Initiatives Concerning Development of Applications Utilizing Blockchains

Atsushi Nakadaira, Shigenori Ohashi, Hiroki Watanabe, Shigeru Fujimura, Satoshi Sakuma, and Shingo Kinoshita

Abstract

The development of services utilizing blockchains is increasing. In this article, we explain issues related to the design of applications using blockchains that require further investigation and use cases that exploit the advantages of blockchains. The use cases focus on the distribution management of management targets, namely, data managed by blockchains. Development of a common-function module for supporting development of applications is also described.

Keywords: blockchain, bitcoin, distributed application

1. Introduction

Blockchain technology was announced by a person (or persons) going by the name of Satoshi Nakamoto, and it is known as a core technology of the cryptocurrency called bitcoins, which emerged in 2008 [1]. The advantage of blockchain technology is that it enables data to be managed in the manner of an autonomous distributed system that does away with a centralized organization; consequently, it is difficult to falsify data. Thanks to this feature, blockchain technology is drawing attention in regard to not only cryptocurrency but also applications such as management of banking systems, property, and rights. In addition, the application of this technology is expected to be extended to *sharing* services (i.e., services that do not depend on a specific management organization) and services utilizing the Internet of Things (IoT) [2].

With blockchain technology, there seems to be more focus on discussing the ideas and methods related to the mechanism of the technology itself than on discussing its necessity or how best to utilize it. As a result, there is a need to conduct trials and verifications concerning utilization of the technology for developing actual services and promoting business development. In this article, we first discuss the blockchain technology that is practically applicable to services. Then we describe elements that must be confirmed when developing applications utilizing blockchain technology. We also explain NTT's initiatives to efficiently develop applications. These initiatives essentially target the application layer.

First, services that would be applicable to blockchain technology were investigated. One highly anticipated application of blockchain technology that was identified was the concept of *smart property*. Smart property refers to assets that can be managed on a computer network in the manner of a cryptocurrency. These assets include both physical and digital assets. The former is managed in terms of usage rights of vehicles, ownership of land, stock certificates, and so on, and the latter is managed in terms of viewing rights of digital content, utilization rights of IoT data, and so forth. Registering information about assets (namely, an identifier (ID) that denotes a particular asset) in a blockchain and distributing that information in the manner of circulating currency is expected to enable the smart and flexible utilization of assets while also ensuring transparency. This kind of utilization is being investigated, but use cases other than cryptocurrency (e.g., services) that can inherently exploit the advantages of blockchains have not

yet been clarified. Accordingly, we summarize in this article use cases that take advantage of the benefits of blockchains.

Additionally, we explain issues that should be considered when developing applications. Blockchain technology is being developed not only as a simple means of transferring value via a cryptocurrency but also as a system for executing digital contracts in an autonomous and decentralized manner. It is conceivable that such contracts—known as *smart contracts*—will be applied in a broader range of fields as blockchain technology becomes further developed.

In 2014, Ethereum, a new blockchain implementation that certifies program execution, was proposed [3], and it has been drawing attention ever since as a blockchain platform. In comparison with bitcoin blockchains, Ethereum makes it easier to manage extremely high-level data. However, it makes it more complicated to implement data structures of transactions, structures of blocks, and methods of managing a variable number of programs. To utilize the Ethereum platform, it is necessary to develop applications specialized for particular program-execution environments. At the same time, it is necessary to develop a framework for developing applications. Accordingly, we propose implementing common basic functions on the application layer and modularizing them in order to improve the efficiency of application development.

2. Utilization of blockchain technology

Blockchain technology has been proposed for use as the platform of various services. Such proposals are not limited to the transfer of value by cryptocurrency but also include management of assets and rights. Efforts concerning PoC (proof of concept) are also advancing. Various arguments have been made for use cases and applications exploiting the features of blockchains, but these arguments have not been put forth in a clear and orderly way. When data management in a distributed environment is considered in vague terms, the result of that consideration is likely to be that it is not only impossible to exploit the features of blockchain technology but also that it is better to use superior conventional methods. Accordingly, we express our ideas concerning key points of use cases utilizing the features of blockchains. The four conditions listed below must be considered when utilizing blockchains for managing data such as assets and digital content:

(1) Management is not performed by any single particular authority.
(2) Management targets can be reconfigured during the distribution process.
(3) The utilization form and distribution process after distribution starts are not determined (i.e., fluidity exits).
(4) Objective traceability of the distribution process is paramount.

