Blockchain Contract: A Complete Consensus using Blockchain

Hiroki Watanabe, Shigeru Fujimura, Atsushi Nakadaira, Yasuhiko Miyazaki, Akihito Akutsu
NTT Service Evolution Laboratories
Yokosuka-City, Kanagawa, Japan

Jay (Junichi) Kishigami
Muroran Institute of Technology
Muroran-City, Hokkaido, Japan

Abstract—**A proposal is made to use blockchain technology for recording contracts. A new protocol using the technology is described that makes it possible to confirm that contractor consent has been obtained and to archive the contractual document in the blockchain.**

Keywords— blockchain; smart contract; bitcoin;

I. INTRODUCTION

The bitcoin [1], which is the first and most popular cryptocurrency, has been receiving a lot of attention [2]. One of its technical features is that it enables reliable transactions without a centralized management mechanism even if there are unreliable participants in the network, and this feature is obtained by the invention of blockchain technology. A blockchain is something like a ledger in which all transactions have been recorded, and it is shared by the participants of a bitcoin network. The structure of a blockchain is that a block that consists of multiple transactions is connected with a previous block in chain-like form. To ensure reliability, when a new block is added to the previous block, a little special process of solving a puzzle, called proof-of-work, is needed and this puzzle is not easy. This is because this process can prevent attackers from forging the blockchain on their own. With the number of bitcoin transactions becoming larger and larger, discussion of blockchain applications other than those for currency has been thrust into the spotlight. This is because the reliability of the technology has been maintained even when it is put to use on a large scale. Sometimes the approach of these applications that take advantage of the features of blockchain is called “bitcoin 2.0”.

In today’s contract society, a tremendous amount of contractual documents, such as those relating to “purchase and sale agreement”, “deed of assignment” and “license agreement”, are created every day all over the world. Computers make it possible to record and manage these documents easily. However, they are harder to protect for a long period of time and to verify in later years because computer records are quite easy to change. We believe that blockchain technology has great potential for use in recording a trail of consensus. This is because the blockchain itself is strong against attack, anyone can verify its records, and it is difficult to change its history.

The rest of this paper is as follows. The next section describes problems in applying blockchain technology to verifying contracts. Our approach to these problems and our proposed protocol using blockchain technology are described in Section 3. The paper is concluded in Section 4 with a summary of important points and a mention of future work.

II. DISCUSSION ON APPLYING BLOCKCHAIN TECHNOLOGY TO CONTRACT VERIFICATION

A. The importance of verifying contractor consent

In cryptocurrencies, transactions are issued in a one-way manner from a sender to a recipient. It is not necessary for the recipient to confirm reception, like the remittance to the bank account. For contracts, however, a single one-way transaction is insufficient even if it is used for a contract between two people, because confirmation on the part of both parties is required. The consent confirmation process is further complicated if three or more parties are involved.

When blockchain technology is used, transactions are carried out in a one-way by default direction. Consequently, to solve the aforementioned problem it is necessary to devise a new way to use blockchain in carrying out transactions or to expand transaction specifications to enable transactions to be carried out in a bi-directional manner. Our approach, detailed in the next section, is based on the former strategy because it involves making fewer changes in current blockchain technology than would need to be made in choosing the latter strategy.

B. Method for archiving contractual documents

With contracts, it is desirable for each contractor to archive the contractual document by himself or herself. However, it is not easy to archive documents over a long period of time even if the documents are in digital data form because there is a possibility that storage devices may become out of order as a consequence of time-related deterioration or the occurrence of a disaster of some sort. Therefore, it is not enough to store transactions including the hash value of the document as metadata, although this method, which applies the current blockchain technology, is the simplest one. Taking this into consideration, we attempted to expand the transaction in the blockchain to store contractual documents.

III. PROPOSED METHOD

To address the issues described in the preceding section, we designed a new protocol for recording a trail of consensus

978-1-4799-8751-1/15/$31.00 ©2015 IEEE

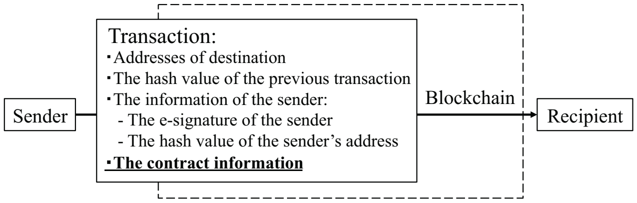
Transaction:
・Addresses of destination
・The hash value of the previous transaction
・The information of the sender:
- The e-signature of the sender
- The hash value of the sender's address
・The contract information
Sender
Blockchain
Recipient

Fig.1. The transaction of our proposed protocol

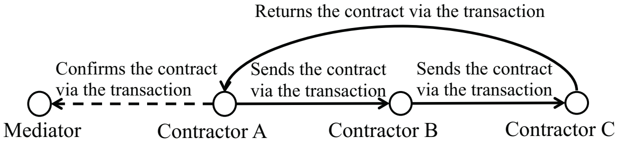
Returns the contract via the transaction
Confirms the contract via the transaction
Sends the contract via the transaction
Sends the contract via the transaction
Mediator
Contractor A
Contractor B
Contractor C

Fig.2. Making of the transaction chain by the contractors

onto the blockchain. In this protocol, a transaction is used as evidence of contractor consent. The transaction is associated with the contract information as shown in **Fig. 1**. For solving the first issue, we propose that a recipient of the transaction generates a new transaction referring to the received transaction, which represents his intention of consenting to it. The contractors make a chain of transactions (e.g., as shown in **Fig. 2**) and the last transaction data is returned to the first contractor, who generated the contract transaction at the beginning. The first contractor then confirms the contract contained in the transaction and generates a transaction addressed to someone like a mediator as a trail of confirmation.

