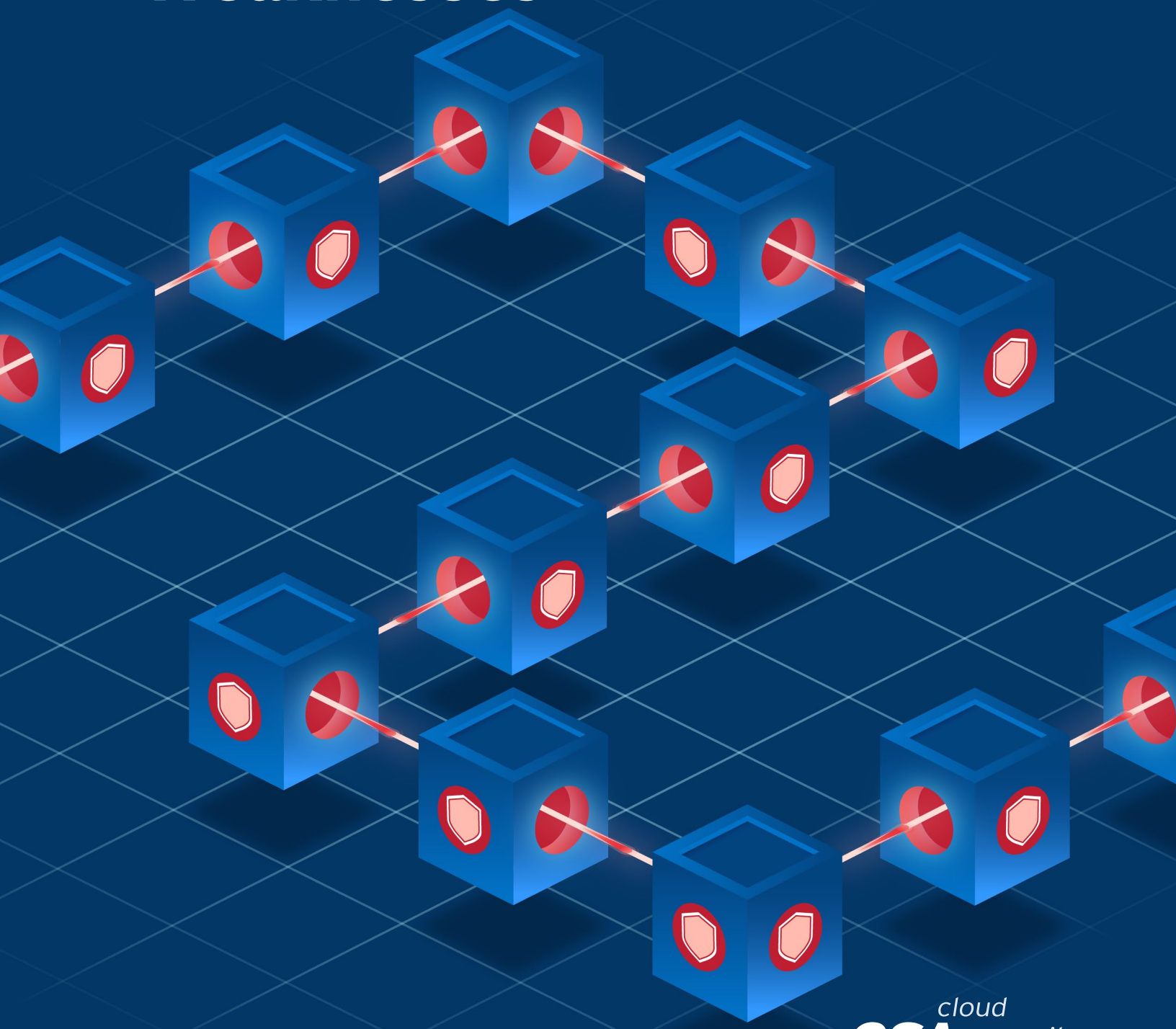
Top 10 Blockchain Attacks, Vulnerabilities & Weaknesses



cloud security alliance®

The permanent and official location for Blockchain/Distributed Ledger Working Group is
https://cloudsecurityalliance.org/research/working-groups/blockchain/

Acknowledgments

Authors:

Julio Barragan
John Jefferies
Dave Jevans

Key Contributors:

Bill Izzo
Ashish Mehta
Jyoti Ponnapalli
Kurt Seifried
Adalberto Valle

CSA Program Manager, Research:

Hillary Baron

CSA Staff:

Claire Lehnert (Design)
AnnMarie Ulskey (Cover)

Special thanks to CipherTrace

Table of Contents

Acknowledgements 3
Table of Contents 4
Executive Summary 5
Top 10 DLT Attack Types 6
1. Exchange Hacks 6
2. DeFi Hack 8
Case Study 9
Notable DeFi Hacks in the Last Three Years 10
3. 51% Attack 12
Case Study 12
Mitigating a 51% Attack 12
4. Phishing 13
Case Study 14
5. Rugpull/ Exitscam 14
Case Study 15
6. Ransomware 16
Ransomeware-as-a-Service (RaaS) 16
Combating Ransomware 16
Best Practices to Minimize Damage 17
7. SIM Swap 17
How a SIM Swap Works 18
Protecting Against SIM Swapping 18
Case Studies 18
8. Investment Scam 19
9. High-Profile Doubler Scam 20
Case Study 21
Mitigating Doubler Scams 22
10. Extortion 22
Preventing Extortion Attacks 22
Case Study 23
11. Bonus: Wallet Security 24
Fake Software Wallets 24
Fake Hardware Wallets 25
Conclusion 27
References 28

