A Short Introduction to the World of Cryptocurrencies

Aleksander Berentsen and Fabian Schär

In this article, we give a short introduction to cryptocurrencies and blockchain technology. The focus of the introduction is on Bitcoin, but many elements are shared by other blockchain implementations and alternative cryptoassets. The article covers the original idea and motivation, the mode of operation and possible applications of cryptocurrencies, and blockchain technology. We conclude that Bitcoin has a wide range of interesting applications and that cryptoassets are well suited to become an important asset class. (JEL G23, E50, E59)

Federal Reserve Bank of St. Louis *Review*, First Quarter 2018, *100*(1), pp. 1-16.
https://doi.org/10.20955/r.2018.1-16

1 INTRODUCTION

Bitcoin originated with the white paper that was published in 2008 under the pseudonym "Satoshi Nakamoto." It was published via a mailing list for cryptography and has a similar appearance to an academic paper. The creators' original motivation behind Bitcoin was to develop a cash-like payment system that permitted electronic transactions but that also included many of the advantageous characteristics of physical cash. To understand the specific features of physical monetary units and the desire to develop digital cash, we will begin our analysis by considering a simple cash transaction.

1.1 Cash

Cash is represented by a physical object, usually a coin or a note. When this object is handed to another individual, its unit of value is also transferred, without the need for a third party to be involved (Figure 1). No credit relationship arises between the buyer and the seller. This is why it is possible for the parties involved to remain anonymous.

The great advantage of physical cash is that whoever is in possession of the physical object is by default the owner of the unit of value. This ensures that the property rights to the units

Aleksander Berentsen is a research fellow at the Federal Reserve Bank of St. Louis and a professor of economic theory at the University of Basel. Fabian Schär is managing director of the Center for Innovative Finance at the Faculty of Business and Economics, University of Basel.

Figure 1

Cash Transaction

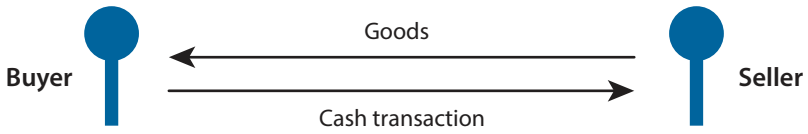
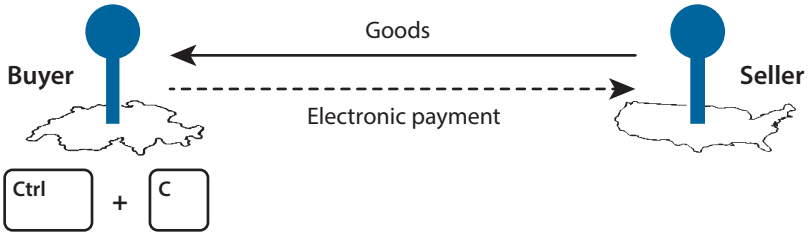


Figure 2

Electronic Payment



of value circulating in the economy are always clearly established, without a central authority needing to keep accounts. Furthermore, any agent can participate in a cash payment system; nobody can be excluded. There is a permissionless access to it. Cash, however, also has disadvantages. Buyers and sellers have to be physically present at the same location in order to trade, which in many situations makes its use impracticable.

1.2 Digital Cash

An ideal payment system would be one in which monetary value could be transferred electronically via cash data files (Figure 2). Such cash data files retain the advantages of physical cash but would be able to circulate freely on electronic networks.[1] A data file of this type could be sent via email or social media channels.

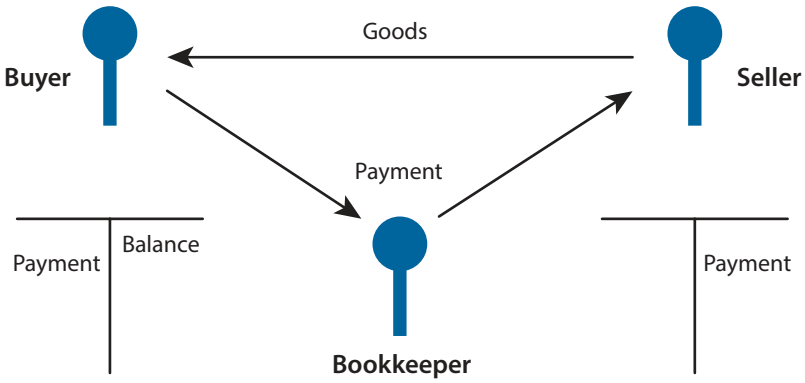
A specific feature of electronic data is that it can be copied any number of times at negligible cost. This feature is highly undesirable for money. If cash data files can be copied and the duplicates used as currency, they cannot serve as a payment instrument. This problem is termed the "double spending problem."

