platforms for IoT and SC&C.

In addition, with the developments of blockchain-enabled applications, the inherent characteristics of blockchains to process data will have negative impacts on IoT networks, including at a minimum:

– huge numbers of P2P connections and the broadcasting of messages may block IoT networks causing a network signalling storm and potentially resulting in network instability;

– huge replications of distributed ledgers may add pressures to the IoT networks.

Those negative impacts are due to the contradictions between the traditional centralized or distributed mechanisms and decentralized ones. Current IoT networks and service platforms usually use traditional centralized or distributed mechanisms and do not adapt to the decentralized applications of blockchains.

Blockchains and blockchain applications will bring adverse effects to current IoT networks and service platforms. However, if introducing blockchain-related technologies to IoT networks and service platforms, then they acquire the advantages of the blockchain-technologies and can overcome those adverse effects.

9.2 Promoting high-speed, low-latency services of IoT networks for data transmission and processing

Blockchain-based technologies can help IoT networks to serve for connections of 10s of billions of IoT things with other technologies, e.g., software-defined network (SDN), network function virtualization (NFV) and edge computation. Through blockchain-based technologies, the capabilities of network scalability, collaboration and security can be improved, and trusted networks can be established with higher efficiency and lower costs of construction and operation.

Currently, IoT networks are centralized or distributed, in which their edge nodes are restrained by core nodes in core networks. Through the use of edge computation technologies, IoT networks become flatter and flatter. Blockchain can be combined with edge computation technologies. Using the decentralization approach for blockchains, almost all capabilities of core nodes can be moved down to the edge nodes. In a blockchain-enabled IoT network (see Figure 9-1), core nodes just act as coordinators, and the edge nodes cooperate with each other to provide connection services and the capabilities usually performed by core nodes, e.g., authentication and accounting.

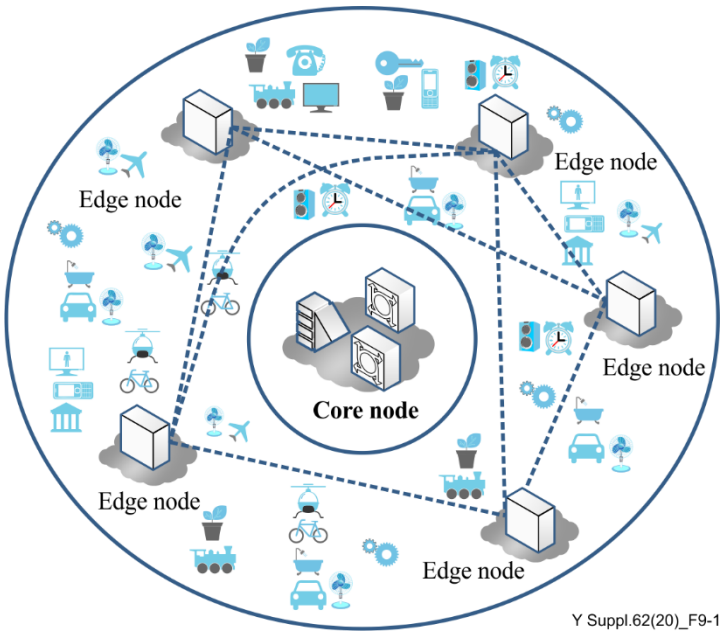

Figure 9-1 – Overview of a blockchain-enabled IoT network

In a blockchain-enabled IoT network, edge nodes have good independence. Edge nodes with this feature could effectively and efficiently cooperate with each other, even if they are from different IoT networks.

In a blockchain-enabled IoT network, data can be stored, managed, transmitted and processed in the edge nodes. Because the data and the relevant services are near to the IoT devices, they can get services from the edge nodes for data transmission and processing with high speed and low latency.

In addition, a blockchain-enabled IoT network can have good stability and anti-interference ability. Current centralized or distributed IoT networks may be vulnerable when they are attacked, especially at their core nodes, and the entire network may be implicated. However, in the blockchain-enabled IoT network, the influence of the attacks on it in a certain area will not affect networks in other areas. At the same time, blockchain-enabled networks can also support hot-swap edge nodes and add and replace edge nodes at any time without affecting the normal operation of other edge nodes in the area.

9.3 Promoting the network and data security for IoT networks and services

For many reasons (e.g., costs, technical improvements), in practice, IoT devices usually have limited security capabilities and can easily be hijacked. It is dangerous if a large number of hijacked IoT devices is used to attack communication networks or services at the same time, e.g., in a distributed denial of service (DDoS) attack, especially in the era of the Internet of everything. The challenge of how to promptly recognize and screen hijacked IoT devices is great.

