Updates
February 19, 2019
Blockchain Attacks and the Fight for Immutability

The Ethereum Classic blockchain was the victim of a 51% attack (often called a majority or Sybil attack) on January 5, 2019 that reorganized portions of the blockchain and allowed the attackers to double-spend 219,500 ETC ($1.1 million). As a result of this attack, and similar majority attacks over the past year, the concept of immutability within blockchain technology has been revealed to be a potentially costly oversimplification. If determined foes can alter a blockchain, even temporarily, then many blockchain systems may be more fragile than is commonly perceived. These attacks show that protecting the permanence of data on the blockchain cannot be assumed, but instead is an evolving challenge and an important consideration for those who design, manage, participate in and rely upon blockchain networks for their businesses.

This update presents a more nuanced understanding of blockchain immutability, along with providing a practical understanding of mining algorithms, market trends and how they relate to the efficacy of blockchains serving as immutable repositories of transaction data. The update concludes by summarizing some of the ways that market participants are using legal solutions to mitigate risks and respond to attacks.

Describing Immutability for Public Blockchains

When applied to blockchains, the term "immutability" is relative. In practice, immutability often means different things to different people, and not all blockchains are created equal when it comes to the irreversibility of transactions. Most people can agree that data permanence and auditability are a critical part of the design for public-permissionless blockchains. For example, it is the driving force behind Bitcoin and many other virtual currencies that need to make sure that the same virtual currency is never spent more than once, duplicated or falsified (i.e., avoiding the double-spend problem). To accomplish this goal, virtual currency protocols utilize various hash functions[1] to link blocks of transactions and implement a competitive (and often resource intensive) mining process to validate each consecutive block on the ledger. The combination of these methods allows for users to have certainty that each block follows orderly from the last without missing any transaction previously written to the chain.

Many public blockchains, particularly Bitcoin and Ethereum, have largely managed to avoid catastrophic cybersecurity issues related to their core function because their core architecture is robust. An element of this sturdiness comes from several sources, including their well-understood and simple hashing algorithms (SHA-256 for Bitcoin and KECCAK-256 for Ethereum), the number of nodes in operation, and the straightforward method by which mining and validation is accomplished.[2] For Bitcoin, Ethereum and many other public blockchains that rely on proof-of-work mining algorithms, any node can directly participate in mining. Further, each node's expected revenue from mining is proportional to its mining power—also known as "*hash rate*." These activities combine to provide a robust and (usually) immutable system that ensures a significant computational effort must be employed to validate the next block in the chain. This computational cost of mining is also magnified the deeper you go into the chain, making it exponentially more resource intensive for any one miner (or group of miners) to expend enough computing power to change older transactions in historical blocks.

Until recently, the most commonly perceived threats to virtual currencies were not associated with the security of the blockchain protocols themselves. Instead, the greatest risks (outside of losing your private key) appeared to be from cybercriminals who, through hacking, social engineering or other means, gained access to exchange accounts or other digital wallets outside of the blockchain itself.

Majority Attacks, Block Reorganizations and Eclipse Attacks

Generally, a participant's proportion of the total network hash rate determines the likelihood that it will decide the next block in the chain (and therefore decide the current shared truth among all participants in the network). However, if a participant (or group of participants) gains a sufficient proportion of the total hash rate (i.e., a 51% majority of the network resources), it can undermine the integrity of the network by reordering blocks, or otherwise altering the shared truth through a number of attack vectors. This potential weakness is inherent in many blockchains built on proof-of-work mining algorithms, and that is key reason that blockchain developers support a diverse and distributed hash rate pool.

If attackers can control 51% of the total network hash rate, there are many paths at their disposal to damage the network. Under certain conditions, attackers can build their own chain faster than the actual network and can broadcast their false version in a manner that the network accepts as real. During the time that the attackers have control, they can reverse any transaction that they submit or prevent transactions from being included in a block. Attackers can also reorder subsequent transactions (i.e., block reorganizations) that change past transactions in historic blocks that have already been confirmed.

Fortunately, there are things that attackers cannot do when they control 51% of the hash power of a blockchain network. Generally, they cannot change the main parameters of the network within the core protocol. It also becomes exponentially more difficult to change older blocks the further into the past you go. For better or worse, many digital assets today are built on existing blockchain networks (e.g., ERC-20 standard digital assets on Ethereum). This concentration is a double-edged sword. On one hand, it means that young blockchain projects that use an ERC-20 token are relatively safe in relying on Ethereum hash power to protect their transactions. On the other hand, it means that if Ethereum (the underlying blockchain network) is compromised, all other digital assets built on the blockchain network will be similarly affected.

To be clear, majority attacks are not the only attacks that blockchain networks face. There are many other well-documented and researched attack vectors on public blockchains. One other style of attack that warrants mention is an eclipse attack because such an attack does not rely on hash rate to execute successfully. An eclipse attack occurs when an attacker identifies the specific set of nodes on a blockchain network that the victim utilizes to monitor and commit transactions (Bitcoin and Ethereum connect with 8 or 13 nodes respectively). Once these nodes are identified, the attacker isolates its victim by hijacking the connecting nodes and impersonating the nodes in future transactions. A successful eclipse attack allows the attacker to dictate its own version of the truth to the victim without expending computational resources on a majority attack (i.e., eclipsing the victim's access to the broader network).

