PROGRAM MATERIALS
Program #3078
May 7, 2020

Demystifying Blockchain and Cryptocurrencies

Copyright ©2020 by David Kalat - Berkeley Research Group LLC. All Rights Reserved.
Licensed to Celesq®, Inc.

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

Demystifying Blockchain and Cryptocurrencies

By David Kalat

In conventional usage, the term “hacking” generally refers to an unauthorized user gaining access to an electronic resource. Hackers use various means to steal, guess, calculate, or otherwise obtain credentials to access systems and data they are not allowed to access.

When we talk about “hacking” a blockchain, however, this does not adequately or accurately describe what has happened and blinds us to understanding where the real risks lay in this new technology of distributed ledgers and crypto-assets. The high-profile, most destructive, and expensive “hacks” in blockchain environments represent *authorized* users misbehaving. In some cases, these authorized users act on their own behalf to exploit weaknesses in the system to their own gain at the expense of other users; in other cases, these authorized users are misusing the trust placed in them by their customers. The key to protecting yourself against fraud in this new alien world of blockchains is to become acquainted sufficiently with the technology and its peculiar jargon.

The Rai of Yap

There are many places where the story of blockchain technology can be said to have begun, but for our purposes the most productive is to start not with the technology or the immediate motivations behind the invention of Bitcoin, the first blockchain, but rather with the underlying concept of how monetary value depends on trust. This brings us to the Micronesian island of Yap. Historically, its economy was so distinctive that it became the focus of a famous paper by Nobel Prize-winning economist Milton Friedman in 1991.

In the early twentieth century, there lived a Yap family of immense wealth. For generations, this family had controlled a staggering amount of the local currency. What was striking about this family’s wealth, however, was that no living soul on the island had ever seen it or had the ability to touch it.

Yap’s local currency was strange. Inhabitants used large, doughnut-shaped limestone disks called “Rai” (or “Fei,” depending on the whims of the translator). Because Yap had no limestone of its own, Rai stones had to be quarried from other islands and transported at great difficulty. Although anthropologists suspect the earliest forms of Rai were sensibly sized beads, by the late nineteenth and early twentieth centuries, Rai stones were massive, larger than people, and too heavy to be easily moved.

A Rai stone can be as large as twelve feet in diameter and weigh in at four tonnes (8,800 pounds). “Coins” of this immensity cannot be easily exchanged or even be reasonably moved. Instead, Rai stay fixed in place in prominent ceremonial locations in public view, and the people exchange *ownership* without exchanging *physical possession*. Each transaction is witnessed by neighbors and other members of the community, whose collective society serves to remember and enforce those ownership rights.

The fact that *ownership* is fully divorced from *physical possession* is best exemplified by an anecdote related in Friedman’s paper. A wealthy family had sent out an expedition to mine limestone from another island, possibly Palau or Guam. On the return journey, however, the ship was buffeted by a terrible storm. The people survived, but the Rai stone they were towing on a raft had to be cut loose and was lost to the sea. The stone was only *physically* lost, however—the ship’s crew all agreed the stone was huge and of exceptional value, and they also agreed that its current location at the bottom of the sea was an unfortunate accident. As Friedman put it, “Thereupon it was universally conceded in their simple faith that the mere accident of its loss overboard was too trifling to mention, and that a few hundred feet of water off shore ought not to affect its marketable value, since it was all chipped out in proper form. The purchasing power of that stone remains, therefore, as valid as if it were leaning visibly against the side of the owner’s house…”[1]

Nowadays, the people of Yap use Rai only for special ceremonial purposes and have transitioned to conventional currency for everyday transactions. Meanwhile, the modern world has started to build a new electronic version of the “community memory” that empowered the Rai-based economy.

Trust and Verify

Although certain aspects of the story of the Yap economic system seem strange at first, there is more common ground than we might expect. Westerners routinely think of “owning” money that we cannot see and that has no physical form. My employer deposits my paycheck directly into

[1] Friedman, Milton. "The Island of Stone Money.” Working Papers in Economics. E-91-3. Stanford, California: Hoover Institution, 1991.

my bank account, from which I make transfers to other banking institutions to pay my various bills. No object changes hands, but “ownership” is transferred from party to party.

In conventional modern banking, these exchanges of ownership are logged and recorded in data systems maintained by the individual banks. Users of the system place their trust in those institutions to accurately record transactions and maintain them reliably over time.

The principal difference in the Yap economic system, and the critical detail in this context, is not that Rai can lie unobserved on the bottom of the sea without losing their value, but that the history of transactions is logged and recorded *collectively* by the community at large.