First, it is presupposed that management is not performed only by any single particular authority. Alternately, it is presupposed that although management might be performed by a certain body taking a centralized role, it is necessary to ensure the *inspectability* of management status and information registration in regard to bodies and organizations that are independent of that central body.

One feature of blockchains is exploited that is relevant to the first condition, namely that authority is distributed among multiple bodies and managed accordingly. Under the first presupposition, it is conceivable that use cases will involve the repeated circulation* of information and digital content while the configuration of management targets is changed.

As for the second condition, namely, reconfiguring management targets during the distribution process, we use as an example the management target of video content. In this case, other images and sound are combined, and the combined content is distributed. In another example, if the management target is IoT-data groups, it is supposed that the data are smoothed, combined with other data, and further distributed alongside the results of analysis.

As for the third condition (concerning the distribution process), it is conceivable that blockchains can provide hitherto unavailable value not under the condition that the distribution process is set from the outset and managed under that status, but under the condition in which the distribution process cannot be specified. If the distribution process cannot be predetermined, two details are registered and managed: first, what kind of information is taken, how someone processes that information, and what kind of information is generated as a result; second, what rights and authority are granted to the people or organizations that took, processed, and generated the information.

Under the conditions described above, the place of origin and transitions of information being utilized can be confirmed by referring to the information registered in a blockchain. As a result, it is possible to

* Repeated circulation: The wide circulation of goods and rights by the ability to transfer them between users and changing owners in succession.

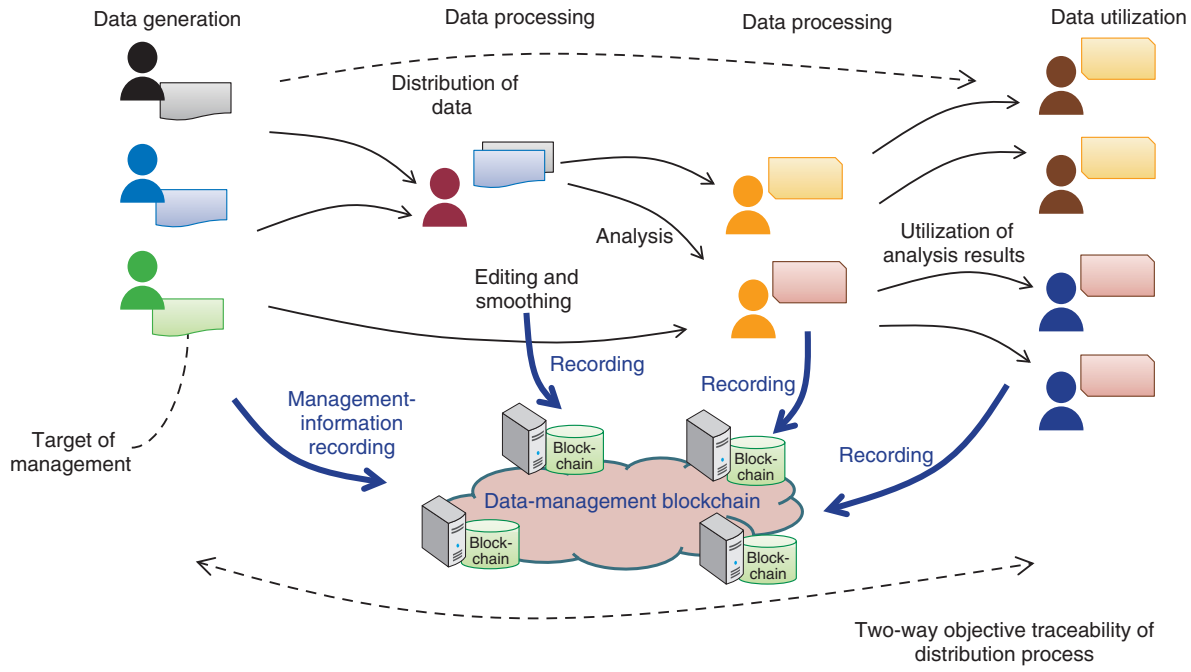


Fig. 1. Model of blockchain utilization service.

