Chapter 8

Bitcoin and Blockchain Technology

Kazumasa Omote and Makoto Yano

A ledger can be defined as a “book of permanent record.” With modern information technology, data have become economic resources if they are associated with exclusive owners and put into a ledger. It is shown in Chaps. 3 and 4 that IoT data can be transformed into productive resources while Chaps. 5 and 6 show that transaction data can be turned into money-like bank deposit currencies.

Blockchain is a technology that put data into such a ledger without a central authority like banks managing deposit currencies. Instead, many independent people with technical knowledge contribute to put together a ledger that associates data pieces with their owners. In this chapter, we explain this technology by focusing on the original blockchain for Bitcoin.

The Bitcoin blockchain is the first decentralized ledger that turned data into an economic resource. Such a ledger must have several basic features:

1. Timestamps
2. Immutability
3. Accuracy
4. Uniqueness
5. Authenticity

This article is based on our final report to the study group “Blockchain and Society 5.0—The Creation of a New Marketplace based on Distributed Consensus” at the Research Institute of Economy, Trade, and Industry (RIETI). We are grateful to all the participants for useful discussions and, in particular, to Chris Dai for insightful comments. The second author gratefully acknowledges the financial support of a Grant-in-Aid for Scientific Research (A) (#16H02015) from the Japan Society for the Promotion of Science.

K. Omote
University of Tsukuba, Tsukuba, Japan

M. Yano (✉)
Research Institute of Economy, Trade and Industry (RIETI), Tokyo, Japan
e-mail: yano-makoto@rieti.go.jp

A timestamp is a marker that specifies the time and date at which a record is made. Putting a timestamp on each piece of data is important if the ownership of a data piece changes overtime. For example, if a ledger is for recording the ownership of properties, it would become impossible to tell who owns a particular property at a particular moment without a timestamp.

By immutability, we mean that data cannot be tampered with or altered by malicious attack. This implies that no one can make a counterfeit version of an existing ledger.

Accuracy implies that a ledger must record data correctly and satisfy any constraints imposed on the ledger. For example, a ledger for monetary transactions must ensure that for each transaction, no one can spend more than the existing balance in his/her account.

Uniqueness implies that every ledger must be a unique book of record for that particular kind. If two different books of record are created, it will invite disputes; for example, if a ledger is to record the ownership of land, each piece of land must be associated with a unique owner. Historically, many territorial disputes have resulted from the failure to maintain a unique book of record of land ownership.

By authenticity, we mean that each data piece on the ledger must describe the exact intention of its owner. If it is a ledger for monetary transactions that a bank maintains, records on deposits to or withdrawals from accounts must be conducted in the exact way in which owners intend. If a transaction is to be made through an automatic teller machine (ATM), this could be achieved by using the proper password for the account, which assures that an order is authentic.

Conventional ledgers have been maintained by central authorities; records on bank transactions by banks and those on marital status by local governments, and so on. Blockchain technology makes it possible to build such a ledger in a decentralized manner without any central authority. Instead, a blockchain is based on algorithms that computers can follow.

It is not an easy task to come up with such algorithms. In what follows, we explain the implementation of such an algorithm by focusing on the Bitcoin blockchain, which was the first to show the potential of a decentralized algorithm-based ledger system.

The Bitcoin algorithm adopts four important ideas in designing a monetary ledger. They are:

1. Chain of blocks
2. Proof-of-work
3. Decentralized consensus algorithm
4. Open-key cryptographic accounts

1 Chain of Blocks

In a blockchain, a block is a file containing data with a timestamp. Bitcoin blockchain is a chain that connects blocks in one single row. Every time a new block is built, this is attached to the most recent block on the chain.

2 Proof-of-Work

To build a ledger, a new block must be “glued” to the most recent block. A cryptographic riddle plays the role of glue that permanently connects a block to the previous block. It takes a large amount of computing power (i.e., electricity) to solve this riddle. This process is referred to as proof-of-work, implying that a block embedded into a blockchain shows that a sufficient amount of computing power was expended for its creation.

