Bitcoin vs. Traditional Payment Systems: How Do They Compare?

When Bitcoin was first presented to the world in a white paper published under the pseudonym Satoshi Nakamoto back in 2008, it had the support of just a handful of enthusiasts. However, things have changed dramatically in recent years, and the cryptocurrency has grown to become one of the most widely watched technological developments in the world.

Introducing the concept of 'blockchain' for payments, Bitcoin promised to bring a greater level of trust and security to financial transactions. And while other blockchain systems have been launched since Bitcoin's arrival, Bitcoin is still considered by many as the most developed and reliable system; evidenced in part by the fact that the infrastructure built around Bitcoin still surpasses that of its alternatives.

Today, Bitcoin handles a significant number and a large dollar-value of transactions, which has drawn the world's attention to its potential as a payment system. But how does it compare to traditional payment systems? Is it more effective?

In this paper, we will look at the fundamental differences between Bitcoin and traditional payment systems and examine the strengths and weaknesses of each.

What is Bitcoin?

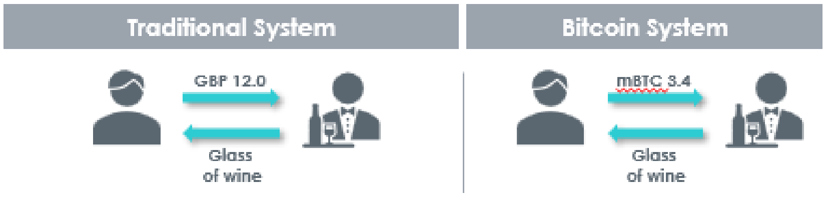
Designed as a payment system, Bitcoin enables the transfer of value in the same way that bank transfers or card payments do. However, the term 'Bitcoin' can be confusing at times, as it does not always seem to refer to the same thing. Indeed, the term is used to refer to a currency, a protocol, and a network. At a very high level, these subcomponents are similar to those that make up traditional electronic payment systems, yet there are key differences in the way the two systems operate. Before we compare the Bitcoin system to traditional payment systems, let's explore Bitcoin's subcomponents in more detail.

A Currency

A currency is a generally accepted form of money that is used as a medium of exchange, a store of value, or a unit of account. Traditional currencies such as the US dollar, the euro, or the British pound––which are often referred to as fiat currencies––are government-backed and derive their value from that endorsement. Today, currencies are not directly backed by gold or any other commodity or asset.

Bitcoin is similar to its traditional counterparts in that it is used as a medium of exchange, a store-of-value, and a unit of account. And like fiat currencies, the cryptocurrency is not backed by any commodity or other asset. However, a key difference between bitcoin and traditional fiat currencies is that while fiat currencies are legal tender that are backed by a government and controlled by a central bank, bitcoin is a 'distributed' global currency that is not controlled by any centralized entity and its supply automatically increases at a pre-determined rate.

Figure 1: Fiat transaction versus bitcoin transaction



mBTC = millibitcoin. GBP = British pound sterling.

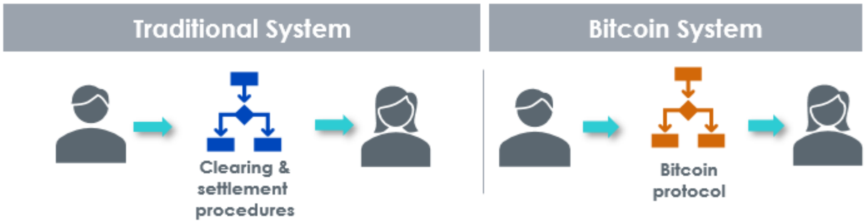
A Protocol

A protocol can be described as a set of rules governing action or communication under certain conditions.

The term Bitcoin also refers to the protocol underlying transactions, or the set of rules and mechanisms that enable the system to work securely, while being distributed rather than centralized.

The Bitcoin protocol uses Distributed Ledger Technology (DLT)––a consensual, distributed database––as well as cryptography (which protects information) to verify and record transactions, while solving for the ‘double-spending’ problem––the risk of digital cash being copied and spent several times. The Bitcoin protocol is the first system to handle this issue without the need for a centralized authority.