certify the authenticity and credibility of data or the existence of rights to use data as objective data. Since the data sources and the history of data changes are traceable, it is possible to evaluate the contributions to the value of data by dating back to the source of the data. Under those circumstances, to successfully utilize that traceability of data (and thereby assure objectivity), it is necessary to fully exploit the benefits of blockchains (**Fig. 1**).

As a result of utilizing blockchains in the manner of the use cases described above, information management (which has been conventionally governed by specific bodies) can be converted to decentralized co-management. Consequently, it is conceivable that on the business side, it is possible to eliminate intermediaries and thereby cut costs. However, it is considered unlikely that the important roles played in business by such intermediaries and wholesale firms will diminish, as a result of information matching, information arrangement, and other practices, and that the role itself will become unnecessary. In other words, it is conceivable that instead of such intermediaries simply disappearing, it is possible that the roles of intermediaries and wholesale businesses will become clarified through data traceability, and their value can be optimized accordingly.

3. Technical aspects required in designing applications

By applying blockchain technology in the manner described in the preceding section, it is possible to provide value that has hitherto been unavailable. However, in designing applications, the three technical aspects listed below must be considered:

(1) Assuring authenticity of registered data
(2) Devising methods for storing and managing appropriate data
(3) Assuring traceability of data

First, it is essential to assure the authenticity of registered data. In contrast to assuring authenticity of *coins* generated by a system in the manner of bitcoin, it is considered that when information is being managed, it is essential to affix extra information that confirms the authenticity of the registered information. A scheme for registering information while certifying the person who registered that information (by means of a digital signature) is thus required.

In accumulating data, it is necessary to manage methods of storing data as well as methods of accessing the stored data. Various data storage methods are conceivable, including a method in which both data and the data's management information are recorded in the blockchain, and a method that utilizes external

storage for data with a huge volume such as video content, while the management information of that video content is managed via a blockchain. As mentioned previously, the latter scheme is referred to as *smart property*.

With smart property, it is essential to firmly link the main body of content stored in external blockchains and the management information within those blockchains. In managing access to stored data, it is necessary to manage not only access to the content itself but also access to the management information managed by blockchains. In a blockchain, each node can synchronize and hold the same ledger data as other nodes as well as browse the ledger content. Therefore, it is necessary to conceal the management information managed by blockchains when managing access to that information. We have been investigating information-access management by processing data via distributed applications as well as methods for encrypting and managing data for management information managed via blockchains.

Regarding the traceability of data, it is necessary to ensure that traceability of noteworthy data is not lost while enabling data accumulated in blockchains to fluctuate fluidly.

To meet these requirements, it is necessary to develop technologies for (i) registering data, (ii) storing and managing data, and (iii) tracing data.

In our focus on use cases so far, we have investigated content management by applying blockchains [4]. In particular, we have been developing elemental technologies by taking an application-layer approach for practically applying blockchains [5, 6].

We use the case of video images taken with a camera as an example to describe our data-registration technology for managing content. In this case, digital-content information listed by the content creator is recorded at the moment the content is created. The reliability of recorded information is validated using the digital-content information and information concerning applications (such as cameras used for creating content) for the verification. The application information is assumed to be recorded by the application developer in blockchains before it is distributed. Separating digital-content information and application information in this way makes it possible to integrate the reliability of individual digital content and attain overall reliability of shared applications.

