International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(7 April 2019)

ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities

Technical Report D3.5

Overview of blockchain for supporting IoT and SC&C in DPM aspects

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 procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. ITU-T Study Group 20 set up the ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities (FG-DPM) at its meeting in March 2017. ITU-T Study Group 20 is the parent group of FG-DPM.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

Technical Report D3.5

Overview of blockchain for supporting IoT and SC&C in DPM aspects

Summary

Blockchain presents opportunities for disruptive innovations, which enables global businesses to transact 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.

There are many benefits and challenges to addressing blockchain and IoT and SC&C together. This Technical Report provides overview of blockchain aspects related to data processing and management (DPM) for IoT and SC&C.

Acknowledgements

This Technical Report was researched and principally authored by Xiongwei Jia (China Unicom) and Zheng Huang (ZTE Corporation) under supervision of Gyu Myoung Lee (Korea, Rep.of).

Additional information and materials relating to this Technical Report can be found at: www.itu.int/go/tfgdpm. If you would like to provide any additional information, please contact Denis Andreev at tsbfgdpm@itu.int.

Keywords

Blockchain; DPM; Internet of things.

Technical Report D3.5

Overview of blockchain for supporting IoT and SC&C in DPM aspects

CONTENTS

Technical Report D3.5

Overview of blockchain for supporting IoT and SC&C in DPM aspects

1 Scope

This Technical Report provides overview of blockchain related to data processing and management (DPM) for supporting IoT and SC&C.

The scope of this Technical Report includes:

- Analysis on the advantages, challenges, characteristics, common reference model of blockchain in aspects of DPM for supporting IoT and SC&C;
- Analysis on key issues for blockchain to support IoT and SC&C in DPM aspects;
- Analysis on the effects when using blockchain to support IoT and SC&C in DPM aspects, include positive and negative effects.

2 References

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

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

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

3 Terms and definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 application [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 Internet of things (IoT) [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 – In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

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

3.1.4 smart sustainable city [ITU-T Y.4900]: A smart sustainable city (SSC) 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.

3.1.5 thing [ITU-T Y.4000]: In the Internet of Things, object of the physical world (physical things) or of the information world (virtual things), which is capable of being identified and integrated into the communication networks.

3.2 Terms defined here

This Technical Report defines the following terms:

3.2.1 blockchain: 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.

3.2.2 blockchain data: 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.

3.2.3 blockchain peer: 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.

3.2.4 blockchain transaction: 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).

3.2.5 consensus: Agreements to confirm the correctness of the blockchain transaction.

3.2.6 smart contract: 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 – All the herein definitions related to blockchain may need to be consistent with those defined in deliverable of FG-DLT D1.1 and those defined by the ISO SC 307, as well as those defined by other SDOs.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

DPM Data Processing and Management

DPoS Delegated Proof of Stake

FBA Federated Byzantine Agreement

IoT Internet of Things

IT Information Technology

NFV Network Functions Virtualization

PBFT Practical Byzantine Fault Tolerant

PoS Proof of Stake

PoW Proof of Work

P2P Peer to Peer

SDN Software Defined Network

SDO Standard Development Organization

SQL Structured Query Language

SSC Smart Sustainable City

SC&C Sustainable smart City and Community

VM Virtual machine

5 Conventions

None.

6 Overview of convergence of blockchain and IoT and SC&C in DPM aspects

Blockchain is one type of peer to peer distributed ledgers based on a group of technologies (such as peer to peer communication, distributed ledger, crowding consensus, etc.), 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 peer to peer distributed ledgers. If no specified, in this Technical Report, the key word "blockchain" refers to peer to peer distributed ledger, and also refers to a decentralized system which support peer to peer distributed ledger.

Some of the blockchains are reliant on the exchange of cryptocurrencies with anonymous users on a public network (e.g. Bitcoin [b-1], Ethereum [b-2]); and others are for business and working on permissioned network (e.g. Hyperledger [b-3], Enterprise Ethereum [b-12]), with known identities and without the need for cryptocurrencies.

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

6.1 Main advantages and challenges of blockchain in DPM aspects

It is a distinct characteristic of blockchain to process data with decentralized mechanism. All or part of the participants of a blockchain can store and maintain data in the blockchain in whole or in part. This characteristic makes advantages for the blockchain to manage IoT data, and also takes challenges of processing the IoT data as stored in blockchain.

The main advantages of blockchain in DPM aspects include:

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

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

– In a blockchain, data are secure and immutable to be changed although the blockchain is working in un-trust environment. The data in a blockchain can only be extended and previous records cannot be changed. The participants can trust the blockchain to store their data.

– In a blockchain, the processes of transactions are transparent to the participants and it also can provide a certain amount of privacy protection for the participants. Every participant involved in a transaction can contribute the transaction and can 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, the data is uneasy to be lost for the data may be stored by whole or part of the participants of the blockchain.

