A Bitcoin Primer

by CoinLab.com
Authors: Chris Koss, Mike Koss
January 1, 2012

What if you could store and transfer money safely, securely, cheaply and quickly anywhere in the world yourself, without relying on anyone else?

Bitcoin is a new technology that has the potential of supplanting many of our contemporary banking and money transfer services (at least in the online economy).

What is Bitcoin?

The term ***Bitcoin*** refers to both the digital unit of stored value and the peer-to-peer network of computers transmitting and validating transactions of these units. The project was publicly launched in January 2009, by a mysterious inventor using the pseudonym "Satoshi Nakamoto," whose identity is still a mystery. For the first couple of years, it was mostly just a novelty for computer geeks, hackers, and idealistic anarchists.

In April 2011, Forbes Magazine's Andy Greenberg wrote an article describing the qualities of Bitcoin: it cannot be forged or double-spent, controlled or inflated by any government, it is not impeded by international boundaries, has a geek-friendly economy of $30,000 per day, and some digital drug-dealers have started accepting it.

The price of a Bitcoin surged from less than a dollar to over $30 as a new demographic became interested: speculators. Geeks who had casually collected Bitcoin as a curiosity in 2009 found themselves sitting on tens, or even hundreds, of thousands of dollars. Over the next several months, Bitcoin prices were extremely volatile, dropping suddenly after each of a half dozen high profile incidents. Exchanges were hacked, Bitcoins were lost from carelessness, viruses popped up which stole any Bitcoin it could find, and some services closed without warning, disappearing with their customers' money.

As users learned better and safer practices for handling their Bitcoin, price volatility decreased, and the price of a Bitcoin has climbed to over $5. Many new services popped up including margin trading and short selling, digital downloads, banking and escrow services, a World-of-Warcraft-style MMORPG where you can gamble on everything with Bitcoin, web hosting, domain name registration, web design, and currency exchanges.

How does Bitcoin work?

A Bitcoin ***address*** is like a bank account, into which a user can receive, store, and send Bitcoins. Instead of being physically secured in a vault, Bitcoins are secured with public-key cryptography. Each address consists of a public key, which is published, and a private key, which you must keep secret. Anyone can send Bitcoins to any public key, but only the person with the private key can spend them. While addresses are public, nobody knows which addresses belong to which people; Bitcoin addresses are pseudonymous.

The Bitcoin protocol uses the strongest algorithms used by the NSA for encrypting Secret level documents. Anyone can generate as many addresses as they want for free. There are approximately as many possible Bitcoin addresses as there are atoms in the Earth, so generating duplicate addresses (and thus having access to someone else's funds) is practically impossible. Most Bitcoin users maintain a number of addresses, stored in a digital wallet.

When someone wants to send money to another user, they use software which creates a transaction containing the receiver's address

and an amount, and cryptographically signs it with their private key. This is published on a peer-to-peer network which validates it against the sender's public key, checks that the sending address's balance is sufficient, and propagates it to all the other nodes on the network.

A transaction does not become certified until it is included in a Block in the Bitcoin Block Chain.

Today, there are thousands of computers ***mining*** on the Bitcoin network. Each computer collects transactions broadcast by other nodes and tries to guess a number which solves an unpredictable cryptographic problem. A powerful home computer can try 100's of millions of numbers every second. The more computers that mine, the more difficult finding a solution becomes; the difficulty is self-adjusting so that, on average, a new block is found every 10 minutes. The lucky computer that is the first to find each block earns 50 Bitcoins for its owner.

As each Block is found, it is added to an ever-growing ***Block Chain*** (now standing at over 150,000 Blocks). Any transaction listed in the Block Chain is deemed to be valid, and eliminates the possibility that Bitcoins can be doubly-spent. Since the only way to re-write history in the Block Chain is to use more computing power than is available in the rest of the Bitcoin network, it is generally deemed too costly for any single party to cheat (the raw computing power of the Bitcoin network is 10 times that of the world's largest supercomputing center).

The Block Chain allows every Bitcoin client to examine the complete historical transaction record to determine the current account balance of every public address in the system.

Since newly created Bitcoins are constantly issued to miners, one would think that the currency is inherently inflationary (with an ever expanding money supply). While that is true in the short-term, the rate of issuing coins is scheduled to be cut in half every four years. So, while 2.6M Bitcoins are created each year (until January 2013), there will never be more that 21M total Bitcoins created. And since Bitcoins are almost infinitely divisible (up to 8 decimal places), there is no fear that we won't have enough Bitcoins to deal with an ever expanding economic base of Bitcoin-denominated transactions.