- Digital-content information

1) Digital-content hash value
2) Information concerning creator and creation conditions
3) Digital signature corresponding to recorded information (i.e., signature for application used for creating digital content)

- Application information

1) Identification information (e.g., package name and application name, version, and developer's name)
2) Public key of application
3) Information about creation metadata (i.e., item information including user-setting availability)

The digital-content hash value and information concerning the creator and creation conditions of digital-content information are automatically configured by an application compatible with the proposed method as metadata on the terminal of the creator. For example, the creator registers the address of a wallet account used for issuing transactions. The digital-content hash value is used as an ID for uniquely indicating content. However, if the encoding method is changed, for example, to ensure that content can be identified, it is conceivable that video fingerprints can be registered alongside the hash values of content and that those fingerprints can be used to create IDs to replace the hash values.

Additionally, the date, time, and location are registered during the content creation. However, it is conceivable that multiple acquisition sources corresponding to that information exist. For example, if a time and date are registered, clock times from external NTP (network time protocol) servers as well as times on other devices are also registered. Accordingly, a means of registering those acquisition sources is implemented. A digital signature is assigned multiple purposes: specifying the application used for creating content; discriminating items that can be handled by people from those that cannot, in addition to discriminating application information; and confirming that information has not been rewritten.

Although the storage and management of data differ according to the target to be managed, the volume of video content itself is very large. As a result, a method for managing the content itself outside blockchains but managing content-management information and rights information via blockchains has been proposed [4].

A method exists for managing licenses to use content via blockchains; in concrete terms, access to externally managed content encrypted by a common key is managed by exchanging that key. There is also a method for exchanging an encrypted common key via blockchains. At the source (i.e., sender), the sender can encrypt the common key as the public key

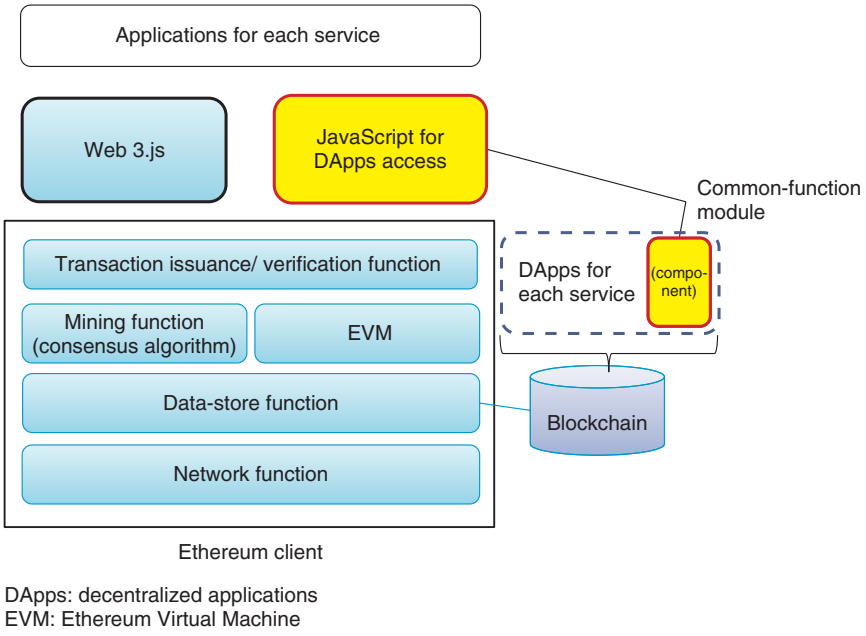


Fig. 2. Proposed module for managing authority and concealing data used in developing blockchain applications.

of the destination and register it in a blockchain. This makes it possible to disclose the common key at the destination only. We are currently investigating how to manage access to externally managed content itself.

Traceability of data is generally achieved by recording data in blockchains and referencing that data by means of a specific ID like a hash value. However, for content, it is necessary to ensure compatibility with derivative works. As for such derivative works, by incorporating a mechanism for confirming the existence (or non-existence) of permission from the original creator of content in distributed applications, we can ascertain the legitimacy of derivative works in terms of rights. Moreover, by confirming features as timestamps of blockchains and details of the above-mentioned registered data, it is possible to manage the originality of content.