A conventional bank’s data system represents a single point of failure. If by accident or malice the data system fails to accurately record a transaction and/or reliably maintain that record, then the ownership of certain monies or units of value will be in doubt. By contrast, a communitywide set of transactional records (that is to say, a *distributed ledger*) can afford to have certain subcomponents forget or make errors, because the rest of the network can serve as an error-correcting backstop.

A tight-knit island community with strong oral traditions may rely on the integrity and goodwill of each person to remember reliably the ownership of tokens of value, but for an international community of strangers to transact with one another, there needs to be a way to *commodify* trust. A blockchain is a technological mechanism for administering a distributed ledger at a large-scale using cryptography.

Use Cases

Some companies have been managing their supply chains by using a custom blockchain to track and record the movement of certain foodstuffs from farm to consumer. This initiative was inspired in part by traumatic experiences with food safety issues. The discovery of contaminants in milk, romaine lettuce, and meat have resulted in massive waste as entire supplies have been discarded, contaminated and uncontaminated alike, while authorities have spent weeks trying to trace the origins of any outbreak. Blockchain systems allow retailers to trace the history of any given product recorded on that ledger almost instantly.

Another common application for blockchain technology is digital rights management and licensing. Other applications include managing voting platforms, maintaining identity authentication systems, recording securities transactions, and tracking chain of custody for electronic evidence.

In the popular mind, however, blockchains are nearly synonymous with cryptocurrencies.

A Pre-History of Cryptocurrency

The idea of using cryptographic techniques to design a secure online currency actually predates modern cryptocurrencies like Bitcoin by decades. In the early 1980s, computer scientist David Chaum pioneered and implemented a form of digital cash that was the first of its kind to try to disintermediate online transactions from banks. Chaum's motivation was his concern that the database structures used by banks to record and maintain transactional information was eroding the privacy that was inherent in cash transactions.

Transactions involving the exchange of physical possession of money allow both parties to confirm that an exchange of value has occurred, without requiring any lasting record of that exchange to be associated with specific individual identities. A bank has no way to know how a user intends to spend the cash she withdraws from her account; a merchant has no way to know the identity of the customer who pays in cash. Transitioning to electronic transactions has generally meant trading away anonymity and privacy in exchange for convenience.

In the early 1980s, Chaum, a privacy-minded student at the University of California at Berkeley at the time, devised an alternative. He developed his idea from an analogy about voting by sealed ballot. The electoral authority verifies a voter's identity, ensures the voter does not vote twice, and protects the integrity of the process, without ever knowing which candidate the voter selected. The same principle can be applied, via cryptography, to online transactions. As Chaum told *Forbes* magazine in 2019, "Cash is a bearer instrument, and is peer-to-peer, permissionless, and confidential. Digital cash should ideally share these same characteristics."

Chaum's 1981 thesis, "Blind Signatures for Untraceable Payments," proposed one kind of cryptography to mask the content of a message and a second kind to digitally sign that masked message. The digital signature provides a means to mathematically prove that the message came from a specific trusted sender, but in this scenario that verification does not expose the content of the communication. In Chaum's proposal, this technique would be used to allow a payer to instruct a bank to deduct a certain value from her account and to separately convey instructions to the bank to deposit value to a payee's account. The bank however would not know the transactions were related and the payee would not know from whom the purchase came.

In 1983, Chaum developed his idea further into a proposal for anonymous electronic money he called "eCash." Using cryptographic blind signatures, eCash software could allow users to make purchases from vendors without having to open accounts, exchange credit card numbers, or leave an audit trail identifying themselves.

By 1989, Chaum had launched the DigiCash Corporation to implement his idea on a commercial scale. But DigiCash suffered from being too early a pioneer. Almost no one used the Internet at the time. Until there was a sufficient volume of online ecommerce to protect, Chaum was selling a solution to a problem no one had. DigiCash fell into bankruptcy in 1998.[2]

Bitcoin: A Peer-to-Peer Electronic Cash System

In 2008, a white paper entitled *Bitcoin: A Peer-to-Peer Electronic Cash System* introduced a new technology called blockchain and proposed a practical application of it for digital currency. Put simply, a blockchain is a database that derives its integrity and security from decentralized distribution across countless individual nodes. To attack and modify a record in a blockchain database would entail the logistical challenge of simultaneously attacking millions upon millions of independent copies of that database on computers scattered across the world. Bitcoin in particular leverages the integrity and security that derive from that peer-to-peer network as a base upon which to build trust in a public ledger of financial transactions, thereby creating an online alternative to banks.