1.3 Electronic Payment Systems

To counteract the problem of double spending, classical electronic payment systems are based on a central authority that verifies the legitimacy of the payments and keeps track of the current state of ownership. In such systems, a central authority (usually a bank) manages the accounts of buyers and sellers. The buyer initiates a payment by submitting an order. The

Figure 3

Payment System with a Central Authority



central authority then ensures that the buyer has the necessary funds and adjusts the accounts accordingly (Figure 3).

Centralized payment systems solve the double spending problem, but they require trust. Agents must trust that the central authority does not misuse the delegated power and that it maintains the books correctly in any state of the world—that is, that the banker is not running away with the money. Furthermore, centralized systems are vulnerable to hacker attacks, technical failures, and malicious governments that can easily interfere and confiscate funds.

1.4 Stone Money of Yap

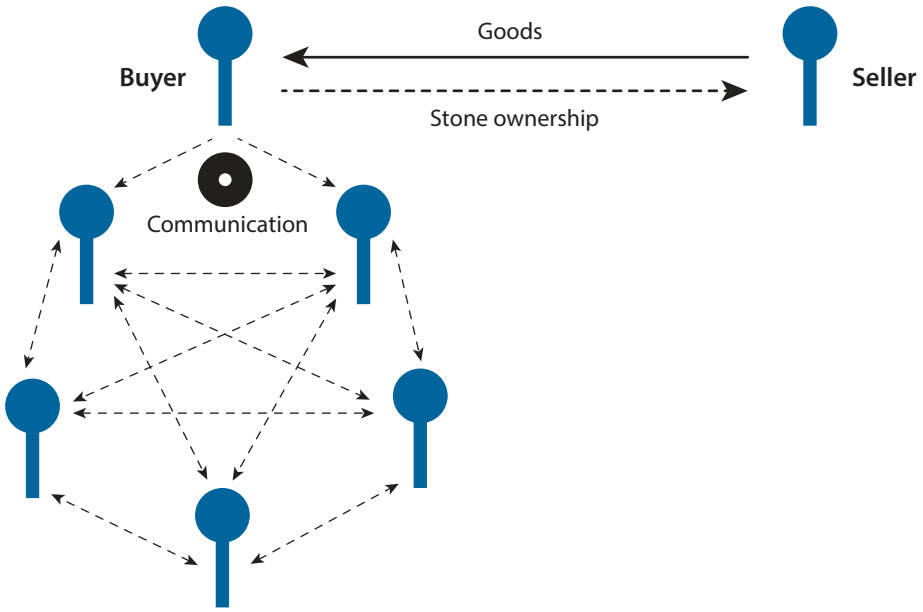
The key feature of the Bitcoin system is the absence of a centrally managed ledger. There is no central authority with an exclusive right to keep accounts. In order to understand how this is possible, we will first discuss a historical payment system that has certain similarities with the Bitcoin system.

On Yap Island, large millstone-like stones were used as a medium of exchange.[2] The stones were quarried almost 280 miles away on the island of Palau and brought to Yap by small boats. Every inhabitant could bring new stone money units into the system. The money creation costs, in the form of labor effort and equipment such as boats, protected the economy from inflation.

Instead of having to laboriously move the stones, which are up to 13 feet in diameter, with every transaction from a buyer's front yard to a seller's front yard, the ownership rights were transferred *virtually*. A stone remained at its original location, and the unit of value could be detached from it and circulated irrespective of the stone's whereabouts. It was sufficient that all the inhabitants knew who the owner of every stone was. The separation between the unit of value and the stone went so far that even the unit of value for stones that were lost at sea remained in circulation. The stone money of Yap can therefore be described as a quasi-virtual currency, as each unit of value was only loosely linked to a physical object.

Figure 4

Payment System with a Distributed Ledger



The Yap system was based on a distributed ledger, in which every inhabitant would keep track of a stone's ownership. When a buyer made a purchase, this person told his or her neighbors that the stone now belonged to the seller. The neighbors then spread the news until finally all of the island's inhabitants had been informed about the change in ownership (Figure 4). Through this communication, every islander had a precise idea of which unit of value belonged to which person at any point in time.

In its essential features, the Yap payment system is very similar to the Bitcoin system. A major difference is that in the Yap system false reports could not be immediately identified, so conflicts regarding the current state of the implicit ledger would have to be argued and settled by the group. The Yap system therefore was restricted to a group of manageable size with close relationships, in which misconduct could be punished by the group. In contrast, the Bitcoin system is designed to function in a network where no participant can trust any other participant. This feature is necessary because it is a permissionless payment system in which participants can remain anonymous through the use of pseudonyms.

