Bitcoin
& the Virtual Currency Phenomenon

Presented to Quest Club, Fort Wayne, IN
By William B. Johnson
November 21, 2014
Money has a fascinating history that would be an interesting lead-in to talking about virtual money like Bitcoin, but as usual, we struggle with the constraints of time and audience attention. Hopefully you find the presentation interesting, as I was fascinated with the topic.

We’ll first look at the beginnings of virtual money back in the early 1990’s, which grew out of a concern over privacy in electronic communication, and follow the evolution of virtual money up to the creation of Bitcoin in 2008. Then, we’ll explore the properties of the Bitcoin system, including the use of cryptography to insure privacy and the digital ledger used by the system, which is named the Blockchain. The Blockchain tracks the provenance, or literally, the place of origin, of all Bitcoin holdings in real time and is thought by some to be the most exciting and far reaching idea to come out of Bitcoin’s creation. Finally, I’ll recount to you my setting up of an online digital wallet, purchase of Bitcoin in the wallet, and subsequent purchase of merchandise with Bitcoin.

Timothy May, a retired Intel physicist, invited a group of friends to his home outside Santa Cruz, CA, in 1992 to discuss privacy and the nascent internet. In the prior decade cryptographic tools like Whitfield Diffie’s
public-key encryption and Phil Zimmerman’s program named Pretty Good Privacy had proven useful for controlling who could access digital messages. Fearing a sudden shift in the ability to control information and a commensurate reduction in their power, governments around the world had begun threatening to restrict access to such cryptographic protocols. May and his guests looked forward to everything those governments feared. “Just as the technology of printing reduced the power of medieval guilds and altered the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions,” he said. By the end of the meeting, the group had given themselves a name – “cypherpunks” – and the superhero like task of defending privacy across the digital world. In just one week, cofounder Eric Hughes wrote a program that could receive encrypted emails, scrub away all identifying marks, and send them back out to a list of subscribers. When you signed up, you got a message from Hughes that read:

*Cypherpunks assume privacy is a good thing and wish there were more of it. Cypherpunks acknowledge that those who want privacy must create it*
for themselves and not expect governments, corporations, or other large, faceless organizations to grant them privacy out of beneficence.

Hughes and May were deeply aware that financial behavior communicates as much about you as words can, if not more. But outside of cash transactions or barter, there’s no such thing as a private transaction. We rely on banks, credit card companies, and other gatekeepers to keep our financial system running, but they struggle to secure privacy in a system originally designed to handle physical coins and bills. Hardly a week goes by without news of another data breach involving millions of accounts. This struggle of the gatekeepers to maintain the privacy and integrity of the personal information you and I supply to them is ever more costly and increasingly invasive of individual privacy. JP Morgan Chase, the largest bank in the United States, expects their cybersecurity expenditures to double in the next five years from the current level of $225 million annually.

One magazine article called Bitcoin “The Anarchists Cryptocurrency”, which is an apt description of virtual money as thought of by some of the cypherpunks. These individuals saw no way to insure individual privacy
with the existing financial system, and hence the only answer was a total replacement of that system. This dream of wholesale replacement of the existing financial fabric of society certainly fits the definition of anarchy, and hence the moniker for Bitcoin. Jim Bell, a onetime Intel engineer, took the anarchist fancies of the cypherpunks further than anyone, introducing the world to an odious thought experiment called an assassination market. Citizens needed an effective way to punish politicians who acted against the wishes of their constituents, he reasoned, and what better punishment than murder? With an anonymous digital coin, argued Bell, you could pool donations from disgruntled citizens into what amounts to bounties. If a politician made enough people angry, it would only be a matter of time before the amount in the bounty pool pushed him out of office or cost him his life. Bell’s essay “Assassination Politics” eventually attracted the attention of federal agents. His spiral through the U.S. court system started with an IRS raid in 1997 and ended in March, 2014, with his release from prison.

While cypherpunks like Bell were dreaming up potential uses for digital currencies, others were working on the technical details to implement currency in cyberspace. Nick Szabo was one of the first to imagine a new
digital currency from the ground up. Many consider his scheme, which he
called “bit-gold” to be a precursor to Bitcoin, although privacy was not
foremost on his mind. His primary goal was to turn ones and zeros into
something people valued. “I started thinking about the analogy between
difficult to solve problems and the difficulty of mining gold,” he says. If a
puzzle took time and energy to solve, then the solution to the puzzle could
be considered to have value, reasoned Szabo. The solution could then be
given to someone as a digital coin. This approach to creating a virtual
currency has an obvious problem, however, because once a string of ones
and zeros has been designated a digital coin, it is easy enough to copy and
paste it, creating multiple coins. This has been described as the “double
spending” problem and one way to address it is by relinquishing some
control to a central authority, such as a bank, which keeps track of each
accounts balance. This solution was unacceptable to Szabo. He said “I was
trying to mimic as closely as possible in cyberspace the security and trust
characteristics of gold, and chief among those is that it doesn’t depend on a
trusted central authority.”