4. Support for application development

We are implementing the functions of the above-mentioned technical items in our development of blockchain applications. In the meantime, when efficiency of development on the application layer (i.e., within the code of smart contracts) is considered, it becomes clear that shared functions should be modularized. For example, in use cases other than management of digital content, functions that conceal information in blockchains (such as methods for exchanging encryption keys for content) must also be widely shared. Transparency, correctness, and traceability of transactions are often mentioned as advantages of blockchains. However, in actual business situations, data that cannot be disclosed to other companies are present among customer information and transaction data between businesses. Consequently, it is imperative to protect such highly confidential data.

To satisfy this requirement, it is effective to incorporate functions for concealing information and restricting the right of access. At present, however, methods for implementing such functions in contracts are entrusted to individual developers. It is possible that depending on how the developer writes the code, vulnerable code will be written, and/or dispersibility by blockchains will be weak when the content management is implemented by a central server. In particular, it is difficult for developers who are unused to developing blockchains to appropriately design and implement contracts. We aim to solve this problem while applying our accumulated experience in utilizing blockchains for content management and are therefore proposing and implementing a shared module for creating a framework for managing authority within code, concealing certain stored data variables, and other functions (**Fig. 2**).

The proposed module for managing authority and concealing data is compatible with Ethereum (a type of blockchain platform). With Ethereum, the code of contracts is written in a proprietary language called Solidity. Accordingly, the proposed module is composed of Solidity code (by which the methods for authority management and information concealment are created as templates) and JavaScript code (which provides an interface compatible with that template). By adding the required logic based on the template of the proposed module, the developer can easily develop contracts for handling authority management and information concealment. The functions provided by that template for managing authority management and concealing information are explained in the following.

The template for providing the authority-management function uses a manager contract (for managing access to contracts). The developer registers function calls to which access should be restricted and addresses of contracts with stored data in the manager contract. When the authority-management template is used, the user references individual contracts invariably through the manager contract; as a result, it is possible to centrally restrict access to individual contracts.

To create the template for concealing information, a method for encrypting and storing the values of contracts (that are stored in blockchains) is utilized, and a method for securely managing keys for deciphering those encrypted values is provided. The encryption on the contracts is executed using a common-key method, and the common key is encrypted and stored by means of the public key of each user holding reference authority. The user with authority for decryption executes a function for acquiring a common key encrypted on a blockchain via a JavaScript interface compatible with the template and deciphers the common key by using his/her own private key. In that way, the concealed information can be displayed and viewed by that user.

Modularizing the above-described common functions, regardless of external systems, makes it possible to improve the efficiency of developing applications for disclosing contract data stored in blockchains to the specified user only and applications for the managing authority to overwrite certain data. We believe that creating sufficient functions for modularization and library creation as common functions will contribute to improving the efficiency of development and the quality of applications utilizing blockchains.

5. Concluding remarks

This article described NTT's initiatives concerning blockchains from the viewpoint of the application layer. In particular, factors and items that must be investigated when designing applications using blockchains were explained as use cases exploiting the benefits of blockchains. Implementation methods for managing content were introduced as concrete examples. Additionally, issues concerning the modularization of basic functions and actual implementation of those functions to improve the efficiency of application development were described.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-peer Electronic Cash System," 2008.
https://bitcoin.org/bitcoin.pdf

[2] S. Underwood, "Blockchain Beyond Bitcoin," Communications of the ACM, Vol. 59, No. 11, pp. 15–17, 2016.

