

Blockchain Threat Report

Blockchain, a Revolutionary Basis for Decentralized
Online Transactions, Carries Security Risks



Table of Contents



- 5** Blockchain attacks
 - 5 Phishing
 - 6 Malware
 - 8 Cryptojacking
 - 9 Endpoint miners
 - 11 Implementation vulnerabilities
 - 13 Wallet theft
 - 13 Technology attacks
 - 15 Legacy attacks modernized
 - 15 Dictionary attack



- 20** Exchanges under fire
 - 20 Major events
 - 24 Recovery



- 26** Conclusion



Blockchain consumers are often the easiest targets—due to a start-up mentality in which security takes a backseat to growth

Introduction

In late 2017 the cryptocurrency Bitcoin hit the headlines in a big way. Its value skyrocketed to almost **US\$20,000 per coin**, waking up major news organizations and catching the eyes of would-be investors. Bitcoin, the leading cryptocurrency, is based on blockchain, a revolutionary new technology. **Blockchain**, which records transactions in a decentralized way, has begun to change the way we look at money and offers a path to solve old business problems in new ways.

However, with new technologies come new security concerns. Bad actors have already targeted many blockchain implementations using social engineering, malware, and exploits. As additional groups begin using blockchain and building tools around it, they must understand the security risks. In this report we will look at current security problems and specific incidents within blockchain implementations. We will cover bad actors' techniques, targets, and malware used for attacks.

In 2009, the first implementation of a blockchain, Bitcoin, raised excitement among technologists and researchers. It appeared to be a feasible solution to an age-old problem: how to ensure agreement among peers. Blockchain accomplished this by means of rigorous research resulting in a decentralized payment system in which peers could agree and trust a ledger, which represents the current state of the network. This agreement enabled previously untrustable decentralized payment systems and promises much more.

This report was researched and written by:

- Charles McFarland
- Tim Hux
- Eric Wuehler
- Sean Campbell

Follow



Share



REPORT

What exactly is blockchain? A blockchain is a series of records or transactions, collected together in a block that defines a portion of a ledger. The ledger is distributed among peers, who use it as a trusted authority in which records are valid. Each block in the ledger is linked to its next block, creating a chain—hence the name. Anyone can look at the latest blocks and their “parent” blocks to determine the state of an address. In the case of cryptocurrencies, we can determine the value of an address and trace every transaction leading to the creation of each contributing coin. Validating the transactions is vital. Each node can individually verify the accuracy of each chain.

But how does each node know that a chain has not been modified even if the transactions add up? A key element of blockchain technology is how it chains blocks together. Using hashing functions, a new block embeds integrity information of its parents. If information from a parent changes, then the hash will change—breaking the validation process. Further, at the creation of each block, a proof must be supplied. This proof shows that some resource was expended to create the block.

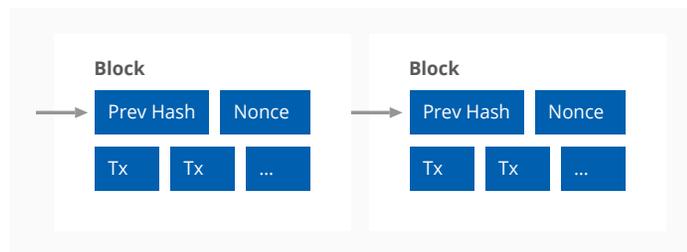


Figure 1: Proof-of-work blockchain

Source: <https://bitcoin.org/bitcoin.pdf>

The creation of each block is called mining, and the proof required to mine is different with each blockchain implementation. The most common is proof of work, a CPU-intensive algorithm that requires a solution to all steps of a problem. There are no known mathematical shortcuts. Discovering the correct solution to a problem proves that the all steps have been completed, in this case using CPU resources. It takes a lot of work to discover the answer, but it is relatively simple to validate that an answer is correct. Because each block requires extensive proven work and subsequent blocks are chained together, one can validate that the longest chain required the most work and is the most trustworthy. It would take an enormous amount of resources for an attacker to create a longer chain and overtake any popular ledger. Combining the integrity checks with the hashing functions within blocks as well as the proof of work allows entire networks of people to trust the records in a distributed ledger.

Cryptocurrencies are blockchain implementations primarily focused on monetary value and transactions. They represent the most common use of blockchain. However, not only money can be recorded in a blockchain ledger. Bitcoin allows a small amount of additional data to be stored in its transactions. [Researchers have found](#) leaked documents, arbitrary data, and even pornography stored and retrievable in the Bitcoin ledger. Some ledgers are designed to store entire programs that can be executed by participants of the blockchain. Ethereum, the second-most popular cryptocurrency, does this with a “smart contract.” In that implementation, the code, or contract, is uploaded to

Follow



Share



REPORT

the ledger. That code can then be executed by anyone. The effects of executing the contract depend upon the rules programmed by its creator. In a simple example, the contract could set up an escrow account to hold funds until both sides meet their obligations. When someone wishes to execute the contract, the computing power is paid by using “gas,” a form of payment for miners. Gas assigns a cost, in Ethereum coins, to all smart contracts to prevent excessive executions that could slow the network.

Some industries are looking at solving their business problems with custom blockchains. For example, [a major retailer](#) has filed patents to use blockchain to track and secure shipments. Enterprise blockchain platforms [have been developed](#) to tackle the growing demand for additional implementations.



Blockchain attacks

In most cases, the consumers of blockchain technology are the easiest targets. Due to a widespread start-up mentality, in which security often takes a backseat to growth, cryptocurrency companies often fall in this category. This category includes those in the business of large, well-adopted blockchain implementations such as Bitcoin and Ethereum. Attackers have adopted several methods to target consumers and businesses using well-established techniques. The primary attack vectors include:

- Phishing
- Malware (examples: ransomware, miners, and cryptojacking)
- Implementation vulnerabilities
- Technology

Phishing

Phishing scams are the most familiar blockchain attacks due to their prevalence and success rate. Consider the Iota cryptocurrency. [Victims lost \\$4 million](#) in a phishing scam that lasted several months. The attacker registered `iotaseed[.]io`, providing a working seed generator for an Iota wallet. The service worked as advertised and enabled victims to successfully create and use their wallets as expected, providing a false sense of security and trust. The attacker then waited, patiently taking advantage of the building trust. For six months, the attacker collected logs, which included secret seeds, and then began the attack. In January, using the information previously stolen, the attacker transferred all funds from the victims' wallets.

Follow



Share



REPORT

Cybercriminals do not generally care who their phishing victims are. As long as cryptocurrency ends up in the attackers' hands, all victims are fair game. Such was the case in a Tor man-in-the-middle attack. The Tor network is commonly used to hide a browser's location from snooping third parties. Many employ Tor to create hidden services from which consumers can buy and sell goods. Cryptocurrencies are the preferred or only form of payment. These services are also where ransomware families often hide their payment systems. Some are not aware of Tor, so for convenience, easily accessible Tor proxies are provided to help victims reach these sites and recover their files. Generally, these include Tor proxy domains they have found through a search engine or were directed to by ransomware instructions. Unfortunately for the victim, the attacker may not receive the victim's ransom. In some cases, funds were redirected to an unrelated wallet using a malicious proxy. This happened in early 2018 when a Tor proxy service [was discovered](#) replacing Bitcoin addresses related to ransomware with addresses under its control. Security researchers found the operators scouring sites on the dark web for Bitcoin wallets behind the Tor-to-web proxy service onion[.]top. When a wallet was located, the cyberthieves replaced the address with one of their own.