– In a blockchain, the participants can deploy and/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:

– How much of the participants can be participated in a transaction? When the participants become more and more, the speeds and efficiency to make consensus and transaction may be decreased rapidly and become more and more unacceptable.

– How much of the duplications of data to be stored in blockchain? Too much duplications of data waste storage resources and network bandwidth, and slow the blockchain.

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

– How to improve the speed and efficiency to find and access data of a blockchain? It's uneasy to search and access data which 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, such as smart meters, e-health etc. However, there are some key challenges for DPM that IoT and SC&C must be faced, especially in the forthcoming era of internet of everything, for example:

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

– Huge amounts of IoT devices means huge volumes of IoT data, how to keep balances between data storages and data accessibilities;

– Unease to building trust on the un-trust Internet for the diverse IoT devices and their data, many of the IoT devices are too vulnerable to be trusted;

– Lack of solutions to meet the needs 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 aspect

There are many benefits to making blockchain and IoT and SC&C together, and the key benefits are from building trust, reducing costs, accelerating transactions, and increasing security:

– 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 IT infrastructure. Data protection of blockchain fosters stronger working relationship among the participants and provides greater efficiency as the participants take advantage of the data protected.

– Making IoT and SC&C and blockchain together enables IoT devices to participate in blockchain transactions. Specifically, IoT devices can send data to public, consortium or private blockchain for inclusion in shared transactions with distributed records which 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 traded, without requiring a central point of control.

– Blockchain is good at data privacy protection. All data in a blockchain can be encrypted, and only allows the authorized stakeholders could access the data. Blockchain with IoT and SC&C

together becomes a potential game changer by opening the door to invent new styles of digital interactions, 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 above, there are some key challenges of blockchain for supporting IoT and SC&C in DPM aspects, mainly in scalability, privacy protection and data exchangeability:

– Scalability: In the era of Internet of everything, there will be huge numbers of IoT devices connected and IoT data collected. Current blockchains are hard to meet those needs, for instance, how to make consensus among the huge amount of the IoT devices, how to store and manage data for the IoT devices. Almost all of the current blockchains are built for human, not for IoT devices, much less for huge amount of IoT devices.

– Privacy protection: Current blockchains provide some solutions to protect data privacy. Although data privacy is protected, the transactions yet could be traced in public or in special stakeholders' cycles, which has hindered to deploy or migrate businesses into blockchains.

– Data exchangeability: There are many types of blockchains which storing different kinds of IoT data. And currently there is no standards or systems to facilitate the exchanges of IoT data among the various types of blockchains.

7 Analysis on key technologies and common reference model of blockchain in DPM aspects for supporting IoT and SC&C

7.1 Key technical technologies of blockchain for DPM

Blockchain has some key technical characteristics, including, but not to be limited:

– Peer to peer communication: Blockchain peers interact with each other using peer to peer communication technologies, and the underlying communication networks are transparent to the blockchain peers.

  NOTE – Blockchain peers may also utilize other types of communication technologies to participate in the activities of blockchains, although peer to peer communication technologies are used commonly.

– Distributed and sustainable services: A blockchain is a decentralized systems which has the pros of distributed systems. And blockchain is more sustainable for the blockchain peers are easy to participate in the blockchain and its functionalities can be extensible through deploying diverse smart contracts.

– Transparent and auditable procedures: It's transparent and auditable that the blockchain peers participate the activities in a blockchain, such as making blockchain consensus, making blockchain transaction, store blockchain data.

– Crowding consensus and transaction: The blockchain is decentralized and is not dependent on centralized entities. Part or whole of the blockchain peers participate in making consensus and transaction subject to the deployment and policy of the blockchain.

– Flexibility and plug-ability: The blockchains are usually pluggable on permission management, consensus mechanism, transaction approach, contract management, and storage policy.

The followed sub-sections introduce two key technologies (crowding consensus and smart contract) of blockchains from the aspects of DPM.

7.1.1 Crowding consensus

Crowding consensus is one of the main features of blockchains, which allows the blockchain data could be distributed, maintained and processed among the participants according to some specific

transition rules. The participants are given the right to collectively perform transitions through a consensus algorithm. And the participants should be securely decentralized, which makes sure that no single participant or a set of colluding participants can take up majority of the set.

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

1) Proof of Work (PoW)

The PoW [b-6] is currently the most common consensus for public blockchain systems, for example, in Bitcoin and Ethereum. In PoW consensus, many participants (or named miners) are competing at the same time to solve a computationally intensive puzzle to gain the right of publishing the next block (and a financial award if applicable). The winner in 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 blockchain for IoT and SC&C derived from the public platforms, such as Bitcoin and Ethereum.