The use of blockchain-related technologies can reduce or solve this problem. In general, IoT devices and IoT service platforms connect to communication networks via gateways. By upgrading these gateways, they form a blockchain with each other to jointly record and respond to the sabotage of hijacked IoT devices.

As an example, as shown in Figure 9-2, if a home smart device (e.g., a light) is hijacked and used to attack service platform A or service platform B, when such an attack occurs and is recognized, the gateway of service platform A or service platform B may record the attack behaviour of the light in the blockchain. Then, when the light is used to attack other service platforms, the corresponding gateway can refuse illegal access to it, and at the same time, the gateway where the light is located, can refuse to provide access service for the light and can notify the owner of the light to rectify it.

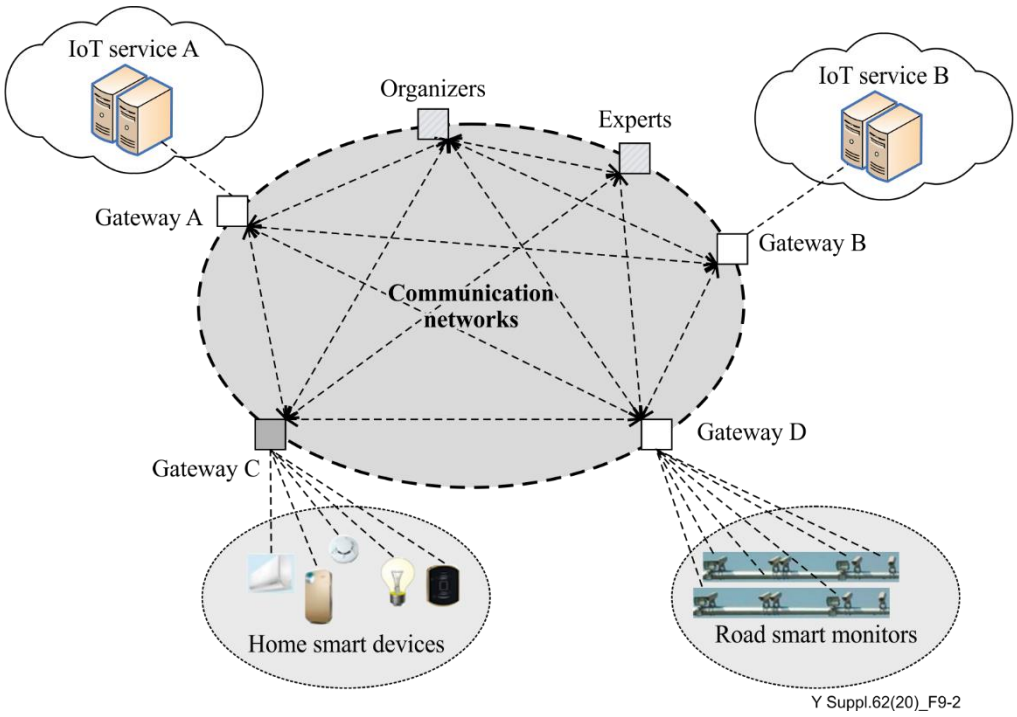

Figure 9-2 – Improving the capability for network and data security

Appendix I

Representative blockchain platforms and their key features for DPM

According to the access ability of participants and the way to provide services, blockchains can be generally divided into three types: public, consortium and private as follows.

– A public blockchain is publicly available for all participants; its blockchain data is viewable by anyone, anywhere. Additionally, it is completely open to participation in the blockchain and to the ability to submit transactions. The participant is identified by a global unique network token in a blockchain. All participants having a token have the same rights to participate in the blockchain, deploy smart contracts and make transactions. Any blockchain peer may contribute, as a volunteer, to secure entries to establish consensus. Furthermore, the ability to participate in consensus and resolution of transactions is completely open to any participant.

– A consortium blockchain is usually deployed and maintained by a consortium. A consortium blockchain is distinguished primarily by its method of establishing consensus. The consortium decides which participants in the blockchain will have the authority to deploy smart contracts and make transactions, as well as how to open the blockchain data to them.

– Private blockchains are usually deployed and maintained by private organizations. A private blockchain is the inverse of a public one in almost all key features. Blockchain data in a private blockchain is not open to those outside the private organization. Usually, there are inner governance rules to participation, smart contracts, transactions, consensus and data openness.