Malware

In 2016 new ransomware families exploded in number. They were the primary tool used by bad actors to acquire cryptocurrency. Ransomware was not new but became a favorite due to the benefits of transferring and hiding funds through cryptocurrencies. Cybercriminals also had easy-access tools, especially HiddenTear, which was meant to be an "educational" tool on ransomware but was quickly used by bad actors to build [hundreds of variants](#). These variants generally required Bitcoin payments for ransom, with a few exceptions such as [Monero](#) with the [Kirk ransomware](#).

In 2017, ransomware developers broadened their interest in currencies. Malicious actors began experimenting with various alternative cybercurrencies, also known as altcoins. Monero was a favorite alternative, while lesser-known coins, such as Dash, attracted attention. The ransomware GandCrab discarded Bitcoin in favor of Dash. [GandCrab was added](#) into the popular RIG exploit kit, along with a variety of malware. GandCrab and other malware launched frequent attacks against Microsoft Internet Explorer and Adobe Flash Player through malvertising.

Follow



Share



REPORT

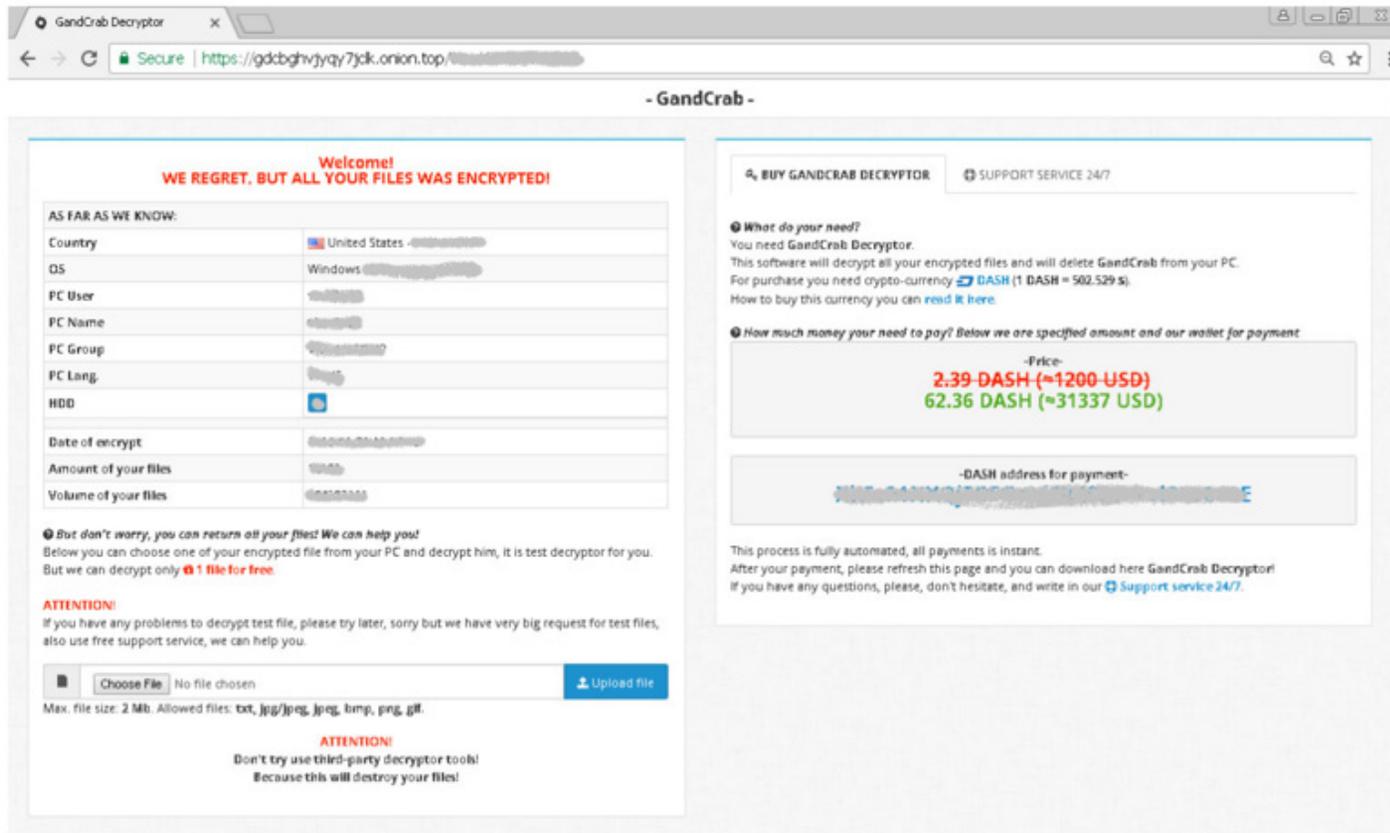


Figure 2: A GandCrab decryption page accessed through an onion.[.]top Tor proxy.

Ransomware developers also adopted the mainstream coin Ethereum in early 2018. Planetary, a variant of HC7, is the first ransomware known to target Ethereum, though not exclusively. To give victims options and

greater incentive, Planetary allows them to pay the equivalent of \$700 per infected system or \$5,000 for all the nodes infected on the victim's network. The ransomware also accepts Bitcoin and Monero.