The PoW has some inherent disadvantages which limit its applicability on applications and services for IoT and SC&C. Firstly, it's resource exhaustive. Due to the computational resources needed, the miners in the PoW consensus based blockchains (such as Bitcoin and parts of Ethereum) consume huge electric power each year. Secondly, secure transaction settlements in those types of blockchains suffer from expected latencies in the minutes or tens of minutes, that affects scalability.

2) Proof of Stake (PoS) and Delegated Proof of Stake (DPoS)

In PoS [b-7] consensus, the mining is done by stakeholders in the economic set who have the strong incentives to be good controls of the blockchains. The purest form of PoS is to make mining easier for whom can show they control a large amount of the currency. PoS starts by an owner consuming his coin, thereby giving him a pre-determined privilege of generating 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 the search space is unlimited. In PoS, mining is eliminated and energy from computing power is saved.

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-8] 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 appetite for computational resource and PoS (including DPoS) is appetite for "currency" resource, that affect their scalability, and not suitable for scaled applications and services for IoT and SC&C.

3) Practical byzantine fault tolerant (PBFT)

PBFT [b-9] consensus could be used in distributed systems. The participant in PBFT-based blockchain system supports asymmetric encryption and has a couple of keys (a public key and a private key). The participant publishes the public key and could verify and sign the 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, such as Hyperledger.

The PBFT has two common features. Firstly, all parties have to agree on the exact list of participants. Secondly, 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 (such as permission management, efficiency and low power consumption) make it applicable to scaled applications and services for IoT and SC&C.

4) Federated Byzantine Agreement (FBA)

In FBA [b-10] consensus, it is assumed that the participants know each other, and can distinguish which it considers important. The participant in question then waits for the vast majority of the others to agree on a transaction before themselves, considering the transaction settled. In turn, the important participants mentioned do not agree to the transaction until the participants they consider important agree as well, so on and so forth. Eventually, enough of the participants would 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 would reach consensus, based on the fact that some of the trusted participants did. Good behaviour of participants would ascend into 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.

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 [b-11] consensus is often used for private blockchains or consortium blockchains, where parts or whole of the participants take turns in creating block. This model ensures no one node creates the majority of the blocks and no one node to cause a halt in block production.

Round Robin consensus usually uses straightforward approach, no cryptographic puzzles, and has low power requirements. Due to the need for some level of trust amongst participants, Round Robin is not applicable to the permission-less applications and services for IoT and SC&C.

7.1.2 Smart contract

Some of the blockchain systems (such as Ethereum and Hyperledger) support smart contract, which allow the participants to deploy smart contracts on the blockchains and allow the smart contracts could 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 could be trigged by the participants and executed automatically.

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 are discarded. This mechanism not only rewards the 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 of the applications and services for IoT and SC&C. When IoT devices are connected to a blockchain, through smart contracts, they could exchange data each other, without humans' interruptions.

7.2 Abstract common reference model of blockchain and its capabilities for DPM

There are several types of representative blockchain (such as Bitcoin, Ethereum, Hyperledger and Tangle) which have features to process and manage data (see Appendix I). This section provides an abstract common reference model of blockchain to illustrate the common features of the blockchains.

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

NOTE 1 - It should be noted that it does not mean that every blockchain uses this abstract common reference model and supports the same functionalities.

