**Bitcoin Cheat Sheet**

[Jean-Marie Choffray](https://www.amazon.com/kindle-dbs/entity/author/B00DNUGN64?_encoding=UTF8&node=283155&offset=0&pageSize=12&searchAlias=stripbooks&sort=author-sidecar-rank&page=1&langFilter=default#formatSelectorHeader)\*

Liège, Oct. 31, 2023

My *one-page summary* of [Satoshi Nakamoto’s seminal paper](https://bitcoin.org/bitcoin.pdf), published on October 31, 2008. Fifteen years later, the technology he developed and programmed has aged remarkably well. Bitcoin’s market cap exceeds $ 650 Billion, substantially more than Belgium’s GDP (~$580 B) and five times the market capitalization of International Business Machines Corporation (IBM). Millions of people use the *Bitcoin Network* to save and transfer economic value without a *trusted third party*. El Salvador has made it legal tender in the country. Several ETFs are available in Europe and Canada and are expected in the United States. Excluding possible “Black Swans”, the *Bitcoin Network* could become the backbone of the *Internet of Money*.

\* Emeritus Professor of Computer Science, University of Liege School of Management.

PhD-77, Management Science, Massachusetts Institute of Technology.

*“Bitcoin is hope […] It’s a bank in cyberspace, run by incorruptible software, offering a global, affordable, simple, & secure savings account to billions of people that don't have the option or desire to run their own hedge fund.”*

[Micro*Strategy*](https://www.hope.com/?_gl=1*ttnp1b*_ga*MTY0MTQzNDQ1NC4xNjY2MDg0NDAy*_ga_0C9LVNZBZY*MTY5ODc4MDIwOC4zLjAuMTY5ODc4MDIwOC4wLjAuMA..)

**Bitcoin Cheat Sheet**

**The problem…**

How to make *non-reversible payments* for *non-reversible services* without a *trusted third party*?

**The solution…**

A *peer-to-peer network* using *proof-of-work* to record a *history of encrypted transactions*.

**The technology…**

A payment system based on *cryptographic proof* instead of trust. A *distributed timestamp server* to generate proof of the chronological order of transactions.

A *bitcoin* is a chain of *digital signatures*. Each owner transfers the coin to the next by *digitally signing* (with a *private key*) a hash of the previous transaction and the *public key* of the next owner and adding these to the end of the coin.

Transactions are *publicly announced*. Participants agree on a *single history* of the order in which they were received.

A *distributed timestamp server* includes the previous *timestamp* in its hash, forming a chain, with each additional *timestamp* reinforcing the ones before it. The *proof-of-work* involves scanning for a value that when hashed, such as with [SHA-256](https://csrc.nist.gov/glossary/term/sha_256), the hash begins with a number of zero bits (the *difficulty*).

*Proof-of-work* is essentially one-CPU-one-vote. The majority decision is represented by the *longest chain* which has the greatest proof-of-work effort invested in it.

The steps to run the network are as follows:

1) New transactions are broadcast to all *nodes*.

2) Each node collects new transactions into a *block*.

3) Each node works on finding a difficult *proof-of-work* for its block.

4) When a node finds a proof-of-work, it *broadcasts the block* to all nodes.

5) Nodes accept the block only *if all transactions in it are valid* and not already spent.

6) Nodes express their *acceptance of the block* by working on creating the next block in the chain, using the hash of the *accepted block* as the previous hash.

*Nodes* always consider the *longest chain* to be correct and will keep working on extending it.

By convention, the *first transaction*in a *block* is a special transaction that starts a *new coin* for the *creator of the block* (i.e. the *miner*) until the limit (21 million coins) is reached in 2140.

A new *key pair* should be used for each transaction to avoid being linked to an owner.

Source: [Satoshi Nakamoto: Bitcoin, a peer-to-peer electronic cash system](https://bitcoin.org/bitcoin.pdf).