Regarding the second issue, the contract data needs to be encrypted in order to store contractual documents in the blockchain. This is because the blockchain is public and anyone can view it. To protect the privacy of the contract, our protocol uses not only a key pair for an e-signature but also a key pair for encrypting contract data.

The following example specifies how the proposed protocol works: Alice, Bob, and Cory try to contract each other over the issuing of a license of some sort. Alice makes the contract, and then Bob followed by Cory consent to it. The processing flow of this example is shown in **Fig. 3**.

1. Each of them generates a key pair for encrypting the contract in their own terminal and transfers a public key for encryption to the sender of the transaction beforehand. Namely, there are different encryption keys from Bob to Alice, from Cory to Bob, and from Cory to Alice.
2. Alice makes the contract and encrypts it using the encryption key transferred from Bob. Then she generates transaction data including the encrypted contract data, and broadcasts this transaction data to the peer-to-peer network.
3. When a miner succeeds in generating a block, it means that Alice's transaction is recorded on the blockchain via the proof-of-work process.
4. Since the blockchain is synchronized with the network, Bob takes Alice's transaction data (addressed to Bob) from the blockchain, and then decodes the encrypted contract data using his decryption key.
5. Bob checks the contract, and if he consents to it, generates a transaction referring to Alice's transaction, which is addressed to Cory. Bob encrypts the contract from Alice using Cory's encryption key, includes the encrypted contract in the transaction, and broadcasts it.

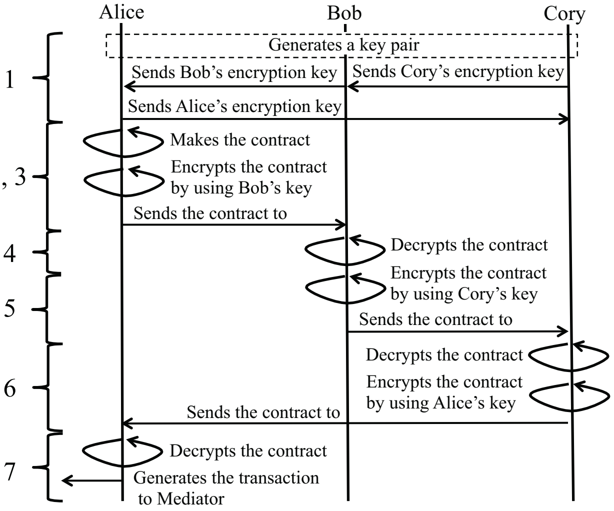
Alice
Bob
Cory
Generates a key pair
1
Sends Bob's encryption key
Sends Cory's encryption key
Sends Alice's encryption key
2, 3
Makes the contract
Encrypts the contract by using Bob's key
Sends the contract to
4
Decrypts the contract
5
Encrypts the contract by using Cory's key
Sends the contract to
6
Decrypts the contract
Encrypts the contract by using Alice's key
Sends the contract to
7
Decrypts the contract
Generates the transaction to Mediator

Fig. 3. The processing flow of the example (Numbers at left are associated with numbers in the main text)

6. In a similar procedure, Cory also checks the contract using his key. Then he sends the contract to Alice via a transaction. This means that the transaction from the last contractor is returned to the first contractor in the chain.
7. Finally, Alice receives Cory's transaction and confirms whether the encrypted contract she has received is correct. If she accepts the consensus, she generates a transaction referring to Cory's transaction addressed to the mediator requesting a trail of confirmation.

By completing the above procedure, they can record the trail of consensus. If they want to check the contract in the future, they can each take the contract data from the blockchain. Since the records are encrypted, only people having a decryption key (i.e., in this case only Alice, Bob, and Cory) can decode the contract.

IV. Conclusion

In this paper, we described the use of blockchain technology to verify contracts and proposed a new protocol to make this usage possible. The protocol makes it possible to confirm the consent of each contractor and protect the privacy of the contract using blockchain. In future work, we will try to implement this protocol on an actual cryptocurrency. We will also try to develop an effective algorithm as an alternative to the proof-of-work algorithm in order to provide more secure protection against contract falsification.

References

[1] S. Nakamoto, “Bitocoin: A Peer-toPeer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf, 2008.

[2] J. Bonneau et al, “SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies,” in 36th IEEE Symposium on Security and Privacy, May 18-20, 2015.