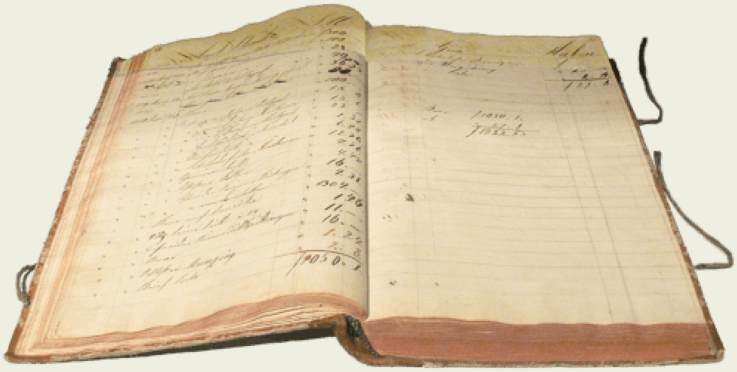
Blockchains and Bitcoins

People have been making records as long as they have been writing. Money serves as a unit of account, which makes the consistent tracking of finances and business interests possible. The assets, liabilities, income, expenses, and equity of businesses and banks have been tracked in books and files known as ledgers for centuries.

The word **ledger** comes from the same ancient roots as the word lay, as in something you would lay down or put and keep in place. When books were scarce, it was common to have a copy of important books (like scriptures) kept in one place so they could be located and accessed easily. The important accounting books of a business inherited this word.



An old ledger book

As information technology improved, the original books were replaced with computer files containing the same kinds of information.

A digital ledger file

Even with the move to digital ledgers, it was important to only have one official version so that everything could be controlled properly and tracked accurately.

Trust Problems

What happens if someone you don’t trust has access to your important records? They could destroy or change or replace them. They could take the documents and make you pay to get them back.

Having only one copy of a record may seem like a good way to keep things private, but it also means that there is only one copy that a bad actor would need to get access to. It also requires a lot of trust in the few people that control authorized access to it. To avoid problems like these, you could choose a system that is decentralized rather than centralized.

Centralized and Decentralized Systems

Centralized systems rely on a model of central decision making and authority. Centralized systems are susceptible to hostile takeover, catastrophic failure, and systemic collapse.

Decentralized systems distribute responsibility and authority away from a single source or location. Decentralized systems cannot be controlled or shut down as easily. They are less likely to fail since each part of the system can operate independent of a central authority. If any part of the system fails or becomes unavailable, the other parts continue operating anyway.

In computer terms, this decentralization is known as peer-to-peer technology. In a centralized model, there are server systems that control access and client systems that access server system resources based on rules set and enforced by the server systems. In a peer-to-peer model, the relationship between machines is one of equals that share responsibility and authority. Each peer in this model has control only over its own resources and operates with other peers based on rules enforced by the peers themselves. Any peer not obeying the rules is ignored.

But decentralizing a record keeping system only solves trust problems related to central control.

Cryptography and Information Security

Another trust problem arises when storing or transmitting sensitive information: security. Information cannot be stored in containers that are not leaky (including and perhaps especially people’s minds).

People have used cryptography (from the Greek words *kryptos* = hidden and *graphein* = to write) to protect private information for a very long time. If a message is encrypted, it can only be unencrypted and understood properly using a key.

Simple keys like alphabet sliders simply substitute one character for another. Such systems are considered symmetrical because the same key can be used to encrypt and decrypt the information.

A simple alphabet ring decoder

Modern cryptography methods make use of computer technology to generate very complex keys to encrypt and decrypt information. Not long after computer systems were interconnected, a new type of asymmetrical encryption came about that used two keys for encoding and decoding information: a public key (which can be shared openly with others) and a private key (which may never be known to by any except the owner). This new public-key cryptography allowed messages to be encrypted by anyone, but only decrypted by the intended recipient.