Figure 2: Bank transaction versus Bitcoin transaction



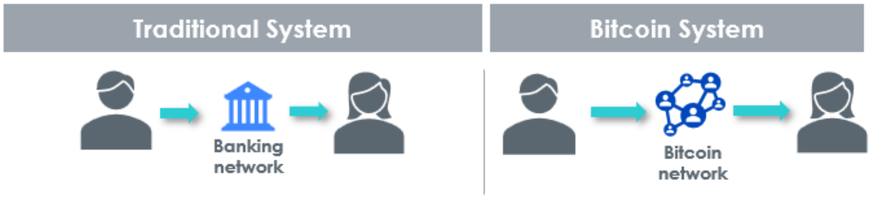
The traditional banking system also relies on communication standards and various sets of rules and mechanisms to authorize, clear and settle transfers. The critical core difference, once again, is the fact that the traditional system relies on centralized counterparties, while the Bitcoin protocol eliminates the need for these intermediaries.

A Network

The traditional payment system relies on the banking network to process transactions. Banks around the world are directly or indirectly connected to each other and when a payment is initiated from a payer’s bank, it goes sequentially through various checking processes across a network of intermediaries.

By contrast, the Bitcoin network is a peer-to-peer network or an ecosystem of interconnected computers that verify and approve transactions while maintaining a ledger of all past transactions––the blockchain. This ledger is public, and anyone can install Bitcoin software and see the entire history of all Bitcoin transactions ever processed. These computers are called ‘nodes’.

Figure 3: Bank network versus Bitcoin transaction



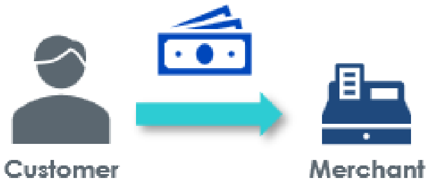
How does the Bitcoin system differ from traditional payment systems?

At the core of every transaction system lies one essential element: trust. When you agree to sell a product in return for money, you need to know that you will actually receive the money. Does the customer have the money? Can he or she stop the payment after it has been initiated? Let's look at how cash and card transactions compare to Bitcoin transactions.

Cash Transactions

A cash transaction handles the trust issue quite effectively. If a customer gives you a banknote, you have the money from the sale. There is no intermediary. However, flaws still exist. For example, the customer could give you a counterfeit banknote.

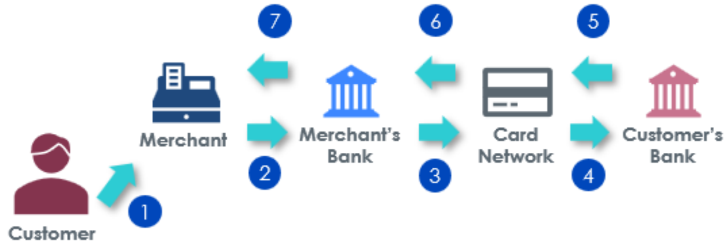
Figure 4: A cash transaction



Card Transactions

With a card payment, the payment has to be processed by a card network such as VISA or Mastercard as well as a banking network for authorization, clearing and settlement. Trust is generated by relying on well-established financial institutions that run a number of checks while the transaction is in progress. In Figures 5 to 7 below, we show the process flow for card payments.

Figure 5: Card payment authorization process

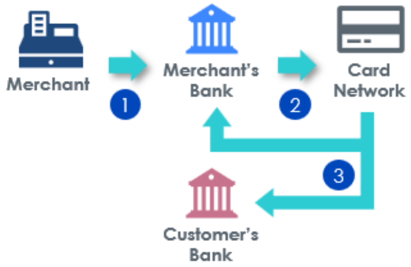


The authorization phase aims to verify a customer's identity as the owner of the funds they are trying to use, as well as the availability of the funds.

