



ROBERT PRECHTER

# The Elliott Wave THEORIST

A publication of Elliott Wave International

[www.elliottwave.com](http://www.elliottwave.com)

[customercare@elliottwave.com](mailto:customercare@elliottwave.com)

770-536-0309 • 800-336-1618

September 2010 issue

© September 17, 2010

## Bitcoin Electronic Currency: The Future of Money

by Elliott A. Prechter

### What is Bitcoin?

Cryptography expert Satoshi Nakamoto<sup>[1]</sup> has created the first completely decentralized, anonymous, electronic currency, called Bitcoin. Bitcoins are divisible digital tokens that can be exchanged across the internet or stored on disk. Bitcoin differs greatly from traditional government issued fiat currency and regulated banking in several important aspects:

- **Bitcoins have no central issuer**, whereas fiat currency is issued at will by a central bank. Currently, Bitcoins are slowly being issued in a decentralized manner, but eventually new issuance will forever halt.
- **Bitcoin transactions are private and anonymous**, whereas current law allows only licensed financial institutions to conduct wire transactions within the banking system. With Bitcoin, no third party can spy on overall transactions.
- **Bitcoin ownership is safe**, so confiscation is nearly impossible.

Bitcoin also differs from gold in important ways. Gold has the advantage of thousands of years of historical precedent as money, as well as having physical form. Unlike any “soft” currency, gold lasts forever. The only disadvantage of gold is that ownership cannot be transferred electronically (or with paper certificates) without requiring a central repository. The unfortunate fate of both E-Gold and the Liberty Dollar is evidence of the fact that any centralization of a currency system is vulnerable to outside monitoring, tampering or outright confiscation. With Bitcoin “there is no central database for police to raid and no way for your Bitcoins to be stolen”<sup>[2]</sup> at the institutional level.

### How do I use Bitcoin?

To use Bitcoin, the place to start is [bitcoin.org](http://bitcoin.org). There’s no registration or payment required to start – just download the software. Alternatively, you can create and use a free Bitcoin web account at [mybitcoin.com](http://mybitcoin.com). Either way, you’ll soon be ready to exchange Bitcoins with others around the world. If you want a few coins to start with, go to [freebitcoins.appspot.com](http://freebitcoins.appspot.com) for some initial bit-capital.

The quantity of services using Bitcoin is small but steadily growing. Notable websites thus far are [bitcoinmarket.com](http://bitcoinmarket.com) and [mtgox.com](http://mtgox.com), which allow exchange between various fiat currencies and Bitcoins, and [biddingpond.com](http://biddingpond.com), which is the first Bitcoin-based auction site. [Bitcoinwatch.com](http://Bitcoinwatch.com) provides an overview of the entire Bitcoin economy, which is valued at just over a quarter of a million US dollars as of August 2010. You can visit [bitcoin.org/trade](http://bitcoin.org/trade) to see a list of services that accept Bitcoin.

### How does Bitcoin work?

Bitcoin users have balances stored in their accounts. Balances can be changed by sending and receiving Bitcoins in transactions. A transaction involves Bitcoins changing ownership from one account to another; it specifies the payer account, the amount, and the receiver account. When you want to make a transaction, you announce the details of it publicly.

Each user has the ability to render a *digital signature*, which operates just like a normal hand-written signature. Before announcing a transaction, the payer *signs* the transaction first. In this way, everyone can take a look at any publicly announced transaction and know that the paying account owner truly agreed to that transaction.

When a transaction is announced, anyone can audit the transaction to ensure that it is valid. This is possible because everyone knows the balance of each account. Despite this knowledge, nearly

complete privacy is achieved because account ownership is not public knowledge, and each user can own an unlimited number of accounts. One could even specify a new account to receive each new transaction. For convenience when using Bitcoin, your own accounts appear to you to be integrated even though others see them as separate accounts.