In the years that have followed that white paper, blockchains have been deployed in a variety of scenarios. In addition to cryptocurrencies like Bitcoin and Ether, blockchains can be used to monitor supply chains, manage identity authentication, enforce intellectual property rights, transfer property rights, among many possibilities.

[2] Although his work on eCash is mostly notable in hindsight, Chaum's relevance to the world of blockchain technology continues today. He has introduced his own Bitcoin rival, Elixxir. Chaum has noted that cryptocurrencies like Bitcoin and Ether rely on digital signatures, much like his 1980s version of eCash, but handle those signature calculations in inefficient ways. This limits the number of concurrent transactions those blockchains can handle. Chaum claims to have devised more efficient digital-signing techniques to allow exponentially more transactions per second. Introduced in late 2018, Elixxir began as a free messaging application, intending to build its network base before enabling payments between users at some point in the future.

But despite growing public interest and attention to blockchain technology, the identity of its creator remains strangely obscure. The 2008 white paper is attributed to a "Satoshi Nakamoto," a pseudonym for an unknown person or persons.

The unknown identity of "Satoshi Nakamoto" is a curious but telling detail in this story that deserves some closer attention. To understand the significance of this pseudonym, it is helpful to compare Bitcoin's situation to that of Theranos, the troubled bio-science company that claimed to have developed technology capable of performing sophisticated blood analysis on minute drops from pin-pricks. Theranos purported to offer a fantastical new technology, but would not describe it in detail—the nuances of its operation were protected as a proprietary trade secret. Instead, the company sought to persuade investors, customers, partners, the press, and the world at large on the basis of its leaders' reputations. Theranos founder Elizabeth Holmes projected a carefully cultivated public image, and she surrounded herself with a board comprised of luminaries. The star power of that leadership was meant to be persuasive in place of detailed technical information. Theranos is now defunct, its officials have been sanctioned, and members of its leadership have been indicted for wire fraud and conspiracy charges.

By stark contrast, Bitcoin did not attempt to sell anyone based on the reputation of its creators *because its creators remain unknown*. Instead, the pseudonymously-authored white paper describes the technical operation of the platform. Now that the Bitcoin blockchain exists, it is publicly viewable. Any and every transaction ever executed on the Bitcoin blockchain can be examined, and the software itself is open source and available to all. Unlike Theranos, every aspect of the technological operation of Bitcoin can be directly probed and interrogated by anyone, while its creators remain ghosts.

Ghosts in the Machine

It should be noted that not only are the creators of Bitcoin ghosts, but the way the system works, most users of a blockchain are as well.

In a traditional banking relationship, a bank or similar financial institution uses an account number to represent within their database systems a specific person or entity. The bank's actual customer is that person or entity, and the electronic records are methods of associating transactions and other data with that customer. In a bank setting, an "account" is an aggregation of records pertaining to a single customer.

There is no corresponding concept of an “account” in a blockchain, although the gravity of that term is strong enough that the word “account” is likely to be used on occasion even if it does not fully apply. Blockchains like Bitcoin and Ethereum do not have any records of the identities of their users. Anyone who wishes to be a part of such a blockchain community only needs to create a public key, which is a string of alphanumeric characters associated with a second, secret cryptographic key. In many blockchains, the word “wallet” is used for such a user ID, instead of “account.” As that wallet engages in transactions, the respective credits and debits are logged in the blockchain’s records and thereby document the history of that wallet and its present total value, which is in some sense a set of account records. Nevertheless, there are no personally identifying details, such as a name or address, by which to tie that wallet to any specific person or organization.

A blockchain such as Bitcoin does not have “customers.” A blockchain is a tool, like a knife or a toothbrush or a leaf blower. A knife does not have customers, it has users. The person who holds the knife gets to cut with it. Similarly, the person who has the necessary cryptographic key to access a particular blockchain wallet gets to transact with its contents.

This is a potentially counter-intuitive point, and needs to be emphasized up front because it has enormous ramifications for information security: from the perspective of the blockchain itself, the user *is* just a cryptographic key, not a person.

The Double-Spend Problem

One fundamental problem in establishing and managing an economy built around virtual currency is how to prevent the “double spend problem.” In an economic system that revolves around the physical possession of money, whether that physical money be seashells or paper bills, the *physicality* of possession provides clear boundaries around transactions. Once a dollar has been exchanged for some kind of good or service, the buyer no longer has it and cannot spend it again. In the digital world, those boundaries have to be constructed artificially.

