METI
Ministry of Economy, Trade and Industry

# Evaluation Forms for Blockchain-Based System ver. 1.0

12 April 2017

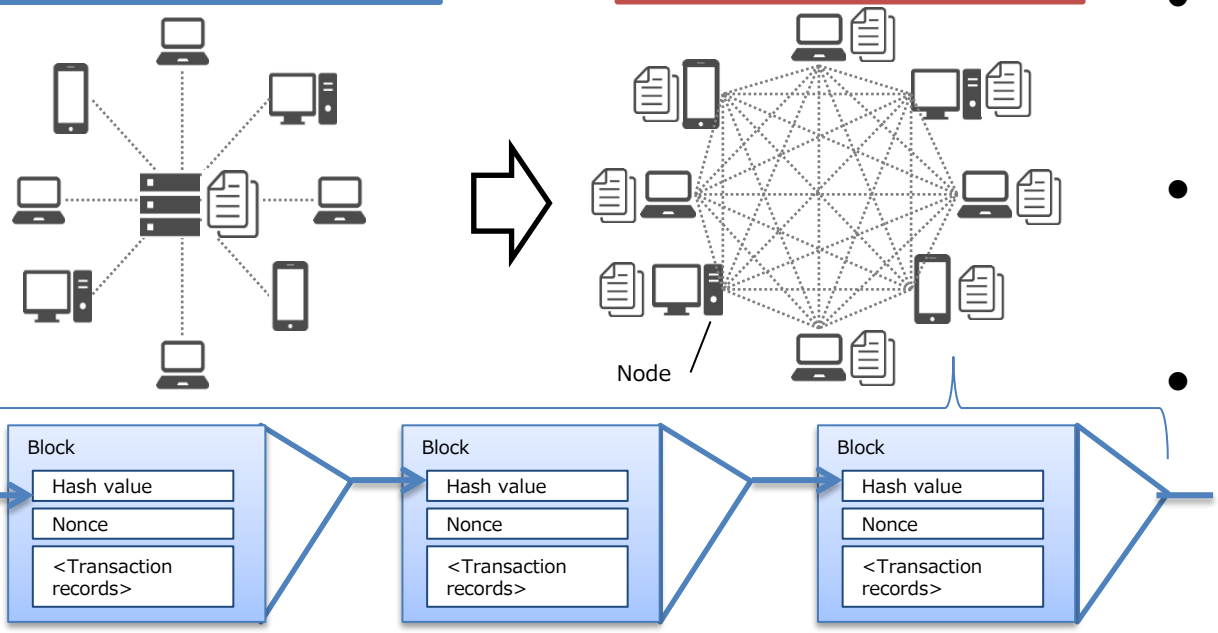
Information Economy Division
Commerce and Information Policy Bureau

# Background of this Survey

- Blockchain technologies are new types of technology used for trading virtual currencies, e.g., Bitcoins. The important features of blockchain technology are that it is extremely difficult to falsify compared to conventional systems, and that inexpensive systems that cause no downtime in effect could be built. Therefore, the technologies are expected to be applied in a wide variety of fields.
- However, no evaluation indices or criteria had been established to adequately assess the features of the technologies and to compare them with existing systems. This causes the public anxiety, misunderstanding, and unreasonable hopes to blockchain technologies, and leading to a potential unwillingness to introduce the technology.

**Centralized system (Conventional system)**

**Blockchain-based system**



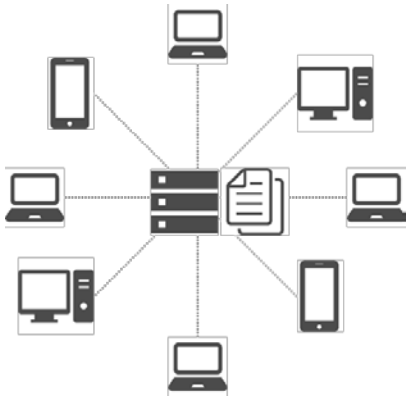

## Characteristics of Blockchain (examples)

- Each node owns the same transaction histories, thus single point of failure doesn't exist, enabling "***no downtime in effect***"
- Transaction records are successively stored in blocks, and these are added to a chain of existing blocks. Therefore, it is ***extremely difficult to falsify***.
- Blockchain-based systems can be developed at ***lower cost*** than existing systems of similar secureness, by combining technology elements such as node distribution, consensus algorithm.

# Value of Evaluation Forms of Blockchain-based Systems

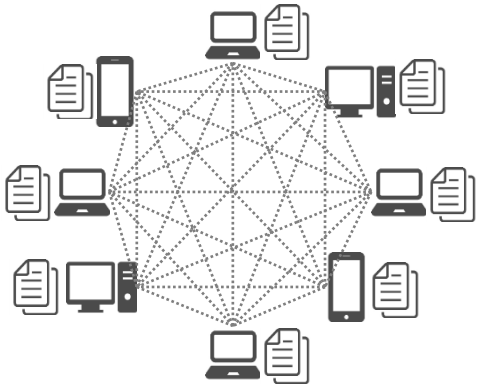
- ISO/IEC has already established evaluation models for conventional IT systems, which are used by corporates/organizations in discussing the introduction of a new system.
- However, this model can't be directly used for blockchain-based systems, due to unique tradeoff caused by the structure of blockchain (e.g. Consensus between multiple nodes)

**Centralized system (Conventional system)**



- Performance of this kind of systems can be evaluated with specification of one single equipment, because generally it greatly varies depending on performance of computer hardware composing this equipment or its number.
- Discussion concerning the quality of this type of systems & related software have been advancing, leading to the formulation of series of international standards as ISO/IEC 25000(SQuaRE).

