SPRING 2018 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss leading cryptocurrency fundamentals, blockchain infrastructure basics and the regulatory, security and legal impact.

Bitcoin and Blockchain Basics

Throughout the history of human trade, money has taken various forms including salt, cocoa beans, and of course, precious metals. At this point, fiat currencies, those backed only by the "faith and credit" of the issuing governments, remain the most widely accepted. What, however, does a person do when faith in the governments controlling fiat currencies is shaken, such as during the 2007-2008 global financial crisis? For many, the answer has been to exchange fiat currency for a cryptocurrency, like Bitcoin, a virtual currency spawned as a reaction to the global financial crisis which preceded it. While cryptocurrencies have passed the early-adopter stage, there are still many wondering what exactly Bitcoin is, and how it works. In this article, we'll address the basics of Bitcoin and the underlying technology, blockchain. As Bitcoin was the first and most widely known cryptocurrency, we'll focus on Bitcoin with the caveat that there are now in excess of five hundred cryptocurrencies available including Ethereum, Litecoin, Ripple, and Bitcoin Cash, many of which follow the same protocols as Bitcoin.

An Itty-Bitty Paper

On October 31, 2008, a whitepaper entitled Bitcoin: *A Peer-to-Peer Electronic Cash System* was published under the pseudonym Satoshi Nakamoto (http://nakamotoinstitute.org/bitcoin/). The brief, nine-page paper proposed a "purely peer-to-peer version of electronic cash" that "would allow online payments to be sent directly from one party to another without going through a financial institution." The innocuous description of the system proposed by Nakamoto is, in fact, a significant departure from traditional means of financial exchange.

Bitcoin is a decentralized currency, meaning neither bank nor government is required to issue or exchange Bitcoin for goods or services. The primary benefit of a decentralized currency is that should a government experience a financial crisis, said government cannot devalue Bitcoin by issuing more, nor can it freeze Bitcoin accounts by ordering banks to cease processing transactions. The down-side of this is that in the event of a disputed transaction, there is no intermediary to refund money or pursue a perpetrator.

Bitcoin's potential to service the "unbanked" populations of the world is seen as an additional and important benefit of decentralized cryptocurrency. For nearly 2 billion people who do not have access to a bank account, cryptocurrency could be a financial game changer. Even without a bank account or banking access, if a person can access the internet, including via a cell phone, they can utilize Bitcoin.

Transparency as Security

Bitcoin accounting is done by a volunteer network of computers called "nodes," across an open ledger system, which we'll discuss in the section on Blockchain below. The system is "permissionless," meaning anyone can join, and computers can join and leave the network anytime. In order for a transaction to be verified, a majority of nodes working on the ledger must accept it as a valid transaction. Once accepted, all currently functioning copies of the ledger are updated with the most recent information, and thus, the transactions are, to the extent that they are published on a publicly available ledger, public information. According to Nakamoto and other Bitcoin enthusiasts, it is this level of transparency that helps keep Bitcoin secure, as the odds of a fraudulent transaction being accepted by a majority of the nodes are near impossible.

Nodes processing Bitcoin transactions are paid in Bitcoin as an incentive to participate, and this processing for pay system is referred to as "mining." Despite the limitless space for miners on the Bitcoin processing system, Bitcoin is a limited currency: only 21 million Bitcoin will ever be released.

The 21 million figure isn't random. A calculation was run to determine how divisible the currency would need to be so that anyone in the world could adopt Bitcoin as a currency, and yet, not dilute the value of the currency by issuing more just to make Bitcoin accessible. What Nakamoto determined was that every Bitcoin needed to be divisible to a hundredth of million, or eight decimal places, (0.00000001) and the smallest fractional amount is called a "satoshi," as a homage.

What's it Worth to You?

One area which continues fostering debate is the intrinsic value of Bitcoin. Early adopters were quick to embrace the decentralized, publicly audited monetary system and recognized a certain intrinsic value derived from the computing power and corresponding electricity required in mining. Economists in favor of cryptocurrencies believe that like any new exchange medium, the acceptance of the commodity as a form of payment will either make or break it. More than one hundred enterprises such as 1-800-FLOWERS, Amazon, and Apple's App Store accept Bitcoin, and many more are coming aboard, including more traditional businesses with online and brick and mortar presences like DISH Network and CVS. Almost a full decade on, Bitcoin has at least a toe, if not a full foot hold in global financial markets.