[3] Ethereum Community, "A Next-generation Smart Contract and Decentralized Application Platform," 2014.
https://github.com/ethereum/wiki/wiki/White-Paper

[4] A. Akutsu, K. Hidaka, M. Inoue, N. Ito, T. Yamaguchi, S. Fujimura, and A. Nakadaira, "Delivering Technologies for Services that Deliver the Excitement of Games Worldwide," NTT Technical Review, Vol. 13, No. 7, 2015.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201507fa2.html

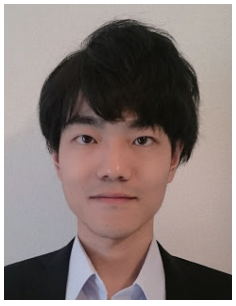
[5] S. Fujimura, H. Watanabe, A. Nakadaira, T. Yamada, A. Akutsu, and J. Kishigami, "BRIGHT: A Concept for a Decentralized Rights Management System Based on Blockchain," Proc. of the 2015 IEEE 5th International Conference on Consumer Electronics - Berlin, pp. 345–346, Berlin, Germany, Sept. 2015.

[6] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain Contract: Securing a Blockchain Applied to Smart Contracts," Proc. of the 2016 IEEE International Conference on Consumer Electronics, Las Vegas, NV, USA, Jan. 2016.

Trademark notes

Atsushi Nakadaira
Senior Research Engineer, NTT Service Evolution Laboratories.
He received a B.S. in physics from Kyoto University in 1992, an M.S. in physics from the University of Tokyo in 1994, and a Ph.D. in applied physics from the University of Tokyo in 2001. He joined NTT in 1994 and has been studying III-nitride semiconductors, display devices of polymer distributed liquid crystals, interactive systems of three-dimensional displays, and visual communication systems. He has been involved in research on content management systems leveraging blockchain technology since 2014. He is a member of the Japan Society of Applied Physics and the Institute of Image Information and Television Engineers.

Shigenori Ohashi
Research Engineer, NTT Service Evolution Laboratories.
He received an M.S. in astrophysics from Tohoku University in 2009 and joined NTT the same year. He has been engaged in research and development (R&D) of a virtual co-presence system, metadata management system, and multi-device cooperation system. He has been conducting research on content management systems leveraging blockchain technology since late 2015.



Hiroki Watanabe
Research Engineer, NTT Service Evolution Laboratories.
He received an M.S. in engineering from Waseda University, Tokyo, in 2011 and joined NTT the same year. Since then, he has been researching human interfaces of interactive television (TV), a distribution system for web applications, and content management systems leveraging blockchain technology. His research interest is smart contract systems using blockchain technology.

Shigeru Fujimura
Senior Research Engineer, NTT Service Evolution Laboratories.
He received an M.S. in information science and technology from the University of Tokyo in 2005 and joined NTT the same year. Since then, he has been engaged in research on web mining and web engineering, especially on effective methods of implementing web applications. He is a member of the W3C (World Wide Web Consortium) Web and TV Interest Group.

Satoshi Sakuma
Senior Research Engineer, Supervisor, NTT Service Evolution Laboratories.
He received an M.S. in instrumentation engineering from Keio University, Kanagawa, in 1995 and joined NTT the same year. Since then, he has been engaged in R&D of medical image processing and object recognition. He has also been conducting research on service visualization using NTT's advanced technology since 2014. He received the SPIE Medical Image Processing 1998 Best Poster Award.

Shingo Kinoshita
Executive Research Engineer, Supervisor, and Project Director, NTT Service Evolution Laboratories.
He received a B.E. from Osaka University in 1991 and an M.Sc. with Distinction in technology management from University College London, UK, in 2007. Since joining NTT laboratories in 1991, he has been engaged in R&D of distributed computing systems, security, big data computing, and machine learning. He was a senior manager of the R&D planning section of the NTT holding company from 2012 to 2015, where he established and operated NTT Innovation Institute, Inc. in North America and managed R&D alliance and venture investments. He is presently in charge of the overall direction of various R&D experimental activities toward 2020 including assistance services for foreigners and entertainment services such as kabuki and SXSW. He received the 2005 IPSJ R&D Award from the Information Processing Society of Japan, the 2003 CSS (Computer Security Symposium) Best Paper Award, and the 1998 DICOMO (Multimedia, Distributed, Cooperative, and Mobile) Symposium Best Presentation Award.