**Blockchain-based system**



- Performance of this kind of systems is difficult to be evaluated with one single value, because it depends on various unique tradeoff characteristics, such as consensus algorithm or number of nodes.
- No discussions on the evaluating the quality of this type of system have started yet inside or outside Japan.

**The world's first Evaluation forms of Blockchain-based systems are established, by taking account of comparability with existing systems & comprehensiveness, and by examining tradeoff between evaluation items**

# Strategy for Establishing Evaluation Forms

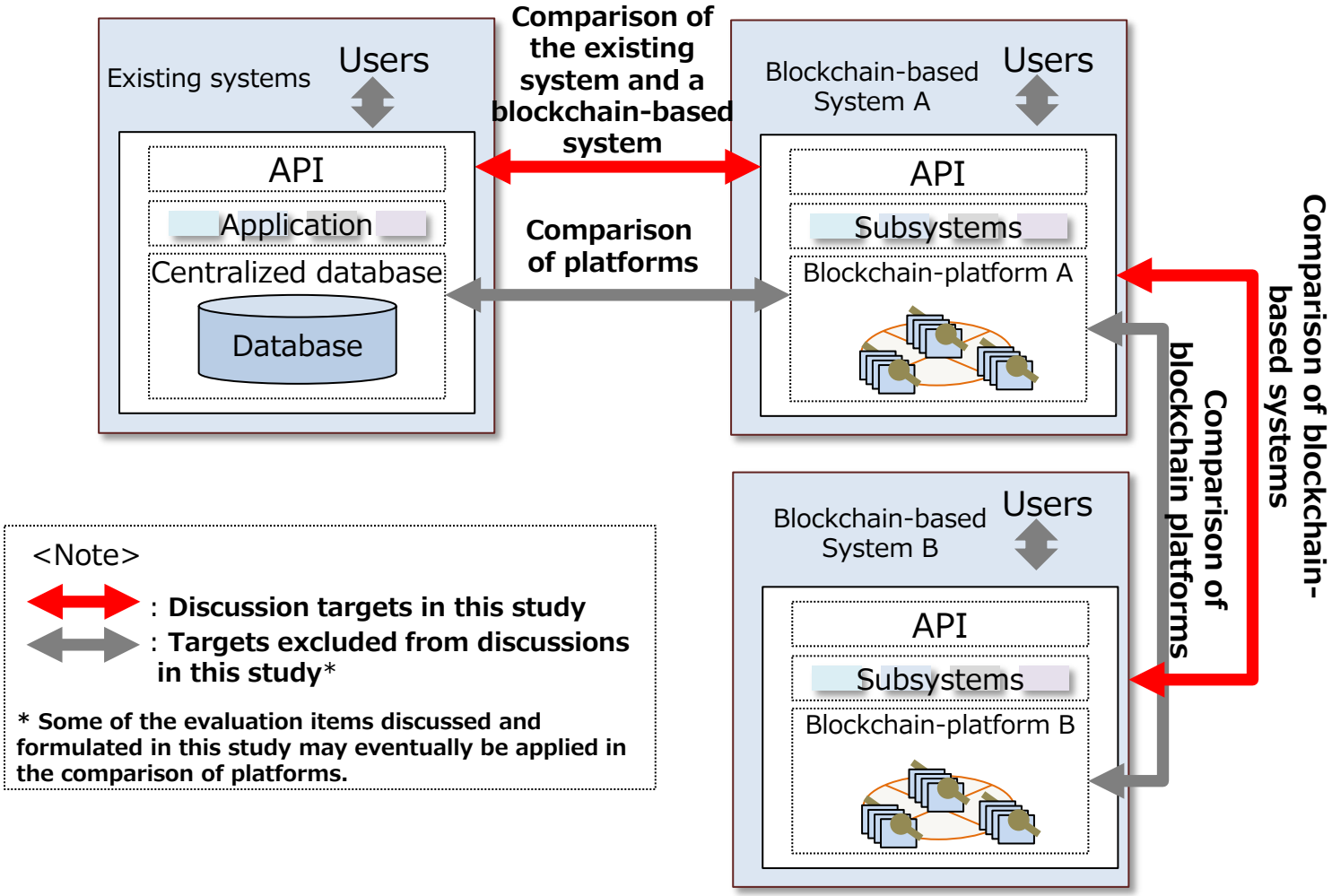
Evaluation forms were established according to the following strategy, through domestic/global surveys of literatures & actual use cases of blockchain-based systems, and discussion in the Study Committee of Experts*. *Appendix

