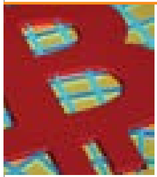
PIXABAY MASTERTUX

BITCOIN AND BLOCKCHAIN

BY: DR. BRANDEN R. WILLIAMS



Blockchain, as a technology buzzword, may not be as familiar to you as one of its most famous implementations, Bitcoin.

What started as an innovative type of currency–beyond the control of any country or bank–that could be mined using spare compute cycles has turned into the currency of choice for many people, including some criminals. The underground online market Silk Road brought Bitcoin right into the mainstream as the preferred currency because it was peer to peer and exempt from the laws governing currency. Want to avoid using a currency subject to inflation and deflation based on the policies or popularity of the issuing government? Want to avoid the risk of your bank teller deciding your transaction is "suspicious" and reporting you to officials who can seize your account without a warrant? Bitcoin could be your answer. Do you want to pay for illicit or illegal substances? People have used Bitcoin for that too.

Of course, Bitcoin as a currency has its drawbacks as well. While government controlled currencies have fluctuated in value, the dollar has demonstrated comparative stability so far within our life-times. Bitcoin's exchange rate is volatile.A wallet full of Bitcoins might buy you a McLaren today and only a Honda tomorrow. It also relies on exchanges to convert Bitcoin into traditional currency, and just like traditional banks are subject to robbery, Bitcoin exchanges have fallen to heists as well.

THE RISE OF BITCOIN

Perhaps one of the most perplexing topics around Bitcoin is its genesis and the true identity of its creator, Satoshi Nakamoto, who has virtually disappeared from anything related to Bitcoin. He or she is the largest holder of Bitcoins at over one million (valued at around $1.2B using a recent exchange rate) with rumors abound on who is this person's real identity. Imagine for a moment that you created a virtual currency while solving key problems around virtual currencies (preventing double-payments being one) and then ended up with a massive amount of this currency. Keeping your identity secret would probably be a massive priority if you now held $1.2B worth of a virtual currency you created—you could be a target for both criminals interested in financial gain as well as institutions dependent upon preventing the rise of a popular new currency that many will prefer.

Industry pundits and journalists speculate on what drove the price of Bitcoin to be the same as an ounce of gold, a price it is nearly back to today. The speculation on its' rise in value comes in a few different themes. The first is acceptance. As more places accept any type of currency in its early days, it becomes more valuable as a medium to exchange goods and services.

The decentralized nature of the blockchain prevents any one individual (such as an influential party or bank) or group from controlling or compromising the system.

Silk Road was an online darknet marketplace, only accessible via Tor, the traffic anonymizing network discussed in earlier articles in this publication *(See the Sept, 2015 T&P article, "Protect Your Digital Footprint" Ed.)*. Buyers and sellers used Silk Road to create a black market of illicit and illegal substances. They exclusively dealt in Bitcoin, no cash or card allowed. While drugs and drug paraphernalia were the most common types of goods exchanged, buyers could also buy erotica, hitmen, ATM hacking tutorials, and many other things you won't find in your local Walmart. The Silk Road darknet marketplace was shut down, but the currency continued to build steam. This is the second major area of speculation on its increase in value.

Saying that Bitcoin is volatile against many traditional currencies is an understatement at best. The roller coaster extremes have the Bitcoin/USD exchange valued at $.01/Bitcoin in 2009 to over $1,200/Bitcoin today with dips and spikes in between. You can divide Bitcoin into infinitesimal amounts, meaning that there are businesses who value the whole Bitcoin as much as there are businesses who value those tiny fractions for transaction validation.

It's still used as a currency to exchange for goods and services today, and often used for ransom demands for cyber security attacks. Hospitals, businesses, and individuals who have suffered from ransomware attacks (when a piece of software steals your files and asks for a ransom to unlock them) are asked to pay their ransom in Bitcoin. It's virtual, peer to peer, untraceable (without advanced analytics or close surveillance of the individual using it or the machines executing the transaction), and isn't subject to the dye bombs that might taint physical currency in old fashioned bank robbers.

