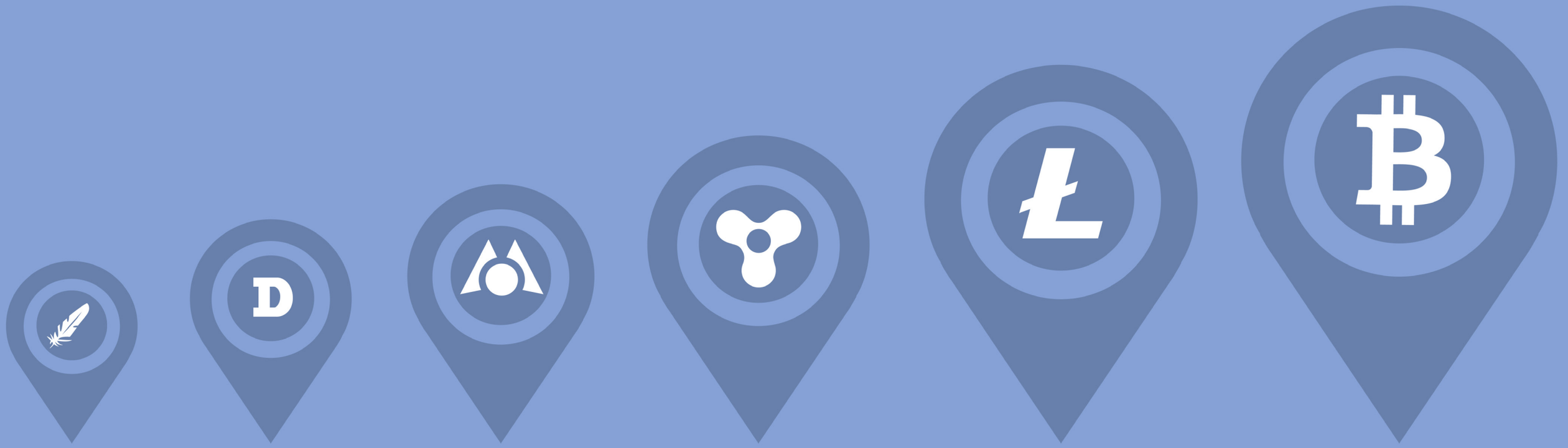
Rise of the Cryptocurrency



The Most Powerful Cryptocurrency

Bitcoin is a decentralized, peer-to-peer digital currency that can be transferred from person to person over the Internet without an intermediary institution such as a bank or currency broker. Bitcoin requires little or no fees and there is no risk of your account being seized or frozen. Originally introduced as open source software code in 2009 by Satoshi Nakamoto, Bitcoin has quickly grown to become the most popular cryptocurrency in the world.

As with most cryptocurrencies, only a certain amount of bitcoins will be produced determined by a pre-established value that is made known to the public. One of Nakamoto's goals in developing Bitcoin was to create an economy that would render fractional reserve banking computationally unfeasible. Many view this decentralized digital currency as a positive alternative to the restrictive and often dubious activities of our current banking systems.

How it Works

Bitcoins are stored in a digital wallet installed on your computer or mobile device. More precisely, the digital wallet contains your Bitcoin credentials. Your Bitcoin wallet generates unique addresses that you use for sending and receiving bitcoins to and from other parties. A Bitcoin address should be used only once, but your Bitcoin wallet can generate new addresses for each transaction.

The Bitcoin network is composed of thousands of miners. For the most part, miners are powerful computing clusters or servers that execute extremely demanding and complex calculations. These calculations are performed on blocks of transactions comprising all the Bitcoin transactions that were made in the last 10 minutes. One miner or one group of miners will find a mathematical solution to a block and be awarded 25 bitcoins.