| Discussion topics | | Strategy for establishing Evaluation forms |
|---|---|---|
| **Purpose of Evaluation form** | | ■ Appropriately describe features of blockchain-based systems<br>■ Cover all items required in assumed use situations※<br>※ Major use situations of this Evaluation forms are assumed as evaluation by system vendors to compare conventional systems and blockchain-based systems, to evaluate replacement options. |
| **Evaluation object** | Object of comparison | ■ Comparison of conventional systems & blockchain-based systems<br>■ Comparison of multiple blockchain-based systems |
| | Scope (detail①) | Whole systems using blockchain (blockchain platform + related subsystems) |
| | Treatment of systems with business process restructuring | ■ Systems enabling brand-new services, or drastic changes in business process/requirement, are out of scope of this study, because there are no conventional counterparts to be compared.<br>■ Systems leading to slight changes in business process is still in scope |
| | Platform classification (detail②) | ■ All patterns of platforms are in scope of evaluation, despite platform classification (public/consortium/private) or consensus algorithm<br>■ Evaluation points to note for each pattern are specified in the remarks |
| | Coverage/comprehensiveness of use cases | ■ Covering all required items, taking account of different requirements in various use cases |
| **Components** Item Index Method (detail③) | | ■ Evaluation items strongly relevant to blockchain-based systems are selected from ISO/IEC25010 for quality, and from IPA reference model for maintenance/operation.<br>■ Cost evaluation form is composed of cost items directly recognized by system vendors (≒prices for system users)<br>■ No evaluation indices or methods are specified. Evaluation points to note are described in detail. |

# Study of Evaluation Forms① (Scope of Evaluation)

- Scope of this Evaluation forms is whole system (blockchain platform + related subsystems)
- It is assumed that evaluating functions or performance of “system as a whole” is important in the assumed major use cases (evaluation by system vendors & investment decision by system users)

## Schematic of the Scope of Evaluation Forms



# Study of Evaluation Forms ② (Classification of Platform)

- Public/Consortium/Private blockchains are different in governance, identity of users, etc., and own different characteristics. Evaluation forms are aimed to cover all of these patterns.
- Evaluation points to note due to these difference are described for each evaluation items.

## Typical classification of blockchain platform by governance scheme

*Modified from IBM release document

| | Public | Consortium | Private |
|---|---|---|---|
| Governance | - | Several parties | One single party |
| Identity of users | Free | Permissioned | |
| | Not specified, may contain malicious members | Specified, composed of reliable members | |
| Consensus algorithm | PoW etc. | PBFT etc.<br>(Practical Byzantine Fault Tolerant) | |
| | Multi-block confirmation<br>Large electricity consumption | Immediate block confirmation<br>Simple / Fast / Small electricity consumption | |
| Processing time of transaction | Long (e.g. 10 min) | Short (e.g. a few sec) | |
| Use case | Virtual currency etc. | Business network as interbank transfer, stock exchange etc. | |
| Example | Bitcoin, Ethereum etc. | Ripple, Hyperledger Fabric etc. | |

# Study of Evaluation Forms ③ (Component)

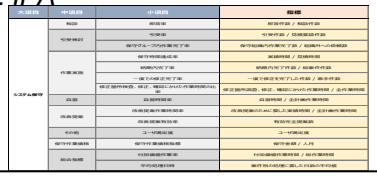
- Quality evaluation items, which are strongly related to technology & characteristics of blockchain, are excerpted from ISO/IEC25010 (system and software quality model)
- Maintenance/Operation evaluation items are similarly excerpted from IPA (System Reference Manual, Chapter 4 “Maintenance and Operation,” 2005)
- Cost items directly recognized by system vendors, in deciding pricing for customers, are summarized

## Structure of Evaluation form

＊BC= blockchain

Quality model of system & software
*Source: ISO/IEC 25010*

Evaluation criteria for system maintenance & operation
*Source: IPA*



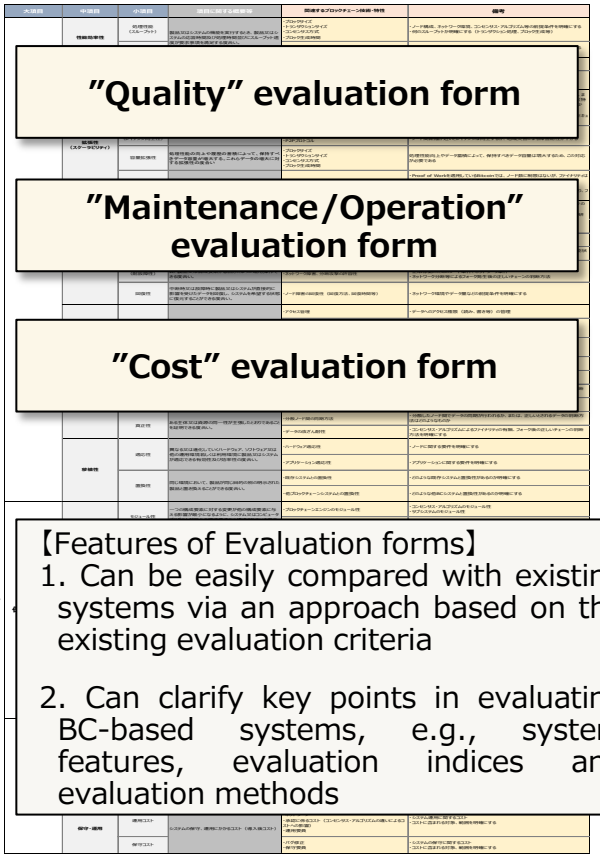
Cost perspective concerning
- Research & Development
- Implementation
- Maintenance/operation

Characteristics of BC-based systems
- Opinion and discussions among the members of the Study Committee of Experts
- Interview-based surveys targeting experts
- Document-based study