Once a block is built, it is converted into a cryptographic riddle. To understand this riddle, it is necessary to know a cryptographic algorithm called a secure hash algorithm (SHA). The SHA transforms any digital data of any length into a unique sequence of seemingly random numerals with a fixed length. A number of SHAs have been developed. The most common algorithm currently is called SHA 256, which transforms any sentence into a 256-digit number in the binary numeral system. For example, SHA 256 transforms the word “blockchain” into

SHA (blockchain)

=EF7797E13D3A75526946A3BCF00DAEC9

FC9C9C4D51DDC7CC5DF888F74DD434D1 (1)

which is expressed in the hexadecimal numeral system (with numerals 0–9 and letters A–F). This value is called the hash value of word “blockchain” by SHA 256.

SHAs are designed in such a way that it is practically impossible to guess the original sentence from a hash value. A particular sentence is always translated into the same hash value. Moreover, the chance with which two different sentences are associated with an identical hash value is practically zero.

One use of a SHA is to store a password. For example, a password for an ATM must be stored in association with an account number. If passwords were stored in the naked values chosen by account owners, it would create a huge problem if passwords were stolen. A secure hash algorithm is useful to hide a password from anyone other than the associated account owner. Even if someone sees the hash value of the password associated with an account, he/she can never find the password. At the same time, whether the password inputted into an ATM is authentic can be easily determined by transforming the inputted password by the SHA adopted by the bank.

The cryptographic riddle called proof-of-work requires a sequence of numerals that can be attached to the end of a particular sentence so that the hash value of the particular sentence plus the attached sequence starts with X number of zeros that is required by the algorithm. If the proof-of-work riddle asks to find a sequence of

numerals to attach to “blockchain” so that the first number of the hash value is zero, a solution is the sequence of 34 zeros at the end of the word “blockchain.” That is to say,

```
SHA(blockchain00000000000000000000000000000000)
= 088C389A0BC33DE6A7D8DD9012DBD6
C5E9276B94C2639E72725F40E98A7163AA (2)
```

If a 16-digit hash value is a sequence of randomly selected numerals from 1 through F (actually it is not), the probability with which the first number is zero is $1/16$, and that for the first two numbers is $1/16^2$. Thus, it is clear that there are many solutions for each proof-of-work riddle. Moreover, as the required number of zeros is increased, it becomes increasingly difficult to find a solution where a sequence of numerals is attached to a given sentence so that zeros will line up at the beginning of the value as the algorithm requires.

If this algorithm is used for filing a piece of information (or if “blockchain” is the piece to be filed), it can serve as a simple proof that a certain computing time is spent before filing the information. This is because it takes time to find a correct sequence of numerals to attach to a message, and it is very easy to check whether the attached sequence is correct. For this reason, the algorithm is regarded as providing a proof-of-work.

A proof-of-work algorithm was invented in 1997 for software called Hashcash. This software separates meaningful emails from spam mails. For example, if every nonspam mail is required to include a solution that lines up a certain number of zeros at the beginning of the hash value of email sentences, it takes a certain length of computing time before a sender sends out the email. Because of the costly computing time, no spam sender dares to solve the riddle imposed by Hashcash, and no spam mails are delivered with the solution to the riddle. As a result, mail receivers can separate real mails (with solutions to the riddle) from spam mails.

The Bitcoin blockchain adopts a proof-of-work algorithm. To create and attach a new block to the existing chain, it is required to find a solution such that a specific number of zeros lines up at the beginning of the hash value of the solution added to what is written in the existing block and to write the solution in the new block. The number of zeros that the Bitcoin blockchain requires is set in such a way that it takes, on average, about 10 min for a fast computer to find a solution.

This wipes out any incentive to tamper with a blockchain because rewriting part or all of blocks on a chain requires solving the riddles all over again, which is extremely costly. In short, a blockchain built on a proof-of-work algorithm is immutable.

3 Decentralized Consensus Algorithm

Blockchain technology makes it possible to build an accurate ledger by relying not on a central authority but on an algorithm involving many independent people or computers called network nodes. This algorithm is called a (decentralized) consensus algorithm.