For those who believe in the stability offered by governments, and the services offered by banks, Bitcoin may never replace fiat currency. A positive sign for enthusiasts however is that governments and banks are working to accommodate cryptocurrencies, even investing in them. There is substantial trading of Bitcoin from cryptocurrency to fiat currency. Many merchants who accept cryptocurrency for payment convert the remittances to their local currency for more flexibility.

As of this writing, Bitcoin is trading around $9,000, off approximately 55% from its all-time high of about $20,000 in late 2017. Only seven countries have placed a complete ban on

cryptocurrency, while many more, including all but two countries in the Western Hemisphere, allow their use to some degree. The United States is currently considered a “permissive” country with regard to the use of cryptocurrency.

Blockchain: The How of Bitcoin

As stated above, the technology that underlies cryptocurrency is called blockchain. Like much of the nomenclature of the electronic world, the name isn’t far from the process. Blockchain is literally a chain of data blocks. A helpful analogy might be to imagine every dollar bill has an individual serial number (currently, there are 832 bills per serial number for US paper currency). With blockchain, each dollar bill would be tracked by its serial number each time the bill changes possession. So, if one were to purchase a new smartphone with four hundred-dollar bills, the transfer from buyer to seller of those dollars would be recorded in the blockchain. If the seller then used two hundred of those bills to pay an employee, that transaction would be recorded in the blockchain, again by the serial numbers. Of course, this is a simplified analogy of how blockchain works, but it gives us a foundation onto which we can add detail.

Blockchain Nature

Blockchain is possession-based and transactional. For all intents and purposes, blockchain is a ledger, and the compilation of the data is referred to as a ledger. The technology records the transfer of data from one entity to another. The data represents “items,” and those items can include money (both cryptocurrency and fiat in electronic form), ownership (property titles, including deeds), events (health records, academic records), even contractual relationships can be recorded and tracked via blockchain technology. Depending on the various factors at hand, the rules by which various blockchains function differ.

The ledger, called a “distributed ledger,” is copied onto each participating computer, called a “node.” In the case of a public ledger, there is no restriction on the number of nodes that can be part of the distributed ledger. If a particular blockchain is a private ledger, permissions are required to join the ledger, however, true blockchain technology does not limit the number of potential nodes per blockchain. At the initial setup, each node receives the code to store the full blockchain, and as long as the node remains part of the ledger, it will continue to store the full ledger. Blockchain technology allows for nodes to leave the ledger and return at a later date. When a node returns, it simply receives the latest block in the chain, and it is not necessary to load the missing blocks that predate the most recent. Additionally, if a node joins the ledger after the initial setup, the new node receives only the most recent blocks and builds from there.

Blockchain assembles data into blocks through a system called “hash.” Hashing allows for a string of data of any length to be put through a mathematical operation that transforms it into a new string of data of a standardized size, with no loss of information. New transactions are hashed into new blocks and added to the chain in chronological sequence. Hashing allows for disk space to be reclaimed by eliminating blocks that have been incorporated into a sufficient number of subsequent blocks. For example, blocks “A,” “B,” and “C” must have already been proven to add block “D” to the chain. By the time block “M” is added, there is no reason to have blocks A-D in the chain.

One of the key elements of blockchain, especially as cryptocurrency is concerned, is that the data is immutable, it cannot be changed by going back to rewrite a single transaction. If a hacker wanted to alter the ledger, they would need to (1) break the hash for a certain block, (2) alter all blocks that follow the altered hash, (3) redistribute the altered ledger to all nodes in the network,

and (4) do so fast enough to supersede any blocks on which a majority of the nodes are already processing data to add new blocks to the chain. The improbability of even the most sophisticated hacker being able to accomplish all four elements is so remote that blockchain is considered so secure that a distributed ledger can be a permissionless peer-to-peer network without much worry.