Those types of blockchain are not completely distinct and separate. The differences come from the approaches to deployment, not from the underlying technologies.

Bitcoin [b-Bitcoin], Ethereum [b-Ethereum], Enterprise Ethereum [b-Enterprise Ethereum], IOTA [b-IOTA] and Hyperledger Fabric [b-Hyperledger] are several representatives of blockchains.

I.1 Bitcoin

Bitcoin is an innovative payment network and one of a new kind of cryptocurrencies, which uses P2P technologies to operate with no central authority or banks.

Bitcoin is the origin of blockchain. Figure I.1 depicts the general framework for Bitcoin. Bitcoin usually consists of five groups of functionalities:

– data processing: functionalities to process data, including block data management, chain management, data signature, hash algorithms, Merkle tree management and crypto (symmetric and asymmetric encryption);

– networking: functionalities to network communication, including P2P communication, broadcast and communication validation;

– consensus: functionalities to make consensus, only supporting PoW consensus;

– motivation: functionalities for motivating, including announce and issue coin (e.g., Bitcoin) to the participants who forward the consensus and transaction;

– applications: functionalities for transaction and accounting etc.

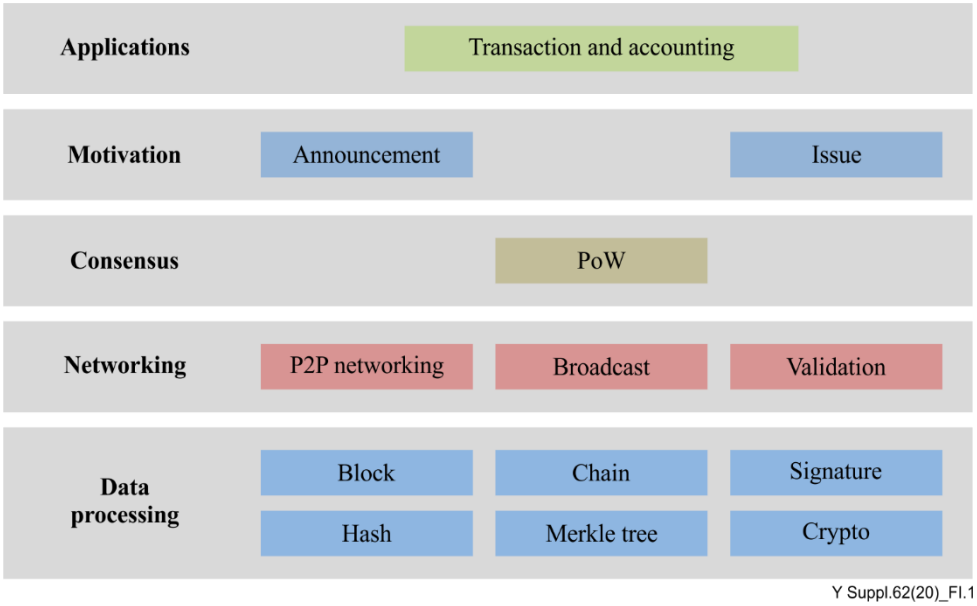

Figure I.1 – General framework for Bitcoin

The consensus of Bitcoin, PoW (see clause 7), limits its applications to the IoT and SC&C.

I.2 Ethereum and Enterprise Ethereum

Ethereum is an open blockchain platform which focuses on providing smart contracts, though it also provides a cryptocurrency, Ether. Smart contracts are programs that exist on the Ethereum that can be accessed by Ethereum participants. The Ethereum participants can both receive and send funds while performing arbitrary computation. A properly designed smart contract can act as a trusted third party in financial transactions, since its code is both public and immutable. Mining peers receive funds through mining and transaction fees.

The submission of a transaction to an Ethereum contract causes a program to be run in parallel on mining peer computers. The resulting state of the smart contract is stored in the blockchain by the user that publishes the next block. Figure I.2 depicts a general framework for Ethereum, which consists of five groups of functionalities:

– data processing: similar to that in Bitcoin;
– networking: similar to that in Bitcoin;
– consensus: pluggable, using PoW, PoS, DPoS or other consensus algorithms;
– motivation: similar to that in Bitcoin;
– smart contract: functionalities-related, including VM and contracts.