“Spending” a digital form of money means transmitting a record of that transaction to all the components of the relevant computer network. Inevitably there will be some measure of time lag, when that transaction has not yet been recorded by all the parts of the network. This is a window of opportunity for a bad faith actor to try to send out a competing transaction, “spending” the same digital money somewhere else.

Banks and traditional financial institutions act as moderators of that system, and run the risk of having to absorb losses if a disputed transaction has to be reversed. To mitigate those risks, banks impose fees on transactions and regulate which parties are approved to conduct transactions. The premise behind blockchain technology was to replace that top-down system with cryptography.

Blockchains accomplish this by treating each individual unit of the cryptocurrency (generally called "tokens") as a distinct item. Paying someone in Ether, for example, means more than just decreasing your share of Ether and increasing their share of Ether by the same amount—it means transferring ownership rights of specific Ether tokens (much as paying someone in cash means handing over specific bills).

When a user wishes to engage in a blockchain transaction, that request is broadcast to all the nodes on the network—that is, a draft of the transaction is sent to all the computers running instances of that blockchain ledger. The transaction is not counted as having occurred until a process of verification confirms that transaction as valid. This process has its own implications for security, and is discussed more fully below, but for now, the important point is that a transaction has to be validated by the other users on the network to be accepted. This is comparable to gaining the consensus of the Yap community to agree that ownership of a given Rai has been transferred—the new owner will not be able to count that Rai as theirs unless the wider community gets on board with that new reality.

At that point, the transaction is recorded on the blockchain and becomes a part of the ledger. Here is where a clever cryptographic trick called hashing comes into play.

A hash function is a cryptographic algorithm that takes a chunk of data as its input and converts it into an encrypted string of data of fixed length. The input value can be of any arbitrary size, but the output will always be of the same compact length. Additionally, the same input will always produce the same hash. Instead of having to manually scrutinize a large data set to look for changes, one can quickly hash it and compare it to a previous hash—if the hashes match, the data set is known to be electronically identical. The term hash comes from cooking—the practice of transforming something by slicing and dicing it. A hash conversion is strictly one-way. There is no way to "un-hash" the encrypted string, any more than a cook can turn hash browns back into a raw potato.

Hashes have many uses in computer science, but in the context of blockchain ledgers, they provide powerful anti-fraud mechanisms.

Once a new transaction is verified by the community and added to the ledger, it is added in the form of a "block" that contains both the details of the new entry and a hash of *all previous entries* (the blockchain is, literally, just the chain of such blocks). Because the hash contains a mathematically verifiable accounting of all prior transactions, it serves to establish the order in which entries have been added to the ledger. If a user were to attempt to double-spend, this would send out two or more competing transactions involving the same tokens, the first one to be verified would be accepted and added to the chain as a legitimate transaction, but any subsequent ones would fail the verification test because they would be out of synch with the order of events established by the hash.

Additionally, this process of hashing all past transactions and embedding that history in each new entry means that any attempt to fraudulently alter or insert past entries into the ledger becomes a monumentally difficult task. It is not sufficient to alter or insert the target transaction—the fraudster would need to update the embedded hashes in every subsequent entry as well, including the active ones undergoing verification. This process of updating would have to be accomplished on at least 51% of all the computers in the network all at the same time, because the consensus of the majority of the computers in the network are what set the agreed-upon truth.

One especially interesting consequence of this design is that the security of a blockchain community increases with each user. On traditional computer networks, adding users often tends to *decrease* security, on the premise that a chain is only as strong as its weakest link--each new node adds a new attack surface, a new possible point of failure. On a blockchain, however, each new node represents one more hurdle any attacker would have to clear.

Mining Your Own Business

The security and integrity of a blockchain depend on the network effect of a wide base of users, but this means that for a blockchain to be effective it needs to encourage an engaged user network. As a means of cultivating its own network, the creators of Bitcoin and the blockchain communities modeled after its example implemented a process of incenting users to do the work in validating transactions and adding them to the ledger.

At its simplest, validating a transaction means checking the details of the proposed transaction against the history of the ledger to confirm that the parties actual own the assets they claim, and that the transaction is not contradicted by prior events. As noted above, if this is determined to be the case, the new transaction is bundled with a copy of that history and appended to end of the ledger as a new block. In a clever use of technology to leverage humans' natural sense of competition and game-play, Bitcoin and many other blockchain algorithms encourage people to perform this mathematical auditing by actually making it *harder*.