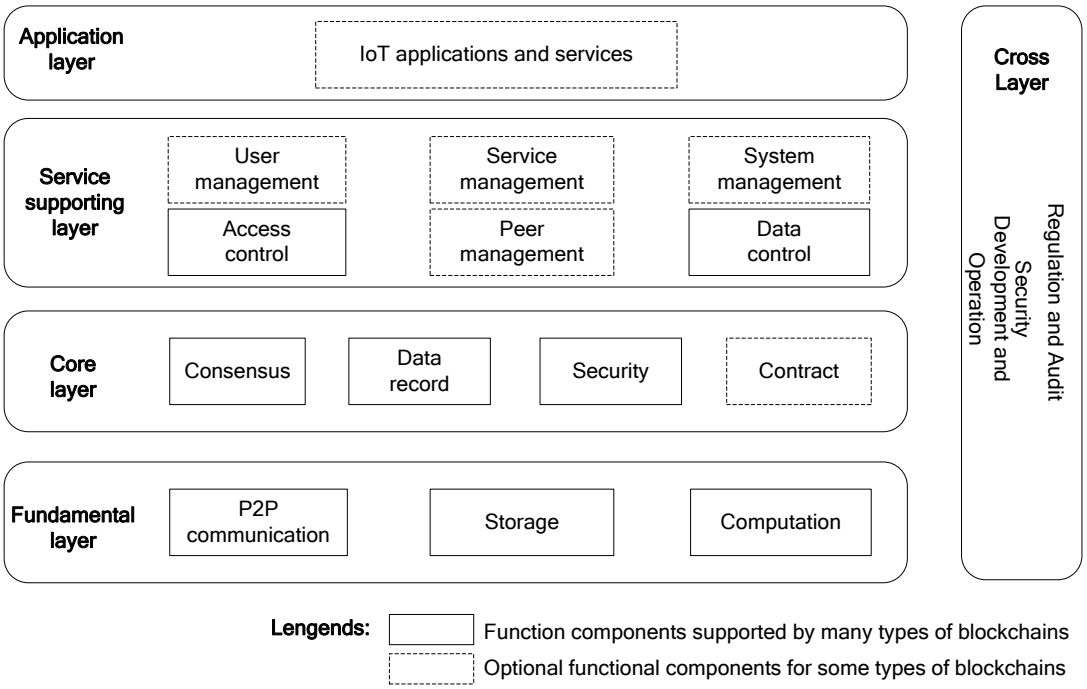

Figure 7-1 – An abstract common reference model of blockchain

NOTE 2 - In this diagram of Figure 7-1, the logical functional units in dashed boxes are optional for some types of blockchains, 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:

- P2P communication functional component: It supports the blockchain peers to interact with each other and to exchange blockchain data with P2P communication technologies. The underlying communication networks are transparent to blockchain.
- Storage functional component: It supports the blockchain peers to store and query blockchain data in effective, secure and steady way.

- Computation functional component: It provides the running environment and computing capabilities including container, virtual machine (VM) and cloud technologies which can be applied by each blockchain peer.

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

7.2.2 Core layer

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

The functional components in this layer include:

- Consensus functional component: It supports the blockchain peers to make consensus, which usually provides the following capabilities, including:
  - supporting multiple blockchain peers to participate in the consensus and confirmation process;
  - supporting independent blockchain peer to validate the relevant data transformed in blockchain;
  - preventing any independent blockchain peer to record or modify data without the confirmation of other blockchain peers involved;
  - possessing a certain fault tolerance capability, including un-malicious failure such as blockchain peer physical failure or network malfunction, as well as the malicious failure such as blockchain peer suffering from illegal control.

  NOTE 1 – Section 7.1.1 lists some of the consensus model. Usually, in most of the blockchains, consensus models are pluggable.
- Data record functional component: It provides distributed storage for blockchain data, which provides the following capabilities, including:
  - supporting the persistent storage of blockchain data.
  - supporting complete data record among multiple blockchain peers.
  - supporting to provide genuine data record to authorized users.
  - ensuring data consistency among the records of each blockchain peers.

  NOTE 2 – Blockchain data could be stored in a blockchain, or out of a blockchain (such as in a cloud). When the blockchain data is stored out of a blockchain, the blockchain could store relevant signature and addresses in order to keep the data consistent and accessible.
- Security functional component: It guarantees underlying security for blockchain data and transactions, generally which includes mathematical processes such as encryption and decryption, digest and digital signature etc.
- Contract functional component: It supports the operations related to smart contract, including deploying, executing and searching the smart contract.

7.2.3 Service supporting layer

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

The functional components in this layer include:

- Access control functional component: It performs the access controlling to the blockchain data about the user accounts, ledgers, transactions and interfaces.

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

- Peer management functional component: It supports the blockchain peer of information query and management, additionally including the functions, such as peer configuration, monitoring and authorization.

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

- Data control functional component: It supports the following capabilities:
  - data residing 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.
- User management functional component: It supports user managements and transaction committing which is optional for some public blockchains.
- Service management functional component: It supports service selection and subscription, and cross chain linkage and data exchange.
- System management functional component: It supports the managements for monitoring, event and security.

7.2.4 Application layer

The application layer includes blockchain applications which utilized the functionalities provided the lower and cross layers.

7.2.5 Cross layer

The cross layer is a vertical layer, which provides function supports across the multiple layers. Functional components in this layer include developing and operation, security, regulation and audit, etc.

8 Analysis on key issues for blockchain to support IoT and SC&C in DPM aspects

8.1 Identification and authentication

In a blockchain, usually there are two types of identities, one is for blockchain data, another is for participants (IoT things, individuals and organizations). Identifiers for blockchain data (such as for transactions, for blocks) usually are random hash strings and global unique which is used to be generated with hash algorithms (such as SHA256).

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

1) Permission-less blockchain

In permission-less blockchains, the identifiers for the participants are random hash strings and global unique as similar as the identifiers for blockchain data. And the permission-less blockchains can use passwords or other solutions (such as biometric solutions) to authenticate participants. There are some key issues for permission-less blockchains from the perspective of identification and authentication for blockchain participants：

- 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. It makes it difficult when supporting large-scale IoT devices to participate the blockchains.

2) Permissioned blockchain

There are many solutions for permissioned blockchains to identify and authenticate the participants, such as 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 the blockchain peers, after then they can be authenticated by the blockchain peers with passwords or other solutions (such as biometric solutions).