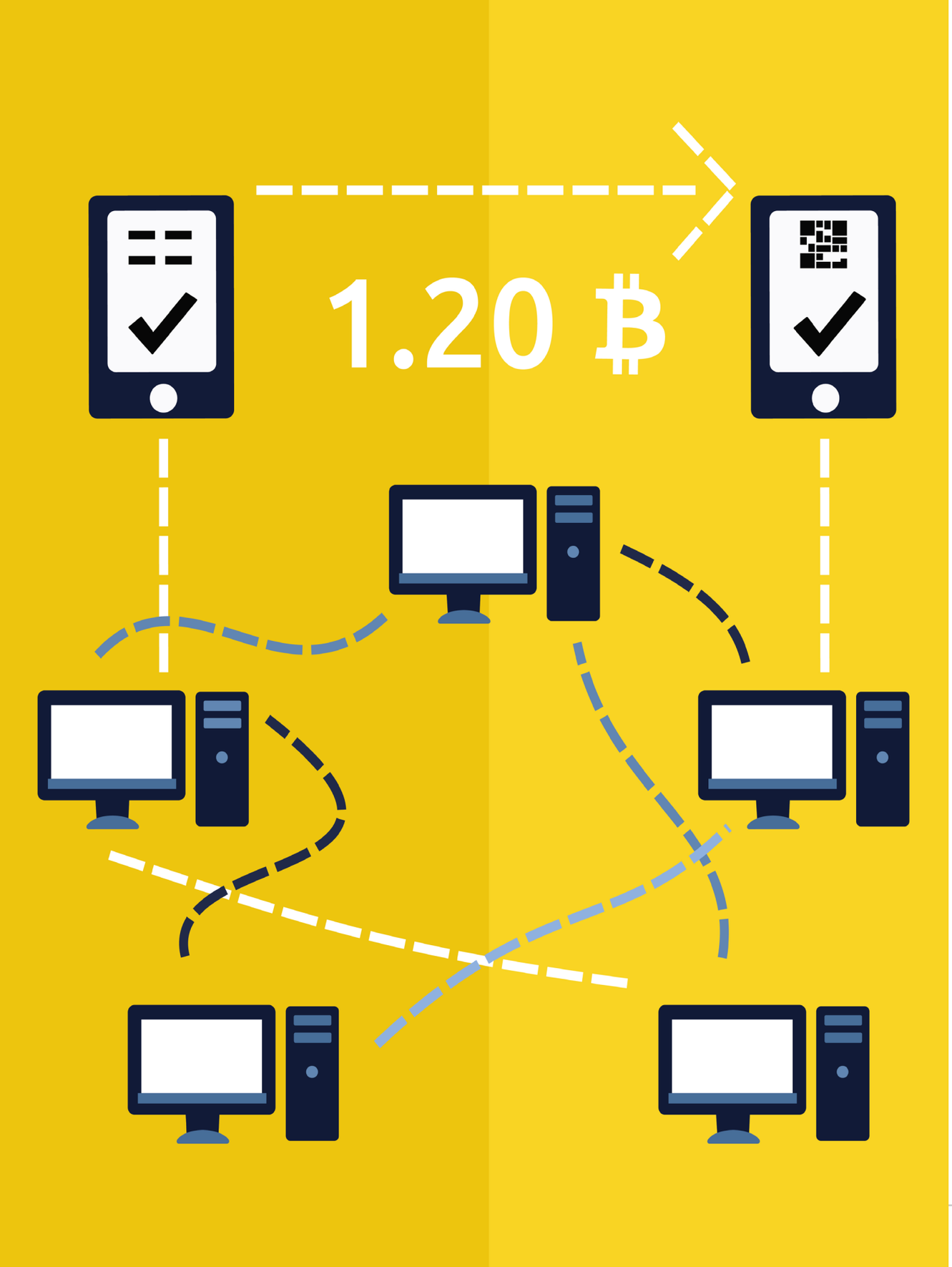
This is called the “coinbase” transaction, and it describes how new bitcoins are generated. All the transactions are kept in the block chain, which is a ledger showing every transaction ever done since the origin of the network, and every Bitcoin client has a copy of that block chain. The software that performs these calculations is open source and anyone can review the code.

Cryptography

Cryptography is the set of techniques and complex mathematics that makes it possible for the Bitcoin code to create mathematical proofs that deliver high levels of security and data integrity using public and private encryption keys. In short, a public key can decrypt data encrypted by a private key, and vice versa. This technique is referred to as asymmetric cryptography. Since the beginning of online commerce and banking, cryptography has played a vital role in maintaining the security and reliability of transactions. In the Bitcoin system, asymmetric cryptography makes it quasi-impossible for a malicious user to spend bitcoins from another user's wallet or to compromise the integrity of the block chain.

