Featured Articles I

Work on the Potential and Challenges of Blockchain Technology

Nishio Yamada
Miwa Tsukuda
Jun Nemoto
Ken Naganuma
Nao Nishijima
Tatsuya Sato

OVERVIEW: Blockchains have attracted interest as an innovative technology designed to lower transaction costs by securely enabling direct transactions among an indeterminate number of mutually untrusted users. Hitachi is working on blockchain R&D by drawing on the security technology and distributed data processing technology it has accumulated from building mission-critical systems. This article discusses the challenges that were of greatest concern in discussions with blockchain user companies, and summarizes Hitachi's work on overcoming these challenges. Through Hyperledger Project community activities, Hitachi aims to develop standardized blockchain platforms, to develop highly dependable functions, and to create blockchains that can be applied in social infrastructure.

INTRODUCTION

BLOCKCHAINS have attracted interest as an innovative technology expected to offer significant cost reductions by enabling transactions to be executed as peer-to-peer (P2P) processes directly between users. It offers an alternative to the conventional method of using a trusted third-party organization (such as a financial institution or government agency) as an intermediary. Currently past the Technology Trigger phase of the hype cycle, blockchains are now positioned somewhere after the Peak of Inflated Expectations. Many vendors and user companies are conducting their own demonstration tests to uncover the technology's challenges, working independently to improve it and to enable its practical application. Surmounting the anticipated Trough of Disillusionment on the hype cycle and expanding the range of blockchain applications further will require standardizing today's messy array of blockchain technologies and developing technology to enable cross-industry use cases such as those coordinating finance and logistics, or settling small amounts from devices connected to the Internet of Things (IoT). Since today's blockchain technology still has many challenges to overcome, making it more reliable is a crucial requirement when using it in the systems that underpin social infrastructure in areas such as finance or government.

This article discusses the challenges facing blockchains and presents the results of repeated discussions with financial institutions and related government agencies that are blockchain user companies. The article also looks at Hitachi's approach to working on these challenges, its community activities in The Linux Foundation's[*1] Hyperledger[*1] Project, and its work on developing highly dependable functions.

BLOCKCHAIN FEATURES AND CHALLENGES

Blockchain Features

Blockchains have attracted interest as the technology underlying the Bitcoin[*2] cryptocurrency. Various derivative technologies based on the three Bitcoin blockchain design concepts below have been proposed and are currently evolving.

(1) P2P transactions among users on a blockchain network by participant approval without using a third-party organization as an intermediary

(2) Grouping multiple transactions into blocks, recording them in distributed ledgers chained together, and performing hash calculations on consecutive blocks to make modification effectively impossible

(3) Enabling transactions to be verified by all participants by sharing the same ledger data among all participants

[*1] Hyperledger is a trademark of The Linux Foundation. Linux Foundation is a registered trademark of The Linux Foundation. Linux is a registered trademark of Linus Torvalds.

[*2] Bitcoin is a registered trademark of bitFlyer, Inc.

Table 1. Blockchain Challenges

The table shows the top five challenges that were of greatest concern in discussions with user companies. The challenges mainly concern the private domain.

No.	Challenge
1	User privacy protection
2	Processing speed, number of processes per unit of time
3	Finalizing transactions
4	Coordination with existing systems
5	Blockchain reliability

Blockchain Challenges

Hitachi has held repeated discussions with over 50 blockchain user companies, including financial institutions and government agencies, that have studied the use of blockchains. Table 1 lists the top five challenges discussed.

Almost all the user companies mentioned privacy protection, processing speed and finalizing transactions in the discussions. These are security and system performance issues related to non-functional requirements. Since block data is shared by all network participants, analyzing all the data could create issues, such as the ability to track the amount of a remittance made from a payer to a payee (No. 1 in Table 1). Since processing time is needed to approve a transaction and maintain ledger consistency, the number of processes per unit of time will be low (No. 2 in Table 1). When using an approval algorithm called a proof-of-work (POW) to approve a transaction, the probability of transaction finality increases over time, and the transaction is not finalized rigorously (No. 3 in Table 1).