1.5 Bitcoin and the Bitcoin Blockchain

Bitcoin is a virtual monetary unit and therefore has no physical representation. A Bitcoin unit is divisible and can be divided into 100 million "Satoshis," the smallest fraction of a Bitcoin. The Bitcoin Blockchain is a data file that carries the records of all past Bitcoin transactions, including the creation of new Bitcoin units. It is often referred to as the ledger of the Bitcoin

system. The Bitcoin Blockchain consists of a sequence of blocks where each block builds on its predecessors and contains information about new Bitcoin transactions. The average time between Bitcoin blocks is 10 minutes. The first block, block #0, was created in 2009; and, at the time of this writing, block #494600 was appended as the most recent block to the chain. Because everyone can download and read the Bitcoin Blockchain, it is a public record, a ledger that contains Bitcoin ownership information for any point in time.

The word "ledger" has to be qualified here. There is no single instance of the Bitcoin Blockchain. Instead, every participant is free to manage his or her own copy of the ledger. As it was with the stone money, there is no central authority with an exclusive right to keep accounts. Instead, there is a predefined set of rules and the opportunity for individuals to monitor that other participants adhere to the rules. The notion of "public record of ownership" also has to be qualified because the owners of Bitcoin units usually remain anonymous through the use of pseudonyms.

To use the Bitcoin system, an agent downloads a Bitcoin wallet. A Bitcoin wallet is software that allows the receiving, storing, and sending of (fractions of) Bitcoin units.[3] The next step is to exchange fiat currencies, such as the U.S. dollar, for Bitcoin units. The most common way is to open an account at one of the many Bitcoin exchanges and to transfer fiat currency to it. The account holder can then use these funds to buy Bitcoin units or one of the many other cryptoassets on the exchange. Due to the widespread adoption of Bitcoin, the pricing on large exchanges is very competitive with relatively small bid-ask spreads. Most exchanges provide order books and many other financial tools that make the trading process transparent.

A Bitcoin transaction works in a way that is similar to a transaction in the Yap payment system. A buyer broadcasts to the network that a seller's Bitcoin address is the new owner of a specific Bitcoin unit. This information is distributed on the network until all nodes are informed about the ownership transfer. We will examine some technical details of this step in Section 2.

For a virtual currency to function, it is crucial to establish at every point in time how many monetary units exist, as well as how many new units have been created. There must also be a consensus mechanism that ensures that all participants agree about the ownership rights to the virtual currency units. In small communities, as with the Yap islanders, everyone knows everyone else. The participants care about their reputation, and conflicts can be disputed directly. In contrast, within the Bitcoin system the number of participants is substantially larger, and network participants can remain anonymous. Consequently, reputation effects cannot be expected to have a significant positive impact, and coordination becomes very difficult. Instead, there is a consensus mechanism that allows the Bitcoin system to reach an agreement. This consensus mechanism is the core innovation of the Bitcoin system and allows consensus to be reached on a larger scale and in the absence of any personal relations.

1.6 Bitcoin Mining

To understand the consensus mechanism of the Bitcoin system, we first have to discuss the role of a miner. A miner collects pending Bitcoin transactions, verifies their legitimacy, and assembles them into what is known as a "block candidate." The goal is to earn newly cre-

ated Bitcoin units through this activity. The miner can succeed in doing this if he or she can convince all other network participants to add his or her block candidate to their copies of the Bitcoin Blockchain.

Bitcoin mining is permissionless. Anyone can become a miner by downloading the respective software and the most recent copy of the Bitcoin Blockchain. In practice, however, there are a few large miners that produce most of the new generally accepted blocks. The reason is that competition has become fierce and only large mining farms with highly specialized hardware and access to cheap electricity can still make a profit from mining.

For a block candidate to be generally accepted, it must fulfill a specific set of predefined criteria. For instance, all included transactions must be legitimate. Another important criterion is the so-called "fingerprint" of the block candidate. A miner obtains this fingerprint by computing the block candidate's hash value using the hash function dSHA256.

For example, we will look at the hash value for the text, "Federal Reserve Bank of Saint Louis." The fingerprint of this text, which was calculated using the hash function dSHA256, is

72641707ba7c9be334f111ef5238f4a0b355481796fdddfdaac4c5f2320eea68.

Now notice the small change in the original text to "federal Reserve Bank of Saint Louis." It will cause an unpredictable change of the fingerprint, which can be seen from the corresponding new hash value:

423f5dd7246de6faf8b839c41bf46d303014cffa65724ab008431514e36c4dba.

As suggested by this example, a data file's hash value cannot be prognosticated.