Transaction

A transaction is an exchange of Bitcoin amounts between Bitcoin wallets that is recorded in the block chain. Bitcoin addresses are made from a public key, and the Bitcoin wallets contain a private key for each of those public keys. This key is used to digitally sign all transactions, which associates each transaction with the previous transaction that contained those same bitcoins. Private keys can be stored on a hard drive or in your Bitcoin wallet. If using an online wallet like Coinbase, private keys are stored on their servers. In order to protect your bitcoins, you should never reveal your wallet private key because it allows anyone to spend bitcoins from its associated Bitcoin wallet.



The cryptographic signature functions as a safeguard by preventing the transaction from being modified or tampered with once it has been released. Bitcoin transactions are then processed by the network within minutes, thanks to the process of mining.

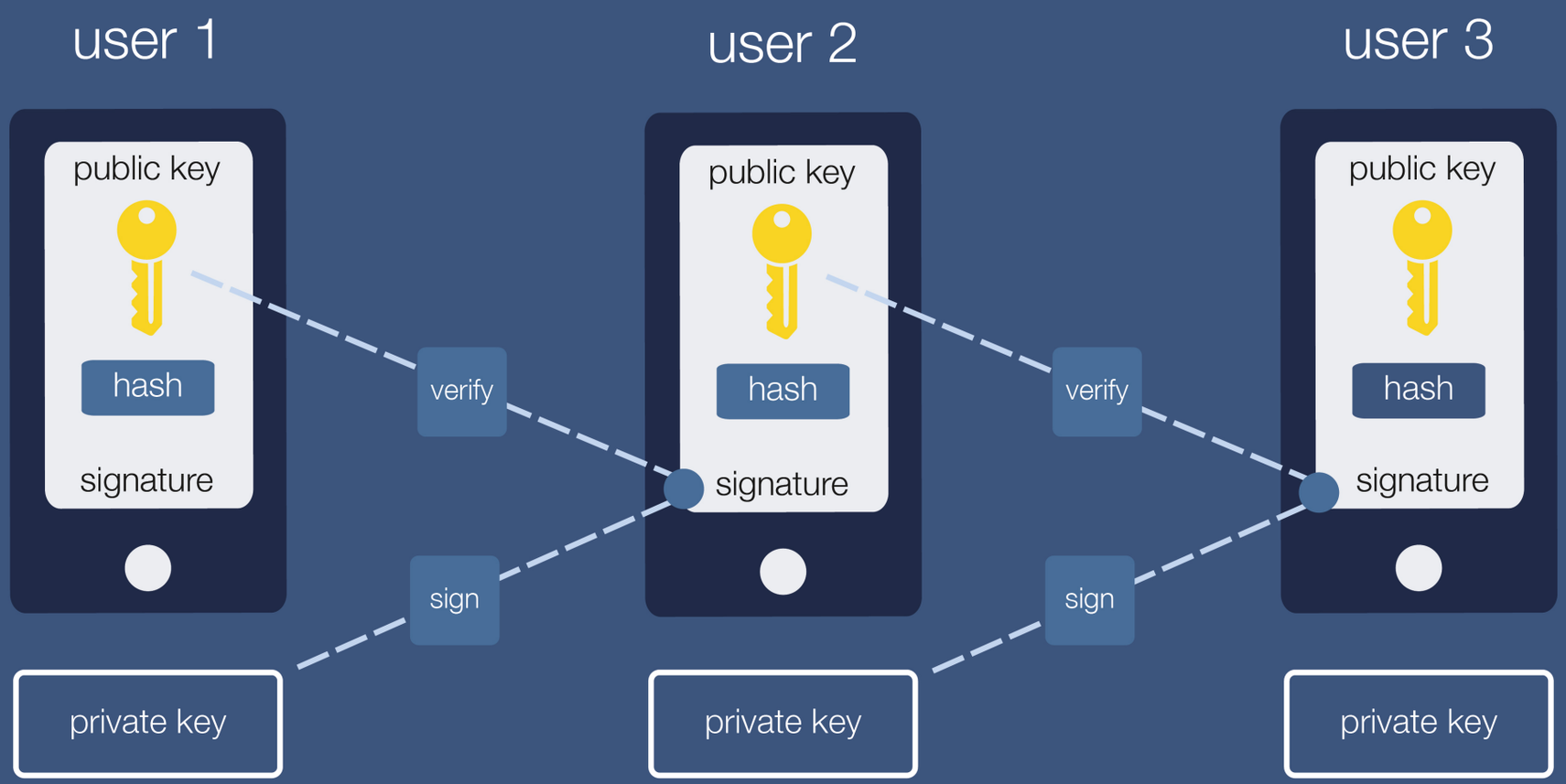
The Primary Elements of the Bitcoin System

A block is a record of transactions made from the past approximately 10 minutes and then appended to the block chain. The block is digitally linked to the previous block through mining and can be viewed by the public and anyone running a Bitcoin client.