What are the benefits of Bitcoin?

Financial Self-Determinism and Control

The Bitcoin system is unique because it is the first digital store of value which can be safely and securely saved and transacted by individuals, without having to rely on a trusted third party. Once acquired and properly secured, Bitcoins can't be taken from their owner, by a thief, a bank, or a government. Neither can any entity freeze any account, nor prevent the owner from performing (essentially free) transactions on the Bitcoin network.

Irrevocable Transactions

Chargebacks are a big problem for many merchants. Virtually all current payment systems (credit card, inter-bank transfer, PayPal, etc.) allow the consumer to refute a transaction, and have their funds returned to them. Merchants have to follow an expensive dispute process to receive their money and sometimes pay fees of $10-$50 per chargeback. Merchants can be charged additional penalties up to $25,000 if they have an unusually high rate of chargebacks.

Online merchants have chosen to live with a certain amount of fraudulent chargebacks while expending company resources on various anti-fraud detection measures. In an effort to minimize chargebacks, merchants typically ask their customers to reveal personal information about themselves beyond what is necessary to deliver their product or service, leading to a loss of personal privacy for the consumer.

Bitcoin transactions reverse the role of trust by being inherently irrevocable. Once certified in the Block Chain, a transaction cannot be

(practically) reversed. It is incumbent on the consumer to trust each merchant they are ordering from. Since there are many ways to establish the credibility of a merchant (e.g., online ratings and word-of-mouth reputation), the Bitcoin trust system is a good match for Internet commerce (verifying the trustworthiness of merchants is much easier than verifying the trustworthiness of all consumers).

Because Bitcoin payments cannot be reversed (without the consent of the merchant), merchants can offer their products to a wider audience and require less personal information from their customers.

No Need for Middlemen

The policies of payment processors are sometimes not well aligned with those receiving money; e.g., people who take donations.

In December 2011, Regretsy, a humorous snarky craft blog, raised donations to buy Christmas presents for children in families undergoing financial hardship. After raising thousands of dollars, Regretsy's PayPal account was frozen.

When Regretsy's writer, Helen Killer, contacted PayPal support, she was told that her account was frozen because PayPal's "Donate" button can only be used by non-profit organizations. PayPal later admitted this is false: any company can use a "Donate" button. But PayPal support told her "it's not a worthy cause, it's charity," and that she would need to make a new website if she wanted to keep raising money, and that gifts couldn't be shipped to a different address from the customer who paid for them (which was odd during the holiday gift-giving season).

By publicizing her frustrating experience on her blog, she eventually got an apology from PayPal, and they unfroze her account. But there are many similar stories from other PayPal users who have had accounts closed or funds frozen. Without an audience to create a public outcry, many still haven't had their situations remedied.

Alex King is an open source software developer who stopped accepting donations when some of them started costing him money. In 2009, after an anonymous user donated $1 ($0.67 after PayPal's fees), they charged back their donation. PayPal then passed a $10 chargeback fee onto King, without any prior warning. He says, "I was never able to issue a refund to avoid this charge - the refund link was unavailable as the payment was listed as in dispute."

PayPal exposes sellers to the risks of frozen accounts and chargeback fees. The benefit of PayPal, giving customers the ability to get their money back if they don't receive what they paid for, does not apply in the donation scenario. Bitcoin transactions are irreversible and can be accepted without a middle man. As a result, Bitcoin donations can be accepted without worrying about these risks.

Low Cost Transactions

In addition to the unanticipated risks of using payment processors (e.g., frozen accounts and chargebacks), the known per-transaction costs of these services can significantly cut into the profits of some businesses. PayPal, Google Checkout and Amazon Checkout's rates all start at 2.9% + $0.30 per transaction, decreasing to 1.9% for merchants with over $30,000 of transactions per month. Otherwise viable businesses with low profit margins or requiring many small transactions may not be profitable due to these fees.

Bitcoin transaction fees are voluntary and payments can be accepted directly by merchants. Assuming a gross profit margin of 20%, eliminating processing fees would increase a merchant's profit by 10%, as these expenses would come directly off the bottom line.

A World-Wide System

Unlike current payment processing systems, Bitcoins are inherently world-wide and multi-national. There are no artificial barriers for making payments across national boundaries; in fact, it's impossible to verify a transaction's country of origin. A merchant accepting Bitcoins immediately has access to a world-wide market, without any risk of non-payment from those outside his own country's legal enforcement system.