Many users said they want to start using blockchains on a limited basis and gradually expand their usage, but there are challenges with linking one blockchain to another and with coordinating blockchains with existing systems (No. 4 in Table 1). There were an equal number of discussions about system reliability once blockchain use gets fully underway in the future (No. 5 in Table 1). For example, there were discussions on continuous system operation and the potential for database expansion.

HITACHI'S EFFORTS

Work Approach

Hitachi takes a three-phase approach to expanding the application of blockchains (see Fig. 1).

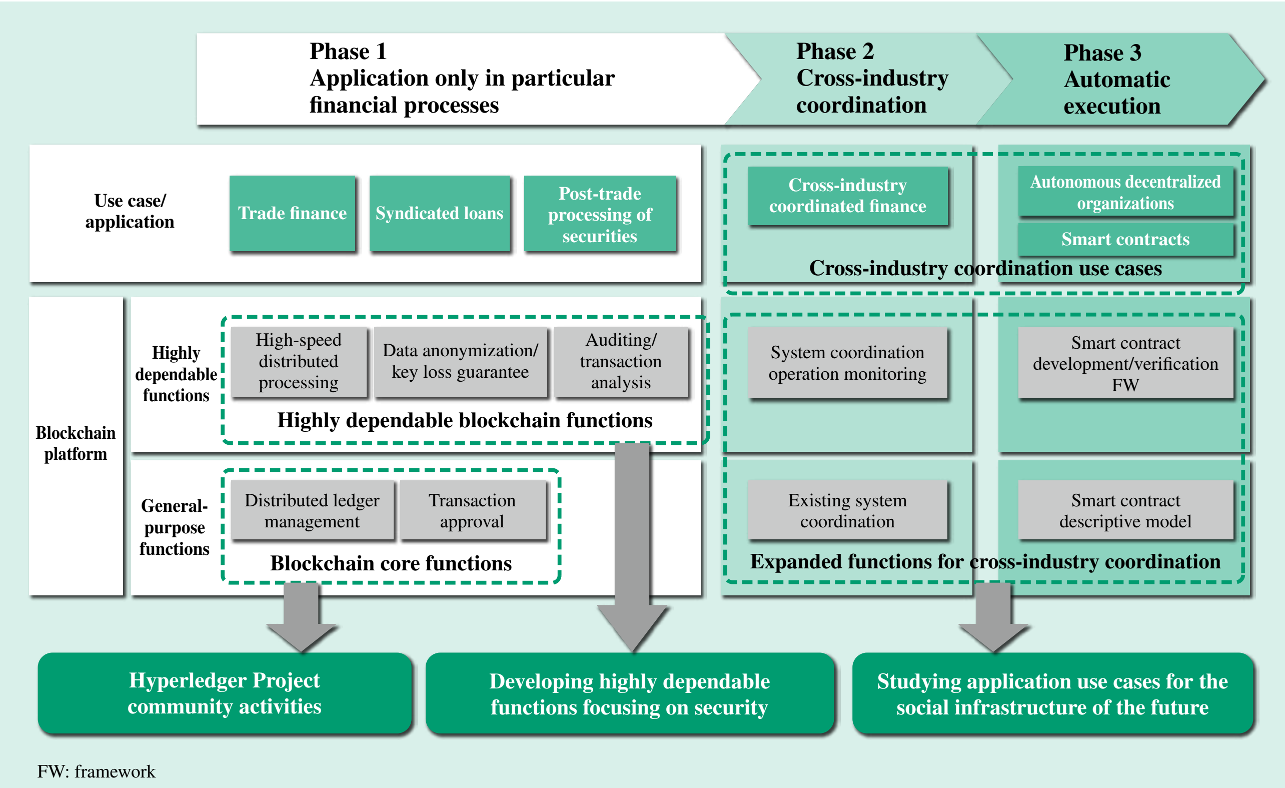
Phase 1
Application only in particular financial processes
Phase 2
Cross-industry coordination
Phase 3
Automatic execution
Use case/ application
Trade finance
Syndicated loans
Post-trade processing of securities
Cross-industry coordinated finance
Autonomous decentralized organizations
Smart contracts
Cross-industry coordination use cases
Blockchain platform
Highly dependable functions
High-speed distributed processing
Data anonymization/ key loss guarantee
Auditing/ transaction analysis
Highly dependable blockchain functions
System coordination operation monitoring
Smart contract development/verification FW
General-purpose functions
Distributed ledger management
Transaction approval
Blockchain core functions
Existing system coordination
Smart contract descriptive model
Expanded functions for cross-industry coordination
Hyperledger Project community activities
Developing highly dependable functions focusing on security
Studying application use cases for the social infrastructure of the future
FW: framework