Decentralized self-sovereign identity combines the 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 the identity of themselves.

There are some key issues for permissioned blockchains from the perspective of identification and authentication for blockchain participants：

- If using traditional identity, how to support large-scale IoT devices to participate the blockchains.
- If using decentralized self-sovereign identity, how to authorize the participants to create and manage their self-sovereign identities.

8.2 Data generation and storage

Blockchain data are generated by blockchain peers under crowding consensus when they participate in transactions, and is decentralized and stored by whole of blockchain peers or part of the blockchain peers which involved in the transaction.

There are some key issues for data generation and storage for IoT and SC&C:

- When large-scale IoT devices are participating in a blockchain, how to make consensus and how to decentralized and stored blockchain data.
- Usually the IoT devices have limited computation and storage capabilities, how those types of IoT devices to participate in blockchains.

8.3 Data management

The operations of data management for blockchain data include adding, searching and accessing. Blockchain data cannot be changed (deleted, inserted and updated), but can be set to expired or updated through adding new blockchain data.

Deliverable of ITU-T FG-DPM, Technical Specification "*Blockchain Based Data Management for supporting IoT and SC&C*" (D3.7), provides more analysis on this topic.

8.4 Data exchanging and sharing

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

Deliverable ITU-T FG-DPM, Technical Specification "*Blockchain-based data exchange and sharing technology*" (D3.6), provides more analysis on this topic.

8.5 Cross-chain interaction and data mitigation

There are many kinds of blockchains for IoT and SC&C, and those blockchains are independent to each other. It's lack of standards for cross-chain interactions among the different blockchains, similarly there are issues on data mitigation from one blockchain to another blockchain.

8.6 Data security and privacy

Blockchain can keep data security for blockchain data. The blockchain data in a blockchain are hard to be changed, and because of the decentralized storages the blockchain data are uneasy to be lost.

In a blockchain, transaction progresses are usually transparent to whole or part of the blockchain peers according to its policies. It means that almost every participant can access all of the blockchain data. Transaction contents in a transaction can be encrypted, which provides privacy protection to a certain extent. However, there are some potential crisis for blockchain to process blockchain data for IoT and SC&C.

There are some key issues for data security and privacy for IoT and SC&C:

- In views of the capabilities of computation of majority of the 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.
- In views of the transparency of the transactions among the blockchain peers involved, this solution may leak some sensitive information of the participant.

8.7 Data auditing, tracking and tracing

As for the permission-less blockchains, the participants are anonymous to participate the blockchains with a random name (random hash string). It's uneasy or even unworthy to be audited the blockchain data in those types of blockchains.

In permissioned blockchains, the participants have authorized identities and it is worthy to be audited, tracked and traced.

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 database mode (centralized mode);
- Distributed database mode (distributed mode);
- Decentralized database mode (decentralized mode).

In centralized mode, data are located, stored and maintained in a single location (such as in a single data centre). In this mode, usually databases are managed by one maintainer. In distributed mode, data are located, stored and maintained in a single location, or spread across a network. Similar as in a centralized mode, although the data are distributed to be stored 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 not know each other and not trust each other.

There are some key issues for data generation and storage for IoT and SC&C:

- 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, it is needed to improve the efficiency of searching/accessing to blockchain data.
- Blockchain data are decentralized and stored by participants involved. When accessing the blockchain data from one participant, although the blockchain data stored are trusted, integrity of stored blockchain data by the participant should be validated.
- It is uneasy for the third-party applications to search and access blockchain data with SQL query language and interfaces in blockchains.

9 Analysis on the effects when using blockchain to support IoT and SC&C in DPM aspects

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

With the rapid evolutions of IoT networks and services of IoT and SC&C, more and more things (physical things and virtual things) are connected to the networks. According to industry statistics, the connections of things had exceeded the connections of human since 2017, and predictably, the connections of things will be to around 500 trillion to 2020 and 1000 trillion to 2025. The huge things' connections will reshape the IoT 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 take negative impacts on the IoT networks, including at least:

- Huge numbers of peer to peer connections and broadcast of messages may block the IoT networks, and take network signaling storm and network instability.
- Huge replications of distributed ledgers may make pressures for the IoT networks.

Those negative impacts are due to the contradictions between the traditional centralized/distributed mechanisms and decentralized mechanisms. Current IoT networks and service platforms are usually used traditional centralized/distributed mechanisms, and they don't adapt to the decentralized applications of blockchains.

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

9.2 Promoting the high-speed and low-latency services of IoT networks for data transmitting and processing

The blockchain-based technologies can help the IoT networks to serve for connections of tens of billions of IoT things with other technologies, such as SDN, NFV and edge computation. Through blockchain-based technologies, the capabilities of network scalability, collaboration and security could be improved, and trust network could be established with the higher efficiency and lower construction and operation cost.