**New evaluation criteria based on the existing evaluation criteria**
- Accessibility to comparison with existing systems
- Ensuring comprehensiveness

**Elimination/Addition of Evaluation items focusing on characteristics of BC-based systems**
- Evaluation items specialized for BC tech. and characteristics
- Providing a sufficient number of remarks and key points to be included

Evaluation forms of BC-based systems



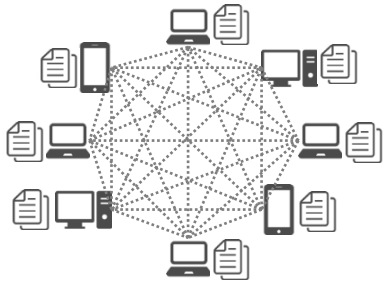

【Features of Evaluation forms】
1. Can be easily compared with existing systems via an approach based on the existing evaluation criteria
2. Can clarify key points in evaluating BC-based systems, e.g., system features, evaluation indices and evaluation methods

# Study of Evaluation Forms ④ (Consideration of Characteristics of Blockchain)

- Characteristics of blockchain are taken into account for relating evaluation items.
- Various evaluation items & characteristics are in tradeoff relationship.

## Examples of characteristic of blockchain

- **The same transaction histories are stored by distributed nodes**

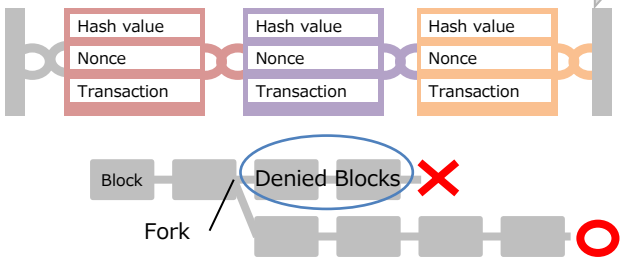


## Examples of relevant evaluation items

- Generally, availability and fault tolerance are high.
- Various characteristic are affected by node structures, network, consensus algorithm etc., and are in tradeoff relationship.

<Example of Quality Evaluation items>
availability, fault tolerance, network latency (& its scalability), data reference etc.
<Example of Maintenance/Operation Evaluation items> Analyzability etc.
<Example of Cost Evaluation items> Implementation cost etc.

- **Several records are stored in one block, and it is connected to existing blocks with cryptographic signature**




(Schematics of “fork”)
After fork happens, produced block may be denied later.

- Generally it is difficult to falsify however, block size and confirmation time etc. are related with various characteristics (scalability etc.), making tradeoff.
- Depending on applied consensus algorithm, possibility exists that branched (forked) blocks are later denied.

<Example of Quality Evaluation items>
Throughput, capacity scalability, block confirmation, non-repudiation, authenticity etc.
<Example of Maintenance/Operation Evaluation items> Modifiability etc.

# Evaluation Forms for Blockchain-Based System ver. 1.0 Overview

- Evaluation forms are composed of the following 32 evaluation items, which are especially closely related to the characteristics of blockchain technology.

| Large Category | Category | Evaluation items |
|---|---|---|
| Quality | Performance Efficiency | Throughput |
| | | Network latency |
| | | Block confirmation |
| | | Data reference |
| | Interoperability | Interoperability with existing systems |
| | | Interoperability with other blockchain systems |
| | Scalability | Throughput |
| | | Network latency |
| | | Capacity |
| | Scalability | Number of nodes |
| | Reliability | Maturity |
| | | Availability |
| | Reliability | Fault Tolerance |
| | | Recoverability |
| | Security | Confidentiality |
| | | Integrity |
| | | Non-repudiation |
| | Security | Authenticity |
| | Portability | Adaptability |
| | | Replaceability |

| Large Category | Category | Evaluation items |
|---|---|---|
| Maintenance / Operation | Maintainability & operability | Modularity |
| | | Reusability |
| | | Analyzability |
| | | Modifiability |
| | | Testability |

| Large Category | Category | Evaluation items |
|---|---|---|
| Cost | R&D | R&D of Blockchain platform technical elements |
| | | R&D of subsystems |
| | Implementation (Commercialization) | Hardware cost |
| | | Software cost |
| | | System implementation cost |
| | Maintenance & operation | Operational cost |
| | | Maintenance cost |

# Evaluation Forms for Blockchain-Based System ver. 1.0 - Quality (1/5)

＊BC= blockchain

| Category | Evaluation item | Outline of category | Related BC technology & BC characteristics | Points to remember and remarks on using Evaluation form |
|---|---|---|---|---|
| **Performance Efficiency** | Throughput | This characteristic represents the performance relative to the amount of resources used under stated conditions. | ・Block size<br>・Transaction size<br>・Consensus algorithm<br>・Block confirmation time | ・ Clarify the preconditions for the node configuration, network environment, consensus algorithm etc.<br>・ Clarify the definition of throughput. For example, “the target is transaction processing and theoretical performance.”<br>・ Clarify the tradeoff between with other evaluation items.<br>*For details of the tradeoff, see the item “Scalability - Throughput.” |
| | Network latency | | ・Network environment<br>・Node Distribution | ・ Clarify the preconditions for the node configuration and network environment etc.<br>・ Clarify the definition of latency.<br>For example, “select two nodes randomly and measure the time taken to transmit ● kB data between the nodes. Average the iteration values”. |
| | Block confirmation | | ・Consensus algorithm<br>・Network environment<br>・Node Distribution | ・ Clarify the definition of block confirmation time (e.g., time from when a transaction is thrown until when a block is generated).<br>・ Clarify the characteristics and tradeoff of the used consensus algorithm, as in the following: “In the case where the block is confirmed completely, it is the time until confirmation. In the case where the block is not confirmed completely, it is the time until confirmation with a probability of ●%.”<br>For example, “this system adopts PoW, thus the block cannot be confirmed completely. When the block depth is 6, the probability is ●%. Also, there is no restriction on the number of nodes.”<br>・ Clarify the tradeoff with other evaluation items.<br>*For details of the tradeoff, see the item “Scalability - Throughput.” |
| | Data reference | | ・Node Distribution<br>・Network environment<br>・Block structure | ・ Performance for referring to a specific block and transaction.<br>Clarify the preconditions of the node configuration and network environment. |