HOW IT WORKS

Blockchain's technology base is well documented as a number of firms scramble to capitalize on implementation of blockchain as a transaction ledger. This is probably the best real-world analogy to how blockchain works, as described by IBM in their Blockchain Basics web page. Blockchain combines the concepts of non-repudiation and distribution to create a record of transactions that is available to anyone and can be verified through the applied mathematics that drive the cryptographic elements of the blockchain. Non-repudiation is essentially an assurance that an individual cannot deny something happened. Perhaps an example of this in the physical world could be a notarized document. With that record (provided the notary is not corrupt,) the signers of the document cannot deny that their signature was authentic. In the virtual world, this is accomplished through dual-key (public key) cryptography.

Let's say you (Bob) want to exchange information with Alice in a way that Charlie cannot read the information. Assuming that Charlie can see all of Alice and Bob's transmissions today, it would be impossible for them to exchange a password without Charlie capturing that password. Alice and Bob both create a key pair, called a public and private key, that are mathematically related, but serve separate purposes. The private key is used to decrypt messages that are encrypted with the public key, and to sign messages sent to essentially guarantee that the message is authentically from the sender. The public key half of the key pair validates mathematically the signature from the private key, and the private key half can decrypt messages encrypted with the public key. The system relies on the private key being kept secret and only available for use by the owner of the key. The public key can be published anywhere and that does not affect the security of the private key.

Back to Bob and Alice. Bob will encrypt the message to Alice with her public key and will sign the message with his private key. When Alice receives the message, she will decrypt the message using her private key to see what Bob wants to tell her, and she will validate Bob's signature of the message to ensure the message actually came from him by using his public key. All the while Charlie is aware of communications between Alice and Bob, but does not have the ability to see the message.

Blockchain is built on similar technologies, but only based on the non-repudiation element of the key pair. Let's say that you want to track all the transactions related to a funding grant draw down. A generous donor puts $20 million in a charitable account to be used only for road repairs in a small town. If we leverage blockchain to track the transactions, every ledger transaction to pay out portions of that $20 million will be recorded, can be made public across multiple sites (this prevents fraud on a single site as the network must reach consensus,) and anyone can validate the accuracy of one or all of the transactions by validating the cryptographic hashes generated by the digital signatures from the private keys of each individual who draws down the balance.

The decentralized nature of the block chain prevents any one individual (such as an influential party or bank) or group from controlling or compromising the system. Before blockchain, books could be cooked, fraud could be committed and funds embezzled. With blockchain, all of these items are reduced or eliminated while providing transparency and resilience through a peer-to-peer validated network.

OVERSTOCK AND HYPERLEDGER

Firms are still trying to find ways to deploy blockchain in innovative ways. While big banks are still experimenting trading stocks and money via the block chain, Patrick Byrne recently distributed a very real several thousand shares of his company Overstock.com to a new stock trading platform called t0 (www.t0.com)[1]. It's rather unique name comes from how its implementation of blockchain technology can take the three days it takes to settle a stock transaction (T-3) to zero days (T-0.) While t0 is the first real-world implementation of its kind, this proof of concept demonstrates that the traditional ways of trading stocks and bonds has lots of room for improvement. t0 works as a platform and could remove the need for many of the intermediaries who currently touch stock orders as they go from order to settlement.As the exchange matures, expect them to take on more transactions while cutting out middle-men whose purpose can be solved by the blockchain. The potential to dramatically reduce transaction time and costs due to the removal of intermediaries and the elimination of theft losses (that are often far greater than people may realize) is enormous.