This characteristic is employed in the mining process as follows. For a block candidate to be accepted by all miners, its fingerprint must possess an extremely rare feature: The hash value must be below a certain threshold value—that is, it must display several zeroes at the beginning of the fingerprint. An example of a fingerprint of a block that was added to the Bitcoin Blockchain in 2010 is given in the following example:

Block #69785 (July 23rd, 2010, 12:09:36 CET)

$\underbrace{0000000000}_{\text{Need to be zero}}293b78a2833b45d78e97625f6484ddd1accbe0067c2b8f98b57995$

Miners are continuously trying to find block candidates that have a hash value satisfying the above mentioned criterion. For this purpose, a block includes a data field (called the nonce) that contains arbitrary data. Miners modify this arbitrary data in order to gain a new fingerprint. These modifications do not affect the set of included transactions. Just as with our example, every modification results in a new hash value. Most of the time, the hash value lies above the threshold value, and the miner discards the block candidate. If, however, a miner succeeds in creating a block candidate with a hash value below the current threshold value, he or she broadcasts the block candidate as quickly as possible to the network. All the other network participants can then easily verify that the fingerprint satisfies the threshold criterion by computing it themselves.

1.7 Consensus Mechanism

The consensus among miners is that every miner who receives a block candidate with a valid fingerprint adds it to his or her own copy of the Bitcoin Blockchain. From a game theoretical perspective, a strategy profile where all miners add valid blocks to their own copies of the Bitcoin Blockchain is a Nash equilibrium. If a miner believes that all other miners are acting accordingly, then it is a best response for that miner to add a valid block candidate to his or her own copy of the Bitcoin Blockchain. A deviation is not worthwhile, because it is not profitable to work on a version of the Bitcoin Blockchain that is not generally accepted. Any reward for finding blocks on a version of the chain that is not accepted by anyone else is worthless. Thus, although there is no authority enforcing this rule and miners are free to modify their copy of the Blockchain as they wish, there is a strong incentive to follow this rule. This self-enforcing rule allows the network to maintain consensus about the ownership of all Bitcoin units.[4]

Mining is expensive, as the computations use large amounts of electricity and are increasingly dependent on highly specialized hardware. Moreover, valid block candidates can be found only through a trial-and-error procedure. The consensus mechanism is therefore called "proof of work." If a miner finds a valid fingerprint for a block candidate, then this is proof that he or she has, on average, performed a large number of costly computations. Adding false information (e.g., illegitimate transactions) to a block candidate would render the block candidate invalid and essentially waste all the computations. Finding a valid fingerprint is therefore proof that the miner helped to maintain the Bitcoin system.

1.8 Monetary Policy

Every payment system needs rules that regulate how new monetary units are produced (or destroyed). The Bitcoin network is calibrated in such a way that, on average, a block candidate with a valid hash value is found every 10 minutes. The winner of the mining contest receives a predefined number of newly created Bitcoin units. The number currently is 12.5.

In the Bitcoin system, money creation is scheduled so that the number of Bitcoin units will converge to 21 million units (Figure 5). This limit exists because the reward for the miners is halved every 210,000 blocks (approximately every four years). Correspondingly, miners will be increasingly rewarded through transaction fees. But even today, the quick processing of a transaction can be guaranteed only if an adequate fee is paid to incentivize the miners to include the transaction in their block candidates.

Most Bitcoin users believe that Bitcoin's limited supply will result in deflation. That is, they are convinced that its value will forever increase. Indeed, up to this point we have witnessed a spectacular price increase from essentially a value of $0 for one Bitcoin unit in 2009 to a value of $7,000 at the time of this writing (Figure 6).

Nonetheless, these beliefs need to be challenged. Bitcoin units have no intrinsic value. Because of this, the present price of the currency is determined solely by expectations about its future price. A buyer is willing to buy a Bitcoin unit only if he or she assumes that the unit will sell for at least the same price later on. The price of Bitcoin, therefore, reacts highly elas-

Figure 5

Bitcoins in Circulation: Scheduled to Converge to 21 Million Units

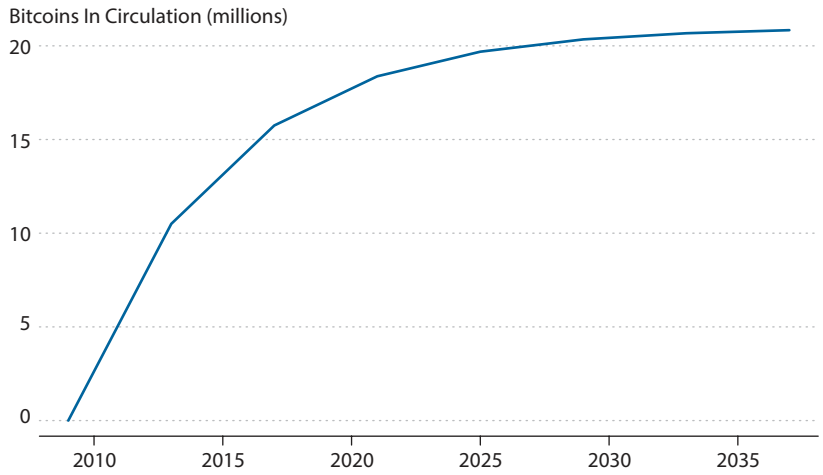


Figure 6

Market Price in U.S. Dollars (USD) for One Bitcoin Unit

SOURCE: Blockchain.info.