Follow   

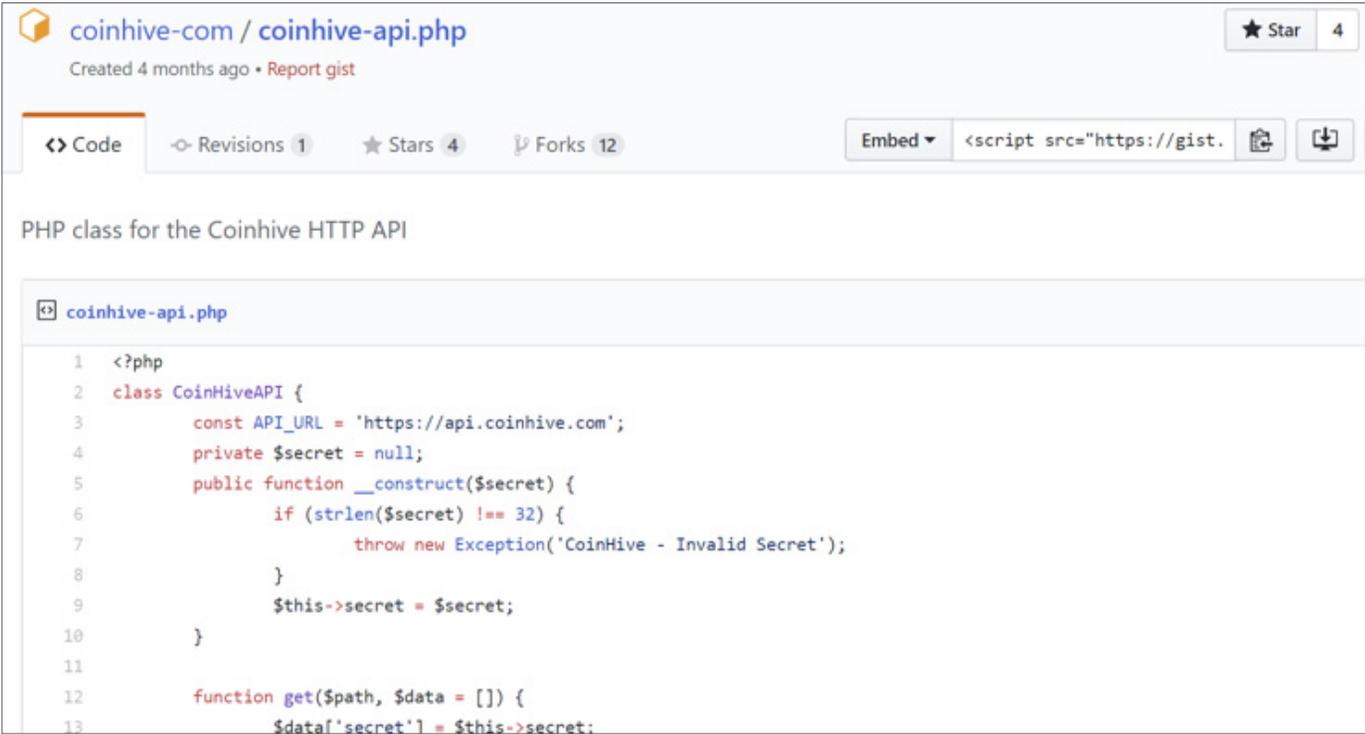
Share   

REPORT

Cryptojacking

Cryptojacking is the method of hijacking a browser to mine cryptocurrency and has surprisingly shown a resurgence. Much like ransomware, cryptojacking campaigns experimented with altcoins. In late 2017, the Archive Poster plug-in for the Chrome browser was found to be [mining Monero coins](#) without consent. Victims first learned of the issue when some started complaining of high CPU usage. By that time more than 100,000 people had downloaded the miner. At least four

versions of the application included the cryptojacking JavaScript code from Coinhive, which easily embeds mining into websites or tools, originally with a simple-to-use open-source API. Cryptojacking resides in a gray area. Many organizations implement Coinhive and other miners to monetize their visitors' device resources. If they agree, then mining is considered not malicious, though potentially unwanted, behavior. However, many sites do not disclose mining, and visitors are left uncertain about slow performance.



The screenshot shows a GitHub Gist page for a PHP class named 'CoinHiveAPI'. The page title is 'coinhive-com / coinhive-api.php' and it was created 4 months ago. It has 4 stars and 12 forks. The code is as follows:

```
1 <?php
2 class CoinHiveAPI {
3     const API_URL = 'https://api.coinhive.com';
4     private $secret = null;
5     public function __construct($secret) {
6         if (strlen($secret) !== 32) {
7             throw new Exception('CoinHive - Invalid Secret');
8         }
9         $this->secret = $secret;
10    }
11
12    function get($path, $data = []) {
13        $data['secret'] = $this->secret;
```

Figure 3: Coinhive API.

Source: <https://gist.github.com/coinhive-com/dc37d300b2f4f909006a07139c9d2c71>

Follow



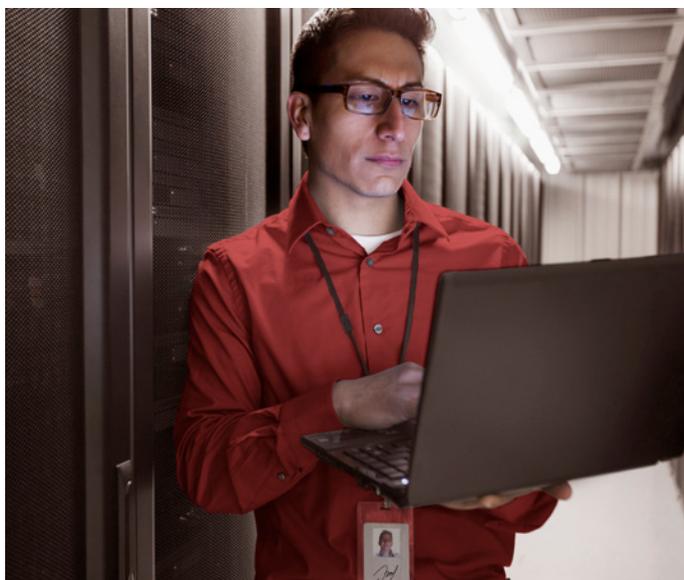
Share



REPORT

The website owner might not be the one who added the cryptojacking code—[this was the case](#) with YouTube. A flaw in the popular video-sharing site allowed malicious advertisers to inject cryptojacking code into advertisements to mine Bitcoin or Ethereum. (YouTube swiftly removed the malicious advertisers from their network and blocked the mining advertisements.) Cybercriminals have taken years of malvertising lessons and customized that knowledge to suit their cryptocurrency campaigns.

Nearly 30,000 sites are known to host [Coinhive code](#) for mining—with or without consent. This count is only of non-obfuscated sites. The actual number is likely much higher. As this behavior receives more scrutiny, we can expect many more cryptojacking miners to be uncovered.



Endpoint miners

Prior to 2016, malicious coin mining was one of the primary methods to acquire cryptocurrency. Although less common than ransomware, mining had an explosive resurgence in late 2017 and early 2018. New miners appeared quickly and old malware was retooled with mining capabilities. Families of ransomware even began to double dip by including mining functionality. For example, Black Ruby was [discovered early 2018](#) and demands \$650 in Bitcoin for ransom. The malware uses the popular open-source XMRig Monero mining software on infected devices. Another large-scale mining operation [discovered in January 2018](#) also uses XMRig. Open-source tools such as these partially contributed to the dramatic increase in mining malware.

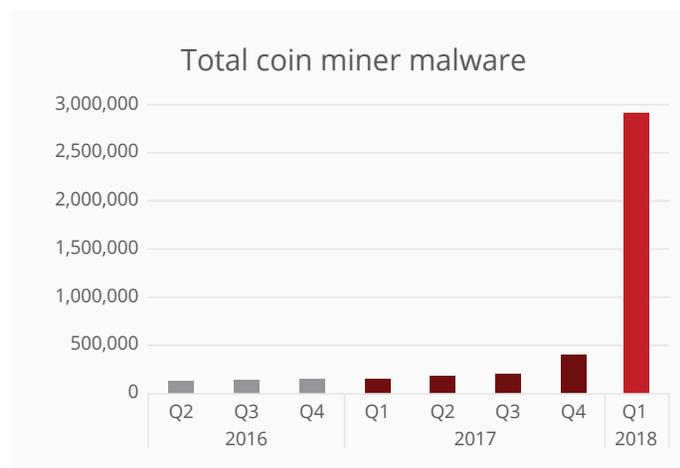


Figure 4: Coin miner malware has grown explosively. Source: McAfee Labs

Follow



Share



REPORT

In the past six months, many malware developers appear to have migrated from ransomware to cryptocurrency mining, according to McAfee® Global Threat Intelligence data that show ransomware attacks declining 32% in Q1 2018 from Q4 2017 while coin mining increased by 1,189%. Miners primarily target PCs, but other devices are also victims. For example, in China, Android phones were exploited to mine Monero coin by ADB.Miner, which acts as a worm and runs over port 5555, which is more commonly used for the ADB debugging interface. Devices were also infected with the XMRig miner. A query on shodan.io shows more than one million internet-facing devices running on port 5555. A subset is the XMRig miner. ADB.Miner was discovered