# Evaluation Forms for Blockchain-Based System ver. 1.0 - Quality (2/5)

＊BC= blockchain

| Category | Evaluation item | Outline of category | Related BC technology & BC characteristics | Points to remember and remarks on using Evaluation form |
|---|---|---|---|---|
| **Interoperability** | Interoperability with existing systems | Degree to which two or more systems, products, or components can exchange information and use the information that has been exchanged. | ・Data structure<br>・API specification | ・ Clarify the preconditions for interoperability.<br>・ Clarify the experience of interoperability with existing systems. |
| | Interoperability with other BC systems | | ・Data structure<br>・Consensus algorithm<br>・API specification | ・ Clarify the preconditions for interoperability.<br>・ Clarify the experience of interoperability with other BC systems. |
| **Scalability** | Throughput | Degree of improvement of performance | ・Block size<br>・Transaction size<br>・Consensus algorithm<br>・Block confirmation time | ・ Clarify the possible method for improving throughput and tradeoff caused by the method.<br>[Tradeoff to be specified]<br>・ Tradeoff related to reliability: For example, “as the throughput improves, the data load becomes heavier, especially for the full nodes which store all the data, and the sites that can function as full nodes decrease. As a result, the reliability is lowered. If the number of full nodes decrease to ● or less, it is difficult to meet the requirements.”<br>・ Tradeoff resulted from applied consensus algorithm: For example, “the throughput is increased by applying high-speed ●● consensus algorithm. This algorithm requires approved nodes that are specifically managed, and the upper limit of such nodes is around 30 for practical operation. If one thirds of these nodes are suspended, the system function cannot be maintained and thus the availability decreases, leading to ▲.” |
| | Network latency | | ・Node Distribution<br>・Network environment<br>・P2P protocol | ・ This system operates in a distributed environment, and performance largely depends on the network environment.<br>・ Clarify the key points of network latency improvement by showing the bottleneck of network latency improvement. |
| | Capacity | The degree to which capacity can be expanded. | ・Block size<br>・Transaction size<br>・Consensus algorithm<br>・Block confirmation time | ・ In accordance with the increase of accumulated data volume, estimate the volume of data stored after a certain period of time and clarify countermeasures. |

# Evaluation Forms for Blockchain-Based System ver. 1.0 - Quality (3/5)

＊BC= blockchain

| Category | Evaluation item | Outline of category | Related BC technology & BC characteristics | Points to remember and remarks on using Evaluation form |
|---|---|---|---|---|
| **Scalability** | Number of nodes | The degree to which nodes can be increased. | ・Data capacity<br>・Consensus algorithm | ・ Clarify the upper limit of the number of nodes of each sort (full node, light node, etc.).<br>As the number of nodes increases, the number of transactions may exceed the processing performance. To prevent this issue, clarify the number of nodes matching the throughput performance.<br>・ Clarify the tradeoff with other evaluation items.<br>*For details of the tradeoff, see the item “Scalability - Throughput.” |
| **Reliability** | Maturity | Degree to which a system, product or component meets needs for reliability under normal operation. | ・Existing practical technology (cryptographic technology etc.)<br>・Newly developed technology (consensus, algorithm, etc.) | ・ Maturity is usually evaluated based on the actual implementation results. However, the actual introduction of blockchain technology is very few, and it is difficult to evaluate it briefly. Therefore, since a BC system is made up of existing technologies (cryptographic techniques, etc.) and new technologies (incl. consensus algorithm) that have been researched and developed to improve performance and functions (throughput, etc.) , the maturity as a system shall be shown based on the results of actual implementation of individual elemental technologies, operation results of similar systems, operation results in a test environment, and the like. |
| | | | ・Maturity and operating results as a practical system utilizing blockchain technology | |
| | Availability | Degree to which a system, product or component is operational and accessible when required for use. | ・Single point of failure | ・ Clarify the existence of a single point of failure (SPOF) node.<br>・ In the case where there is no SPOF node, clarify the rough number of ineffective nodes caused by disconnection or other failures that affects the reliability as a system. |
| | | | ・Consensus algorithm | ・ Clarify the conditions (number of nodes, etc.) for obtaining the correct consensus.<br>・ Clarify the conditions where the consensus will not function, such as an invalid state (51% attack) caused by the consensus algorithm and a consensus disabled state (disconnection with one-third or more nodes in PBFT). |