Another implementation for blockchain is the Hyperledger (www.hyperledger.org), an open-source suite of tools that are designed to bring blockchain to Business to Business (B2B) and Business to Consumer (B2C) transactions across all manner of industries. Like the $20 million charitable donation above, these ledgers could be leveraged to validate all kinds of transactions. The B2B element seems to promote transparency where none exists today. Overall, this could be a benefit to the public. B2C transactions, however, could invade privacy rules if the owners of private keys are revealed.

For example, let's say that the government passes a law criminalizing all non-blockchain firearm transactions in the U.S. So if you go to a gun show and buy a pistol from another person (not dealer) for cash without submitting the transaction to the blockchain, you would be subject to criminal proceedings. Given that each transaction has a buyer and a seller, the seller side might welcome this law—depending on how the firearm was obtained. If I legally obtained a firearm and sold it to my neighbor, I may want a record that shows that the serial number of the firearm does not belong to me anymore. But as a buyer, do I want that same record accessible by third parties? Even with anonymization, data scientists have shown ways to identify individuals based on location, buying patterns, frequencies, amounts and other elements. More data means more ability to de-anonymize the data.

OTHER USES

Because blockchain provides non-repudiation on transactions listed in a ledger through a distributed peer to peer network, several firms are testing the technology to see how it could reduce transaction costs—something that drives the overhead of the firm. Utility companies are testing it for use when it comes to buying solar power from consumers, trading energy with other companies or tracking how electric cars consume power from the grid to bill the owners. Other organizations are looking at blockchain as a way to allow people to prove who they are, almost like a modern birth certificate. Some companies are looking at blockchain as a way to track various materials through supply chains. Essentially, if there is a use case where you need to write something down and keep a record of it, blockchain can help provide a distributed, non-repudiation record of that item.

Blockchain can be used for quickly trading stocks, tracking materials through the supply chain, enforcement of short term contracts, and financial accountability.

Some academics speculate that blockchain could revolutionize the legal system by creating the ability to automate the enforcement of short term contracts[2]. In many cases, long term contracts, which may take months or years to negotiate, are only used for short term deals. This ties up costs in the contract period as well as litigation should things go south. If short term contracts could be easy and simple to draft and execute, with automated enforcement, perhaps everyone can save in legal expenses.

Perhaps one of the biggest advances would be to leverage blockchain in governmental financial matters or public company finances and public service organizations to hold them accountable to their stakeholders or their mission. Corruption would have to take a different form if every transaction could be scrutinized by anyone with access to the blockchain.

Last month the UN announced a pilot program using Bitcoin and Ethereum to distribute humanitarian aid to those in need in war torn parts of the world[3].

CONCLUSION

Blockchain is already changing the world. Applications of blockchain, such as Bitcoin (or a similar currency) stands to revolutionize commerce if unimpeded. Citizens of the Islamic Republic of Iran, North Korea, Venezuela, and other oppressive countries might exercise increasing levels of freedom and liberty using Bitcoin while simultaneously starving these regimes of tax revenue. But even governments like the United States have concerns about total privacy and illegal activities, and harbor no illusions about the consequences of losing its' monopoly on the control of currency.

Anyone considering the use of a blockchain currency will see powerful incentives (as well as risks). Every organization that faces significant loss (virtually every government in the world) from currencies outside their control has a motive to fight or attempt to control its implementation. Only time will reveal all of the benefits and risks of this emerging technology application. Commerce in the near future will certainly have some new features from commerce today. For more info on Bitcoin, you can see this aggregation of talks given at this year's BlackHat conference in Las Vegas: http://brando.ws/BHIoT2016. ✓

BIO

Branden R. Williams (brandenwilliams.com) DBA, CISSP, CISM is a seasoned security executive, ISSA Distinguished Fellow, and technology executive sought after by global companies to consult on their digital business initiatives. His latest book on PCI DSS v3.2 Compliance is available on his website.

NOTES

[1] https://brando.ws/BigBankBlockchain

[2] https://brando.ws/BlockChainOrgChange

[3] https://brando.ws/UNcrypto