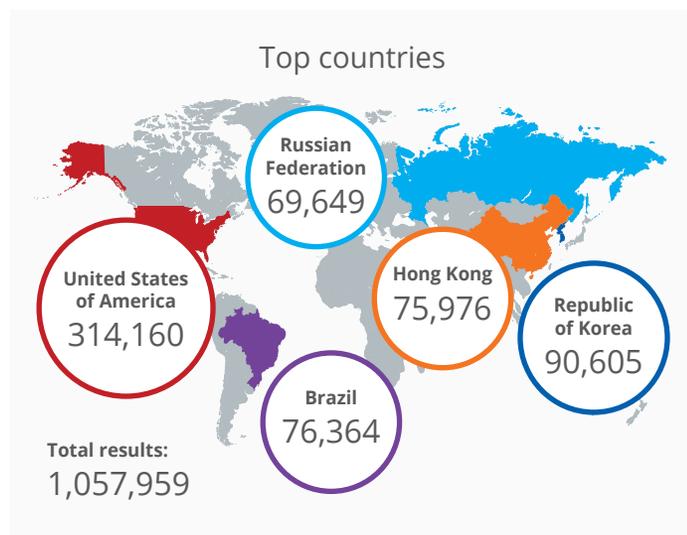


Figure 5: A Shodan.io search for port 5555 devices.

reusing code from the Mirai botnet, which surfaced in mid-2016 and has been observed in a variety of global attacks. As of February 2018, the threat actors behind the malware have infected about 7,000 devices, mostly located in China and Korea.

In some cases, the attacks targeted specific groups rather than using a blanket approach. One malicious miner was aimed at unsuspecting gamers on a Russian forum, with the malware disguised as a “mod” to enhance popular games. Gamers were tricked into downloading the malicious software, which used their computer resources for profit. To maintain persistence and not arouse suspicion, the miner watched for open window titles, such as Windows Task Managers, Process Hacker, or other process managers. If seen, it halted mining operations, thus hiding its activity. The suspected author behind this operation is alleged to be the key actor behind other game “cheat” software and is known to post his malware on multiple Russian forums with little concern for maintaining anonymity.

It can be costly and time consuming for bad actors to write their own malware. Rather than research and write their own exploits, many malware authors choose publicly disclosed exploits and known vulnerabilities, assuming that a significant number of machines remain unpatched and open for attack. This assumption frequently proves to be true. In the second half of 2017, the illegal miner Smominru is estimated to have created more than \$3 million in Monero coins. The campaign

Follow



Share



REPORT

takes advantage of the EternalBlue exploit, which was publicly leaked by the Shadow Brokers hacking group. This exploit made headlines with the highly successful malware [WannaCry](#), which impacted machines across the globe. The exploit, which takes advantage of a flaw in the Server Message Block v1 protocol in Microsoft Windows, was disclosed in bulletin [MS17-010](#).

Smominru was not the only malware family that profited from EternalBlue. WannaMine, a Monero miner, also uses the EternalBlue exploit to propagate through the network. For the initial infection, WannaMine employs common phishing emails to launch a batch file and download a malicious PowerShell script from its control server. It then uses XMRpool to connect the device to public mining pools—turning the victim’s system into an unwilling participant. The following three connections strings were used to connect the victim to the mining pools.

```
stratum+tcp://pool.supportxmr.com:80
stratum+tcp://mine.xmrpool.net:80
stratum+tcp://pool.minemonero.pro:80
```

In another example, using [CVE-2017-10271](#), attackers turned Oracle WebLogic servers into a [Monero mining botnet](#). (Oracle has since patched the vulnerability.) Despite the threat actors having a presence on the servers, they apparently had no interest in stealing data or profiting from ransom. Their lack of action in data theft gave evidence to the value they place in mining.

Implementation vulnerabilities

Another type of threat is an attack against the blockchain implementation itself, as well as its supporting tools. However, the closer one gets to the core of blockchain technology, the more difficult it is to succeed with an attack. Generally, these threats are much more like exploits of traditional software and web applications.

The Bitcoin wiki [maintains a list](#) of Common Vulnerabilities and Exposures related to their official tools. These vulnerabilities have resulted in denial of service attacks, coin theft, and data exposure among others. Although vulnerabilities can be quite impactful, they are commonly discovered and fixed after release. It is difficult to build and maintain secure code; the popularity and explosive growth of blockchain has exacerbated this problem. The discovery of high-severity vulnerabilities related to core Bitcoin tools has slowed, offering consumers a sense of confidence. The same confidence cannot be attributed to community and third-party tools.

In February 2018, a zero-day exploit struck PyBitmessage, a peer-to-peer message transfer tool that mirrors Bitcoin’s transaction and block transfer system. PyBitmessage uses the blockchain concept proof of work to “pay” for message transfers and reduce spam. Attackers used this exploit [to execute code](#) on devices by sending specially crafted messages. They then ran automated scripts looking for Ethereum wallets while also creating a reverse shell for further access.

Follow



Share



REPORT

Third-party tools are generally an easier target because they have smaller communities and fewer resources to secure their code or respond to problems. In rare cases we see a compromise of the implementation itself. Such was the case, [disclosed in mid-July 2017](#), against Iota. The vulnerabilities allowed attackers to create hash collisions and forged signatures, enabling them to steal coins from other wallets. The flaws have been fixed, but they required, in part, a hard fork on the network to remove [the use of Curl](#), a custom-built cryptographic-hashing function. The problem arose from breaking the golden rule of cryptography: “Don’t create your own crypto.” Cryptography is an incredibly difficult technology to get right. Any customized code or changes to crypto-related functions should be heavily vetted prior to production. Even established technologies may have issues arise, as evidenced by the industry’s migration from MD5 to SHA-1 to SHA-256 hashing functions, due to fundamental security flaws.

We can cite more examples of insecure implementations of blockchain. The Verge development team was ill equipped to deal with numerous vulnerabilities in its implementation when it was [attacked in early April](#). Attackers took advantage of the flaws to mine new coins without spending any mining power. The patch had the unfortunate side effect of “forking” the coin—essentially creating a new coin separate from the original coin. The effect on the value of the coins remains to be seen, but it is expected to significantly impact Verge’s ability to stay relevant.

In blockchain implementations such as Ethereum, user code is part of the ledger through smart contracts. A smart contract is written by a user and submitted as part of the ledger. The contract can execute logic based on the rules of the contract. Others can participate, if allowed, creating a self-sustaining decentralized application available to all. Like any code, it may come with bugs and vulnerabilities. The Parity wallet library, used in conjunction with Ethereum smart contracts, was found to have [a critical vulnerability](#) in November 2017. The issue, found by accident, allows an attacker to render some multisignature wallets unusable and to lock out account holders. This resulted [in the freezing](#) of \$150 million worth of Ethereum coins. The scale of this attack surpassed the previously largest smart contract hack, which resulted in the loss of more than \$50 million in value. [In this attack](#) against “the DAO,” an autonomous organization built on Ethereum, a hacker used a recursive bug to siphon funds.

Follow



Share



Wallet theft

In January threat actors [were discovered](#) circumventing internet-facing mining hosts and changing the wallet addresses on the hosts to an address under the actors' control. Cybercriminals made the wallet swap by bypassing the management port of the popular mining software Claymore Miner, which listens by default on port 3333. The malware, Satori.Coin.Robber, is a successor to the well-known Satori botnet, which [wreaked havoc](#) in late 2017 on Internet of Things devices. This variant uses a hardcoded IP address for control server traffic, with most of the IPs scanning for potential targets in South Korea. In addition, the malware author leaves a note behind, stating that the bot is not malicious and that he can be contacted via email.