Here is how it works. New blocks are formed by hashing the components of the transaction, but a block can only be considered valid if they meet certain requirements. Simply hashing the new transaction and the history to-date of the ledger does not, by itself, result in an acceptably formed hash—a third component, the X factor, has to be included. Picking the right value for X to result in a valid hash is a trial-and-error process, however. If a user wants to participate in figuring out an acceptable value for X, their computer will be occupied for a period of time crunching through various options until one works.

The *first* computer to work out a valid answer to the puzzle wins a prize, of a certain quantity of bitcoins. This is called "mining," and it is the only mechanism by which bitcoins can be created.[3]

The puzzle is meant to be reasonably challenging to solve, such that on average a new block is mined every ten minutes. If blocks start to be mined too quickly, the algorithm recalibrates to increase the difficulty of the cryptographic puzzle so that the roughly ten-minute threshold pace is restored.

Like gold or silver, cryptocurrencies like bitcoin are finite resources. This may seem bizarre, given that cryptocurrencies are invented products created by computers and therefore the only limits imposed on them are the limits imposed by their inventors, but this is in fact the point. The creators of Bitcoin and the cryptocurrency platforms modeled after it deliberately created those algorithms to establish a predictable and limited quantity. In the case of Bitcoin, there will ultimately be a maximum of 21 million bitcoins total. That upper limit has not yet been reached, but over 85% have been "mined" to date and introduced into circulation. The ten-minute mining pace is part of the mechanism used to moderate the influx of new bitcoin. Along with it, mining rewards have changed over time. When the platform launched, a mined block was worth a reward

[3] The distinction between "Bitcoin" with a capital B and "bitcoin" in lowercase is meant to distinguish between the blockchain community as a whole and the individual coins transacted on that network.

of 50 BTC. BY 2012, that halved to 25 BTC. In 2016 it halved again to 12.5. Sometime in 2020 the mining reward will again halve to 6.25 BTC, and continue to halve roughly every four years. It is currently estimated that new bitcoins will continue to be mined until approximately 2140.

The $63 Million Pizza

Satoshi Nakamoto's white paper laid out the technical procedures by which Bitcoin users could obtain bitcoin through mining, and exchange them with one another in validated transactions recorded on a public ledger—but left it up to that community to work out what they would want to use this new cryptocurrency *for*. To use bitcoin as a medium of exchange, it needed to have a value with respect to goods and services in the real world.

Establishing a value for bitcoin was a challenge as long as the only exchanges occurred between a small community of hobbyist users experimenting with the technology, which was the state of affairs for the platform's first two years. Then, on May 22, 2010, a software programmer named Laszlo Hanyecz decided to break the ice and actually use bitcoin to buy a real-world object—specifically, some pizza.

At the time, there were no retailers, pizza or otherwise, that accepted bitcoin as payment. In order to effect the transaction, Hanyecz posted to an Internet forum his offer of 10,000 bitcoins for two large pizzas. Another user on the forum, Jeremy Sturdivant, agreed to the offer. Hanyecz sent 10,000 bitcoins from his wallet to Sturdivant's and in turn, Sturdivant called Papa John's and arranged an order of two pizzas to be delivered to Hanyecz. This provided a benchmark of exchange, initially pegging 10,000 bitcoin to $41 (the cost of the pizza order).

The value of bitcoin would fluctuate from that point onward, and ten years later a single bitcoin is traded at $6,365.59 U.S. dollars. At today's rates of exchange, Hanyecz spent the equivalent of $63,656,900 on his dinner. As the initial shock of that price tag sets in, there are two less immediately obvious aspects to this story that deserve attention.

The first nuance is the recognition that bitcoin only trades at such prices today *because* Hanyecz made his purchase. Bitcoin would be worth nothing if its users could find no use for it.[4] The bigger issue, though, is the extraordinary speed with which $41 turned into $63 million. This

[4] It is also noteworthy that the price fluctuation is volatile. When I first started writing this article, the exchange rate was closer to $9,000, but the onset of the coronavirus pandemic had a significant effect on the market. It is likely the price will be meaningfully different by the time you read this.

makes bitcoin look like, to coin a phrase, a “get rich quick” scheme, and it attracted the attention of people with that ambition.

Trouble at the Mine

The premise behind mining rewards was to incentivize the behavior desired from the bitcoin community—to encourage users to participate in validating the integrity of the ledger by committing their computing resources in return for the chance to earn a reward. The sudden and precipitous inflation of bitcoin’s worth had the effect of incentivizing highly undesired behavior.