# Evaluation Forms for Blockchain-Based System ver. 1.0 - Quality (4/5)

＊BC= blockchain

| Category | Evaluation item | Outline of category | Related BC technology & BC characteristics | Points to remember and remarks on using Evaluation form |
|---|---|---|---|---|
| **Reliability** | Fault Tolerance | Degree to which a system, product or component operates as intended despite the presence of hardware or software faults. | ・Node failure tolerance<br>・Tolerance of network failure and network attacks | ・ Clarify the definition of normal operation.<br>・ Clarify node conditions and network conditions for normal operation.<br>・ Clarify the main chain determination method after fork generation due to network divisions. |
| | Recoverability | Degree to which, in the event of an interruption or a failure, a product or system can recover the data directly affected and re-establish the desired state of the system. | ・Recoverability of node failure (recovery method and time, etc.) | ・ Clarify preconditions for the network environment and data volume. |
| **Security** | Confidentiality | Degree to which a product or system ensures that data are accessible only to those authorized to have access. | ・Access control | ・ Clarify the management method of the access authority (reading, writing, etc.) to the data, setting level, etc. |
| | | | ・Data anonymization | ・ Clarify the existence of a function to conceal data.<br>・ Clarify the object and scope of concealment.<br>・ Clarify concealed data verification method by third party. |
| | | | ・Transaction anonymization | ・ Clarify the existence of a function to conceal transactions.<br>・ Clarify the object and scope of concealment.<br>・ Clarify the verification method by third party. |
| | Integrity | Degree to which a system, product or component prevents unauthorized access to, or modification of, computer programs or data. | ・Membership management | ・ Clarify the existence of membership management functions. |
| | | | ・Access control | ・ Clarify the management method of the access authority (reading, writing, etc.) to the data, setting level, etc. |
| | Non-repudiation | Degree to which actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later. | ・Consensus algorithm | ・ Clarify the existence of block confirmation by consensus algorithm. Also, clarify how to decide the main chain after fork. |
| | | | ・Hard fork policy | ・ Clarify the rule, method, and the extent of the influence of block rollback. |

# Evaluation Forms for Blockchain-Based System ver. 1.0 - Quality (5/5)

＊BC= blockchain

| Category | Evaluation item | Outline of category | Related BC technology & BC characteristics | Points to remember and remarks on using Evaluation form |
|---|---|---|---|---|
| **Security** | Authenticity | Degree to which the identity of a subject or resource can be proved to be the one claimed. | ・Synchronization method between distributed nodes | ・ Clarify whether the data are synchronized between distributed nodes. Also, clarify how to decide the data that should be considered as correct at the time of synchronization. |
| | | | ・Consensus algorithm | ・ Clarify the existence of block confirmation by consensus algorithm. Also, clarify how to decide the main chain after fork. |
| **Portability** | Adaptability | Degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments. | ・Hardware adaptability | ・ Clarify requirements on nodes. |
| | | | ・Application adaptability | ・ Clarify application requirements. |
| | Replaceability | Degree to which a product can replace another specified software product for the same purpose in the same environment. | ・Replaceability with existing system | ・ Clarity what kind of existing systems has substitutability. |
| | | | ・Replaceablity with another BC system | ・ Clarify what kind of other BC-based system has substitutability. |

# Evaluation Forms for Blockchain-Based System ver. 1.0 - Maintenance / Operation (1/2)

＊BC= blockchain

| Category | Evaluation item | Outline of category | Related BC technology & BC characteristics | Points to remember and remarks on using Evaluation form |
|---|---|---|---|---|
| Maintainability & operability | Modularity | Degree to which a system or computer program is composed of discrete components such that a change to one component has minimal impact on other components. | ・Blockchain platform | ・ Clarify the components of the blockchain platform and the modularity of technical elements. For example, “since the consensus algorithm is a highly modular implementation, it is easy to change to another algorithm.” |
| | | | ・Subsystem | ・ Clarify the components of subsystems and the modularity of technical elements. For example, “regarding the ●● function of the subsystem, upgrading the ●● function is easy due to modular design considering high functionality.” |
| | | | ・Contract code | ・ Clarify the specifications of the contract code (e.g., description language etc.). |
| | Reusability | Degree to which an asset can be used in more than one system, or in building other assets. | ・Blockchain platform | ・ Clarify the reusability of a consensus algorithm. For example, “the consensus algorithm implemented on the BC platform ●● can be implemented on the BC platform ▲▲.” |
| | | | ・Subsystem | ・ Clarify the reusability of a subsystem. For example, “the subsystem ●● can be used in the ▲▲ system.” |
| | | | ・Contract code | ・ Clarify the specifications of the contract code (e.g., description language etc.). |
| | Analyzability | Degree of effectiveness and efficiency with which it is possible to assess the impact on a product or system of an intended change to one or more of its parts, to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified. | ・Fault detection | ・ Clarify the existence of a function to detect a failure.<br>・ Clarify the existence of a function to identify where a failure has occurred (e.g., node failure, network failure, etc.).<br>・ Clarify the existence of a function to identify the range of the influence of a failure. |
| | | | ・Performance analysis | ・ Clarify the existence of performance monitoring function such as throughput, network performance, and scalability. |