Cybercriminals have even repurposed other known techniques and tailored them for cryptocurrency attacks. An attack discovered in late 2017 [replaced digital wallets](#) in a victim's clipboard. While scraping data and replacing content is not new, these attackers were specifically after cryptocurrency. The CryptoShuffler Trojan, which attacks clipboards, has been in operation since 2016 and targets a range of digital currencies, including Bitcoin, Dogecoin, Litecoin, Dash, Ethereum, Monero, and Zcash. The same author [also released](#) the clipboard-targeting Trojan Evrial. Each Trojan sits on a victim's computer waiting for strings that resemble a cryptocurrency address and replaces the address with one under the attacker's control. This technique can be quite profitable—substituting the digital wallet [has netted](#) more than \$140,000 for CryptoShuffler.

Just because new malware may use old tricks does not mean old malware cannot change its behavior. Banking Trojans also target cryptocurrencies. Two in particular appeared in 2016. The infamous banking Trojan Dridex [added wallet-stealing functionality](#) to its usual banking-credential theft. The Trojan Trickbot [targeted both](#) financial institutions and cryptocurrencies. Trickbot added [coinbase.com](#), a popular cryptocurrency exchange, as one of its attack vectors. Once a system was infected, the malware injected a fake login page whenever the victim visited the digital currency exchange, which allowed the cybercriminals to steal the victim's login data, along with a range of digital assets, including Bitcoin, Ethereum, and Litecoin.

Technology attacks

Before the release of the first blockchain implementation, there was no trusted alternative for decentralized banking. However, the security concerns of building such a system were studied well before then. Years of research, including Haber and Stornetta's chain of blocks, established trust in the concept of blockchain. Yet the security of a blockchain depends on certain assumptions. If those assumptions are not met, then security is at risk.

One of the primary assumptions for a blockchain is that the contribution to the network, the "hash rate" for Bitcoin, is distributed. Specifically, no one entity or collaborative group processes more than 50% of the network at any time. [A majority attack](#) occurs when an actor owns more than 50% of the network. If they exceed 50%, they essentially can process blocks faster than everyone else—creating their own chains at will.

Follow



Share



REPORT

This ability leads to or simplifies other attacks, such as double spending, in which the same coin can be spent multiple times and leave one receiver empty handed. A majority attack has never been implemented successfully against Bitcoin due to its large base, but it has been successfully implemented against Verge and other coins. Much smaller coins are acutely at risk. Soon after Krypton was proven susceptible to such an attack, the group [51 Crew](#) targeted other small coins and held them for ransom. This risk also applies to internally developed blockchains. Many organizations are examining blockchain technologies to manage inventory, data, and other assets. If the contributing base, or hash rate, of these custom networks is not large enough, an attacker could use cloud technology, botnets, or pools to attack the system.

A related assumption is that most nodes are “honest,” meaning there is a high likelihood that at least one connection is to a legitimate node. Failure to link to one honest node allows a [Sybil attack](#), in which the attacker forces the victim to talk only to malicious nodes. The attacker can control what information, including the ledger, the victim can access. It takes only one honest node to thwart this type of attack because it is not feasible for the attacker to prove a longer chain than the network. Recall that a long chain can prove the amount of work required to build the chain. The attacker must overcome the processing power of the entire network if the victim becomes aware of the valid chain. Therefore, this type of attack depends on stopping honest nodes from disclosing information from the real network. An

honest node does not stop attackers from attempting a Sybil attack. Large collections of [nodes were found](#) being created together in 2016. As with the majority attack, a smaller network is an easier target, particularly if additional countermeasures are not built into the system.

A third assumption is that hash collisions are rare. Bitcoin uses a 256-bit length to identify ownership of a wallet. Each key maps to the public address that others can send funds to. As long as an owner has unique access to a key, then no one else can submit transactions out of that wallet. But what if collisions were not rare? An attacker or anyone else might accidentally be able to remove funds from someone's wallet. Ownership of wallets and funds would be hard to prove because, from the network's standpoint, both parties would have the same rights. The good news is that hash collisions using industry-standard algorithms

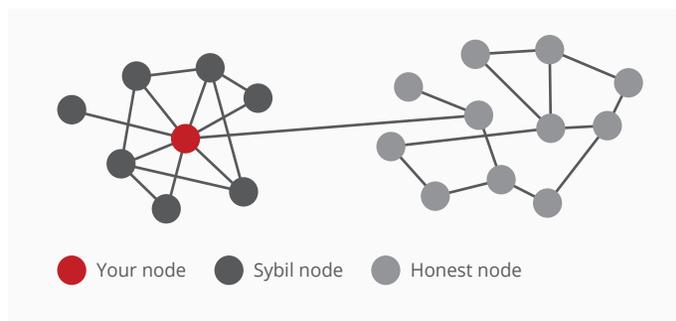


Figure 6: An honest node preventing a Sybil attack.

Source: <https://www.coindesk.com/bitcoins-security-model-deep-dive/>

Follow



Share



REPORT

appear to be rare. No one has been able to intentionally or unintentionally generate someone else's key, at least with Bitcoin, provided those keys were properly made. This does not stop owners from improperly making keys. Prevalent with Bitcoin and, to a lesser extent altcoins, many attempt to make managing their private keys easier with "brain wallets," which have keys generated by a word or easy-to-remember seed. Such behavior makes the wallet susceptible to tailored dictionary attacks. Other keys may suffer from the implementation itself. Iota's reliance on improperly generated keys results in collisions that lead to severe security risks for its adopters. Further research into algorithms, including the current standard, could make collisions much more likely to occur, as we have seen with algorithms such as MD5 and SHA-1.

Legacy attacks modernized

Much of the security focus regarding blockchain looks at the integrity of the ledger and underlying technologies. However, user behavior must also be accounted for to achieve a comprehensive view of the security risk. A well-known attack, viable due to insecure behavior, has been repurposed specifically against current blockchain implementations

Dictionary attack

Dictionary attacks have been around for decades. Typically, they attempt to break a victim's password or other authentication mechanism. Let's look at a typical dictionary attack—specifically a rainbow table attack.

When we create a password for an online account, the service provider should not store the password in plain text. Instead it should take a cryptographic hash of the password and store its value. For example, if we use the highly insecure "password," the server may save it as `5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8`, which is the SHA-1 hash of the string "password." We can use various hashing algorithms and other procedures, such as salting, to make this more secure. However, consider what happens if attackers see the preceding string. They



Follow



Share



REPORT

might recognize that string as the hash for “password.” Although in most cases it is difficult to find a string based on a hash, the reverse is not true. Finding the hash for a string is extremely easy using a command-line interpreter such as Bash.

- `$echo -n 'password' | shasum`

Hashing functions are a one-way algorithm: If attackers know only the hash value, theoretically they cannot calculate the original password. In this case, we happen to know both the password and the hash value, making translating between them simple. What is the SHA-1 value for “password1”? This is also easy to retrieve and results in `e38ad214943daad1d64c102faec29de4afe9da3d`. If attackers see the hash value of “password” or “password1,” they can translate it to the original text.

This translation can be run millions of times across every password imaginable. The only limit is time, but attackers can focus on common passwords. The collection of hash value paired with the clear text password is called a rainbow table. The translation from the cryptographic hash to the clear text password is a rainbow table attack.

A modified rainbow table attack can be implemented against the blockchain, specifically Bitcoin and related cryptocurrencies. For the remainder of this report, all examples will be specific to Bitcoin, but many of the same techniques are applicable to similar cryptocurrencies—and likely to new implementations of the blockchain beyond cryptocurrencies.