tically to changes in the expectations of market participants and is reflected in extreme price volatility. From monetary theory, we know that currencies with no intrinsic value have many equilibrium prices.[5] One of them is always zero. If all market participants expect that Bitcoin will have no value in the future, then no one is willing to pay anything for it today.

However, Bitcoin is not the only currency that has no intrinsic value. State monopoly currencies, such as the U.S. dollar, the euro, and the Swiss franc, have no intrinsic value either. They are fiat currencies created by government decree. The history of state monopoly currencies is a history of wild price swings and failures. This is why decentralized cryptocurrencies are a welcome addition to the existing currency system.

In the Bitcoin system, the path for the money supply is predetermined by the Bitcoin protocol written in 2008 and early 2009. Since then, many changes have been applied to the Bitcoin protocol. Most of these changes are not controversial and have improved the functioning of the Bitcoin system. However, in principle all aspects of the Bitcoin protocol can be amended, including the money supply. Many Bitcoin critics see this as a major shortcoming. Theoretically speaking, this is correct. Any network participant can decide to follow a new set of rules and, for example, double the amount of newly created "Bitcoin" units in his or her version of the ledger. Such a modification, however, is of no value because convincing all the other network participants to follow this new set of rules will be almost impossible. If the change of the protocol is not supported unanimously, there will be a so-called fork, a split in the network, which results in two co-existing blockchains and essentially creates a new crypto-asset. In this case, there would be Bitcoin (the original) and Bitcoin42 (a possible name for an alternative implementation with an upper bound of 42 million Bitcoin42 units). The market would price the original and the newly created Bitcoin42 assets according to the community's expectations and support. Therefore, even though in theory it is possible to increase the Bitcoin supply, in practice, such a change is very unlikely because a large part of the Bitcoin community would strongly oppose such an attempt.

Moreover, the same critique can be raised against any current government-operated fiat currency system. For example, since the Second World War, many central banks have become independent in order to shield them from political interference that yielded some undesirable outcomes. This independence has been given to them by the respective parliaments or related institutions and can be taken away if politicians decide accordingly. Political interference in the fiat currency system can be interpreted as a change in the "fiat currency protocol." Undesirable changes in fiat currency protocols are very common and many times have led to the complete destruction of the value of the fiat currency at hand. It could be argued that, in some ways, the Bitcoin protocol is more robust than many of the existing fiat currency protocols. Only time will tell.

2 BITCOIN TRANSACTIONS

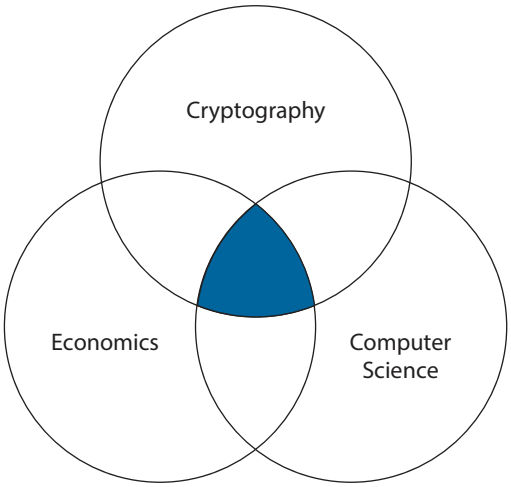
The complexity of the present material is due to interdisciplinarity. To understand the Bitcoin system, it is necessary to combine elements from the three disciplines of economics, cryptography, and computer science (Figure 7).

Having presented a broad overview of the Bitcoin system, we will explain a few technical elements of the system in greater detail. Blockchain uses proven technologies and links these in an innovative way. This combination has made the decentralized management of a ledger possible for the first time.

Berentsen and Schär (2017) argue that transaction processing demands that three requirements are satisfied: (1) transaction capability, (2) transaction legitimacy, and (3) transaction consensus. These three requirements will now be considered. In particular, we will explain how these conditions can be satisfied in the absence of a central authority.

Figure 7

Interdisciplinarity



2.1 Transaction Capability

What has to be resolved is how transactions can be initiated if there is no central authority. In a classical banking system, a client talks to his or her advisor or submits his or her payment instructions via the bank's online banking service. The infrastructure provided by the commercial bank and other central service providers ensures that the transaction will be communicated for execution. In the absence of a central authority, communicating a payment order in this traditional sense is not possible.