To create a ledger in a decentralized manner, it is important to provide incentives for people to willingly contribute to building a ledger. In the Bitcoin blockchain, this incentive is created by separating people who make use of a ledger (users), recording transfers of money between user accounts, from those who add new records to the ledger. An individual who wants to record a transfer of money posts a transaction with a proposed transaction fee. Because the maximum size of each block is fixed, a recorder can select only a few from the pool of transactions and put together a new block. For a particular recorder to place his/her block to the existing blockchain, as discussed above, he/she must be the first to solve the cryptographic riddle created from the latest block of the chain. To attract a sufficiently large number of recorders, a fixed amount of money is given as a prize to any recorder who actually adds a new block to the chain. If this prize is sufficiently large, many people will participate in creating new blocks. No matter how many recorders participating in the creation of a new block at a particular point of time, only one recorder can get the prize. This process is similar to looking for gold in a gold mine and therefore is referred to as “mining.” People who run mining operations and maintain computers that record new blocks are called “miners”.

Another way of looking at this process is to think of the group of miners as a computer network connected through the Internet. Miners are network nodes. The entire blockchain is stored on each node. Each node operates independently according to the node’s own will.

The primary requirement for a ledger is accuracy. Although a proof-of-work algorithm prevents a ledger from being spammed, it is not enough to maintain the accuracy of a ledger. If a block contains false information, it must not be added to a blockchain. For a conventional ledger like a deposit currency, there is a central authority that single-handedly maintains accuracy.

The Bitcoin blockchain adopts a decentralized consensus algorithm. When a particular node joins the network, it is randomly associated with several existing nodes. Once a particular node puts a new block together and solves the riddle, it announces the new block to the associated nodes. Those associated nodes independently check if the new block contains any errors. If they find no error, they announce the new block to the entire network.¹ If the associated nodes find errors, they ignore the block, in which case no other nodes will know the new block. Through this process, the accuracy of blocks can be maintained.

Another important requirement for a ledger is its uniqueness; if it were possible that multiple books of records were created, they could not serve as a ledger. The Bitcoin blockchain is, however, subject to the possibility that multiple chains are

---

¹If you operate a full node, there is a strong incentive to make such an announcement immediately. If you run a full node that is not broadcasting transactions, then when a transaction is made, it becomes immediately obvious to peers as to where that transaction originated. The incentive is to preserve your privacy. Even with a delayed broadcast, you would still be risking privacy because peers would likely become aware of the transaction first from other peers; then as soon as they see you broadcast a transaction that they had not seen from elsewhere, it would be reasonable for them to assume the transaction came from you.

built. As a result, there is a good chance that more than one node will solve the current riddle.

If more than one node succeeds, a blockchain bifurcates; the chain on some nodes will become different from that on other nodes after the point of bifurcation. To correct such a situation and to maintain a single chain, the Bitcoin algorithm sets a rule that the longest existing chain be perceived as the valid chain. If a chain bifurcates into two, at the point of bifurcation, the two chains have the same length, most likely, with different blocks at the end presenting different riddles. Because the length of time that is needed to solve a riddle is completely random, the length of one chain will quickly become longer than the other. As soon as this occurs, most nodes will start working on solving the riddle presented by the longer chain, and the shorter chain will quickly be ignored.

This implies that even if a block is created by solving a proof-of-work riddle, it does not imply that the block (and transactions in the block) will be recorded permanently. That is, those transactions could be recorded in a chain that will later become shorter than another, and, as a result, be forgotten.

4 Open-Key Cryptographic Accounts

Another important issue in building a ledger for the activities of individuals is to make sure that recording is prompted by the wills of the individuals conducting the activities. If a ledger is to record transfers of money from one account to another, the recording must reflect exactly what account owners want. However, how can miners tell that an application for recording a monetary transfer from an account is actually made by the owner of the account? In the case of a bank transfer, it is easy; the bank can simply check if the person asking for a transfer knows the password of the account. However, this task is not as simple if the record is to be produced in a decentralized manner.

Blockchain technology overcomes this difficulty by using “public-key cryptography,” which gives a pair of keys to encrypt and decrypt a text. If a text is encrypted by one of the two keys, the resulting encrypted text can be decrypted into the original text by the other key. It is designed in such a way that it is impossible to identify one key from the other key.

Of course, it is possible for two parties to use a public-key cryptography to communicate just between themselves by assigning one of the two keys to one party and the other key to the other party. However, more common usage is to make one of the two keys public, which explains the terminology of public-key cryptography.