# Evaluation Forms for Blockchain-Based System ver. 1.0 - Maintenance / Operation (2/2)

＊BC= blockchain

| Category | Evaluation item | Outline of category | Related BC technology & BC characteristics | Points to remember and remarks on using Evaluation form |
|---|---|---|---|---|
| Maintainability & operability | Modifiability | Degree to which a product or system can be effectively and efficiently modified without introducing defects or degrading existing product quality. | ・Bug handling | ・ Clarify the method of modifying bugs and the party responsible. |
| | | | ・Contract code | ・ In BC-based systems, since it is impossible to modify (falsify) written code, clarify how to respond when a bug is found in the contract code. |
| | | | ・Hard fork | ・ In BC-based systems, since it is impossible to modify (falsify) written code, clarify the way to rollback a block when a bug or improper data by illegal access is found. |
| | Testability | Degree of effectiveness and efficiency with which test criteria can be established for a system, product, or component and tests can be performed to determine whether those criteria have been met. | ・Blockchain platform | ・ Clarify what kind of function and performance test can be done in what environment and how the platform is influenced when the environment changes because test results are influenced by the structure of nodes and networks. |
| | | | ・Tolerance of node failure and network failure<br>・Scalability<br>・Consensus algorithm | ・ Since resistance tests against the failure of nodes and networks, capacity and node extensibility tests, and testing of consensus algorithm are important in a distributed environment, clarify what kind of test can be carried out. |
| | | | ・Contract code | ・ In BC-based systems, since it is impossible to modify (falsify) written code, contract code needs adequate testing. Therefore, clarify what kind of tests can be carried out. |

# Evaluation Forms for Blockchain-Based System ver. 1.0 - Cost

＊BC= blockchain

| Category | Evaluation item | Outline of category | Related BC technology & BC characteristics | Points to remember and remarks on using Evaluation form |
|---|---|---|---|---|
| **R&D** | R&D of blockchain platform technical elements | R&D cost (pre-implementation cost) | ・New consensus algorithm<br>・Development of high-speed P2P protocol | ・ Estimate the R&D cost for the technical elements of the BC platform for improving processing performance.<br>・ Organize the function and performance levels of existing technologies and estimate the cost by clarifying the target function and performance. |
| | R&D of subsystems | | ・Application development<br>・Contract development environment | ・ Estimate the R&D cost of the subsystem to expand application fields.<br>・ Estimate the cost by clarifying the target function and performance. |
| **Implementation (Commercialization)** | Hardware cost | Cost for system implementation (cost at the time of implementation) | ・Node<br>・Network<br>・Subsystem | ・ Clarify the objects and range included in the cost.<br>・ Clarify that estimation objects and the range of estimation are different between the types (public and private types) of platforms. For example, “in the case of the public type, materials of unspecified participants are not (or cannot be) estimated as a cost“, and“ in the case of the private type, since the number of nodes and participants are clear and equipment that carries a server role is assumed, these costs are included in the estimation“. |
| | Software cost | | ・OS<br>・Middleware<br>・Application | ・ Clarify objects and range included in cost.<br>*Examples of clarification are described in “Hardware cost” |
| | System implementation cost | | ・Assembly, implementation, and test | ・ Clarify the objects and range included in cost.<br>*Examples of clarification are described in “Hardware cost” |
| **Maintenance & operation** | Operational cost | Cost for maintenance and operation of the system (cost after implementation) | ・Node<br>・Network<br>・Cost for consensus （Impact on cost by difference of consensus algorithm) | ・ Clarify the objects and range included in the cost. |
| | Maintenance cost | | ・Bug modification | ・ Clarify the objects and range included in the cost.<br>・ Clarify the modification frequency that it expected to be high due to technology improvement, and the technical level required for modifications. |

# Use Situations of Evaluation Forms (1)
## Comparison for Replacing Existing System with Blockchain-based Systems

Evaluation forms are assumed to be mainly used by system vendors who propose replacing existing systems with blockchain-based system to their client.

- Evaluate the entire system within the evaluation framework currently used by system vendors (such as ISO/IEC 25010 and IPA),
- For the evaluation items which are especially closely related to the characteristics of blockchain, evaluate and compare them by using entire Evaluation forms proposed by METI
- Propose replacement options to the customers using these evaluation results

**<< Use-example for comparison with conventional systems>>**

| **Evaluation form (evaluation items)** | | | **Existing system "A"**<br>・System architecture : ・・・ | **Blockchain-based system "X"**<br>・System architecture : # of nodes, ・・・ |
|---|---|---|---|---|
| Quality | Performance Efficiency | Throughput | ・# of transaction ●●/sec<br>・Latency ●msec<br>Conditions : ・・・・・・・ | ・# of transaction ○○/sec<br>・Latency ●msec<br>Conditions : ・・・・・・・ |
| | | Network latency | ●msec<br>Conditions : ・・・・・・・ | ○msec<br>Conditions : ・・・・・・・ |
| | | Block confirmation | - | ・Block cannot be confirmed completely (consensus algorithm:PoW)<br>・when the block depth is ●, the probability is ●% |
| | | Data reference | ●msec<br>Conditions : ・・・・・・・ | ○msec<br>Conditions : ・・・・・・・ |
| | Interoperability | Interoperability with existing systems | There are experiences of interoperability with existing systems "P" | There is no experience of interoperability with existing systems |
| | | Interoperability with other blockchain systems | - | There are experiences of interoperability with blockchain -based systems "Y" |
| | ・<br>・ | ・<br>・ | ・<br>・ | |

# Use Situations of Evaluation Forms (2)
## Evaluation of Verification Test Results of Blockchain-based Systems

Evaluation forms are also assumed to be used for evaluation of verification test results of blockchain-based systems.