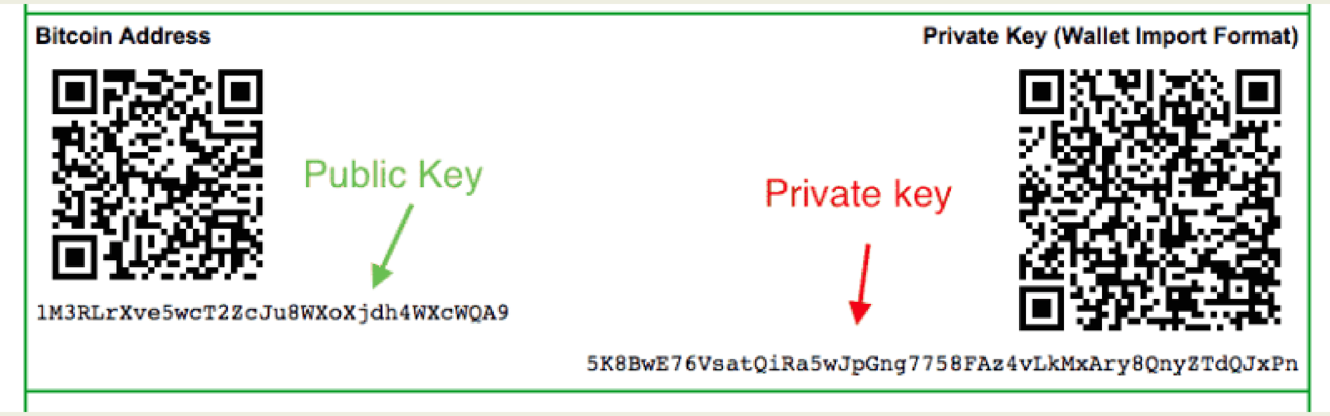
What Blockchains Are and What They Do

Blockchains are distributed, encrypted ledgers/databases. A participating computer system with a copy of the ledger is known as a node, and such nodes form a peer-to-peer decentralized network. Blockchain nodes share ledger changes in timestamped batches called “blocks”, which are “chained” together to show a complete history of changes. Each block of changes is validated by a majority of nodes in a network. Blockchains can be public or private.

The Ins and Outs of Bitcoin

Bitcoin functions as a public blockchain network. It was intended to solve trust problems in central banking schemes. The original author of the system published a famous whitepaper entitled Bitcoin: A Peer-to-Peer Electronic Cash System under the pseudonym Satoshi Nakamoto.

The basic idea is that anyone with your public key (you can think of this as your account number) can re-assign control of bitcoin records they control to you, but only you can re-assign control of bitcoin records you control to others using your private key (you can think of this as your password).


Bitcoin Address
Private Key (Wallet Import Format)
Public Key
Private key
1M3RLrXve5wcT2ZcJu8WXoXjdh4WXcWQA9
5K8BwE76VsatQiRa5wJpGng7758FAz4vLkMxAry8QnyZTdQJxPn

An example of a bitcoin wallet key pair. The QR codes can be scanned to avoid entering keys manually.

To participate in the bitcoin network, you will need to use a software application called a “wallet” that uses public/private key pairs to access the bitcoin network. These wallet systems can be run on internet servers, desktop computers, or mobile devices. Since a wallet contains a copy of your private key, anyone with access to it can make changes to the records assigned to your wallet. For this reason, some people store their keys on a device like a USB drive (called a hardware wallet) or even print them out on paper (called a paper wallet) and put them in a secure location. In any case, if you lose your keys or the device they are stored on fails or is destroyed, access to and control of the bitcoin records they are associated with is lost forever and cannot be retrieved. For this reason, bitcoin participants are encouraged to make backup copies of their keys.

In order to add a new block of transactions to the bitcoin blockchain, the system requires something called “Proof of Work” (PoW). This work is done by “miners” whose machines are used to generate keys randomly until a solution to a randomly generated encryption problem is solved. Miners who solve such cryptographic hashing problems are awarded control of a small amount of bitcoin (paid as fees by users who need transactions verified), which encourages network participation in verification of transactions.

Bitcoin is not property. There are no physical bitcoins to be possessed. Bitcoin is not real money, and neither is any other ledger entry, encrypted and distributed or otherwise. Bitcoin is a speculative investment in a digital record keeping system.