When you insert your card into a terminal and type your pin code (1) during a transaction, the payment details and your card information are sent to the merchant's bank (2), which then submits those details to the card network (3). In turn, the network will request authorization to your bank (4), and if the details are correct and you have the funds available, your bank will send an authorization to the merchant through the same intermediaries, one after the other (5, 6, 7).

This entire process happens within a few seconds, and you can walk out of the shop with your goods. But the process continues in the background. While authorization has been given, the funds are still in your account.

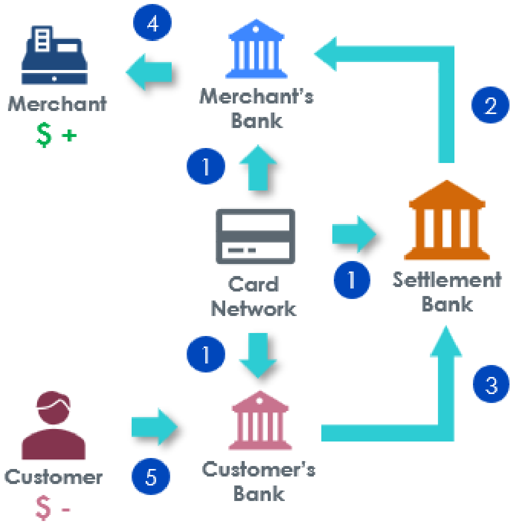
Figure 6: Card payment clearing process



The clearing process involves the exchange of transaction-related information used for the verification of money to be debited from the customer's bank and credited to the seller's bank.

At the end of every day, all the approved transactions for the day are sent from the merchant to the merchant's bank (1), which then transmits the details to the card network (2). The card network validates the information, sends the purchase information to customers' banks, and finally sends reconciliation information to both the merchant's and the customers' banks (3).

Figure 7: Card payment settlement process



Finally, the payment can undergo settlement, as shown in Figure 7. Settlement occurs daily on an aggregated net-basis and involves the actual transfer of funds. The card network computes the net settlement position that the customer's bank needs to pay to the merchant's bank and sends that information to both banks, plus a new actor, the settlement bank (1). The settlement bank pays the merchant's bank (2), and the customer's bank pays the settlement bank (3). Finally, the merchant gets credited (4), and the customer gets debited (5).

This entire process (authorization to settlement) generally takes between 24 and 48 hours. As shown in the diagrams above, it's quite a cumbersome, informationally heavy process and it involves a number of counterparties that need to sequentially create and transmit information.

Yet this system is well established and reliable enough that it has built up a high level of trust among users. Indeed, it has become so widely accepted that countries such as Sweden are aiming to become cashless societies.

In this model, the card network plays an essential role. As a lot of actors are involved, all with their own information systems, so it can be quite difficult to communicate between one another.

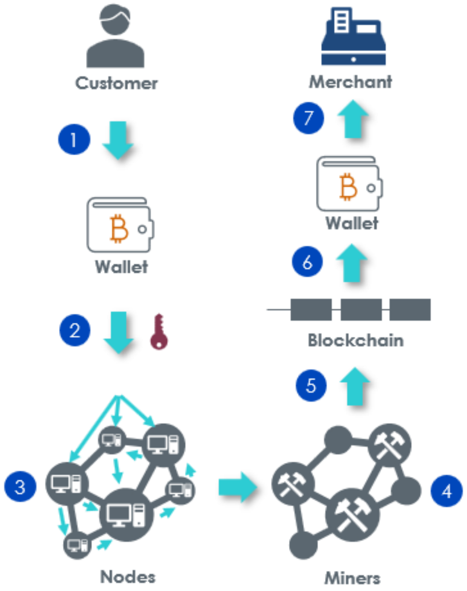
The network "is responsible for collecting all transactions and operating a gateway. It exchanges information between [customers' bank'] and [merchants' banks], establishes rules and processes for participation in the network, creates formatting standards for information going across the network, and facilitates monetary settlement between and among its client banks"[1].

In other words, it provides the standards and infrastructure for information exchange between the parties involved.