One use of public-key cryptography is to receive a message confidentially. For that purpose, a message receiver can create a pair of keys, make one of the keys public and keeping the other key private. If a sender of a message encrypts a message with the public key and sends it to the receiver, the receiver can receive the message by decrypting it with the private key.

Another use is for attaching a digital signature to prove that a message is from the sender and not from another individual. For this purpose, a sender can encrypt a message with a private key and send both the encrypted message by the paired public key and the original message. By using the received public key, the receiver can decrypt the encrypted message. If the resulting decrypted message is the same as the original message, which is sent separately, the receiver can be sure that the sender of the message is the person who knows the private key that is paired with the public key.

This method of digital signature is used by the Bitcoin blockchain. In creating a new account for Bitcoin, a random number is chosen first. By using a public-key cipher, this random number is transformed into the private key. This private key is then transformed into the paired public key. A Bitcoin account is produced from the public key. The public key is announced throughout the Internet. In essence, the public key serves as the base for a user's account whereas the private key serves as the password for the account. The account owner encrypts transactions with the private key and sends both the encrypted transaction and the original transaction, from which the miners can confirm authenticity of the transaction.

5 Concluding Remarks

The Bitcoin blockchain was the first to demonstrate that a ledger, an immutable, accurate, and unique book of record, can be built on the Internet in a decentralized manner. While this process has been accepted with great enthusiasm by many, a number of weak points have also been exposed. Currently, Bitcoin and other virtual currencies function as speculative instruments rather than as mediums of exchange. They are often used for trading illegal commodities such as drugs and for money laundering. These problems may be dealt with as society becomes better informed of what blockchains can do and what they cannot do.

A more fundamental problem may be that proof-of-work blockchains require a large amount of electricity for solving crypto riddles; an extremely large number of miners use their computers to solve blockchain riddles. However, as discussed in Chap. 5, what is attractive about virtual currencies is that production is not costly, which makes it possible to equate the marginal cost of money to the marginal utility of money. This is a necessary condition for efficient use of private goods; traditionally, money has been put outside of this efficiency consideration because goods with no value (like paper) has been used as money.

The Bitcoin blockchain is important because it has demonstrated that a deposit currency can be created fairly inexpensively in a decentralized manner. Once the possibility of such a technology is realized, many other new technologies will be developed that can offer much more than just money at a much cheaper cost.

Kazumasa Omote received his Ph.D. degree in information science from the Japan Advanced Institute of Science and Technology (JAIST) in 2002. He worked at Fujitsu Laboratories, Ltd., from 2002 to 2008 and was engaged in research and development for network security. He was a research assistant professor at JAIST from 2008 and an associate professor there from 2011. He has been an associate professor at the University of Tsukuba since 2016. His research interests include applied cryptography and network security. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and the Information Processing Society of Japan (IPSI).

Makoto Yano is Chairman of the Research Institute of Economy, Trade and Industry (RIETI); he is also a specially appointed professor at Kyoto University, Jochi University, and Chubu University. He is an internationally known researcher who has made a number of substantial contributions in international trade, market theory, and especially on economic dynamics. His contributions in economic dynamics, for example, are represented by articles in *Econometrica* in 1995 and the *Journal of Economic Theory* in 1996, which explained the conditions under which general economic equilibrium shows chaotic behavior. His 1998 *Econometrica* article is recognized as the latest most important work on the characterization of dynamic general equilibrium.

Besides those rather theoretical works, Prof. Yano has also provided influential insights on contemporary real-world phenomena. Those include transfer problems (*American Economic Review*, 1999), voluntary export restraints (*International Economic Review* [IER], 1995), and trade conflicts (IER, 1998), on which there have been a number of follow-up papers.

His recent research on “market quality” addresses various problems in modern economies, including the financial market crisis since 2008 and the recent nuclear accidents in Japan, from the point of view of market quality—a new economic concept that Prof. Yano has developed and is applying to Japanese and international markets. Concerning quality of competition, quality of information, and quality of products, market quality is defined as an index jointly determined by the efficiency of an allocation and the fairness of the prices that are achieved in a market.

Prof. Yano received a B.A. in economics from The University of Tokyo in 1971 and a Ph.D. in economics from The University of Rochester in 1981.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits any noncommercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if you modified the licensed material. You do not have permission under this license to share adapted material derived from this chapter or parts of it.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.