Bitcoin’s mining rewards are an example of a process called “Proof of Work,” in which the reward goes to the party that puts in the most work in the form of computing processing power needed to solve each cryptographic puzzle. This led to a kind of arms race, as different parties vied to equip themselves to be more likely to solve the puzzle first.

Application Specific Integrated Circuits or “ASICs” are special-purpose computer chips designed for the task of mining Proof of Work cryptocurrencies. ASICs are generally so well-suited to their task that when an ASIC designed for a specific type of coin is made available, it typically becomes unprofitable to attempt to mine that coin with anything else. Not only does this incent prospective miners to stock up on that particular hardware, but some organizations go so far as to pack warehouses full of such machines, all running in parallel, in areas known for lower-cost electricity. This state of affairs leads to several unintended and problematic consequences. Consider for example Bitmain, a private company in Beijing, China that is arguably the leading manufacturer of ASIC systems for cryptocurrency mining. Not only does Bitmain sell ASIC systems to enterprising miners, but the company itself operates massive mining farms around the world of its own at a scale few organizations could afford to match.

Meanwhile, the developers working for various blockchains work on creating mining algorithms and other protocols intended to be “ASIC-resistant,” such that the use of specialized hardware does not bring a significant advantage. ASIC manufacturers have responded by developing improved chips that overcome ASIC-resistant protocols—feeding a cycle by which large-scale mining operations are constantly driven to upgrade their hardware.

Individual blockchain users are unable to compete with such concentrated resources, which leads towards a form of centralization of power and authority that ironically the blockchain community was invented to resist.

As previously discussed, one of the security features of a blockchain is that the decentralized ledger is distributed across a large network of cross-referencing users, meaning that unauthorized changes are corrected by the community. This only works, however, if the unauthorized change is attempted by a minority user. If a fraudulent transaction is forced into the system by a user that controls 51% of the network, that change will be accepted as valid because it represents the consensus. Once individual entities come close to controlling 51% of the verification process, the opportunities for abuse increase.

Proof of Work verification systems have other unintended consequences. Mining farms keep their computers running around the clock. In 2017, CBS News reported that Bitcoin mining alone was consuming more energy annually than 159 countries. In 2019, the government of Iceland warned that if demand from mining operations continued at the present pace, the nation's energy resources would be depleted.

For that matter, not all large-scale mining operations are legitimate businesses. Many criminal enterprises pursue the mining rewards without investing in expensive hardware, by hijacking consumer's computers with malware into becoming mining drones.

Proof of Stake

In response to the problems discussed above, some blockchain platforms have rejected the Proof of Work model for alternatives that they perceive to have fewer external side-effects. The most popular alternative approach at the moment is known as Proof of Stake. In a Proof of Stake protocol, the verification of a block does not depend on solving a cryptographic puzzle first but is a lottery where the size of the user's stake increases their odds of winning. The user's hardware plays no role in the outcome, so there is no incentive to bulk up warehouses full of special-purpose machines in areas with cheap energy, nor is there any advantage to enslaving other computers with malware. In order to add a fraudulent block to the ledger, an attacker would need to own 51% of all the cryptocurrency on that platform.

Some cryptocurrencies were created with Proof of Stake algorithms from the outset, such as Tezos and DASH. By contrast, Ethereum was created with a Proof of Work algorithm similar to Bitcoin's, but announced plans to transition to a Proof of Stake system in January 2020. That deadline has come and gone, and it is presently unclear what the new timetable will hold. When and if the moment of transition comes for Ethereum, making such a change to their blockchain will require what is known as a "hard fork."

Hard Forks

"Forking" occurs when a blockchain's underlying software code undergoes a change. Some changes are meant to be backwards-compatible, and are called "soft forks." One example of a soft fork is a feature called "SegWit" that was added to Bitcoin as a way of allowing more transactions to be added in a single block, to increase the overall transaction speed of the network. Some users have added SegWit functionality and enjoy its benefits, but they can continue to share the same Bitcoin network with users who have not adopted that upgrade yet.

Changes that do not permit backwards compatibility, however, split the blockchain into two irreconcilable tracks.

Perhaps the most famous, and most illustrative, example of hard forking concerns the DAO Incident and the Ethereum blockchain in 2016.