Bitcoin Transactions

When sending bitcoins through the Bitcoin network, the process follows a very different path.

Figure 8: bitcoin transaction process



First, as the sender, you enter the recipient's Bitcoin address (this is similar to a bank account number in a bank transfer) and number of bitcoins to send using your digital wallet interface (1). You can think of this step as equivalent to the merchant's payment terminal preparing the payment information in a card transaction. For in-store payments with bitcoins, merchants often scan your items and then create a QR code that you can scan with your digital wallet on your phone, automatically filling the amount to pay and the merchant's address.

The wallet then sends this information to the network, using your 'private key' to digitally sign the transaction (2). The digital signature is in some ways similar to a customer entering their pin code or signing the receipt in a card transaction; its purpose is to prove the sender's ownership of the funds.

A few nodes will receive the transaction, before transferring the details to other nodes, and in a few seconds your transaction has been propagated to the whole network (3). All nodes can independently verify the transaction and check that you actually have the bitcoins you aim to send and that you haven't already previously sent them. Steps 1, 2 and 3 are similar to the authorization step in card payments.

[1] Herbst-Murphy, Susan (2013). "Clearing and Settlement of Interbank Card Transactions: A MasterCard Tutorial for Federal Reserve Payments Analysts".

‘Miners’ will then gather transactions in a batch and begin trying to solve a computationally intensive problem. The first to solve the problem notifies the network that completion has been achieved (4). All other nodes can easily check whether this miner is telling the truth, in which case this new batch––a block––is added to the blockchain (5). Step 5 is similar to the settlement phase in the card transaction example as it’s where the money actually changes ownership.

The purpose of step 4 is to ensure that the blockchain cannot be modified. Modifying the chain would require an extensive amount of computing power, therefore, it is operationally very difficult to do so. As more blocks are added after the block containing your transaction, it becomes exponentially harder to modify that block.

Once the block containing the transaction is added to the blockchain and registered in the distributed ledger, the merchant’s wallet will see the payment as confirmed (6) and the merchant will be the new owner of those bitcoins (7).

The time for this entire process can vary depending on a number of factors. But the average time to mine a block is 10 minutes. So even if you want to wait for five more blocks (six confirmations––the community standard) to really consider the transaction effective, you can reasonably expect it to occur in approximately one hour.

What are Bitcoin’s advantages over traditional payment systems?

While some potential advantages of the Bitcoin system such as its anonymity, transparency, and independence from governments and central banks appear to be a matter of ideology, Bitcoin certainly does offer benefits when it comes to operational efficiency and trust.

Less Intermediaries

When sending bitcoins to another party, there are basically only two necessary intermediaries needed for the coins to effectively be transferred: your wallet and the Bitcoin network. Nodes and miners are only sub-parts of the network and adding or removing some of them does not affect its functioning. By contrast, the card payment system requires a minimum of four intermediaries, and often more in reality.

Improved Efficiency

As a distributed system, the Bitcoin protocol allows all components of the system to access and verify all pending transactions and past transactions, all of the time and simultaneously, which creates time efficiency. And errors cannot occur along the way; as long as you entered the right address when initiating the transaction, the funds will get to their intended destination.

Not only does the traditional payment system have more intermediaries, but it also multiplies the communication exchanges back and forth, which need to happen sequentially. This takes time, and errors can occur along the way.

Distributed Trust and Single Points of Failure

Yet the key advantage of Bitcoin really resides in the way it handles trust in transactions and eliminates single points of failure.

With the traditional system, you need to trust that the rules and mechanisms will not lead to errors and that every single counterparty involved operates properly. If one counterparty along the chain is somehow compromised, then the whole chain will be compromised.

With Bitcoin, the set of rules and mechanisms underpinning the system makes fraud, manipulation and errors impossible. As Bitcoin software is open source, anyone in the world can access it and review it. In Bitcoin’s 10-year track record, no security flaw has ever been uncovered. No one has found a way to change a signed transaction, or modify the blockchain.

Additionally, the beauty of a distributed system is that you don't need to trust any single one of its components as there is no single point of failure. Compromising one or a few nodes would not compromise the network. To fraudulently modify pending transactions or the blockchain of past transactions, one would need to take control of the majority of the computing power of the network.

Ultimately, where the risk lies is your digital wallet, as it stores your private keys. Anybody who accesses your private keys can spend the funds in the wallet. This is the reason why offline wallets, referred to as 'cold-storage', are frequently used to prevent hacking. But from the moment your transaction is signed, there are no single points of failure, and you don't need to place your trust in any single party. This does not mean that trust is obsolete, but it minimizes the burden that trust places on any single potential point for failure.

Important Information

This material is for informational purposes only and contains the opinions of the author, which are subject to change, and should not be considered or interpreted as a recommendation to participate in any particular trading strategy or deemed to be an offer or sale of any investment product, and it should not be relied on as such. This material is not intended to provide investment recommendations and is not an official statement of WisdomTree. This material represents an assessment of the environment discussed at a specific time and is not intended to be a forecast of future events or a guarantee of future results. Readers of this information should consult their own financial advisor, lawyer, accountant, or other advisor before making any financial decision.

There are risks associated with investing, including the possible loss of principal. Crypto assets, such as bitcoin and ether, are complex, generally exhibit extreme price volatility, are unpredictable, can become illiquid at any time, and should be viewed as highly speculative assets. Crypto assets are frequently referred to as crypto "currencies," but they typically operate without central authority or banks, are not backed by any government or issuing entity (i.e., no right of recourse), have no government or insurance protections, are not legal tender and have limited or no usability as compared to fiat currencies. Federal, state or foreign governments may restrict the use, transfer, exchange and value of crypto assets, and regulation in the U.S. and worldwide is still developing. Crypto asset exchanges and/or settlement facilities may stop operating, permanently shut down or experience issues due to security breaches, fraud, insolvency, market manipulation, market surveillance, KYC/AML (know your customer / Anti-Money Laundering) procedures, non-compliance with applicable rules and regulations, technical glitches, hackers, malware or other reasons, which could negatively impact the price of any crypto asset traded on such exchanges or reliant on a settlement facility or otherwise may prevent access or use of the crypto asset. Crypto assets can experience unique events, such as forks or airdrops, which can impact the value and functionality of the crypto asset. Crypto asset transactions are generally irreversible, which means that a crypto asset may be unrecoverable in instances where: (i) it is sent to an incorrect address, (ii) the incorrect amount is sent, or (iii) transactions are made fraudulently from an account. A crypto asset may decline in popularity, acceptance or use, thereby impairing its price, and the price of a crypto asset may also be impacted by the transactions of a small number of holders of such crypto asset. Crypto assets may be difficult to value and valuations, even for the same crypto asset, may differ significantly by pricing source or otherwise be suspect due to market fragmentation, illiquidity, volatility and the potential for manipulation. Crypto assets generally rely on blockchain technology and blockchain technology is a relatively new and untested technology which operates as a distributed ledger. Blockchain systems could be subject to internet connectivity disruptions, consensus failures or cybersecurity attacks, and the date or time that you initiate a transaction may be different then when it is recorded on the blockchain. Access to a given blockchain requires an individualized key, which, if compromised, could result in loss due to theft, destruction or inaccessibility. In addition, different crypto assets exhibit different characteristics, use cases and risk profiles. Information provided by WisdomTree regarding digital assets, crypto assets or blockchain networks should not be considered or relied upon as investment or other advice, as a recommendation from WisdomTree, including regarding the use or suitability of any particular digital asset, crypto asset, blockchain network or any particular strategy. WisdomTree is not acting and has not agreed to act in an investment advisory, fiduciary or quasi-fiduciary capacity to any advisor, end client or investor, and has no responsibility in connection therewith, with respect to any digital assets, crypto assets or blockchain networks.

Cryptocurrency: a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend.

Blockchain: a distributed ledger system in which a record of transactions made in cryptocurrencies is maintained across computers linked in a peer-to-peer network.