An Inflation Hedge for Long-term Savings

Because the lifetime creation limit is 21M Bitcoins, it may be that they will be a good way to store long-term value as a hedge against inflation. This may be especially true for citizens of countries that are experiencing run-away inflation. If they can transfer their earnings to Bitcoins, they can be isolated from the rapid inflation of their native currency, and only convert back when needed to purchase goods or services using their native currency.

While this strategy is premature due to Bitcoin's very volatile valuation today, it may become common as Bitcoin becomes more widely adopted and develops a history of value stability.

What are the Inherent Risks of Bitcoins?

Irrevocable Transactions

Merchants do not have to trust their customers to verify payments, but customers have to now trust merchants to deliver the goods or services they have paid for. There are methods to alleviate this problem; for example, use of third-party trusted escrow services which require merchants to post a performance bond and enter into binding arbitration of disputes.

Underlying Value and Volatility in Prices

What is a Bitcoin worth? The underlying value is a function of the demand of the currency by consumers, and their ability to use it to exchange it for other goods and services. Just as fiat currencies no longer are tied to the value of an underlying commodity, like gold, Bitcoins are only valuable in as much as people want them and use them.

Numerous public exchanges exist for people to buy and sell Bitcoin in exchange for dollars or other currencies. This helps establish an underlying comparative value and allows merchants to cash out of their Bitcoin holdings on a regular (e.g., daily) basis, minimizing their exposure to any currency volatility of Bitcoins. While Bitcoins have fluctuated in value between $1 and $30 in 2011 alone, there are mechanisms for merchants to quote prices in dollar-equivalents (or other currency), and to exchange the Bitcoins they receive for other currencies immediately upon receipt.

An additional concern with the price volatility of Bitcoin is that the total value of all Bitcoins mined so far is just over $30 million. This relatively small market cap, in conjunction with a lack of regulatory oversight, exposes Bitcoin prices to market manipulation.

There is already significant speculation in online forums about who may be manipulating prices and to what end. When Bitcoin speculators talk about surprising market movements, they discuss "The Manipulator," a shadowy individual or group who is manipulating the price of Bitcoin with their great wealth. Whether they have actually recognized a wealthy market manipulator or are anthropomorphizing the Invisible Hand of the market remains unclear.

Anti-Inflationary

Noted economist Paul Krugman wrote an article in the New York Times criticizing Bitcoin's anti-inflationary provision (due to the 21M Bitcoin creation limit). His argument is that Bitcoins will cause people to hoard the currency rather than spend it. But we feel his argument ignores the near infinite divisibility of the

currency. If Bitcoin values go up, people will still desire to spend some of their gains from the currency by using a fraction of what they own. While fiat currencies are artificially inflated by expanding government debts, Bitcoin will remain relatively stable in value over time.

As a creditor, I would be happy to loan Bitcoins as I can be assured that they won't be artificially inflated before they are returned to me (with interest).

Contrary to his argument, we also have examples where deflationary prices in some markets (consumer electronics and computers) would seem to predict consumers refraining from purchases (why spend $2,000 on a computer today when I can wait 2 years and get the same computer for $500). Rather, we see a healthy market providing ever-increasing value to consumers.

Computational Attack

The Bitcoin network recognizes the longest Block Chain as the current valid ledger of all transactions. Block chains can only be extended with computation-intensive cryptographic hashing. Anyone wanting to maliciously re-write the history of the Block Chain must have available greater computational power than the entire remainder of the Bitcoin network.

Creating this "alternate history" does not allow transactions to be created without a private key, but it has the ability to erase transactions in the past. Theoretically, a scammer could buy a product with Bitcoin, and once they receive it, release an alternate block chain, of greater length than the current one, that does not contain the scammer's transaction. Because this new block chain is longer, and thus demonstrates greater past computation, the network will accept it as the current, most-up-to date block chain. This allows the scammer to spend Bitcoin to receive a good, then reverse his transaction to keep both the good and the Bitcoin (i.e., double-spending).

A computational attack would be very difficult to carry out today. The total computational power of the Bitcoin network is the equivalent of over 100 PetaFLOPs (the number of computations it can perform per second). By comparison, this is about 10 times the speed of the world's greatest supercomputer, Japan's K computer, at 10.51 PetaFLOPs. The expense of creating a large supercomputer outweighs any potential gains that could come from the ability to double spend a portion of Bitcoins.