SHA-1 Hashes	Clear Text
<code>5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8</code>	password
<code>e38ad214943daad1d64c102faec29de4afe9da3d</code>	password1
<code>2aa60a8ff7fcd473d321e0146afd9e26df395147</code>	password2
...	...
<code>e13fc576c44eacd178e21b8b253f59fa59aa4cc8</code>	passwordN

Follow



Share



REPORT

Within Bitcoin, an address represents the public interface in which coins reside. Users transfer coins using that address—when they pay someone in coins, the transaction comes from that address. However, to verify that they are authorized to initiate a transaction and spend coins from an address, they must use their private keys. This key should be known only to the owner and must use the Bitcoin’s [elliptic curve digital signature algorithm](#). This effectively means that nearly

all 256-bit numbers that can be generated by the SHA-256 hashing algorithm are valid, which can lead some to foolishly employ a brain wallet. Instead of remembering or storing 64 seemingly random characters, they could just remember their normal passwords and use the SHA-256 hashing algorithm whenever they need their private keys. In the early days, people did this, and it was incredibly dangerous. Cybercriminals constantly scan for brain wallets.

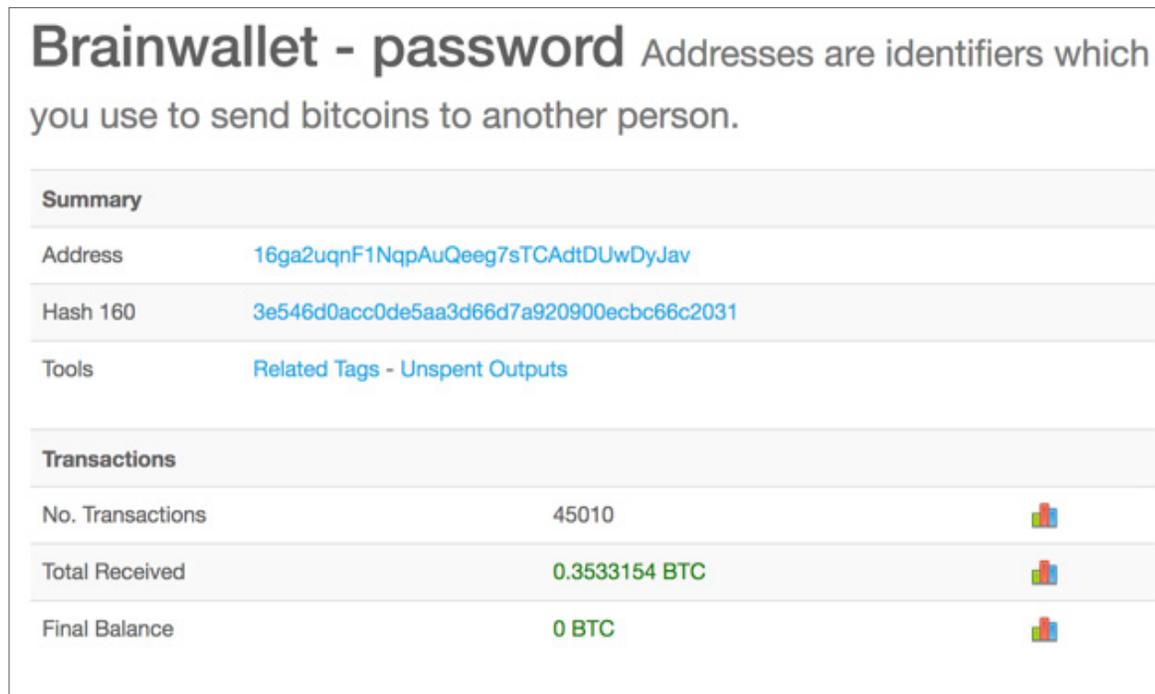


Figure 7: An account with the private key generated by “password,” from March 2018.

Source: <https://blockchain.info/>



REPORT

In the preceding image, we see that 45,010 transactions took place between July 2012 and March 2018, resulting in a balance of zero. Looking through the transactions, we see a pattern of small incoming amounts soon followed by an outgoing transaction. Among accounts using “password,” “password1,” and “password2,” we counted 117,212 transactions in which we could not determine the owner, nor which amounts were stolen. Bitcoin is not the only one with this problem, even though most cryptocurrencies were developed after the brain wallets weakness was well known.

Researchers have studied the weaknesses of brain wallets for some time and [found 18,000 vulnerable wallets](#) in 2016, along with speed optimizations for attacks. The results were not limited only to short, simple passwords. Many in the list [were phrases](#) with spaces, punctuation, and numbers, as well.

In our research, we ran across a very common brain wallet. Unfortunately, we suspect that others may have accidentally used this wallet and subsequently lost their money. Likely due to user error, multiple people have generated the same private key and thus shared this wallet, enabling what they would call theft. See the following two Bash commands for taking a SHA-1 hash of a string:

- `$echo -n "$password" | shasum`
- `$echo -n "$Cryt0p4sswordV3rySecure!" | shasum`

Details for Address		
Address	Lbnu1x4UfToiiFGU8MvPrLpj2GSrtUrxFH	
Balance	0.0 LTC	
Rich List	N/A	
Guesstimated Wallet	none	
Received	0.27232076 LTC	in 1 transactions
Sent	0.27232076 LTC	in 1 transactions

Figure 8: A Litecoin brain wallet.

Source: <https://chainz.cryptoid.info/ltc/>

Follow



Share



REPORT

We might expect two distinct SHA-1 hashes, but both return the same value: da39a3ee5e6b4b0d3255bfef95601890afd80709. This is an easy mistake to make and lies with the user and the details of Bash syntax. The \$ symbol in the password string is a special character in Bash, denoting a variable or special parameter. Using \$ at the beginning of the string makes Bash treat the entire string as a variable—it swaps the intended string for the value of that variable. In this case, neither of the variables exists, so Bash returns the same empty string. Making this mistake results in an unintended shared private key. It may also have resulted in the loss of almost 59 BTC (\$530,120 as of March). (See screenshot below.)

Although there are exceptions, most of the known brain wallets are based on the same common passwords used for other accounts. To get a clearer picture, we built our own rainbow table to test against the Bitcoin ledger. Our table consisted of a relatively small set of the 200,000 most common passwords, more than 160,000 Bitcoin-centric generated passwords, a list of famous quotes, and several readily available books, including *War and Peace* and *Alice's Adventures in Wonderland*. Although our sample size was comparatively small (many dictionaries are measured in the millions), we found 852 vulnerable wallets. More than 102 Bitcoins (almost \$1,000,000 at the time of writing) have been removed from these wallets. These numbers will likely rise as our sample size grows.

Summary		Transactions	
Address	1HZwkjkeaoZFTSaJxDw6aKkxp45agDiEzN	No. Transactions	307 
Hash 160	b5bd079c4d57cc7fc28ecf8213a6b791625b8183	Total Received	58.95924481 BTC 
Tools	Related Tags - Unspent Outputs	Final Balance	0 BTC 
		Request Payment	Donation Button

Figure 9: This wallet recorded two transactions as recently as March 5, 2018. One incoming and one outgoing transaction occurred within roughly 15 minutes.