Fig. 1—Hitachi's Approach to Expanding the Application of Blockchain.
Starting with the application of blockchains only for particular financial processes, Hitachi is expanding its application to cross-industry coordination, and automatic execution using smart contracts.

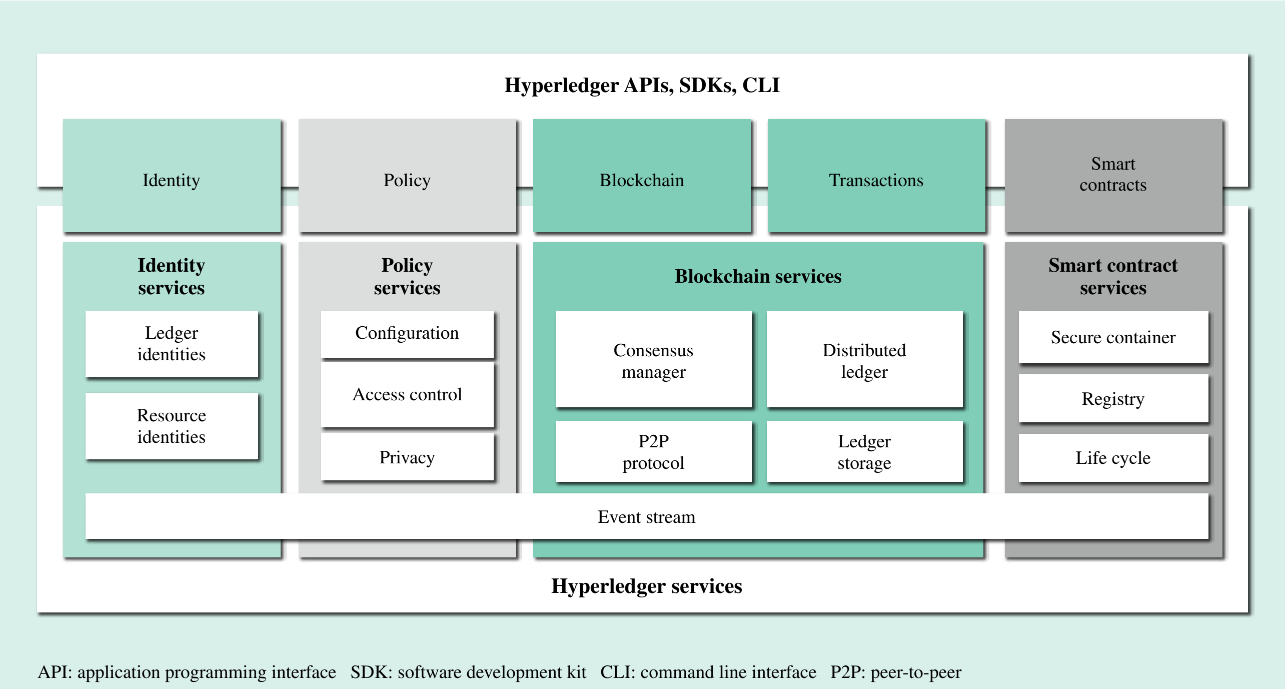

Fig. 2—Platform Architecture Developed by Hyperledger.
The platform architecture consists of five main component elements.