In the Bitcoin system, a payment order can be communicated to any number of network nodes. The network nodes are linked together in a loose network and forward the message until all nodes have been informed about the transaction (Figure 8).

The decentralization of the system has many advantages. In particular, it makes the system extremely robust. There is neither a central point of failure that can be attacked nor any system-relevant nodes that could cause the system to collapse. Therefore, the system functions even when some network nodes are unreachable, and it can always establish new connections and communication channels.

2.2 Transaction Legitimacy

Every participant can generate new payment orders and spread them across the network. This feature carries the risk of fraudulent messages. In this respect, there are two important questions that arise:

1. How do the nodes know that the initiator of the transaction is the rightful owner and that he or she is thereby entitled to transfer the Bitcoin units?
2. How can one ensure that the transaction message will not be tampered with before it is passed from one node to the next?

Figure 8

Bitcoin Transaction Communicated to Network Nodes

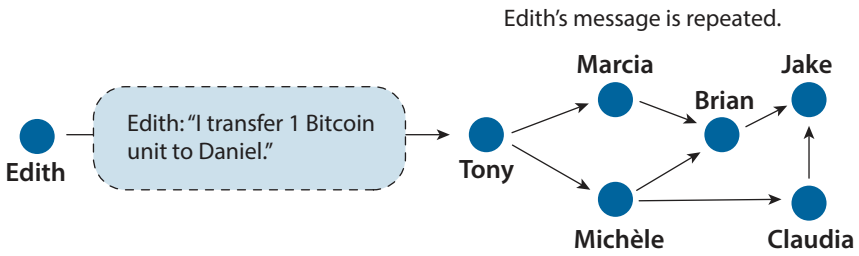


Figure 9

Bitcoin Transaction Manipulation Attempt

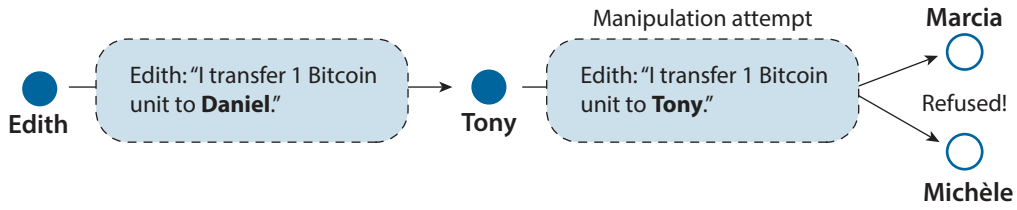
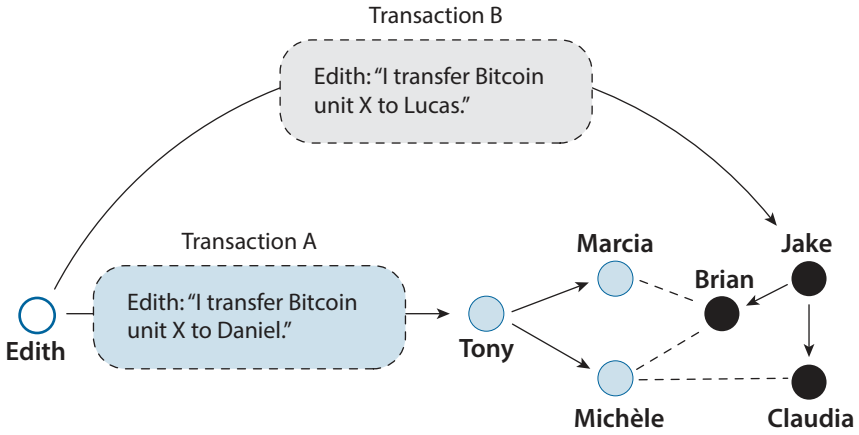


Figure 10

First Bitcoin Transaction Added to a Valid Block Candidate Is Confirmed



In the Bitcoin system, transaction legitimacy is guaranteed using asymmetric cryptography.[6] The idea is based on using pairs of keys consisting of a private and a public key. A private key should not be shared. It corresponds to a random value from an incredibly large set of numbers. A public key, on the other hand, is derived from that number and can be shared freely. It serves as a pseudonym in the Bitcoin network.[7]

A private key is used to encrypt a message that can be decrypted only by using its corresponding public key. This type of encryption is also known as a "signature." The signature clarifies that this approach is not used to hide any of the information in the encrypted message. Anyone can simply decrypt a message using its public key, but the signature serves as proof that the message has been previously encrypted using its corresponding private key; it's like a handwritten signature but much more secure.