Currently, IoT networks are centralized/distributed in which the edge nodes of the IoT networks are restrained by the core nodes in the core networks. Through the use of edge computation technologies, the IoT networks become flatter and flatter. Blockchain could be combined with edge computation

technologies. Using the decentralization approach of blockchains, almost all of the capabilities of core nodes could 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 each other to provide the connection services and to provide the capabilities that usually performed by core nodes, such as authentication and accounting etc.

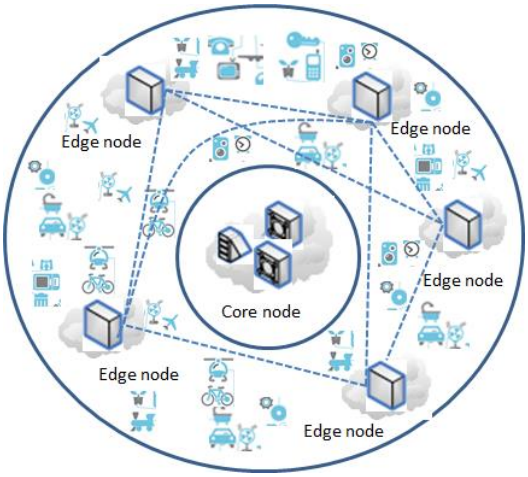

Figure 9-1 – Overview of a blockchain-enabled IoT network

In a blockchain-enabled IoT network, edge nodes have good independence. Those edge nodes with this feature could be effective and efficient to cooperate with each other, even 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 with the IoT devices, the IoT devices can get services from the edge nodes for data transmitting and processing with high-speed and low-latency.

In addition, blockchain-enabled IoT network can have good stability and anti-interference ability. Current centralized/distributed IoT network may be vulnerable when it is attacked, especially when the core nodes of the IoT network are attacked, and the entire network may be implicated. However, in the blockchain-enabled IoT network, the influence of the attacks on the IoT network in a certain area will not affect the 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

Because of many reasons (such as costs, technical improvements), in practices, IoT devices usually have limited security capabilities and can easily be hijacked. It is dangerous of a large number of hijacked IoT devices to be used to attack the communication networks or services at same time, such as Denial of Service (DDoS) attack, especially in the era of Internet of everything. It is big challenge of how to promptly recognize and screen which IoT devices are hijacked.

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, shown in Figure 9-2, if a home smart device (such as 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 to the blockchain. And then, when the light is used to attack other service platforms, the corresponding gateway can refuse the illegal access of the light, 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 repair in time.

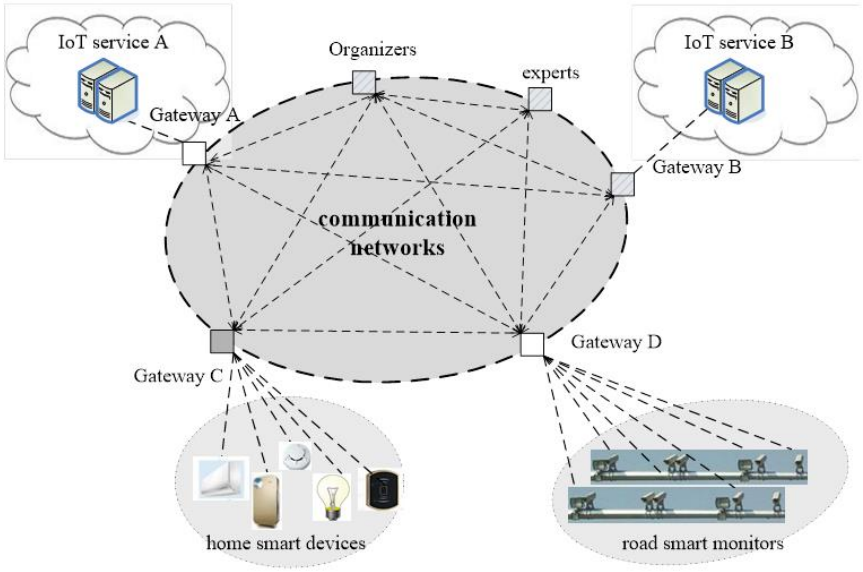

Figure 9-2 – Improving the capability for network and data security

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:

– **Public blockchain**: A public blockchain is public for all participants. In a public blockchain, the blockchain data is publicly available and viewable by anyone, anywhere. And 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. If a participant has a token, it has the same rights to participate into the blockchain, deploy smart contracts and make transactions. Any of the blockchain peers may contribute, as a volunteer, to secure entries to make consensus. And the ability to participate in consensus and resolution of transactions is completely open to any participants.