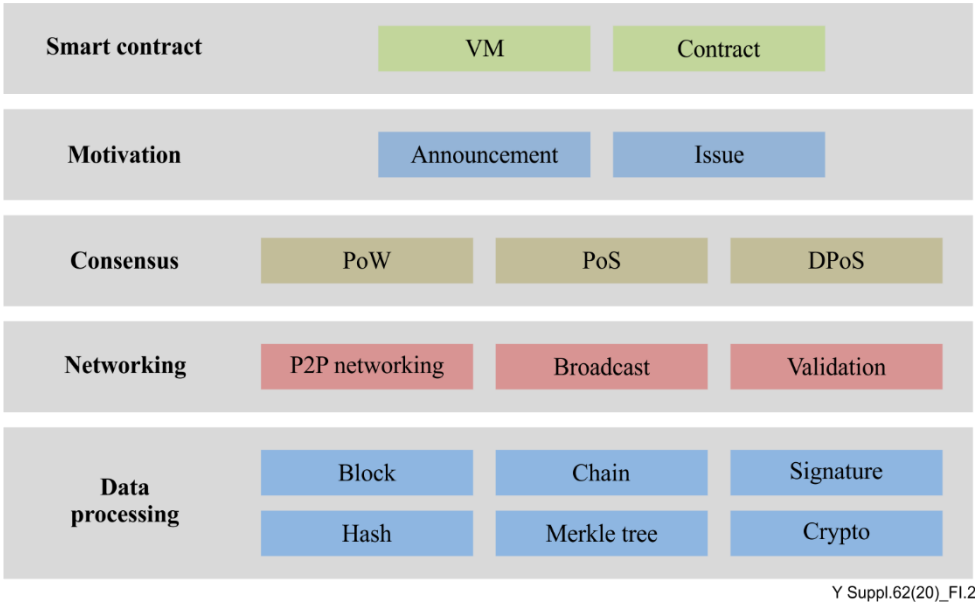

Figure I-2 – General framework for Ethereum

In Ethereum, there are two key features: one supports the pluggable consensus; the other smart contracts. Those features enable wider application of Ethereum to the IoT and SC&C.

The Enterprise Ethereum is founded by the Enterprise Ethereum Alliance. Enterprise Ethereum is a system to enable enterprise-grade transactions on an Ethereum-based blockchain network. Enterprise Ethereum provides a set of extensions to public Ethereum to satisfy the performance, permission management, and privacy demands of enterprise deployments, including the capability to perform private transactions, enforce membership and provide transaction throughput scaling.

The Enterprise Ethereum can be seen as one type of consortium blockchain and is more applicable to the IoT and SC&C than that of the Ethereum.

I.3 Hyperledger fabric

Hyperledger was founded by the Linux Foundation [b-Linux Foundation] aiming to create enterprise-grade, open-source distributed ledgers. It is used to advance cross-industry blockchain technologies. Hyperledger fabric is one of the blockchain projects within Hyperledger. A Hyperledger fabric can have one or more ledger(s), and it supports smart contracts (named chaincode) by which participants manage their transactions in the Hyperledger fabric.

Hyperledger fabric is one type of consortium blockchain and permissioned. The data in Hyperledger fabric can be stored in multiple formats and consensus mechanisms can be switched in and out.

Hyperledger fabric also offers the ability to create channels, allowing a group of participants to create separate ledger(s) of transactions. This is an especially important option for networks where some participants might be competitors and do not want every transaction that they make known to every participant. If two participants form a channel, then those participants – and no others – have copies of the ledger(s) for that channel.

The Hyperledger fabric general framework (see Figure I.3) could be aligned in three logical categories as follows.

– Membership services manage identity, privacy, confidentiality and policy on the network. Participants register to obtain identities, which enables the blockchain to issue security keys for transactions. Membership services manage the identities for ledger and resources, and manage the configuration, access control and privacy.

– Blockchain services manage the distributed ledger through P2P protocols. The data structures are optimized to provide efficient schemes for maintaining blockchain data (e.g., the world state) replicated for many participants. Different consensus algorithms that guarantee strong consistency (toleration of: misbehaviour with BFT; delays and outages with crash-tolerance; or censorship with PoW) may be plugged in and configured on deployment.

– Chaincode services are a secured and lightweight way to sandbox the chaincode execution on validating nodes. Also, the chaincode services manage the chaincodes (deployment, execution, research results, life-cycle control etc.)