For example, consider Edith, who wants to send a Bitcoin payment to Daniel over the Bitcoin network. She uses her private key to encrypt the message. The other network participants can only decrypt this message using Edith's public key. If an attempt is successful, it ensures that the message was encrypted using the corresponding private key. Because no one else has access to Edith's private key, this approach can be used to validate the transaction's origin (Figure 9).

When the transaction circulates in the network, any network participant can decrypt this message and is in the position to subsequently change the payment instructions. However, because the participant does not possess Edith's private key, he or she cannot re-encrypt the manipulated message. The tampered transaction will therefore be identified and rejected by the rest of the network.

2.3 Transaction Consensus

We have now discussed how a transaction message is communicated and how its legitimacy and origin can be verified. We have also explained how consensus regarding ownership of the Bitcoin units is achieved in the Bitcoin network by using the proof-of-work consensus protocol.

However, Edith would be able to generate two transactions that both reference the same Bitcoin units. Both transactions could be propagated simultaneously over the network (transaction capability), and both would display a valid origin (transaction legitimacy). Because of differences in the propagation of these two messages in the Bitcoin network, some of the nodes would first receive a message for transaction A while others would first receive a message for transaction B (Figure 10). In order to avoid double spending, it is important that only one of the two transactions finds its way into the Bitcoin Blockchain. A mechanism that decides which of the two transactions gets included in the Blockchain is therefore necessary.

The Bitcoin system solves this double spending problem in a clever way. The transaction that is first added to a valid block candidate, and therefore added to the Blockchain, is considered confirmed. The system ceases to process the other one—that is, miners will stop adding the conflicting transaction to their block candidates. Moreover, it is not possible for a miner to add conflicting transactions to the same block candidate. Such a block would be illegitimate and thus be rejected by all the other network participants.

3 OUTLOOK

As with any fundamental innovation, the true potential of blockchain technology will become apparent only many years, or possibly decades, after it becomes generally adopted. Forecasting the areas in which blockchain technology will be used to the greatest effect is therefore not possible. We nevertheless would like to mention a few areas where blockchain technology serves as an infrastructure platform that facilitates a variety of promising applications.

3.1 Cryptoassets

The most apparent application is Bitcoin as an asset. It is likely that cryptoassets such as Bitcoin will emerge as their own asset class and thus have the potential to develop into an interesting investment and diversification instrument. Bitcoin itself could over time assume a similar role as gold. Moreover, the potential for trading securities on a public blockchain is large. So-called colored coins can be traded on the Bitcoin (or similar) Blockchain and used in smart contracts, as described below.

3.2 Colored Coins

A colored coin is a promise of payment that is linked to a Bitcoin transaction. This promise is possible because the communication protocol of the Bitcoin network allows additional information to be tied to a transaction. For example, promises for the delivery of an ounce of gold or a dividend payment can be added to a Bitcoin transaction and represented on the Bitcoin Blockchain. Any of these promises are of course subject to issuer risks and require some extent of trust. This is in sharp contrast to native cryptoassets such as Bitcoin units.

3.3 Smart Contracts

Smart contracts are self-executing contracts.[8] They can be used to stipulate that a Bitcoin payment will be executed only when a certain condition is met. The Ethereum network is currently the leader in the field of smart contracts. Similar to Bitcoin, it is based on blockchain technology and provides a native cryptoasset, called Ether. In contrast to Bitcoin, Ethereum provides a more flexible scripting language and is able to track contractual states. Potential applications include but are not limited to e-voting systems, identity management and decentralized organization, and various forms of fundraising (e.g., initial coin offerings).

3.4 Data Integrity

Another application for public blockchains is the potential to monitor data files. We have already shown how fingerprints of block candidates play an important role in the Bitcoin network. The same technology can be used to produce fingerprints for all kinds of data files and then store them in a blockchain. The entry of a fingerprint into a blockchain ensures that any manipulation attempt will become apparent because any change to the data file will lead to a completely different hash value. Because it is very difficult to change a blockchain retroactively, a fingerprint can serve as proof that a specific data file existed at a specific point in time and ensures the integrity of the data.

4 RISKS

Much like any other key innovation, blockchain technology introduces some risks. The following sections will consider some of these risks. As we mentioned in Section 3, we would like to note that this list is non-exhaustive.

4.1 Forks

As discussed in Section 1.8, the Bitcoin protocol can be altered if the network participants, or at least a sufficient number of them, agree on the suggested modification. It can happen (and in fact has happened) that a blockchain splits because various groups cannot agree about a modification. A split that persists is referred to as a "fork." The two best-known examples of persistent splits are the Bitcoin Cash fork and Ethereum's ideological dissent, which resulted in the split to Ethereum and Ethereum Classic.