Bitcoin Strengths

1. Integrity: Proven public-key cryptography technology and PoW/network verification are required to modify the ledger. There is also no central bank to just print more bitcoin records. The original bitcoin system is set to never have more than 21 million bitcoins on record (even though portions of full bitcoins can be controlled and exchanged).
2. Authenticity: Digital signatures created using public/private key pairs cannot be forged, and the blockchain confirmation process precludes non-repudiation and double

spending.

3. Control: The bitcoin blockchain itself has never been shown to be vulnerable to takeover. However, there are caveats here. First, many bitcoin participants use web-based/cloud wallets on third-party server systems run by custodians/exchanges like Coinbase, who they trust with their private keys. Custodians can violate that trust by using the private keys to reassign bitcoins to other wallets. Custodian/exchange systems can also be breached or coerced by governments to disclose private keys. Resulting losses cannot be reversed. Second, it is conceivable that the whole bitcoin network itself could be compromised by a combination of things like large-scale denial of service, surveillance, and collusion between large hardware manufacturers and influential bitcoin network participants. A well-planned and orchestrated corresponding surge in rogue nodes could outvote disabled or compromised nodes and exploit potential glitches in software to approve transaction blocks.

Bitcoin Weaknesses

1. Confidentiality: It is trivial to identify the amount of bitcoin controlled by any given wallet at any given time, and tracing wallets (that get used for much at all for purchasing anything traceable) can be done rather easily (and permanently!) using big data and related analysis techniques, not to mention government oversight of exchanges and businesses and Know Your Customer (KYC) compliance between various financial institutions.
2. Availability: The distributed nature of the bitcoin network makes it rather resilient to hostile takeover, but its digital nature also limits its usefulness to electrical power and internet access being available. There is no built-in physical cash alternative like coins or paper to be traded when electricity and/or the network are unavailable. Even when the network is available, it has been subject to significant delays and scaling issues (some additional technologies like the lightning network have attempted to address these issues). Also, due to confidentiality weaknesses, some bitcoins could become largely nonfungible if governments obligate businesses (including those that manage bitcoin accounts, like Coinbase) to refuse transactions involving bitcoins that have been deemed related to illegal activity and/or block/suspend/close accounts they don’t like for any reason.
3. Utility: If I lose my key, all my bitcoins are permanently gone. Transaction fees are also rather high (some are developing additional technologies in an attempt to alleviate this). The process of buying bitcoin with fiat currency is also generally quite a hassle (not to mention highly regulated, see Confidentiality issues). It also has no relationship to ownership of objects in the physical world and faces innovative competition from lots of “altcoin” technologies and code fork spinoffs (like the ring signatures and stealth addresses of Monero, the flexibility and smart contracts of Ethereum, or the technical/scaling solutions of Bcash), so its value is subject to high volatility and risk.

Bitcoin transactions involving fraud cannot be reversed like they often can with credit card companies and banks.

The Future of Blockchain and Bitcoin

Blockchains have proven to be useful in various applications and are surely here to stay. Bitcoin is an innovative attempt at eliminating trust issues in money and banking, but it just replaces trust in central authority with trust in a community of users to remain loyal to it over various alternatives and ultimately with trust (or perhaps, hope) in the ability of technology to obviate trust itself.

Recordkeeping and information security technology solutions offer good solutions to records and security problems, but they do not address fundamental issues of interpersonal trust and cooperation, societal governance, property management, responsibility, and reputation.

I think that bitcoin introduces at least as many problems as it solves. Utility issues alone keep it far from use in everyday public transactions. It presents even savvy users with a rather insane and high-risk complexity spiral. It could continue to increase in value over time as people seek alternatives to government-manipulated financial systems. It could also be replaced rather quickly by other traditional, digital, or hybrid alternatives and its value could evaporate.

Some see bitcoin and other cryptocurrencies as a fool-proof way to get rich quick or secure their financial future against uncertainty. My advice in preparing for the future is not to hope in unusual virtual investments (whether bitcoin or other), but to become as productive, disciplined, and wise as you can, as well as to build a good reputation with a community of trustworthy people. If you are lazy, unorganized, foolish, and isolated, whatever resources you have access to won’t serve you very well.