In Phase 1, Hitachi will study the use of blockchains for particular operations in the financial industry (which is actively working on blockchains), such as syndicated loans and post-trade processing of securities. It will also examine and improve the functions provided by blockchain platforms. Specifically, Hitachi will take part in Hyperledger Project community activities to develop globally standardized versions of core functions provided by blockchain platforms such as distributed ledger management and transaction approval. Another crucial requirement will be strengthening the blockchain platform functions that are mostly unrelated to blockchain functionality itself (as described in the list of challenges in the previous section), since financial infrastructure demands high reliability. Hitachi will develop highly dependable functions designed for application in financial infrastructure such as data anonymization and auditing functions. This work will be done by demonstration testing informed by Hitachi's expertise in constructing mission-critical financial systems, and by research findings in areas such as security and data processing technologies.

In Phases 2 and 3, Hitachi will investigate coordination between finance and other industries such as logistics or healthcare. It will also draw on knowledge it has acquired from a wide range of business domains to investigate use cases for cross-industry coordination between industries that will underpin social infrastructure in the future. Examples include smart contracts involving the IoT and artificial intelligence (AI) designed to enable the creation of autonomous decentralized organizations. It will develop expanded functions for cross-industry coordination to enable these use cases, further enhancing the reliability of blockchain platforms. These expanded functions will include functions that coordinate blockchains with existing systems, and functions that verify smart contracts have been implemented properly in line with the specifications.

Hyperledger Community Activities

(1) Overview of community activities

The Linux Foundation created the Hyperledger Project in February 2016 as a way to develop blockchain platforms with open source software. Hitachi has been a premier member of the project since its inception, and has worked with other participants such as The Depository Trust & Clearing Corporation (DTCC) and JPMorgan Chase & Co. to engage in community activities such as studying use cases and developing blockchain platforms. Specifically, Hitachi is helping develop standardized blockchain platforms by taking part in the Technical Steering Committee, through which researchers from the Santa Clara-based Hitachi Financial Innovation Laboratory coordinate with researchers in Japan to study technologies.

(2) Architecture

Since different blockchain application use cases will have different platform requirements, the approach being used in the Hyperledger Project development work is to modularize platform functions as much as possible. Switching the modules as necessary to match the use case requirements will improve development speed and reduce cost.

The blockchain platform architecture being developed by Hyperledger consists of five main component elements (see Fig. 2). Table 2 shows the main elements and summaries of the other elements. The Practical Byzantine Fault Tolerance (PBFT) consensus algorithm and the algorithms that extend it are used for approving transactions. Among the challenges listed in the previous section, these algorithms solve the challenge of finalizing transactions[3].

(3) Future approaches

Hyperledger is planning to expand functions, such as those described in (a) and (b) below. Among the challenges listed in the previous section, (a) is one attempt to solve the issue of blockchain reliability, and (b) is one attempt to solve the issue of coordination with existing systems.

(a) PBFT requires that there are a fixed number of verification nodes governing the approval of transactions, which was a challenge because the algorithm is unable to satisfy the desire for continuous system operation. Hyperledger will develop a PBFT algorithm that enables the number of verification nodes to be changed dynamically.

(b) Using blockchains to replace existing systems previously developed by user companies is difficult because of the time and cost required, making a function that coordinates existing systems with blockchains a crucial requirement. These functions will therefore be developed along with functions that coordinate blockchains with each other.

Developing Highly Dependable Functions

Concurrent with the Hyperledger Project community activities, Hitachi is working to enable the use of blockchains in financial infrastructure by developing highly dependable functions that harness the security technologies and distributed processing technologies that are Hitachi's strengths.