4.2 Energy Wastage

Proof-of-work mining is expensive, as it uses a great deal of energy. There are those that criticize Bitcoin and assert that a centralized accounting system is more efficient because consensus can be attained without the allocation of massive amounts of computational power. From our perspective, however, the situation is not so clear-cut. Centralized payment systems are also expensive. Besides infrastructure and operating costs, one would have to calculate the explicit and implicit costs of a central bank. Salary costs should be counted among the explicit costs and the possibility of fraud in the currency monopoly among the implicit costs. Moreover, many cryptoassets use alternative consensus protocols, which do not (solely) rely on computational resources.

4.3 Bitcoin Price Volatility

The price of Bitcoin is highly volatile. This leads us to the question of whether the rigid predetermined supply of Bitcoin is a desirable monetary policy in the sense that it leads to a stable currency. The answer is no because the price of Bitcoin also depends on aggregate demand. If a constant supply of money meets a fluctuating aggregate demand, the result is fluctuating prices. In government-run fiat currency systems, the central bank aims to adjust the money supply in response to changes in aggregate demand for money in order to stabilize the price level. In particular, the Federal Reserve System has been explicitly founded "to provide an elastic currency" to mitigate the price fluctuations that arise from changes in the aggregate demand for the U.S. dollar. Since such a mechanism is absent in the current Bitcoin protocol, it is very likely that the Bitcoin unit will display much higher short-term price fluctuations than many government-run fiat currency units.

5 CONCLUSION

The Bitcoin creators' intention was to develop a decentralized cash-like electronic payment system. In this process, they faced the fundamental challenge of how to establish and transfer

digital property rights of a monetary unit without a central authority. They solved this challenge by inventing the Bitcoin Blockchain. This novel technology allows us to store and transfer a monetary unit without the need for a central authority, similar to cash.

Price volatility and scaling issues frequently raise concerns about the suitability of Bitcoin as a payment instrument. As an asset, however, Bitcoin and alternative blockchain-based tokens should not be neglected. The innovation makes it possible to represent digital property without the need for a central authority. This can lead to the creation of a new asset class that can mature into a valuable portfolio diversification instrument. Moreover, blockchain technology provides an infrastructure that enables numerous applications. Promising applications include using colored coins, smart contracts, and the possibility of using fingerprints to secure the integrity of data files in a blockchain, which may bring change to the world of finance and to many other sectors. ■

NOTES

1 An initial attempt was DigiCash in the 1990s; however, it was not able to establish itself.

2 See Furness (1910) who describes the Island of Stone Money.

3 Strictly speaking, Bitcoins are not "traveling" on the Bitcoin network. A Bitcoin payment is simply a message that is broadcasted to the network to communicate a change in ownership of the respective Bitcoin units.

4 In practice, a split in the Blockchain may occur if the network participants do not agree about changes in the Bitcoin protocol (i.e., the rule set). This issue is discussed further in this article.

5 See Kiyotaki and Wright (1993) for a search theoretic approach to money, Berentsen (1998) for a study of the acceptability of digital money, and Nosal and Rocheteau (2011) for a comprehensive introduction into the search theoretic approach to monetary economics.

6 Similar technologies are also used in traditional electronic payment systems and in many other fields, such as with online banking and shopping.

7 In fact, a public key is usually used to derive a so-called Bitcoin address. This address is then used as a pseudonym. We ignored this additional step to keep things as simple as possible. Both operations—that is, private key to public key and public key to Bitcoin address—are one-way functions. There is no known way to reverse these operations, so it is not feasible to obtain a private key from a corresponding pseudonym.

8 For an introduction to smart contracts and potential business applications, see Schär and Langer (2017).

REFERENCES

Berentsen, Aleksander. "Monetary Policy Implications of Digital Money." *Kyklos (International Review of Social Sciences)*, 1998, *51*(1), pp. 89-117; https://doi.org/10.1111/1467-6435.00039.

Berentsen, Aleksander and Schär, Fabian. *Bitcoin, Blockchain und Kryptoassets: Eine umfassende Einführung*. Books on Demand, Norderstedt, 2017.

Furness, William H. *The Island of Stone Money: Uap of the Carolines*. Philadelphia: J. B. Lippincott, 1910.

Kiyotaki, Nobuhiro and Wright, Randall. "A Search-Theoretic Approach to Monetary Economics." *American Economic Review*, 1993, *83*(1), pp. 63–77.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008; https://bitcoin.org/bitcoin.pdf.

Nosal, Ed and Rocheteau, Guillaume. *Money, Payments, and Liquidity*. Cambridge and London: The MIT Press, 2011; https://doi.org/10.7551/mitpress/9780262016285.001.0001.

Schär, Fabian and Langer, Dominik. "Smart Contracts – eine missverstandene Technologie mit hohem Potenzial." *Synpulse Magazin*, 2017, *3*(17), pp. 38-41.