### **Establishing Consensus**

There needs to be a consensus regarding the validity of transactions. If there weren't, things could become confusing if many auditors disagreed. To achieve consensus, transactions are grouped into "blocks", which are strung together in what is called the *block chain*. Due to the nature of the chain, it takes a lot of computational resources to add a block to the chain. Once a chain is constructed, however, it is easy to share it publicly and widely, and it is easy to verify that it was constructed properly and that the transactions are valid. By helping to build the chain, users earn small transaction fees.

By choosing only to accept the longest known chain as the consensus, users do not have to trust any particular individual or organization. They need only trust that the total honest computing power is greater than the power of any villain.

### **Protection from Vandalism**

Users must keep secret the information that allows them to render digital signatures for their accounts; otherwise a thief could announce transactions that would remove money from their accounts. This information is kept inside of each user's *wallet* file. The FAQ at bitcoin.org explains how to encrypt and back up your wallet. Don't forget: You can have an unlimited number of accounts and therefore an unlimited number of wallets. So, even a successful theft need not be devastating.

### **Initial Issuance**

To bring Bitcoins into circulation, those who construct the block chain are rewarded with newly issued coins in addition to any transaction fees. The amount of new coins awarded will decrease over time, eventually reaching zero when there is a total of 21 million Bitcoins.

### **Conclusion**

Bitcoins have the necessary features of money: medium of exchange (anonymous and across great distances), unit of account (private), divisibility (up to eight decimal places), scarcity (21 million), portability (transferred electronically), and store of value (current exchange rates – as of August 2010 – show 1 Bitcoin, or BTC, equal to 0.065 USD).

While Bitcoin appears to have enormous potential as currency, it will have to stand the test of time and the marketplace. Even if Bitcoins do not catch on in the mainstream, the structure has the virtue of providing an example of a decentralized monetary alternative. As distrust in central banks continues to increase as the financial crisis drags on, the idea of private currencies should grow in popularity.

Finally, for those who say that the Bitcoin's physical non-existence makes it suspect, consider that US dollars are nothing at all, and yet people toil to gain and keep as many of them as they can. The dollar is not valuable of itself; it represents value. So it is with Bitcoins.

### **References**

- <sup>1</sup> Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", [www.bitcoin.org](http://www.bitcoin.org), 2009
- <sup>2</sup> Dr. Phil Maymin, "Is It Time For Digital-Only Dollars?", *Hartford Advocate*, [www.hartfordadvocate.com/commentary/is-it-time-for-digital-only-dollars-2](http://www.hartfordadvocate.com/commentary/is-it-time-for-digital-only-dollars-2), 2010



**THE ELLIOTT WAVE THEORIST** is published by Elliott Wave International, Inc. Mailing address: P.O. Box 1618, Gainesville, Georgia, 30503, U.S.A. Phone: 770-536-0309. All contents copyright ©2010/2024 Elliott Wave International, Inc. Reproduction, retransmission or redistribution in any form is illegal and strictly forbidden, as is continuous and regular dissemination of specific forecasts or strategies. Otherwise, feel free to quote, cite or review if full credit is given. Typos and other such errors are corrected in the online version, which is the official final version of each issue.

The Elliott Wave Principle is a detailed description of how financial markets behave. The description reveals that mass psychology swings from pessimism to optimism and back in a natural sequence, creating specific Elliott wave patterns in price movements. Each pattern has implications regarding the position of the market within its overall progression, past, present and future. The purpose of Elliott Wave International's market-oriented publications is to outline the progress of markets in terms of the Wave Principle and to educate interested parties in the successful application of the Wave Principle. While a course of conduct regarding investments can be formulated from such application of the Wave Principle, at no time will Elliott Wave International make specific recommendations for any specific person, and at no time may a reader, caller or viewer be justified in inferring that any such advice is intended. Investing carries risk of losses, and trading futures or options is especially risky because these instruments are highly leveraged, and traders can lose more than their initial margin funds. Information provided by Elliott Wave International is expressed in good faith, but it is not guaranteed. The market service that never makes mistakes does not exist. Long-term success trading or investing in the markets demands recognition of the fact that error and uncertainty are part of any effort to assess future probabilities. Please ask your broker or your advisor to explain all risks to you before making any trading and investing decisions.