Because of the risk of double spending, it has become common practice in the Bitcoin community to wait for six confirmations (six ten-minute blocks to be added to the block chain after your transaction) before treating a payment as received. While a scammer might get lucky and reverse one or two blocks with an alternate chain and a great amount of computation, each additional block is exponentially more unlikely.

Regulatory Uncertainty

The legal classification of Bitcoin is still unclear: it could be considered a commodity, a currency, a financial product, or legally equivalent to World of Warcraft gold. It remains to be seen what licenses and financial regulations Bitcoin businesses will be required to obtain. The largest currency exchange market, MtGox, reportedly has experienced some difficulties wiring money because of money laundering investigations.

Bitcoin is inherently hard to regulate as there is no central authority. Because transactions are semi-anonymous and accounts cannot be frozen, it could become a medium of choice for money laundering, tax evasion, and illicit trade. Using the TOR anonymizing network, any internet user with some technical savvy can access a service called the Silk Road, a marketplace for illegal drugs denominated in Bitcoin.

In the above respects, Bitcoin has very similar characteristics to governmental paper currency, like US dollar bills (i.e., cash). They can both be

transacted nearly anonymously without an easily auditable paper trail. However, Bitcoin's technological complexity may cause regulators to view it as a threat to the rule of law. The regulatory classification and legality of direct party-to-party business transactions are still uncertain.

Risk of Loss

Users of Bitcoin today have to ensure that they secure their digital wallets from both loss and theft. This can be challenging, requiring use of secure encryption, password management, and information backup methods. There have been some high-profile cases where people made mistakes and lost hundreds of dollars' worth of Bitcoin. With no central authority to appeal to, these funds are truly unrecoverable.

It is important for Bitcoin adopters to employ best practices and use methods commensurate with the potential for loss of their Bitcoin holdings.

Is Bitcoin "The One"?

The Bitcoin system is very young, barely 3 years old. While it has an engaged community of early adopters, many of whom have done a deep technical analysis of the security of the Bitcoin protocol, there may be inherent flaws in the design leading people to abandon the currency in favor of some other design (or to lose faith in the concept of a distributed anonymous currency altogether).

Some competing digital currencies have been proposed, but with much more limited adoption than Bitcoin has seen. It seems likely to us, that Bitcoin, or something very much like it, will be a viable option for many types of transactions and exchanges in the online world.

Applications Well-suited to Bitcoin

1. **Online sales of digital goods**. Customers can receive delivery immediately and the merchant gets a guaranteed irrevocable payment.
2. **Online donations**. Payments can optionally be publicly visible to demonstrate social proof of support for a charitable cause.
3. **Super Vault**. A Bitcoin wallet can be created from a passphrase or stored on one or more USB-keys. Bitcoins can be deposited to the generated public addresses even when the wallet is offline. So there is no risk of loss through online hacking; money can flow in, but is impossible to flow out without retrieving the offline wallet from storage (or the memory of the wallet creator).
4. **Remittances**. Inexpensive money transfer system across national boundaries. Agents could accept cash in a developed country, and transfer Bitcoins to an agent in the home country of a foreign worker, to be picked up by the family of the worker.

References and Links

1. Bitcoin: A Peer-to-Peer Electronic Cash System - by Satoshi Nakamoto (original paper)
2. Bitcoin on Wikipedia
3. We Use Coins - An Excellent introductory video.
4. Bitcoin Forum - Online discussions of Bitcoin by early adopters and enthusiasts.
5. Bitcoin Wiki - Technical information on the Bitcoin protocol, software, and services.
6. Bitcoin.org - Primary download site for the "official" Bitcoin client (source code)
7. BlockChain and Block Explorer - Online browsers of Bitcoin published transactions
8. MtGox - The largest Bitcoin exchange (Dollars exchanged with Bitcoin) - live price and order book chart at MtGoxLive.
9. Bitcoinica - The 2nd most popular Bitcoin trading site, offers margin and short-selling not offered on MyGox.
10. TradeHill - Another popular (international) Bitcoin exchange.
11. StrongCoin - An easy-to-use online digital wallet.
12. InstaWallet - On-demand online wallet with no account needed - creates a private URL per address.
13. DeepBit - One of the largest mining pools for Bitcoin with a combined compute power of 3,000 Giga-hashes per second (3 x 10^12 hashes/sec)