– **Consortium blockchain**: A consortium blockchain is usually deployed and maintained by a consortium. The distinction of a consortium blockchain is primarily on the method of making consensus. The consortium decides which participants in the blockchain will have the authority to deploy smart contract and make transactions, and decides how to open the blockchain data to the participants.

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

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

Bitcoin [b-1], Ethereum [b-2], Enterprise Ethereum [b-12], IOTA [b-5] and Hyperledger Fabric [b-3] are several representatives of blockchains.

I.1 Bitcoin

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

Bitcoin is origin of blockchain. The Figure I-1 provides a general framework of Bitcoin. Bitcoin usually is consisted of four groups of functionalities:

- Data processing: functionalities to process data, including block data management, chain management, data signature, hash algorithms, Merkle tree management, crypto (symmetric and asymmetric encryption), etc.
- Networking: functionalities to network communication, including peer to peer communication, broadcast and communication validation, etc.
- 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.

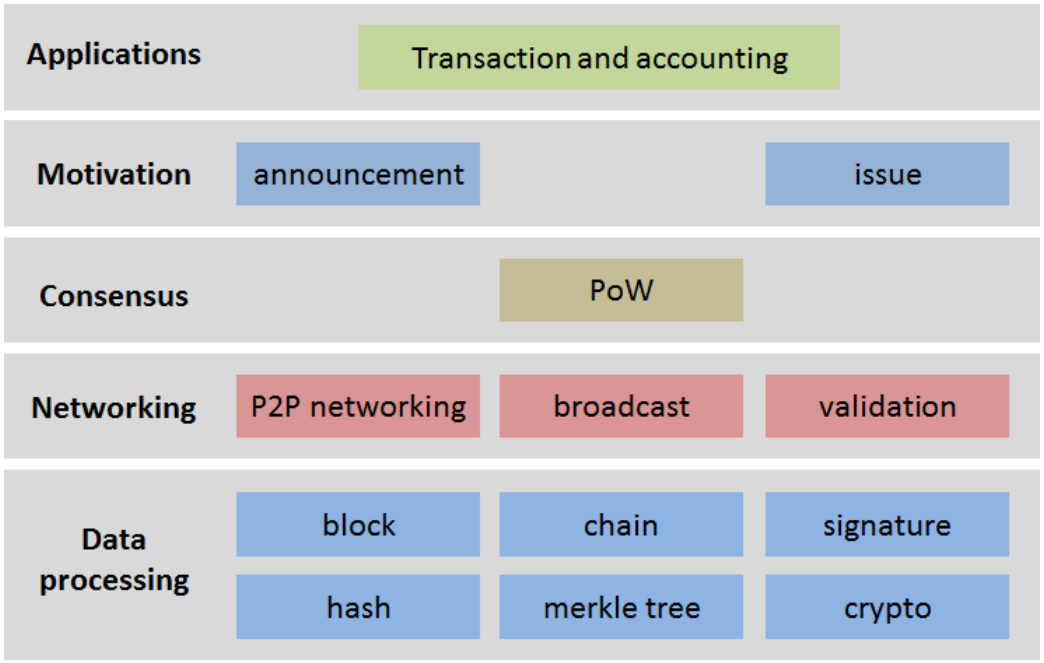

Figure I-1 – General framework of Bitcoin

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

I.2 Ethereum and Enterprise Ethereum

Ethereum is an open blockchain platform which focused 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 the mining peers' computers. The resulting state of the smart contract is stored in the blockchain by the user that publishes the next block. The Figure I-2 provides a general framework of Ethereum, which is consisted of four groups of functionalities:

- Data processing: similar as that in Bitcoin.
- Networking: similar as that in Bitcoin.
- Consensus: consensus is pluggable, PoW, PoS, DPoS or other consensus algorithms.
- Motivation: similar as that in Bitcoin.

– Smart contract: functionalities related smart contract, including virtual machine (VM) and contracts.