Part of what makes Ethereum distinctive and popular as a blockchain is that its infrastructure can be used for purposes unrelated to cryptocurrency. In addition to using the Ethereum blockchain as the backbone of the cryptocurrency Ether, the same blockchain can be used to generate and track tokens that represent other types of digital assets, vouchers, or real-world physical objects. The Decentralized Autonomous Organization ("DAO") was an initiative to help encourage new innovative tokens on the Ethereum network. Like a blockchain version of Shark Tank meets Kickstarter, the DAO provided a place for venture capitalists to set aside a certain stake of Ether to be used to fund new projects. Developers with project ideas did not need to canvas the entire Ether community for backing, and likely waste much of their marketing efforts pitching to users disinterested in investing, instead focusing their efforts on a subgroup of motivated backers.

When the DAO was launched in May 2016, the initial crowdfunding push gathered 12.7 Ether, worth roughly $150 million at the time. In June 2016, roughly a quarter of this was stolen.

The theft exploited a coding flaw in the DAO's software. The DAO was set up to automatically provide funds to any project that received a certain threshold of support—but backers had a fail-safe option to withdraw their investment from the DAO altogether. As it happened, in the event that someone used this recall function to withdraw their funds, the software code would update that user's balance with their refunded balance *before* updating its own balance. In essence, this coding oversight allowed the double-spend problem back into the equation—a user could send multiple withdrawal requests to the DAO in short succession, and these requests would get filled before the DAO system could realize its mistake. A user took advantage of this loophole and withdrew 3.6 Ether before anyone could stop it.

The DAO community then faced a choice. A proposal was put up for a vote that would in effect return the stolen funds to the DAO. This change would be so substantial as to constitute a hard fork. It may surprise you to learn that this proposal was controversial.

Opponents of the proposal that the entire reason people were transacting in blockchains like Ethereum was to rely on a technologically-enforced consensus instead of faith in some external authority.

Crucially, the hiccup in the software code was entirely public from the DAO's inception. Any backer interested in participating in the DAO had the opportunity to review the DAO's code first, and indeed this public availability of code is a central and defining feature of blockchain communities like Ethereum and the DAO. The participants who voluntarily staked in the neighborhood of $150 million worth of Ether before the attack hit had either overlooked this security flaw (one of several in the Dao's code) or had noticed it and decided to proceed anyway.

In other words, the attack had not done anything that the DAO's code had not been explicitly designed to facilitate—it may have been unwelcome, but opponents of the proposal argued it would set a dangerous precedent to allow some users to rewrite the rules for everyone every time they encountered an outcome they did not like.

Supporters of the proposal argued that the "code is law" argument was misguided. By this point of view, blockchain structures were nothing more than tools to help create and support a *human* social consensus that would be infeasible to develop in any community larger than the island of Yap. The attacker had victimized participants who had themselves opted to play fair, and should not be allowed to profit from that anti-social act.

Supporters of the proposal prevailed, with 89% of the vote. The Ethereum blockchain was formally changed, returning the balance to the DAO… and splitting off into a separate blockchain of their own those opponents who refused to go along with the change. That alternate version of Ethereum, where the attacker kept the 3.6 Ether obtained by recursive withdrawals, became known as "Ethereum Classic."

Exchanging Security

Mechanisms like Proof of Work and Proof of Stake are used to regulate the introduction of new coins into a blockchain system, but many users want to convenience and immediacy of being able to buy into and trade cryptocurrencies on demand. While it is possible to approach this question the same way Laszlo Hanyecz approached buying a pizza—that is, to find a willing counterparty and engage in a blockchain transaction in connection with a separate real-world transaction—this is as efficient as wandering the streets of Playa del Carmen hoping to find a local willing to trade pesos for dollars. It is far more sensible to transact using an exchange that brokers the buying, selling, and trading of crypto tokens. This world of brokers and exchanges, however, introduces new considerations for security that may not be immediately apparent.

In the world of traditional banking, a person can open an account with a bank by first presenting a variety of documents to prove their identity. The bank then deploys systems such as PIN codes and biometrics to verify that user's identity in subsequent interactions. In some cases, an attacker can successfully masquerade as that user and engage in fraudulent transactions in their stead, a practice commonly known as "identity theft." Although identity theft can be traumatic and even ruinous for victims, there are institutional and legal processes that victims can leverage to dispute transactions and seek redress. These processes may not always work as intended, but they exist within a context of national and international regulations around banks and financial institutions that are often publicly traded entities with decades or even centuries of history behind them.