- Select evaluation items to be focused in accordance with the purpose of the verification test or the requirement of a use case
- Evaluate test results based on the description in “points to remember and remarks on using Evaluation forms”
- By focusing on the same items, results of various verification tests can be compared.

### << Use-example for evaluation of verification test results >>

| **Evaluation form (evaluation items)** | | | **Blockchain-based system “A”**<br>・System architecture : # of nodes, ・・・<br>・Blockchain platform :“X” | **Blockchain-based system “B”**<br>・System architecture : # of nodes, ・・・<br>・Blockchain platform :“Y” |
|---|---|---|---|---|
| Quality | Performance Efficiency | Throughput | ・# of transaction ●●/sec<br>・Latency ●msec<br>Conditions : ・・・・・・・ | ・# of transaction ○○/sec<br>・Latency ●msec<br>Conditions : ・・・・・・・ |
| | | Network latency | ●msec<br>Conditions : ・・・・・・・ | ○msec<br>Conditions : ・・・・・・・ |
| | | Block confirmation | ・Block can be confirmed (consensus algorithm :PBFT) | ・Block cannot be confirmed completely (consensus algorithm :PoW)<br>・when the block depth is ●, the probability is ●% |
| | | Data reference | ●msec<br>Conditions : ・・・・・・・ | ○msec<br>Conditions : ・・・・・・・ |
| | Interoperability | Interoperability with existing systems | −(N/A) | −(N/A) |
| | | Interoperability with other blockchain systems | −(N/A) | −(N/A) |
| | ・<br>・ | ・<br>・ | ・<br>・ | |

# Next challenges on Evaluation forms and key issues for implementation of blockchain in the real world

- We need to address the following challenges associated with Evaluation forms in order to contribute the application of Blockchain technology;

## Next challenges on Evaluation forms

- **Implementation of Evaluation forms to actual systems & accumulation of evaluation cases**
  - Establishing guidelines for evaluation indices and methods
- **Verification of coverage of Evaluation forms in accumulated use cases / maintenance of Evaluation forms following technology improvement**
  - Assigning the responsible party for maintenance (e.g. managing by public institutions or updating by consortiums like open source)
- **International standardization of Evaluation forms**
  - Leading the international standardization by Japan, without hindering technical innovations

- We recognize the following issues for implementation of the innovative services or mechanisms which utilize the characteristics of blockchain technology in the real world

## Key issues for implementation of the innovative services with Blockchain technology in the real world

- **To understand and notify the characteristics of blockchain technology**
  - Continual discussions on blockchain technology such as the studies in establishing Evaluation forms
  - Accumulation of actual use cases examples and deepening our understanding on blockchain technology
- **To build consortiums of stakeholders to solve specific social problems**
  - Identifying the social challenges which can be solved with the characteristics of blockchain technology
- **To organize the relevant elemental technologies required for constructing blockchain-based systems**
  - Analyzing the gap between the requirement and the realized performance, and identifying gap-filling technologies (e.g. technologies associated with throughput, reliability, data anonymization or data security)
- **To create a desirable legal systems for implementation of blockchain-based systems**
  - Reviewing laws and regulations aimed to utilize blockchain-based systems for audit, certification and proof in various sectors
  - Providing the legal bases for treatment of the data recorded in blockchain as legal evidence

# （Appendix）Detail of Meetings by Study Committee of Experts

- An exploratory committee was organized for discussion, chaired by Dr. Takagi Soichiro, Center for Global Communications, International University of Japan. This committee was composed of experts from academia, blockchain developers, domestic system vendors, and companies participating in international consortium.
- Five committee meeting were held from November 2016 to March 2017 (arranged by Mitsubishi Research Institute, Inc.)

**<<List of committee members>>**

| Name | Title, Organization (March, 2017) |
|---|---|
| **Soichiro Takagi (Chairperson)** | General Manager, Research Division/ Executive Research Fellow/ Associate Professor<br>Center for Global Communications, International University of Japan |
| **Edmund Edgar** | Founder/ CEO, Social Minds Inc. (KK) |
| **Hiroshi Oiwa** | Leader, Cyber Physical Architecture Research Group, Information Technology Research Institute<br>National Institute of Advanced Industrial Science and Technology |
| **Yuzo Kano** | Co-Founder/ CEO, bitFlyer,Inc |
| **Masanori Kusunoki** | CISO Board, Yahoo Japan Corporation |
| **Koichi Shibata** | Chief Researcher, Technical Development/ IoT Evangelist, SKEED Co. Ltd. |
| **Yasunori Sugii** | CEO, Currency Port |
| **Masanobu Takagi** | Blockchain Architect, Cognitive Solutions, IBM Japan |
| **Toshiya Cho** | Senior Vice President, Financial Innovation Center, Hitachi, Ltd. |
| **Shinichi Toriyama** | Manager, Fintech Business Development Office, NEC Corporation |
| **Masayuki Hatta** | Researcher, Surugadai University |
| **Kazumi Hirose** | Cloud Solution Architect, Microsoft Japan, |
| **Shigeichiro Yamazaki** | Professor, Department of Information and Computer Science,<br>Faculty of Humanity-oriented Science and Engineering, Kindai University |