Source: <https://blockchain.info>

Follow



Share



REPORT

As we see in many online accounts including brain wallets, “password” remains popular. We have found many passwords, including some of our cryptocurrency-centric passwords, in leaked databases. Using Troy Hunt’s hash database of passwords from “Have I Been Pwned,” we cross-referenced our results with password hashes known to be leaked from various data breaches. Viewing our Bitcoin-centric dictionary, we found 5,098 unique passwords resulting from 501 million breached records. Of that set, a handful were also brain wallets, with more than 30 Bitcoin suspected stolen.

Exchanges under fire

Some of the biggest players in this field are cryptocurrency exchanges, which have become prime targets. A cryptocurrency exchange helps consumers manage their coins and trade among other cryptocurrencies or physical currencies, such as US dollars. These exchanges behave similarly to traditional banks, providing convenience for many people. Account holders can create accounts, add or distribute funds, and manage their cryptocurrency without knowledge of local wallet software. The largest exchanges deal in multiple coins and handle transactions between them. For many, an exchange is the only way to deal with cryptocurrencies and one of the primary ways that consumers can acquire coins.

Cybercriminals recognize the popularity of exchanges and have targeted them. Similar to the banking industry, exchanges represent a gold mine if not properly secured. Banks have the benefit of experience through decades of dealing with security issues and incident

response. Even so, security issues do arise, as we have seen [with numerous attacks](#) against the SWIFT banking network during the last few years. Exchanges do not have the luxury of that experience and are learning the hard way. These lessons can be quite costly to both the exchanges and their customer base.

Major events

In January 2018, Coincheck, one of Japan’s first and most popular exchanges, [lost \\$532 million](#) in NEM coins, affecting 260,000 investors. Trading was halted while victims were left confused. An attacker had gained access to an employee’s computer and installed malware designed to steal private keys from digital wallets. The attacker managed to attain the private key of a “hot” wallet, which was used online for immediate transactions. After draining the accounts, the result was one of the largest-ever exchange hacks.



Follow



Share



REPORT

The Coincheck attack was not the only one. Exchanges were a target of cybercriminals throughout 2016 and 2017. In that period, we saw numerous successful attacks. In early 2017, we learned of nearly 120,000 Bitcoins [stolen from Bitfinex](#) in August 2016. The coins moved to other exchanges, including LocalBitcoins, Xzxx, BTC-e, Bitcoin.de, Coinbase, Kraken, CoinsBank, and QuadrigaCX. Despite a 5% bounty placed on their value, the stolen coins have not been recovered. “We know generally how it happened,” [wrote Drew Samsen](#), Applications Team Leader at Bitfinex. “It was the work of a profession[al] (or team) over several months who expertly covered his tracks.”

Gatecoin, a Hong Kong exchange, is notable for its early Ethereum support. In May 2016, [Gatecoin disclosed](#) not only a 250 Bitcoin loss but also a whopping 185,000 Ethereum loss (about \$2 million). Both its hot wallets and its “cold storage” offline wallets were affected. The attacker managed to bypass multisignature protections placed on cold storage by altering the exchange’s systems to instead use hot wallets.

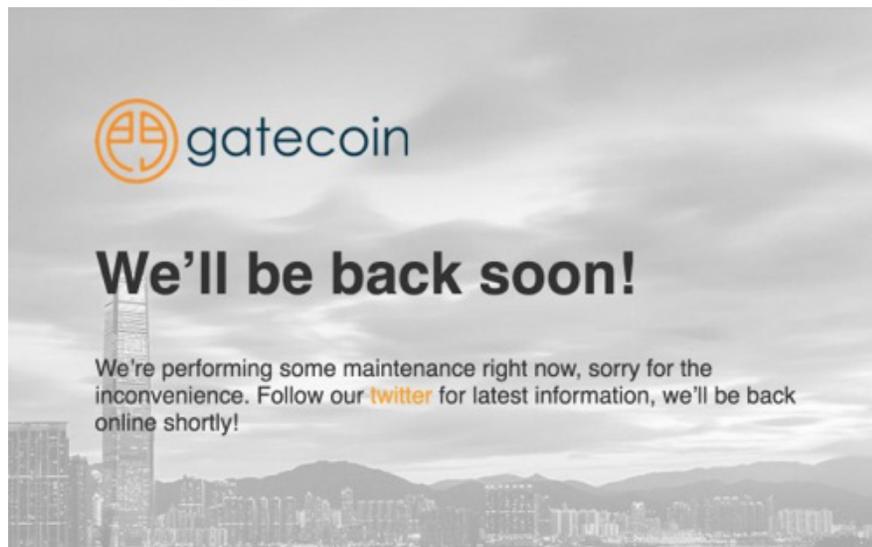


Figure 10: A screen capture from the exchange Gatecoin in May 2016.

Source: CoinDesk.com

Follow



Share



REPORT

The exchange infrastructure itself is not always the main target. Consumers of an exchange can also fall victim to a direct attack. At its prime, Bithumb processed 10% of all global Bitcoin trade and was the largest South Korean exchange of Ether, with around 44% of transactions. In June 2017, Bithumb [reported the loss](#) of the personally identifiable information of 31,800 web users (about 3% of their user base) due to a breach on an employee's computer. Rather than targeting the infrastructure, the attacker went directly after the consumers, in some cases posing as Bithumb executives and using traditional social engineering and phishing techniques.

Customers of Enigma, which operates like an investment platform, were similarly targeted. Using well-known and common social engineering techniques, attackers tricked Enigma customers into using a malicious Ethereum address. By compromising the official Enigma website, newsletters, and Slack accounts, [the attacker distributed](#) incorrect Ethereum payment addresses owned by the attacker. More than 1,500 Ether were stolen, with some transactions occurring after the compromise was disclosed and fixed.

TxHash	Block	Age	From		To	Value	[TxFee]
0xcf6b4ccc0f91b32...	5059624	14 days 8 hrs ago	0x21e229f2d307d7f...	IN	Fake_EnigmaPhish	0.002 Ether	0.000105
0xbf45b27df99f5f74...	4825731	55 days 3 hrs ago	0xdc4ee4e2580b4c...	IN	Fake_EnigmaPhish	0.00124579 Ether	0.00042
0x12580af9ab49fee...	4313854	150 days 6 hrs ago	Fake_EnigmaPhish	OUT	0x99e331fa7c45671...	20.2 Ether	0.000441
0xbd96745cea0723...	4262418	165 days 10 hrs ago	0xf4a2f01cd178b88...	IN	Fake_EnigmaPhish	3 Ether	0.000441

Figure 11: Transaction record.

Source: <https://etherscan.io/>

Follow



Share



REPORT

After several years of notable exchange attacks, the news of the Coincheck hack had a tangible impact on trust. Customers voiced their concerns to other exchanges at the slightest hint of a problem. Binance, which had to undergo unscheduled maintenance, opted to proactively notify its customers to be on the lookout for scams and imposters targeting their accounts.

Although Binance did not suffer a breach, [it was hit](#) by a distributed denial-of-service attack shortly after server maintenance. News of the attack did not mollify users, who were already skeptical of the unscheduled server maintenance claims. To maintain consumer confidence, Binance offered a 70% discount on trading fees through most of February.

Cryptocurrency adopters are increasingly looking for stability in a wildly volatile market. Many consumers are advising others to split coins across several exchanges to protect against the inevitable attacks. For sophisticated users, local or hardware-based wallets are a reasonable alternative. Those choices, however, pose their own security concerns that need to be managed by each individual. The level of user confidence in exchange security is waning from the difficulty the industry has had balancing growth and security.