Cryptocurrencies like Bitcoin emerged out of the financial crisis of the late 2000s when many people came to feel that those institutions and regulators had collectively failed. Blockchain systems eschew the idea that organizations can be expected to behave appropriately because of rules or laws, and instead substitute technological systems that are intended to behave in rigidly defined mechanistic ways. In executing this trade, users of blockchains become individually responsible for their own security. There is no board of directors or federal regulator to whom to turn in the face of a dispute, and if an attacker exploits a flaw in the code to steal your money you cannot even be sure your fellow victims will agree to even try to seek reimbursement.

This background is critical in understanding the special security considerations involved in exchanges. When a user joins a blockchain such as Bitcoin or Ethereum *directly*, to engage in mining and transactions using their own wallet, that user is responsible for protecting the secret key needed to access that wallet. Some people put their secret keys on encrypted flash drives that are kept in locked drawers, not connected to the Internet. Others keep secret keys written in ink on paper, in safe deposit box. Whatever technique is used, the point is that the user is individually responsible for protecting that irreplaceable asset. If it is forgotten or lost, it cannot be recovered—in contrast to the routine practice of resetting a password to an online bank account.

When a user transacts *through an exchange*, however, that intermediary is the one that has the wallets, which are administered on the customer's behalf. The customer typically goes through an authentication process to set up the account with the exchange that resembles setting up a bank account—and probably accesses the exchange through a smartphone app or web portal not unlike a bank's.

The irony of this situation is that the blockchain community arose in part out of a lack of confidence in the reliability of publicly-traded financial institutions overseen by federal regulators, but any user who chooses to participate in the blockchain community through an exchange is choosing to place a comparable level of faith and trust in a business that is more likely than not a private unregulated entity that has been in business less than ten years.

As an illustration, consider the tale of QuadrigaCX, once the largest cryptocurrency exchange in Canada. In December 2018, it was reported that the company's founder and CEP, Gerald Cotton, had died while traveling in India. As initially reported, Cotton's death rendered the totality of QuadrigaCX's digital assets inaccessible, because Cotton was alleged to be the sole party with knowledge of the secret keys to the wallets. At the time, QuadrigaCX had some 115,000 customers with reportedly US$190 million in various digital assets held in those wallets.

There are other dimensions to this story that are still being investigated and litigated, including various allegations that QuadrigaCX had never engaged in any real crypto trading at all. Even if nothing more damning than the originally reported story turns out to be true, that alone is a sobering conclusion. Each of those 115,000 customers thought of themselves as the "owner" of certain cryptocurrencies, but did not directly control the secret keys to the wallets that held them. There is a longstanding aphorism in the blockchain world that "if you don't own the keys, you don't own the crypto."

This maxim is easier said than done, however. Part of the beauty of the Yap economy was the way islanders did not need to carry Rai stones around in order to spend them, but translating that idea into technological terms is imperfect. It is admittedly awkward to have to protect a physical object (like a flash drive or a piece of paper) that contains the key to access an intangible asset like cryptocurrency.

Even technically proficient persons often find the process of securing secret keys to be off-putting, meaning this will likely remain a significant barrier to entry to the larger population of laypersons who may wish to join the blockchain economy. The familiar interfaces and user-friendly interactions provided by exchanges smooth over that awkwardness and make the world of cryptocurrency more accessible to non-technical consumers, but at the cost of reintroducing security risks that the blockchain's design was meant to eliminate. To expand the community of blockchain users without expanding the risk profile, it will be important to develop more user-friendly methods of secret key management.

Presented by David Kalat, Director, Berkeley Research Group – Global Investigations + Strategic Intelligence

Mr. Kalat is testifying expert in digital forensic investigations, electronic evidence, and data analytics. He is a Certified Fraud Examiner (CFE), a Certified Computer Examiner (CCE), a Certified Information Systems Security Professional (CISSP), a Certified Telecommunications Analyst, and a licensed private detective in Illinois and Texas.

He holds a Master's Degree in Information Science from the University of Illinois at Urbana-Champaign, and earned his Bachelor's Degree from the University of Michigan. Mr. Kalat leads the Chicago digital forensics lab for BRG's Global Investigations + Strategic Intelligence practice.

He is a member of the Sedona Conference and EDRM, and publishes a monthly column for LegalTech News on the history of information technology and information security.

David Kalat, CISSP, CCE, CTA, CFE | Director
Global Investigations + Strategic Intelligence

Berkeley Research Group, LLC
70 W. Madison, Suite 5000 | Chicago, IL 60602
O 312.429.7907 | F 312.629.5299
dkalat@thinkbrg.com | thinkbrg.com