Block Chain, the Bitcoin Ledger

As mentioned previously, the transparent nature of the Bitcoin economy dictates that all transactions are viewable on a shared public ledger called the block chain. Whenever someone initiates a Bitcoin transaction, and the network deems the transaction to be valid, the system accepts this new transaction and creates a hash for it. A hash is essentially a mathematical abbreviation referencing the current transaction. These transactions are accumulated and linked to each other by inputs and outputs and then stored into blocks.

When the blocks are combined and linked together, a chain of



links is created that cannot be replaced without performing the previous mathematical problems again, and “convincing” the miners who validated the initial transaction that this repeat is actually valid. This is virtually impossible because transactions and blocks cannot be counterfeited. Bitcoin utilizes a consensus system to confirm pending transactions by inserting them in the current block.

This imposes a chronological order within the block chain, protecting the processing neutrality of the network and consequently permitting computers to “agree” on the validity of the system. Transactions must be structured within a block that adheres to rigorous cryptographic rules that in turn will be confirmed by the network. This system aims to prevent previous blocks from being modified because it would create a domino effect and render all of the subsequent blocks invalid.

Mining

According to bitcoin.org, “Bitcoin mining is the process of making computer hardware do mathematical calculations for the Bitcoin network to confirm transactions and increase security. As a reward for their services, Bitcoin miners can collect transaction fees for the transactions they confirm, along with newly created bitcoins.”

Miners compete for the privilege of crunching the numbers of a Bitcoin block of transactions. In return, the mining entity or “pool” is awarded a certain amount of bitcoins depending on how much of the calculations they perform. It is important to note that not all Bitcoin users are involved with Bitcoin mining. In fact, the computing power required to compete for the increasing amount of Bitcoin transactions involves staggering processing resources. According to Forbes online, as of 2013, the Bitcoin global network was already operating at speeds over 256 times faster than the world’s top 500 supercomputers.

Mining also generates a competitive lottery system that prevents any individual from adding additional blocks consecutively within the block chain. The result is that no single party can regulate the elements contained in the block chain or replace sections of the block chain to roll back their own expenditures.

Confirmation

Confirmation is a vital component of the Bitcoin system and renders the reversal of a transaction highly improbable. Transactions are confirmed when included in a block and each successive block increases the confirmation count by one. Bitcoin employs multiple confirmations for increased security. In general a single confirmation is considered adequate for low value transactions. Experts suggest a minimum of six confirmations for larger amounts. The more confirmations a transaction receives, the greater the chance that a dubious party cannot reverse it.

Double Spend

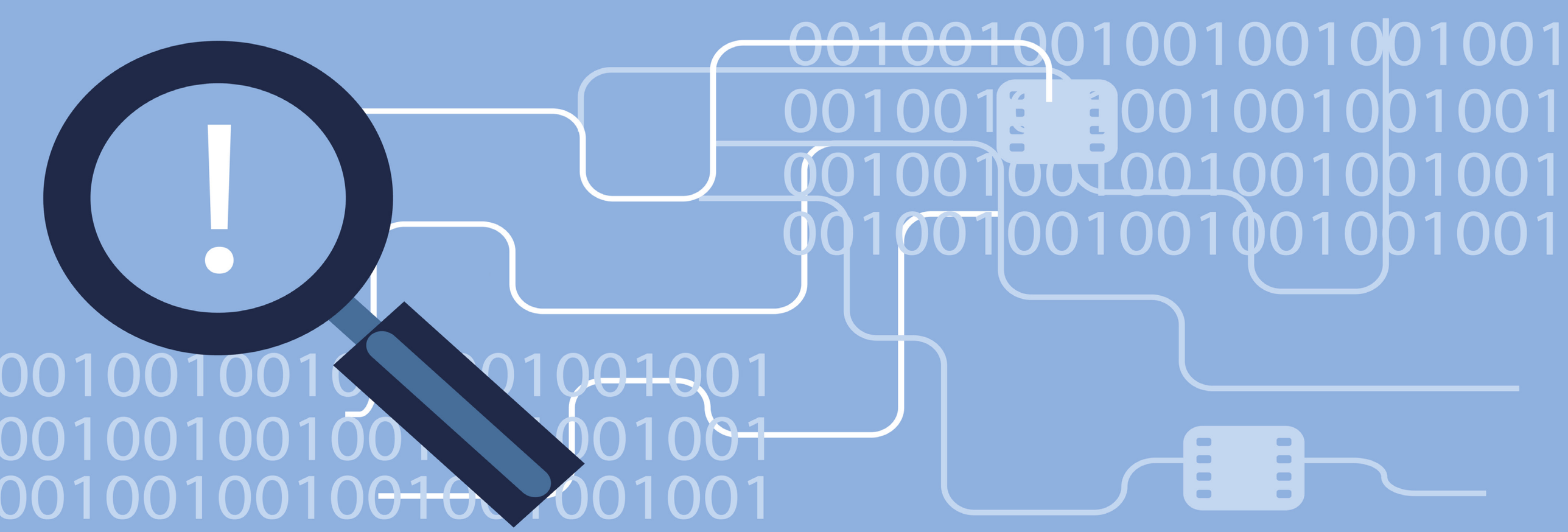
Double spend refers to when a fraudulent party tries to spend a transaction input that has already been spent. Transactions are structured in a linear way, with each transaction's output eventually becoming another transaction's input, making it impossible to double spend outputs. In fact, Bitcoin was originally created to solve the double spend problem.