Bit gold gave credence to the idea that it was possible to turn solutions to
difficult computations into property, but bit gold and other early attempts
at digital currency did not have a complete infrastructure and failed to gain widespread support. The digital currency scene went pretty quiet around the late 1990’s, and then, in 2008, a mysterious figure who wrote under the name “Satoshi Nakamoto” proposed Bitcoin.

A simple way to look at Bitcoin is to think of it as a digital ledger book. Imagine a group of people at a table who all have real-time access to this digital ledger on laptops in front of them. The ledger records how many Bitcoins each person at the table has at any given time. The balance of Bitcoin in each person’s account is public information, since everyone at the table has access to the digital ledger. If one person wants to transfer funds to the person sitting across from him, he has to publicly announce that transaction to everyone at the table. The entire group then computes what the new ledger balances will be after the transaction, and if they all agree, the transaction is entered to the ledger. In this system, money never has to exist in physical form, and yet it cannot be spent twice.

To create a working system, Nakamoto started with the idea of a chain of data, similar to bit gold. But rather than creating a chain of digital property, or digital coins, Bitcoin records a chain of transactions in a digital
ledger called the Blockchain. The infrastructure of Bitcoin consists of the Blockchain, or digital ledger, addresses on a peer to peer network, each of which may contain Bitcoin, and Public-Key Private-Key encryption to encipher the contents of each address. Public-Key Private-Key encryption means there are two keys used to encipher each address, and the contents of the address cannot be deciphered without both keys. The Public-Key is, as the name implies, known to the public, which is everyone on the network. The Private-Key is known only to the address owner. Encryption ensures the privacy of each address’s Bitcoin holdings and the lack of association between an address and a human identity ensures the individual’s privacy.

Now generalize the very simple picture of a group of people sitting around a table, by realizing that the participants who use Bitcoin are not sitting in the same room, but are spread across a global peer-to-peer network. Further, and crucial to understanding operation of the system, transactions take place between addresses on the network, not between individuals. Addresses contain Bitcoin balances, and an individual can have multiple addresses. Parties to a transaction thus need to verify ownership of Bitcoin
in the address given by their counter party without regard to the counter party’s actual identity. The Blockchain digital ledger contains the provenance of all circulating Bitcoin and once ownership of Bitcoin in a customer’s address has been verified, the vendor is confident there is money available to pay for the transaction.

The system turns our idea of banking privacy upside down by processing all transactions in public, but the transactions are between addresses that are difficult to link with a human identity. Maintaining the dissociation between address ownership and human identity takes vigilance on the part of the Bitcoin user and careful decisions about transaction methods, but an informed consumer can do it.

To get started using Bitcoin an individual needs a digital wallet. A digital wallet is a computer file which contains Bitcoin addresses and the Bitcoin balance of each address. A digital wallet is available for no charge from numerous online vendors, including companies named Coinbase and Blockchain. If desired, an individual can have multiple wallets enabled by several vendors. The Bitcoin balances in each Bitcoin address contained in the digital wallet are encrypted using Public-Key Private-Key cryptography,
and this encryption is secure enough to raise the ire of the government. The head of the FBI spoke to the Brookings Institution in Washington, D.C., in mid-October this year decrying the promise of Apple and Google to encrypt all information that they maintain online, and calling on Congress to force the companies to provide a “front door” so law enforcement could read all the encrypted content stored by the companies. Failure to provide such a “front door” would, according to the FBI, severely hamper their ability to ensure national security. The other side of that argument is that failure to provide such a “front door” would substantially enhance the freedom and privacy of United States citizens.

Now for a brief look under the hood of the Bitcoin system by examining a simple buy-sell transaction. None of the detail discussed here is necessary for you to use Bitcoin, since all encryption, transfer, decryption and validation that takes place in the system is handled by the system software and your digital wallet. This tour will help us become informed consumers of a system designed from the ground up to operate in the digital age, utilizing all the tools available to make it fast, private, and secure.
Bob and Alice each have digital wallets on their computers, and their wallets have addresses containing Bitcoin. Bob and Alice have no idea who the other person is, or where the other person is located, and yet want to conclude a transaction. Alice wishes to purchase an item from Bob’s website using Bitcoin as payment. From Alice’s viewpoint, the purchase is no different than a purchase from any online retailer. She goes to Bob’s web
site, places her purchase in an online shopping cart and proceeds to check out, where she specifies payment in Bitcoin rather than with a debit/credit card. Bob now opens a new Bitcoin address to receive Alice’s payment for the item she purchased. Opening the new address creates a new cryptographic key pair consisting of a Public-Key and a Private-Key, and Bob would use the Private-Key to encrypt a message to Alice. The Public-Key then allows everyone on the network, including Alice, to verify that the message signed with the Private-Key is valid. Alice now chooses a Bitcoin address from her digital wallet which contains sufficient Bitcoin, and instructs the digital wallet to transfer the purchase price to Bob’s address. To effect the transfer, Alice’s digital wallet signs her transfer request with the Private-Key for that address and forwards the signed request to Bob’s address. Everyone on the network can now use the Public-Key for Alice’s address to verify that the transfer request is coming from the legitimate address owner. So far everything has gone swimmingly. Bob opened a new address to receive Alice’s payment and Alice verified the address is valid. Alice transferred Bitcoin to Bob’s address and Bob verified that the originating address for the Bitcoin is valid. Verifying that Alice owns the Bitcoin being transferred is the only remaining task before updating ledger balances in the Blockchain.
The diagram goes into more detail than we are going to pursue here about the verification function, so feel free to take the diagram with you and examine it at your leisure. Bitcoin ownership is verified by Miners, who are independent entities that earn newly minted Bitcoin for providing this function. According to Nakamoto’s design, there is a maximum of 21 billion Bitcoin, of which there are approximately 13 billion currently in circulation. In the future, as maximum issuance of 21 billion Bitcoin is approached, the supply of newly minted Bitcoin will disappear and the Miners will then charge a fee for the verification function.