To solve the challenge of privacy protection for users, which is of great interest to user companies, Hitachi is developing data anonymization technology in the form of highly dependable functions driven by its security technologies. This data anonymization technology uses an encryption method called zero-knowledge proof to anonymize blockchain data, and it offers the benefit of making it impossible for a third party to correlate the sender with the receiver even by analyzing all of the data in the blockchain. Only the designated auditor can correlate the sender and receiver.

Transactions can no longer be performed on a blockchain once the key is lost. In the case of a virtual currency, losing the key results in the currency owner no longer being able to perform transactions and losing the currency. To solve this challenge, Hitachi is developing a key loss guarantee function driven by biometric authentication. If the secret key is lost, this function enables the secret key and public key certificates to be reissued using biometric authentication to enable continued transactions.

Table 2. Summaries of Architecture Component Elements

Summaries of the component elements in Fig. 2 are shown below.

Component element	Description
Identity services	This component manages the IDs of all network objects (such as blockchain network participants, smart contracts, and verification nodes used for consensus).
Policy services	This component manages policies. It provides access control and authority management, and manages areas such as participant privacy and consensus rules.
Blockchain services	This component contains elements such as the P2P protocol, distributed ledger, and consensus manager. • P2P protocol: This element provides P2P functions such as bidirectional streaming, flow control, and request multiplexing. It works in coordination with existing networks. • Distributed ledger: This element manages the blockchain and status. • Consensus manager: This element provides the interfaces for plug-in consensus algorithms such as the PBFT interface.
Smart contract services	This component provides the means for executing smart contracts on verification nodes. It contains a secure execution environment, and smart contract life cycle (deploy-update-terminate) management functions.
Event stream	This element provides pub/sub event management functions. For example, it enables outside systems to detect distributed ledger events.
API	This element provides the API for the component elements above. It also contains open source APIs.

PBFT: Practical Byzantine Fault Tolerance pub/sub: publish/subscribe

Hitachi is also working to further enhance the reliability of the system by developing a PBFT algorithm that enables dynamic node addition, a system monitoring function for assisting continuous system operation, and a scalable data store used to ensure blockchain data capacity expandability.

CONCLUSIONS

This article has described the blockchain challenges Hitachi uncovered through discussions with user companies, along with the work Hitachi is doing to overcome these challenges. To enable the use of blockchains in financial infrastructure, Hitachi will work steadily on developing standardized platforms through the Hyperledger Project. Hitachi would like to further enhance the technology's reliability through function expansion, and develop blockchain platforms that enable cross-industry coordination use cases that will shape the social infrastructure of the future.

REFERENCES

(1) S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (2008).
(2) Hyperledger Project website, https://www.hyperledger.org/
(3) Fabric, https://github.com/hyperledger/fabric/

ABOUT THE AUTHORS

Nishio Yamada
System Productivity Research Department, Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of blockchain applications. Mr. Yamada is a member of the Information Processing Society of Japan (IPSJ) and the Japan Society for Management Information (JASMIN).

Miwa Tsukuda
Financial Innovation Center, Financial Information Systems Sales Management Division, Financial Institutions Business Unit, Hitachi, Ltd. She is currently engaged in the planning of blockchains and AI.

Jun Nemoto
Storage Research Department, Center for Technology Innovation – Information and Telecommunications, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of blockchain platforms and data storage. Mr. Nemoto is a member of the IPSJ.

Ken Naganuma
Security Research Department, Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of security technologies for blockchains and cloud computing. Mr. Naganuma is a member of the Japan Association for Medical Informatics (JAMI).

Nao Nishijima
Digital Solution Platform Laboratory, Global Center for Social Innovation – North America, Hitachi America, Ltd. He is currently engaged in the research and development of blockchain platforms and cloud services. Currently, he contributes to the Hyperledger Fabric Project.

Tatsuya Sato
Cloud Research Department, Center for Technology Innovation – Information and Telecommunications, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of blockchain platforms and cloud services. Mr. Sato is a member of the IPSJ and the IEEE.