Blockchain processing also eliminates double spending, when a person is able to execute and reverse a transaction rapidly enough that they can spend the same currency twice. Systems that conduct transactions based on account balances are susceptible to this particular threat. With blockchain, the nodes processing the transactions aren't concerned about the balance in the account but proving that the originating identity is the possessor of the data being transferred, and that transfer can only take place one time in any one direction. Whether it's Bitcoin number 12 going from X to Z, or Lot 7 of Anytown USA being sold from Mary to Steve, or refill number 2 of prescription number 123546 for John Q. with a medical id of ABCD22, that transaction can only happen one time on the chain.

A remote exception to the security of blockchain is called the "51% attack." For a 51% attack to work, one entity would need to control and coordinate at least 51% of the nodes on the blockchain. If that could be achieved, that entity could rewrite and distribute code to alter the rules of that blockchain. While the exact number of nodes working simultaneously is hard to track, as of this writing, there were over 400,000 unique members of the Bitcoin blockchain. In light of the current processing power required to operate a node, the cost of putting together a 51% attack would most likely require the backing of a government willing to invest billions of dollars into the project.

What Makes Cryptocurrency Crypto?

Each piece of the data coming into the blockchain must have a proven owner. This is accomplished by assigning a public key – private key system to the entities and data on the blockchain. All entities wishing to exchange or change possession of data on the blockchain hold public keys, which function as identities. The data subject to the transfer has a private key, which functions as its identity on the blockchain. In order to transfer the data, the holder must transfer the private key through the blockchain to the recipient. The nodes begin to proof this transaction through a series of mathematical processes, and if all the proofs are met, the data, token, or item is transferred via the private key, to the recipient.

Caveat: if the blockchain you're working on is truly a decentralized blockchain, if you lose the private key to your data, token or item, you cannot recover it; and, should your keys be hacked from your phone or your computer, your data, token, or item can be taken from you.

This is the biggest weakness of the decentralized blockchain for cryptocurrencies. In order to spend cryptocurrency, buyers and sellers must have an app called a "wallet." Cryptocurrency wallets function as a vehicle by which cryptocurrencies are transferred on the internet. Not all wallets are created equally, and one is advised to research wallet apps before downloading and engaging, and, to follow best practices for data security.

Another aspect of the public key – private key system is a level of anonymity provided. Because users are identified by public keys which appear as random strings of letters and numbers, as opposed to names or account numbers, the blockchain doesn't record a legal identity of the transaction participants. This led critics to raise the alarm that anonymity would lead to cryptocurrency being the preferred means of funding illegal activities. In response,

cryptocurrency advocates counter that money laundering has been part and parcel of traditional fiat currency transactions, and the fact that it's necessary to police such actions does not invalidate the use of currency irrespective of form. Additionally, like a case of spy versus spy, the antidote to the poison has already been developed, and law enforcement agencies have and continue to develop and employ methods to trace transactions to individuals. Still, the pseud-anonymity afforded by cryptocurrencies is seen as a boon to the privacy conscious.

What's Next for Blockchain?

We're still a while from blockchain's distributed ledger technology becoming the new network standard. One of the major concerns is that the technology requires high levels of computational power, memory, and electricity. The transaction processing can be slow, and when considering something on the scale of medical records, the amount of data involved may make adoption of a blockchain for a large population of patients a cumbersome undertaking. That's not stopping serious industry investigation into the use of blockchain technology. IBM has teamed with various groups to explore the use of blockchain technology. Shipping giant Maersk is looking for ways to streamline logistics with blockchain technology; and, Contractnet is looking to provide a blockchain-based alternative to lawyers with smart contracts.

Whether blockchain technology will supplant lawyers and government-based recording offices, or becomes the new standard for global financial transactions, is still debatable. What is not questionable is that a brief, nine-page whitepaper by the still unidentified Satoshi Nakamoto was definitely the catalyst for yet another innovation in an electronic frontier that only seems to grow more and more expansive.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

ENFUSE 2018
Las Vegas, NV: May 21-24, 2018

MASTERS CONFERENCE
Chicago, IL: May 22, 2018

2018 EDRM WORKSHOP
Durham, NC: May 23-25, 2018

CYBERSECURITY LAW INSTITUTE
Washington, DC: May 23-24, 2018

NINETEENTH ANNUAL INSTITUTE ON PRIVACY AND DATA SECURITY LAW
New York, NY: May 29-30, 2018

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: