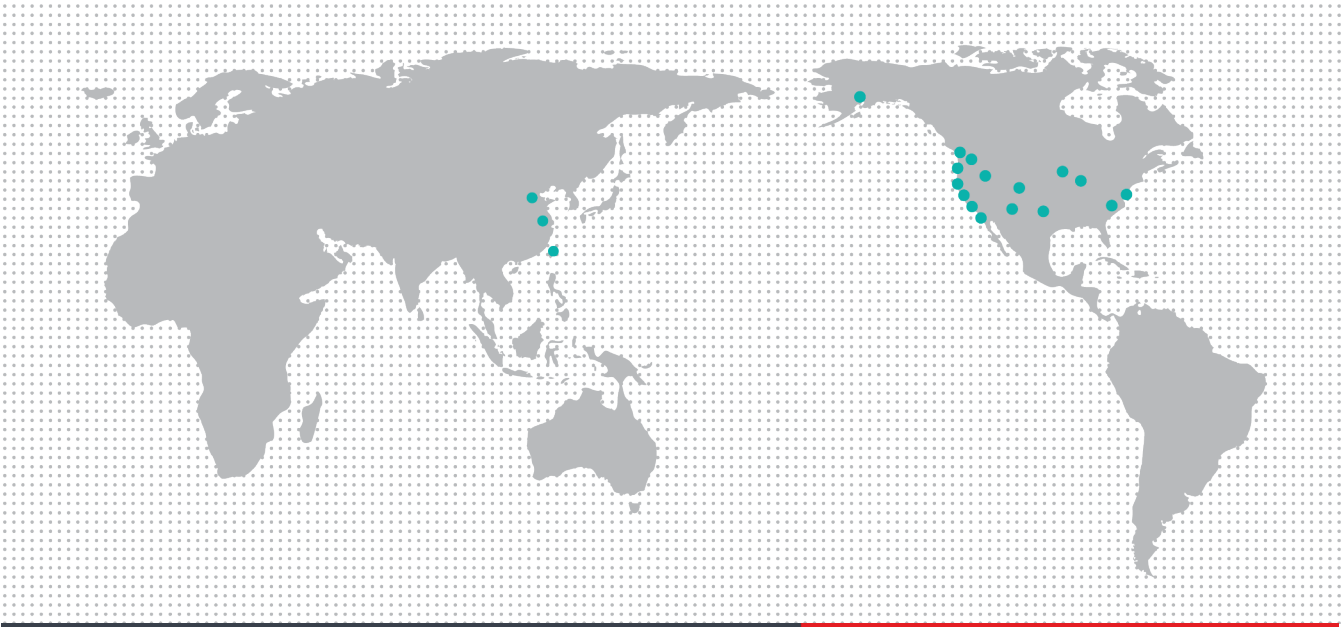
PERKINSCOIE



Perkins Coie LLP and The Bitcoin Foundation

COUNSEL TO GREAT COMPANIES

PREPARED BY PERKINS COIE LLP FOR

Bitcoin: A Primer

AUTHORS

ATTORNEY NAME

J. DAX HANSEN
+1.206.359.6324
DHansen@perkinscoie.com

ATTORNEY NAME

JACOB FARBER
+1.202.654.6268
JFarber@perkinscoie.com

ATTORNEY NAME

PATRICK MURCK
Patrick@bitcoinfoundation.org

Bitcoin

I. BITCOIN IS A DECENTRALIZED, OPEN-SOURCE, PEER-TO PEER-NETWORK

Bitcoin was invented in 2008 as a peer-to-peer payment system for use in online transactions. Bitcoin is revolutionary in that, unlike any prior payment system, Bitcoin is not administered by any central authority, i.e. there is no middleman between the sender/buyer and the receiver/seller as there is with, say, PayPal or a traditional payment card. (Bitcoin is thus referred to as a "decentralized" digital currency.)

Instead, the Bitcoin transaction network consists of computers around the world running the Bitcoin open- source software containing the network protocol for administering Bitcoin network transactions. That software can be downloaded by any Bitcoin user (or anyone else for that matter), and any computer running the software can join the network. Each computer on the network also maintains a copy of a universal ledger that contains the history of every Bitcoin transaction ever made.

As explained in more detail below, the computers on the Bitcoin network collectively verify every Bitcoin transaction, and ensure that no Bitcoin user can spend value that he or she does not have, or that has already been spent. Once a transaction is verified, it is included in a new "block" of transactions that is permanently added to the ledger collectively maintained by all the computers on the network (which is, for this reason, referred to as the "block chain"). The addition of the new transaction block to the block chain serves to confirm that the included transactions took place and, by virtue of the time-stamp included along with the block, when they took place. Each new block added to the block chain contains all of the verified transactions that took place since the addition of the prior block.

II. HOW A BITCOIN TRANSACTION WORKS

Any Bitcoin user can transact directly with any other Bitcoin user. To utilize the Bitcoin network, a user needs a Bitcoin address. While any Bitcoin user can generate an address using the Bitcoin open-source software, in practice, many users have accounts with one or more Bitcoin service providers and store bitcoins at addresses provided through their accounts. A Bitcoin address takes the form of a cryptographic "public key," a string of numbers and letters roughly 33 digits long. Each public key has a matching "private key," known only to the user, and protected by a password or other means of authentication.

To initiate a transaction, the user sends a message to the other computers on the network announcing the transfer of a certain value in bitcoins1 from the user's public key to the recipient's public key. The sending user's private key is used to "sign" the transactions. The private key is mathematically paired with the public key, and through a standard cryptographic process of the sort used to secure website connections, every computer on the network can verify that the transaction is signed with the correct private key.2 The private key signature thus serves to confirm that the transaction originated with, and was approved by, the actual owner of the originating public key, and therefore that the transaction is valid. While this process sounds complicated, it is

---

1 As discussed below, a distinction should be made between the network and protocol over which transactions are made on the one hand, and the unit of digital currency that can be sent or received over that network/protocol on the other hand. By the convention adopted here, "Bitcoin," when capitalized, refers to the network/protocol, and lower-cased "bitcoin" refers to the unit of digital currency.

2 By using the cryptographic process, any computer on the network can compute whether the private key is correct, without ever knowing the private key.

handled automatically and transparently to users through the Bitcoin software. From the user's perspective, sending bitcoins to someone else is no more difficult or arcane than sending funds using PayPal or other traditional payment systems.

Each active computer on the Bitcoin network receives a copy of the transaction message. This serves to notify every other user on the network that the owner of the receiving public key is the new owner of the bitcoins sent by the sending public key (assuming that the transaction bears the correct private key signature that proves that it is genuine). At this point, the transaction has been completed and is irreversible.3

It is not, however, accepted as a verified transaction until it is included in a block of transactions added to the block chain. Like the verification of private keys, the process of grouping transactions into blocks involves a cryptographic process that serves to confirm the validity of the block. Once a block is created, it is broadcast to the network, and the other computers on the network can confirm the so-called "proof of work" required to create the block. Only at that point is the block added to the block chain. Each new block added to the block chain contains a "hash"—a unique identifier—of the previous block that links the blocks and serves to confirm the previous block. Since no central authority controls the Bitcoin network, a consensus process is used to ensure that a common, current block chain always exists that constitutes a universally accepted record of all Bitcoin network transactions. Each computer on the network continuously updates its copy of the block chain to keep it current.

The process of finding the proof of work necessary to create transaction blocks is, by design, computationally very intensive, and requires considerable computing power so as to ensure that only valid blocks are added to the network. In order to incentivize users to expend the necessary computing power, each new block added to the block chain contains a transaction that rewards its creator with new bitcoins. The process of verifying transactions is thus also the mechanism by which new bitcoins are added to the network. (This process is referred to as "mining," and the users who choose to expend computing power to do so are referred to as "miners."4)

In order to ensure that a constant flow of new bitcoins are added to the network, the difficulty of the proof of work necessary to create each new block is steadily and automatically adjusted, such that blocks are created at a constant rate of one new block roughly every ten minutes. At the same time, the number of bitcoins that can ever be mined is capped at 21 million.5 To accomplish this, the number of bitcoins awarded for each new block is periodically halved.6 The last bitcoins to be created this way will be created in approximately the year 2140.

---

3 That the transaction is irreversible does not mean that the bitcoins in question cannot be returned to the sending public key. It just means that the sender cannot withdraw the transaction. The recipient is always free to reverse the transaction by initiating a transaction that sends the bitcoins back to the sender. In the campaign contribution context, this means that recipients can return contributions where necessary or appropriate, such as to comply with donor identification or contribution limit requirements.

4 The analogy to mining is inexact. Gold miners unearth existing gold, whereas the bitcoin mining process results in the creation of new bitcoins.

5 The 21 million cap on the number of bitcoins that can be mined is an arbitrarily chosen limit built into the protocol. To accommodate this limit, each bitcoin is subdivided down to eight decimal places, forming 100 million smaller units called "satoshis."

6 The reward started at 50 bitcoins and is halved every four years. Once the 21 million cap is reached, miners will be rewarded for creating blocks through small transaction fees.

While miners obtain newly-created bitcoins, the vast majority of Bitcoin users do not engage in mining, and therefore must acquire bitcoins from other sources. Some users acquire bitcoins directly from miners. In other instances, users obtain bitcoins from other users in exchange for goods or services, as many stores, restaurants, charities, and online businesses now accept bitcoins. Other users obtain bitcoins by buying or trading for them via one of the numerous exchanges and other service providers that perform those functions.

III. HOW BITCOINS ARE VALUED

Bitcoins are an intangible asset—they exist only in the form of the record of ownership maintained in the block chain. Their value is not tied to the scarcity of a physical resource (like gold), or to their issuance by some recognized central authority (like legal tender). Rather, they have value because users recognize them as a useful way of exchanging value, and have adopted them for that purpose. The limited supply of bitcoins, the increasing computational power required to add new bitcoins to circulation, the growing base of users, and their perceived strengths and weaknesses relative to other forms of value all factor into their value. Several leading exchanges maintain exchange rates that express the prices at which bitcoins trade relative to the dollar and certain other national currencies.

IV. THE ADVANTAGES OF BITCOIN OVER OTHER TRANSACTION SYSTEMS

The decentralized, open-source nature of Bitcoin gives it several advantages over other transaction systems. First, by eliminating the middleman, Bitcoin eliminates the cost and friction inherent in other transaction systems, making Bitcoin transactions nearly instantaneous and free or nearly free. Not only does this offer the promise of dramatically reducing the cost of existing forms of transactions such as overseas remittances, but it also enables new types of transactions like micro-payments.

Second, because every Bitcoin transaction is included in the block chain, the public details of the transaction can be viewed by any Bitcoin user or anyone else running the Bitcoin open-source software. Although Bitcoin transactions are “private” in the sense that there are no names attached to the public keys recorded in the block chain, all transactions associated with any given public key may easily be viewed and analyzed. This provides an unprecedented level of transparency to financial transactions. As we discuss below, this transparency is one of the features of the Bitcoin network that makes it ideally suited for political contributions.

Third, Bitcoin is highly protective of individual freedom. While the public details of every transaction are included in the block chain, Bitcoin users can choose whether to reveal their identity when engaging in transactions. Thus, unlike other financial transaction systems, Bitcoin puts privacy back in the hands of users, letting them determine the level of privacy they wish to maintain for a particular transaction. In instances where users have the legitimate need or desire to protect their identify, such as when paying for mental health services, they can do so. At the same time, where disclosure of personal information is necessary or appropriate (such as in connection with a contribution in an amount for which identification of the donor is required), the user is free to provide such information.

Finally, scholars view the Bitcoin protocol as a stimulus for financial innovation.7 While the Bitcoin protocol is currently used almost exclusively for transactions in bitcoin digital currency, the Bitcoin network/protocol’s neutral, open-source nature lends itself to numerous other uses. Since, bitcoins are, at their core, only a record of the history of ownership of a particular unit of value, they can be adopted as indicators of ownership interests

---

7 See generally Jerry Brito & Andrea Castillo, Bitcoin: A Primer for Policymakers (Mercatus Center, 2013), available at http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_embargoed.pdf.

in other assets as well. For example, bitcoins could be used to designate and transfer ownership in stocks, intellectual property, or ownership shares in a business entity. Moreover, other protocols can be added on top of the Bitcoin protocol to extend its functionality much like email protocols were built to extend the functionality of more basic Internet protocols. Examples of add-on protocols that have already been proposed or created include digital notary functionality to prove document ownership and authenticity, and a protocol for encrypted communications.

Operating a business is no easy task. Competition is intense and businesses must adapt to new laws and new cultures as globalization spurs them to expand domestically and internationally. In addition, companies must be able to raise money when necessary in a timely and efficient manner, even when sources of finance may be tight. Meanwhile, a barrage of new laws and regulations requires executives to reassess both enterprise and personal risks associated with many of their decisions and activities. In this environment, businesses value law firms that offer broad investor and regulator contacts, extensive corporate finance experience and a thorough understanding of the law.