The Vulnerabilities of Bitcoin

The greatest threat to Bitcoin and other cryptocurrencies lies in certain vulnerabilities derived from hackers or malware programs attempting to compromise the exchange system and subvert the security systems in place. An example of this occurred in February 2014, when Mt. Gox, one of the largest virtual currency exchanges in the world, collapsed after hackers gained access to their system and stole over $450 million in bitcoins. It is important to note, however, that the issue was with the lack of adequate security on Mt. Gox servers, and not with Bitcoin itself.

Malware and Unauthorized Mining

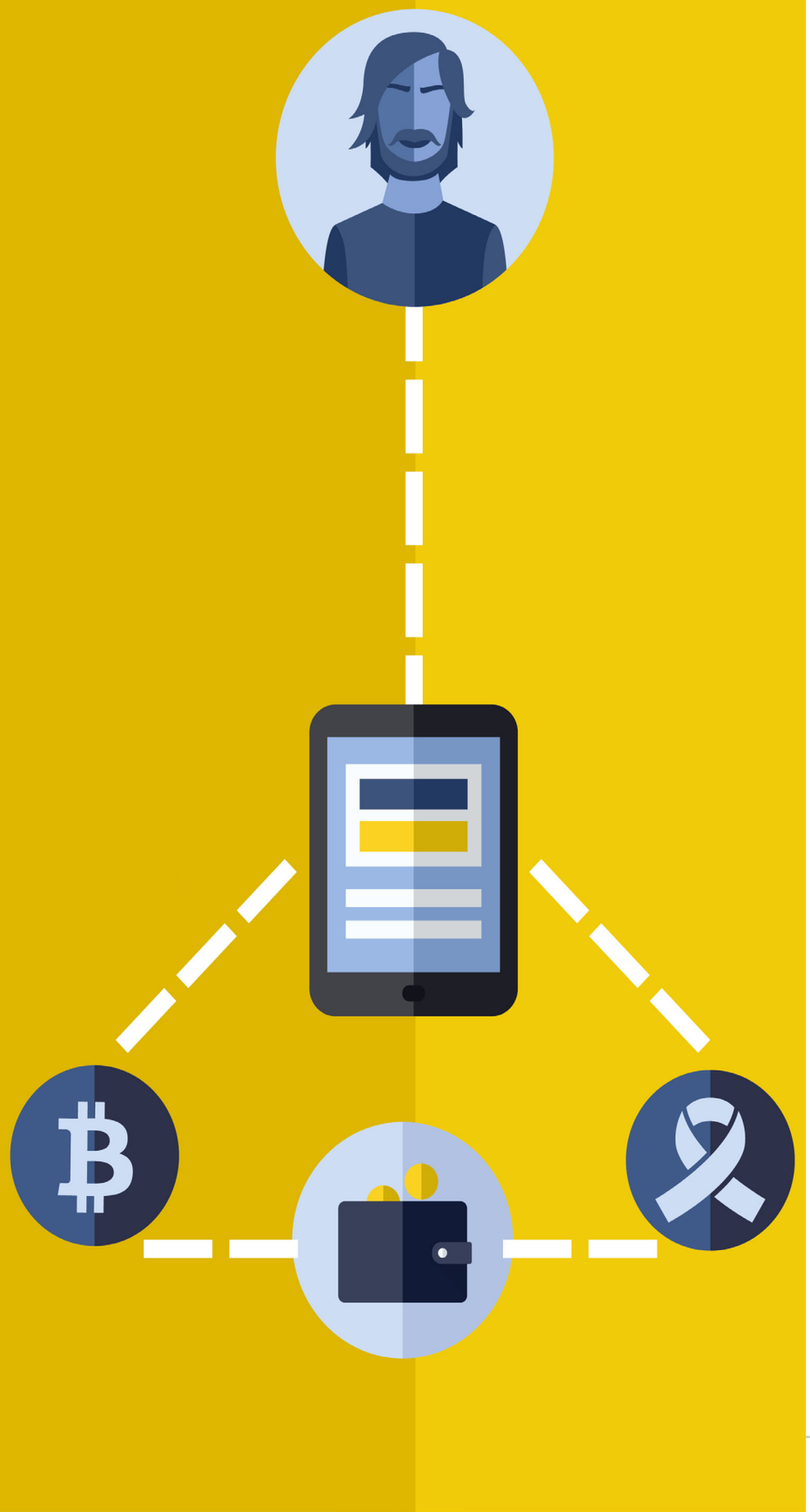
Bitcoin-related malware is essentially software that steals bitcoins from users through an assortment of techniques—software that uses the power of infected computers to mine bitcoins. As of February 2014, approximately 150 types of Bitcoin malware have been identified. Anti-virus companies are scrambling to address the issue and many lack the functionality to detect Bitcoin-related threats.