Current Mining Pools, ASICs Providers and Hash rate Markets

Collectivized mining operations (i.e., mining pools) that pool hash rate for larger and more predictable payouts have existed since the early days of Bitcoin. These operations provide a user-friendly way for ordinary people to contribute (or purchase) hash rate and collaboratively mine without the difficulties associated with setting up and maintaining their own node on a blockchain network.

Because mining pools concentrate hash rate in the hands of pool operators, if they reach the 51% threshold hash rate they could potentially pose a threat to blockchain networks. In practice, however, mining pools are dependent on the many individual miners who participate in the pool, and who may move elsewhere if they disagree with the activities of the mining pool operators. This provides a reputational check on mining pools being used to attack the network. Some mining pools today have also shifted their focus towards other profit

generating activities (e.g., "generalized mining" or "staking") and have ceded significant amounts of the overall hash rate on blockchain networks to other participants.

Network Participants	Activities	Network Security Advantages	Network Security Disadvantages
Mining Pools	Aggregate individual miners for consistent profit.	Pool managers make it easier for hash rate to transition during upgrades to the network. Reputational checks on activity.	Centralization and concentration of hash power, can influence network decisions and self-deal.
ASIC Providers	Develop, use and sell dedicated mining hardware.	Contributes to significant increases in overall network hash power. Competition can check influence.	Centralization and concentration of hash power can cause short-term network hash power imbalances, particularly if provider is mining using ASICs that are not available to the public. New ASIC products can harm the market and hurt consumer mining in particular.
Cloud Miners/Hash rate Rental Markets	Provide remote access to mining resources for a fee.	Trivializes network resource access and increases efficiency of entire mining market. Supports broader competition among service providers and reputation is still important.	Centralization and concentration of hash power, increases access to network resources and broadens potential attack sources.

Figure 1. Network Advantages and Disadvantages for Mining Participants

Increased competition for mining rewards has driven the creation of a market for specialized mining hardware (e.g., application-specific integrated circuits or ASICs) designed to outcompete traditional hardware (e.g., ordinary computer CPUs and GPUs). Companies that specialize in the production, use and eventual sale of ASICs are among the largest contributors of hash rate and consequently may wield a disproportionate level of influence over the technical direction and security of large blockchain networks. Increased attention has been drawn to the question of whether large ASIC mining organizations may assert leverage over blockchain developers and their communities in a way that influences which blockchains are supported through hash power and consequently which networks are most secure.

Among other developments in the mining community is the growth of hash rate rental marketplaces. Hash rate rental markets allow customers to buy and sell hash power for a fee and potentially trivialize the difficulty of gaining access to blockchain network resources. As a positive, these efforts further decentralize network hash power and may diminish the influence of large blockchain mining organizations and their ASICs. Hash rate rental markets have also allowed for greater transparency into the cost to maintain a majority attack against various blockchain networks with some shocking results. However, some experts point to the recent surge of majority attacks on some of the largest blockchain networks that may be the result of hash rate markets.

Recent Attacks, Public Attention and Market Response

The convergence of efforts by some market participants to exploit hash rate and/or compromise blockchain networks has gained increased public attention in the last year. In May 2018, Bitcoin Gold was majority attacked resulting in $18 million in damages. Commentators predicate the attack on Bitcoin Gold making fundamental changes to its core architecture designed to support ASIC resistance. These efforts inadvertently caused Bitcoin

Gold to have a relatively low hash rate to support the network, and this was exploited by the attack. Currently, some websites list the cost of conducting a majority attack against Bitcoin Gold at only $297 per hour. In December 2018, Vertcoin was subject to a majority attack that resulted in $100,000 in double-spends. Vertcoin was exploited in the same way as Bitcoin Gold, where the attackers initiated double-spends by spending virtual currency on the main chain and then publishing their own version of the chain that reorganized or removed the previous transactions, thereby returning their previously spent virtual currency. The most recent high-profile example of a majority attack occurred on the Ethereum Classic blockchain, which resulted in the suspension of trading on several major centralized exchanges and caused millions of dollars in damages and losses.

In each instance, attackers relied on virtual currency exchanges to escape with their ill-gotten gains. As a result, these exchanges have stepped-up measures to monitor anomalous blockchain network activity and have in some instances delisted attack-prone virtual currencies. Developers are also taking steps to improve security. During the recent Ethereum Classic attack, developers encouraged mining pools to take matters into their own hands by increasing confirmation times, thereby making deep blockchain reorganizations more difficult to accomplish. While these activities help address some of the short-term impacts of majority attacks, they do not deal with the broader systemic problem.

Although public attention on majority attacks has increased, blockchain developers have always known about the risk of majority attacks inherent in the blockchain model. Accordingly, some developers have designed processes to combat or avoid this attack vector altogether. For example, some public blockchains do not rely on proof-of-work mining algorithms for consensus and are therefore generally able to avoid hash rate concentration risks (but not necessarily majority attacks). More novel methods of combatting majority attacks are starting to crop up as well. Some companies are researching and developing products designed to combat the economic incentives driving majority attacks, including network bonds that can pay miners to support and protect a network regardless of the coin's profitability, reducing the possibility of an attack.