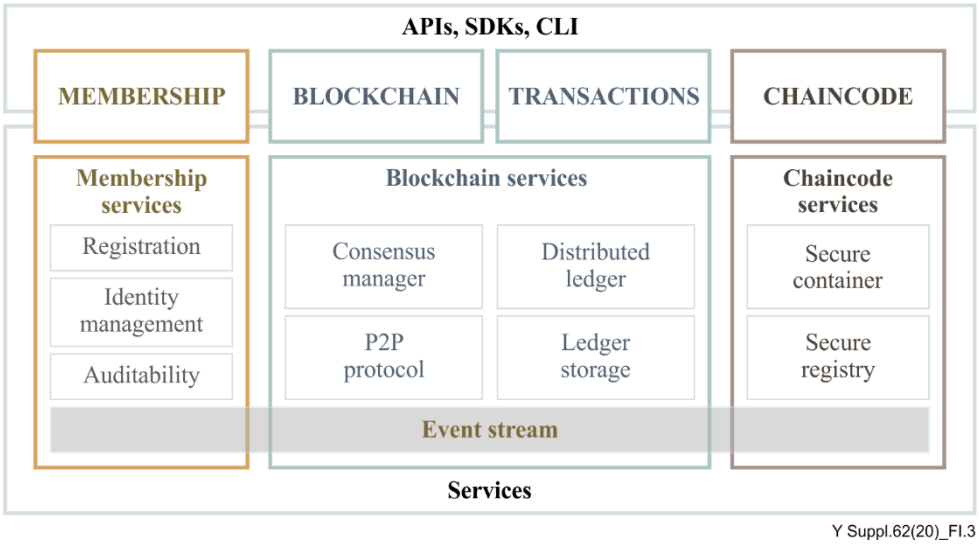

Figure I.3 – General framework for Hyperledger fabric

NOTE – In recent version of Hyperledger fabric, membership services are divided into two types: identity and policy; and chaincode service is also named smart contract services.

Hyperledger fabric has the key features of Ethereum, supporting both pluggable consensus and smart contracts. Further, Hyperledger fabric supports permission management and more consensus models. These features make the Hyperledger more scalable and efficient, more applicable to the IoT and SC&C.

Bibliography

[b-ITU-T FG-DPM TR D3.5] Technical report ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities D3.5 (2019*), Overview of blockchain for supporting IoT and SC&C in DPM aspects.*

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*.

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things.*

[b-ITU-T Y.4900] Recommendation ITU-T Y.4900/L.1600 (2016), *Overview of key performance indicators in smart sustainable cities*.

[b-ISO 22739] ISO 22739 (2020), *Blockchain and distributed ledger technologies – Terminology*.

[b-Bitcoin] Bitcoin.com (Internet). *Bitcoin*. Available [viewed 2020-09-04] at: https://www.bitcoin.com

[b-DPoS] Bitcoinwiki (Internet). *Delegated proof of stake*. Available [viewed 2020-09-04] at: https://en.bitcoinwiki.org/wiki/DPoS

[b-Enterprise Ethereum] Ethereum Foundation (Internet). *Enterprise Ethereum.* Available [viewed 2020-09-04] at: https://entethalliance.org/

[b-Ethereum] Ethereum.Foundation (Internet). *Ethereum.* Available [viewed 2020-09-04] at: http://www.ethereum.org

[b-FBA] Ray, S. (2018). *Federated byzantine agreement.* Medium. Available [viewed 2020-09-05] at: https://towardsdatascience.com/federated-byzantine-agreement-24ec57bf36e0

[b-Hyperledger] Linux Foundation (Internet). *Hyperledger.* Available [viewed 2020-09-04] at: http://www.hyperledger.org

[b-IOTA] IOTA Foundation (Internet). *IOTA.* Available [viewed 2020-09-05] at: https://www.iota.org/

[b-Linux Foundation] Linux Foundation (Internet). *Linux Foundation.* Available [viewed 2020-09-05] at: https://www.linuxfoundation.org

[b-PBFT] Bitcoinwiki (Internet). *PBFT.* Available [viewed 2020-09-05] at: https://en.bitcoinwiki.org/wiki/PBFT

[b-PoS] Wikipedia (Internet). *Proof of stake.* Available [viewed 2020-09-05] at: https://en.wikipedia.org/wiki/Proof-of-stake

[b-PoW] Wikipedia (Internet). *Proof of work*. Available [viewed 2020-09-05] at: https://en.wikipedia.org/wiki/Proof-of-work_system

[b-Round Robin] Computer Security Resource Center (Internet). *Round robin consensus model*. Gaithersburg, MD: NIST. Available [viewed 2020-09-05] at: https://csrc.nist.gov/glossary/term/Round_robin_consensus_model

[b-SHA-256] Bitcoinwiki (Internet). *SHA-256.* Available [viewed 2020-09-05] at: https://en.bitcoinwiki.org/wiki/SHA-256

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020