The Challenge of Fraud Detection within the Bitcoin Economy

Bitcoin is inherently secure and because each transaction is displayed publicly in the block chain ledger, it is not the channel of choice for fraudsters and money launderers. The majority of fraud involving Bitcoin derives from people gaining access to private keys and wallets and conducting unauthorized transactions. Concurrent with the rise of cryptocurrencies though, rule engines, neural networks, genetic algorithms, random forests, hidden Markov models, clustering, support vector machines, outlier detection, and other methods were developed to raise red flags for fraud.

It's essential that many different techniques be utilized, as computing power is rapidly increasing—and, as stated before, the Bitcoin network is hundreds of times faster than 500 of the fastest supercomputers on the planet. Regarding fraud, it is most likely that a fraudster could pose as a Bitcoin exchange, Bitcoin intermediary, or experienced trader and convince the user to send money in exchange for bitcoins that the user will never see. However, there are possible scenarios involving the use of Bitcoin for money laundering or other unlawful transactions.



A few are listed below:

1) Consider that Mr. Chinaski received 10 bitcoins on a Bitcoin address that he publicly advertises for donations of some sort. This could be a fraudulent or legitimate charity. An investigator (or anyone) examining the block chain can easily enter that address in a search engine and find Mr. Chinaski. Now if Mr. Chinaski wants to use 12 bitcoins to buy drugs and then the drug dealer is caught, his Bitcoin's block chain will point directly back to Mr. Chinaski. This scenario can be avoided by increasing the number of Bitcoin transactions, making it more difficult to trace.

2) Mr. Chinaski creates multiple Bitcoin accounts on various Bitcoin exchanges. He can pass the 12 bitcoins he received through those multiple accounts, hold them for short time period, and then send them to a drug dealer. These transactions, however, can still be traced back to Mr. Chinaski. But if Mr. Chinaski uses those multiple accounts for various legitimate transactions, the trail would not lead directly back to Mr. Chinaski.

3) Let's suppose that Mr. Chinaski placed his 12 bitcoins in an account created just for him by a Bitcoin laundering service. And person A and person B do the same thing. The service could send Mr. Chinaski's bitcoins to person A and person B's bitcoins to Mr. Chinaski. Then Mr. Chinaski spends these bitcoins on drugs. Upon examination, the transaction trail is traced and it looks identical to the legitimate example above, except the trail leads straight to person A, instead of to Mr. Chinaski.

In theory, it will always be possible to trace a Bitcoin transaction back to its initial wallet, as all block chains of Bitcoin transactions are public record. A goal of the fraudster would be to use Bitcoin to create multiple layers of plausible deniability.