Executive Summary

Caution: Top attacks against virtual assets will be repeated against enterprise blockchains

There is a strong misconception that the immutable nature of Distributed Ledger Technology (DLT) systems makes them inherently secure. However, there are a broad range of attack vectors targeting blockchain applications, targeting anything from cryptographic primitives to consensus mechanism vulnerabilities or smart contract exploits.

Cryptocurrencies and the platforms that enable them have been the target of attacks since the inception of bitcoin over twelve years ago. The desired outcome: make off with as many crypto profits as possible. To achieve this, bad actors can either target blockchain protocols themselves, exploit a specific platform (centralized or decentralized), or target the individuals holding crypto assets.

This report covers the top tenattack types targeting cryptocurrency and DLT:

1. Exchange Hack
2. DeFi Hack
3. 51% Attack
4. Phishing (for private keys)
5. Rug Pull/Exit Scam
6. Ransomware
7. SIM Swap
8. Investment Scam
9. High Profile Doubler Scam
10. Extortion

This report is a high-level overview of the top ten attacks, as each attack type could easilywarrant a paper of its own. The attacks listed in this report provide illustrative examples and costly lessons that can help anyone, from developers to compliance officers to the day-to-day cryptocurrency user, to educate themselves on how to avoid falling into many of the same pitfalls.

The bearer nature of virtual assets has concentrated attackers' focus on stealing private keys from virtual asset service providers (VASP) and individual cryptocurrency users. The crypto adage "not your keys; not your coins" describes reality; if the attacker controls your private keys, the attacker controls your virtual assets. Techniques such as SIM swapping, which originated as a Twitter account takeover tool, have been redeployed to take control of a user's 2FA and ultimately take over crypto accounts and steal a user's funds.

Nascent crypto companies with inadequate security protocols can suffer unrecoverable losses if administrators with access to hot and cold wallet storage fall victim to these attacks. On top of that, unaudited smart contracts and lapses in security protocols can also result in significant losses for centralized and decentralized exchanges. In the last five years, 43 exchanges have been publicly hacked, and more than 49 DeFi protocols have been exploited, resulting in a loss of more than $2.8 billion.

Cryptocurrencies also enable old fraud models to operate in new ways, as seen by the accelerated growth of ransomware, online extortion, and investment fraud cases. In the last five years, at least 14 exchanges and hosted wallet providers have exit scammed, and 7 DeFi projects have rugpulled, escaping with more than $4.5 billion of misappropriated user funds. At the same time, ransomware attacks have increased in sophistication and severity, with the average ransomware payment in 2020 being over $ — a 171% increase compared to 2019, according to Palo Alto Networks' 2021 Ransomware Threat Report. Fortunately, credible blockchain analytics tools provide unprecedented capabilities to trace virtual assets and identify where these criminals are cashing out their funds.

Ransomware Attacks 2017-2021		
Type of Attack	**Major Attacks**	**Total**
Exchange Exit	14	$ 4.383 billion
Exchange Hack	43	$ 1.702 billion
DeFi Hack	49	$ 1.122 billion
DeFi RugPull	7	$ 124 million
51% Attack	14	$ 24 million in double-spends

Top 10 DLT Attack Types

1. Exchange Hack

With the average daily cryptocurrency exchange volume over $180 billion at the time of this report and the nascent nature of the industry, it is clear why so many hackers are drawn to targeting cryptocurrency exchanges. Mt Gox was the first centralized exchange to experience a significant loss, losing 850,000 BTC worth $450 million at the time of the attack in 2014. In the last five years, 49 centralized exchanges have been publicly hacked, resulting in a loss of more than $1.8 billion.

Now, as exchanges continue to harden their cloud security controls, attackers have pivoted to targeting human users with social engineering attacks and confidence schemes, highlighting the importance of proper security training for staff. Typical exchanges attacks fall into the following categories:

1. Phishing user credentials to gain access to cryptocurrency accounts and move money. These are sometimes combined with SMS hijacking to take over an SMSbased authentication code for a targeted user.
2. Technical attacks against an exchange to penetrate the internal system, including:
    a. SQL injection attacks after an account has been created or accessed.
    b. Vulnerabilities in software used to operate the exchange.
    c. Unpatched software used by an exchange.
3. Spear-phishing of employees at an exchange in order to override controls on withdrawals.