Figure 12: A message from the Binance exchange. The account has since been suspended by Twitter.

Follow



Share



Recovery

Recovering from cryptocurrency theft is more difficult and complicated than with most other currencies due to their decentralized nature. Only the owner of a wallet can make changes to its balance, even if the owner acquired that balance illegally. Although an exchange may be able to track where coins have gone, it needs assistance from the current owner to return those funds. Essentially, the exchange must find the perpetrator and wallet keys to return any stolen coins. In the case of exchange-to-exchange movement, it may be possible to come to an agreement, provided local laws allow, to return the funds. Exchanges generally manage the blockchain keys in house, while accounts are stored centrally, giving the exchange much more control of the wallets. However, if the funds are moved into a private wallet, the victim has no recourse. The only hope is that law enforcement can track down the thief and acquire the private key associated with the wallet. In nearly all scenarios, this is essentially a lost cause due to limited resources and lack of governance or jurisdiction concerns.

In recent incidents, exchanges have attempted to compensate their customers for losses—at least those exchanges that survived the breach. Coincheck, Bitfinex, and Gatecoin are examples of the lucky ones. In March 2018, Coincheck [started reimbursing](#) victims for their losses of NEM coins. In April, 2017 Bitfinex successfully paid back victims for the loss of funds in its August 2016 hack. However, instead of taking funds directly from the business, they used the cryptocurrency version of an

IOU. After disclosing the hack, they created BTX tokens, and promised they would buy each back for \$1 in the future. They distributed these tokens to their account holders and [completed the buyback](#) in April. In February 2017, the Hong Kong exchange Gatecoin [completed the repayment](#) of stolen Bitcoins from a May 2016 hack. The Bitcoins were worth between \$450 and \$750 at the time of theft but around [\\$1,190](#) once the repayment was completed. They also laid out a repayment plan for the remaining stolen Ethereum. In this case, the exchange pulled in profits from other parts of the business, including consulting services and exchange fees and reallocated the revenue to the buyback.

Not all exchanges were able to recover. The most well-known example is the fall of Mt. Gox, a Japanese exchange attacked between 2011 and 2014. More than \$450 million of Bitcoin was stolen. Within the year, this led to [the liquidation](#) and closure of Mt. Gox. Two more recent and notable exchanges also suffered irrecoverable repercussions from cyberattacks. Bitcurex, the largest and one of the oldest in Poland, closed operations within one month of a hack. Initially, vague language disclosed some service problems, but it was discovered that 2,300 Bitcoins went missing.

Follow



Share



REPORT

Bitcurex abruptly closed after a couple weeks of public confusion, leaving users to swallow the losses. In March of 2017, Polish police [announced investigations](#) into the circumstances of the closure and asked all injured parties to come forward.

Youbit, a South Korean exchange, was unable to maintain operations after a compromise. Only a month after the Bitcurex investigation began, Youbit, then called Yapizon, [lost 4,000 Bitcoin](#) to hackers which accounted for roughly 36% of its funds. Details later indicated the currency was stolen after hackers reached internal

systems and accessed four hot wallets. Youbit attempted to use similar methods as Bitfinex to compensate its customers. They spread the losses across all account holders and issued tokens as IOUs and promised to buy back the IOUs later. However, in December 2017, Youbit [suffered another attack](#), losing 17% of its funds and forcing the company into bankruptcy. Customers with remaining funds were allowed to retrieve 75% of their balances, while the rest was left to the bankruptcy process.

“On 13.10.2016 as a result of third-party systems service www.bitcurex.com [was] damaged by external interference in automated data collection and processing of information. The consequence of these actions is the loss of part of the assets managed by bitcurex.com/dashcurex.com.”

—*Statement translated from Polish on bitcurex.com*

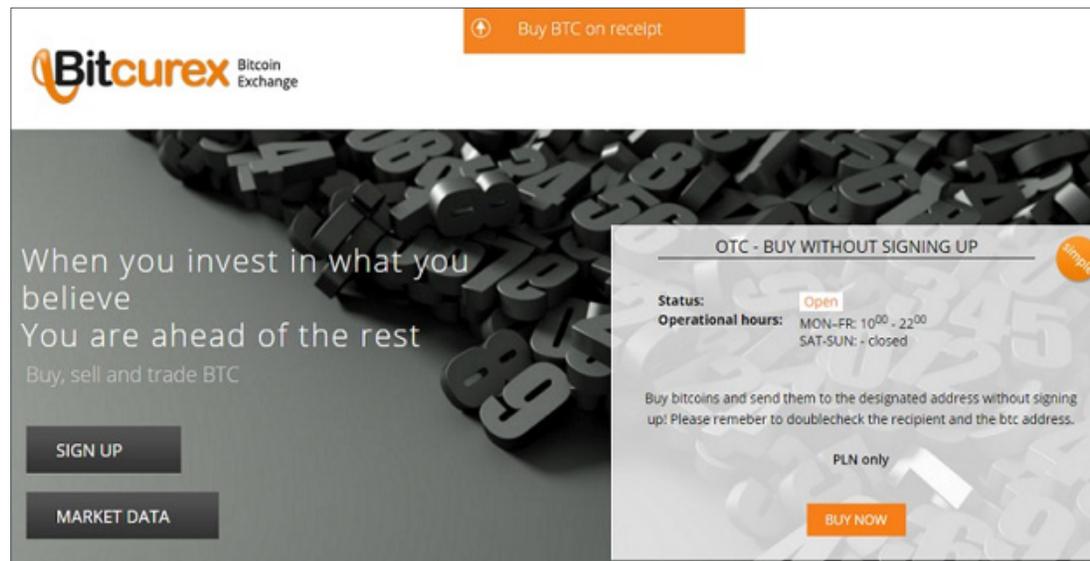


Figure 13: An advertisement for the shuttered Polish exchange Bitcurex.

Follow   

Share   

Conclusion

As blockchain technology continues to both positively and negatively disrupt global industries, we must be diligent about the security implications. As we've seen, cybercriminals will find creative ways to reach their goals. Although the blockchain has been well researched and answers many questions regarding decentralized trust, it does not address the security of users or the applications that connect to its network. We have seen insecure behavior via brain wallets lead to theft of cryptocurrencies. Attackers have used old techniques in new ways with success, such as the dictionary attacks against Bitcoin private keys. Even traditional phishing attacks can work to gain access to wallets or computer resources. And we observed that not only blockchain users are targeted. The primary commercial adopters of blockchain are cryptocurrency exchanges, which have suffered from an unending barrage of successful attacks. Government regulators are struggling to keep up with and understand the legal implications of losses due to cyberattacks.

Businesses must also be diligent. Blockchain technology is attracting a lot of interest for solving various business needs beyond decentralized payments. Entire automated businesses are being built using smart contracts. Retailers and others are looking into blockchain to manage their inventories. The medical industry is examining ways to manage medical documents. The number of successful and impactful

attacks against exchanges extends well beyond the confines of this report and should serve as a warning. It is not enough to implement and use new technologies without performing a tailored risk assessment.

As industries research and implement their own blockchains, we can expect cybercriminals to deploy a combination of known and yet-unknown techniques to compromise them. Without a clear understanding of where the risks are you may place undue trust in your blockchain implementations. As we've seen, mistakes are easy to make. Users are even harder to control and can negatively contribute to the risk. We need to learn from recent events to make better decisions for securing our technologies for tomorrow.



Follow



Share



About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.



2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2018 McAfee LLC. 4003_0518
JUNE 2018