Once the Miners have verified Alice’s ownership of the Bitcoin used to purchase the item from Bob’s web site, the transaction is added to the Blockchain. Adding Alice and Bob’s transaction to the Blockchain adds the Bitcoin purchase price to Bob’s address and diminishes the Bitcoin holdings in Alice’s address. This validation process typically takes a few seconds and then Bob is ready to ship the item to Alice. Contrary to our current system where account balances are only updated once a day, Bitcoin balances are updated continuously in real time. As a consequence, once a transaction is added to the Blockchain it cannot be reversed.
I went through the process of opening a digital wallet on the Coinbase website (https://www.coinbase.com/), linking the digital wallet to a personal bank account, and then purchasing Bitcoin. The screen shot below is where you enter the Coinbase site to create a digital wallet, and after doing this,

![Screenshot of Coinbase website](image)

My Bitcoin account at Coinbase looks as shown below.
Coinbase represents that they host more than 2 million consumer digital wallets and support 37,000 merchants in 19 countries.

My original thought was to purchase a Starbucks gift card and then enjoy a latte, but discovered that Starbucks does business in several currencies, but Bitcoin is not one of them. The web retailer Overstock.com accepts Bitcoin, so I went shopping on their web site and purchased an iPhone cover from them. The checkout page at Overstock looked just like the checkout page at any other online retailer, except that the list of payment options included
Bitcoin, along with PayPal and all the credit cards. The checkout page is shown below, along with the receipt(s) for payment from Coinbase.
Merchant information

United States

http://www.overstock.com

$9.78 USD
0.02988768 BTC

MyBat Hybrid Protector Cover for Apple iPhone 4S/ 4 on Overstock.com invoice ID 141044713.

- Use Coinbase Wallet Coinbase Wallet
- Use Bitcoin Address Bitcoin Address

Signed in as William Johnson, Not you?

Send exactly 0.02988768 BTC to this address:
13mj4zgpNAtaDpMBSWEeHP6rr68uxNe91

9:52
Copy address
Waiting for Payment
Connection lost
Reconnecting now...
Powered by Coinbase.com · Cancel and go back ·

Inserted from <https://www.coinbase.com/checkouts/3e89f39a85f8a4d5e25d9c99a05c92e9>
I also found that Kahn Academy will accept donations in Bitcoin, but you cannot purchase a T-shirt, hat, or anything else from their online store using Bitcoin. The instructions to Coinbase to send a $1.00 donation to Kahn as well as the receipt from Kahn is shown below.
USD
0.003066 BTC
One-time Donation
A free world-class education for anyone, anywhere.
• Use Coinbase Wallet Coinbase Wallet
• Use Bitcoin Address Bitcoin Address
Signed in as William Johnson. Not you?

Send exactly 0.003066 BTC to this address:
1DJDGVXPyGvbSJvYJDfYQRTvZ5YPeMxK
8:04
Copy address
Waiting for Payment
Connection lost
Reconnecting now...
Powered by Coinbase.com

Inserted from
<https://www.coinbase.com/checkouts/2b30a03995ec62f15bdc54e8428c92a87/widget?code=2
b30a03995ec62f15bdc54e8428c92a87&buttonStyle=none&referrer=www.coinbase.com>
We’ve briefly examined the inception of virtual currency Bitcoin, the infrastructure that enables it, and a couple of examples of using it in a transaction. Blockchain, the digital ledger system that enables a real time chain of custody for all issued Bitcoin, has been hailed as the most important development to come out of Bitcoin. Some have even advanced Blockchain as the most important invention of the present century, because its potential is pervasive and extends far beyond virtual currency. I leave you to think about how many places in our life we interact with items having a chain of custody that would benefit from the privacy, up to the
minute accuracy, and security afforded by Blockchain. Think about automobile titles and registrations, real property records, voting registrations, and the list goes on.

No one can predict how evolution of the monetary revolution that is underway currently will proceed or where it will end, but a combination of computers, cell phones, the internet, and cryptography provides great possibilities for privacy, security, and low costs.
References


Works Cited


MLA formatting by BibMe.org.