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

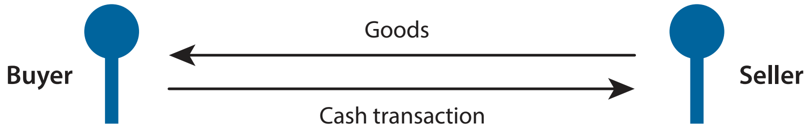
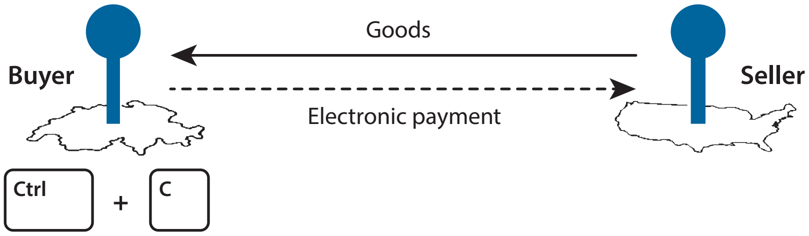


Figure 2

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.

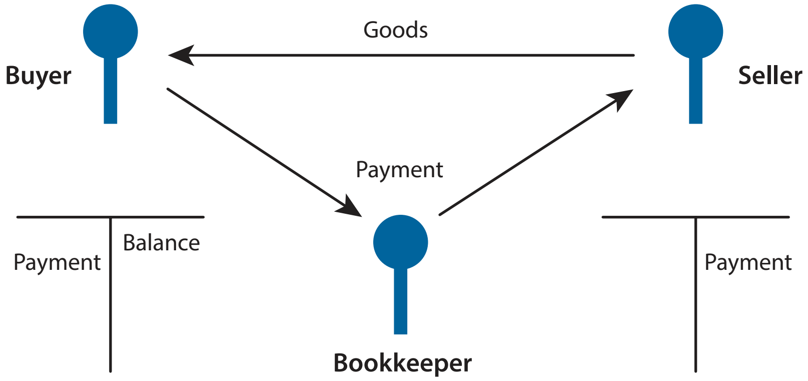
A specific feature of electronic data is that it can be copied any number of times at negligible cost. This feature is highly undesirable for money. If cash data files can be copied and the duplicates used as currency, they cannot serve as a payment instrument. This problem is termed the "double spending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

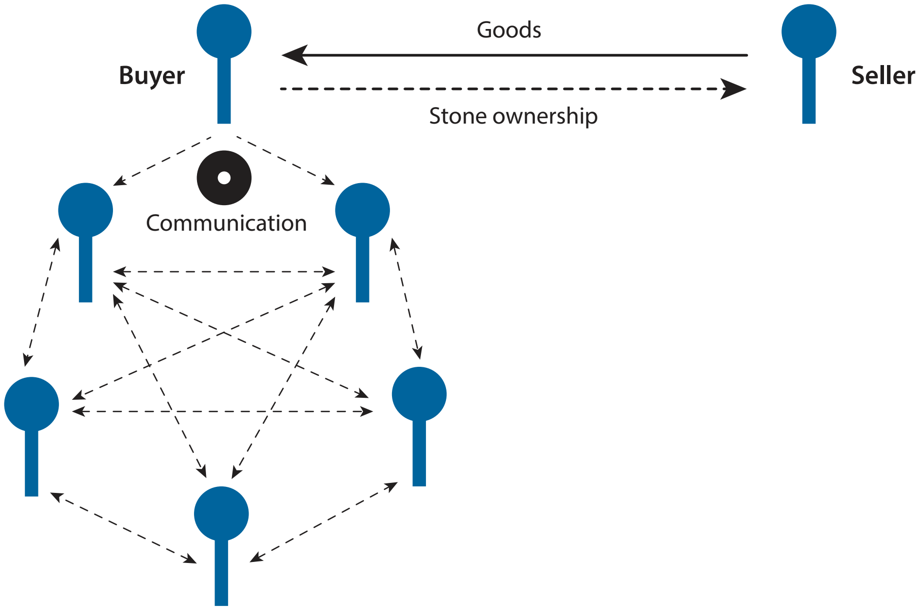
The key feature of the Bitcoin system is the absence of a centrally managed ledger. There is no central authority with an exclusive right to keep accounts. In order to understand how this is possible, we will first discuss a historical payment system that has certain similarities with the Bitcoin system.

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-