Private Rights of Action, Enforcement and Other Legal Solutions

Like traditional cybercrime, attacks directed at virtual currencies and blockchains require both technical and legal solutions. From an enforcement perspective, those who attack the integrity of blockchains may be liable for a range of criminal and civil violations, including wire fraud and the unauthorized access into protected computer networks under the Computer Fraud and Abuse Act (CFAA). The CFAA also allows victims to bring private civil actions in federal court to obtain both compensatory damages and injunctive relief to prevent further attacks. Even in cases where the identity of those responsible for the attack is unknown, which is generally the case, plaintiffs can file "John Doe" complaints against unknown defendants. Plaintiffs can then use the power of the civil discovery process to issue subpoenas to third-party service providers, digital trading platforms, custodial wallet services and a range of other entities that will likely have valuable information that can be used to connect the crime to the perpetrator and assist in the recovery of stolen digital assets.

While there has been much emphasis placed upon the anonymity of Bitcoin and other virtual currencies, there are ways to peel back the layers to identify the internet protocol addresses, nodes and wallets used in an attack. Today more than ever, know-your-customer rules and other anti-money laundering regulations require trading platforms and other money service providers to verify the identities of those using their services. Further, services like Chainalysis, Elementus and Elliptic can be used to conduct blockchain network analysis to trace stolen digital assets to transfer, entry and exit points that can also lead to unmasking the identities of those involved.

Often complementing these private rights of action, the attackers may also become the subjects of fraud investigations by the Commodities Futures Trading Commission (CFTC) pursuant to violations of the anti-fraud

provisions in the Commodity Exchange Act (CEA).[3] The CFTC may use its general anti-fraud and anti-manipulation authority to police public blockchain networks both to deter the risk of cyberattacks from affecting digital asset derivatives markets and for investor protection purposes. It is particularly likely to focus on cyberattacks that could affect the Bitcoin blockchain because several derivatives exchanges currently list bitcoin futures, options and swaps products, which could be affected by majority attacks. Moreover, the CFTC may begin to more closely monitor other blockchains as new derivatives products, such as ether futures, emerge and if the public pressures the agency to protect investors in digital asset markets more broadly.

Majority attacks are also market manipulations that have analogues in traditional commodity markets. For example, "spoofing" is the manipulative practice of entering orders into an exchange's order book with the intention to cancel the orders before they are matched. In such a case, the trader uses a high-speed connection to an exchange to submit false information into the market and withdraw the information within milliseconds to defraud other traders. Similarly, the purpose of a majority attack is to use hash rate to submit false transaction data to the blockchain and defraud digital asset holders. Accordingly, the CFTC is not likely to shy away from these incidents due to the novelty of blockchain technology.

With a more nuanced understanding of blockchain immutability, market participants can make more informed business and legal decisions. This includes decisions about the design and use of various blockchains, the types of legal contracts to create (including digital contracts), and potentially how to assign and diversify risk in advance. For the myriad of companies whose services are now built on blockchains, this also includes not overstating security, making adequate disclosures and developing thorough terms of service. While there may be a need for new laws in certain areas, and clarity from regulators in many others, thoughtful participants can also act to protect themselves under our current legal frameworks.

Please contact experienced counsel with any questions regarding these developments and how they may affect your business.

ENDNOTES

[1] Cryptographic hash functions are mathematical operations run on digital data. By comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity. A one-way hash can be generated from any piece of data, but the data cannot be generated from the hash.

[2] Mining on the Bitcoin blockchain is CPU intensive and relies on a proof-of-work mining algorithm based on SHA-256. By contrast, mining on the Ethereum blockchain is more GPU intensive and relies on a separate proof-of-work mining algorithm known as Ethash.

[3] The commodity laws give the CFTC broad authority to prohibit and prosecute fraud, deception, price manipulation, etc. with respect to transactions in commodities, including in respect of spot transactions and, more specifically, transactions that involve virtual currencies. *See* Sections 6(c) and 9(a)(2) of the CEA and CFTC Regulations 180.1 and 180.2; see also *CFTC v. Gelfman Blueprint, Inc. and Nicholas Gelfman,* No. 1:17-cv-07181 (S.D.N.Y. Sept. 21, 2017); *CFTC v. My Big Coin Pay, Inc., Randall Crater, and Mark Gillespie,* No. 18-10077-RWZ (D. Mass, Jan 16, 2018); *CFTC v. Patrick K. McDonnell, and CabbageTech Corp. d/b/a Coin Drop Markets,* No. 18-cv-0361, (E.D.N.Y. Jan 18, 2018).

Michael Maloney of Themys.io contributed to this article.

Authors

Explore more in

Blockchain & Digital Assets

Related insights

Update

Trends in the Growth of Investment in US Data Centers Under the Trump Administration

Update

California Senate Bill 399: Captive Audience Law Challenged in Federal Lawsuit