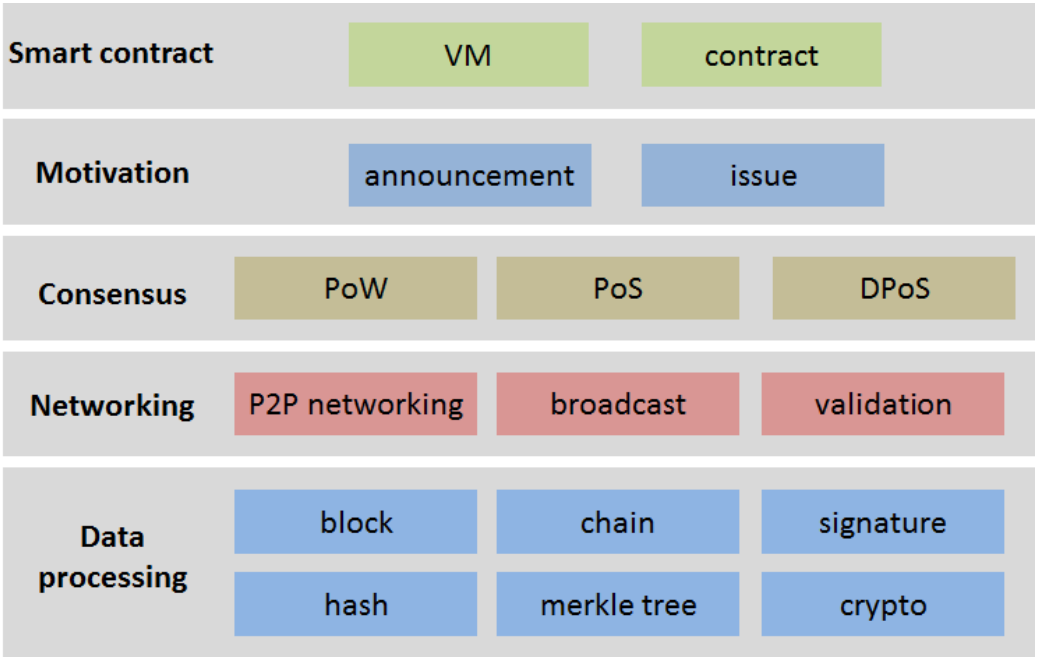

Figure I-2 – General framework of Ethereum

In Ethereum, there are two key features, one is supporting the pluggable consensus, and another is supporting smart contracts. Those features make wider applications of the 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 managing, 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 is founded by the Linux Foundation [b-4] 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 blockchains 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 not want every transaction what 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:

- 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 transacting. Membership services manage the identities for ledger and resources, and manage the configuration, access control and privacy.
- Blockchain services manage the distributed ledger through peer-to-peer protocols. The data structures are optimized to provide efficient schemes for maintaining blockchain data (e.g. the world state) replicated at many participants. Different consensus algorithms guaranteeing strong consistency (tolerating misbehavior with BFT, tolerating delays and outages with crash-tolerance, or tolerating censorship with PoW) may be plugged in and configured per 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, researching results, life-cycle controlling etc.)

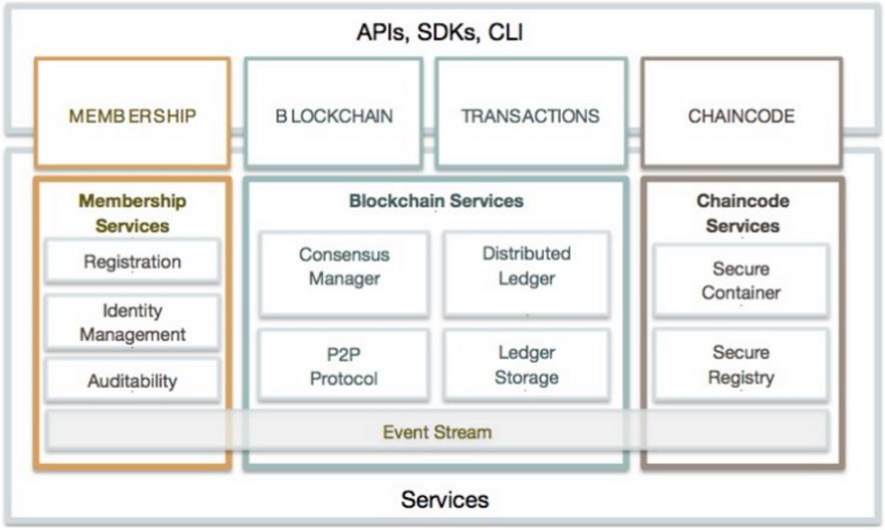

Figure I-3 – General framework of Hyperledger fabric

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

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

Bibliography

[b-1] Bitcoin: *https://www.bitcoin.com*

[b-2] Ethereum: *http://www.ethereum.org*

[b-3] Hyperledger: *http://www.hyperledger.org*

[b-4] Linux Foundation: *https://www.linuxfoundation.org*

[b-5] IOTA: *https://www.iota.org/*

[b-6] Proof of Work: *https://en.wikipedia.org/wiki/Proof-of-work_system*

[b-7] Proof of Stake: *https://en.wikipedia.org/wiki/Proof-of-stake*

[b-8] Delegated Proof of Stake: *https://en.wikipedia.org/wiki/BitShares*

[b-9] Practical byzantine fault tolerant: *https://en.wikipedia.org/wiki/Byzantine_fault_tolerance*

[b-10] Federated Byzantine Agreement:
https://en.wikipedia.org/wiki/Federated_Byzantine_Agreement

[b-11] Round Robin: *https://en.wikipedia.org/wiki/Round-robin*

[b-12] Enterprise Ethereum: *https://entethalliance.org/*