4. Spear-phishing of employees at an exchange to implant malware (particularly remote-access trojans), allowing attackers to access internal systems and hop between infrastructure nodes.
5. Exploitations of API vulnerabilities to obtain stored credentials, such as private keys. Attackers often use credentials stored on computers in the internal system to gain access to other systems.
6. Inadequate or incorrect use of cold wallets (offline storage of private keys) versus hot wallets (online key storage), used for day-to-day operations. Ninety percent of an exchange's cryptocurrency should be stored in cold wallets not connected to the Internet. There must be a protocol for initializing cold wallets completely offline and moving transfer requests between the hot wallets and cold wallets (usually requiring a USB drive with signing instructions). Consider multisig for accessing cold wallets, requiring two employees to sign a transaction before funds are transferred from cold wallets to hot wallets.
7. Insider threats have been common in exchanges. Employees gain access to hot or cold wallet keys and copy them or implant malware or remote access trojans on internal systems, allowing them future access to these keys to steal crypto assets.
8. Decompiling exchange apps (iOS or Android) and discovering secret cloud API keys that are embedded in the app, then using those keys to access internal APIs – which may be used to access hot wallets or user credentials.
9. Copying of wallet recovery keys. Exchanges need to protect their wallet recovery keys with even more diligence than their hot or cold wallets. If an attacker gains a copy of the recovery keys, the entire assets of an exchange—including cold digital wallets—can be stolen. NEVER store recovery keys on electronic media. Store them written down on paper that is kept in a physical vault. There are physical metal devices that are more fireproof than paper.
10. Attacks against specific currencies that exploit vulnerabilities in the exchange's implementation of that currency. For example, many XRP (Ripple) implementations have a bug that allows for partial payments exploits. Suppose an exchange's integration with the XRP Ledger assumes that the Amount field of a Payment is always the full amount delivered—in that case, malicious actors may exploit that assumption to steal money from the institution. This exploit can be used against gateways, exchanges, or merchants as long as those institutions' software does not process partial payments correctly. In the first nine days of September 2020, the XRP holdings of three exchanges were wiped out completely.

Notable Centralized Exchange Hacks in the Last Three Years

Date	Exchange	Amount Lost
2019 Q1	Cryptopia	$16 million
2019 Q1	Coinbene	$105 million
2019 Q1	DragonEx	$1 million
2019 Q2	Bitrue	$4.7 million
2019 Q2	Binance	$40.7 million
2019 Q2	GateHub	$10 million
2019 Q2	Silkkitie	$2 million

2019 Q2	Bitpoint	$32 million
2019 Q2	Bitcoins Norway	Undisclosed
2019 Q4	Upbit	$49 million
2020 Q1	Exmo	$10.5 million
2020 Q1	Altsbit	$72.5 million
2020 Q1	Coinhako	Undisclosed
2020 Q1	Crex24	$11,200
2020 Q3	KuCoin	$281 million
2020 Q3	Eterbase	$1.6 million
2020 Q3	2gether	$1.4 million
2020 Q3	Cashaa	$3 million
2020 Q4	LiveCoin Hack	Undisclosed

2. DeFi Hack

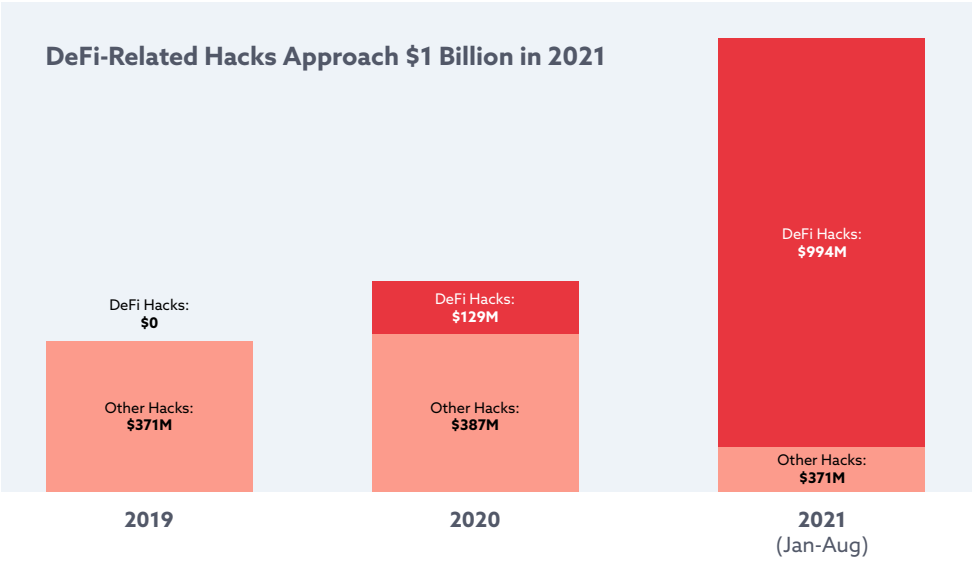
It's common for attackers to fund DeFi attacks through flash loans, which require no collateral or Know-Your-Customer (KYC) identification data, making it increasingly difficult to catch bad actors. While more decentralized exchanges are beginning to audit their contracts in the hopes of preventing an attack, vulnerabilities continue to be discovered by savvy hackers.

For example: On May 8, 2021, an "evil contract" exploit in the Rari Capital ETH Pool associated with the protocol's new Alpha Homora integration led to the theft of $10 million in assets.

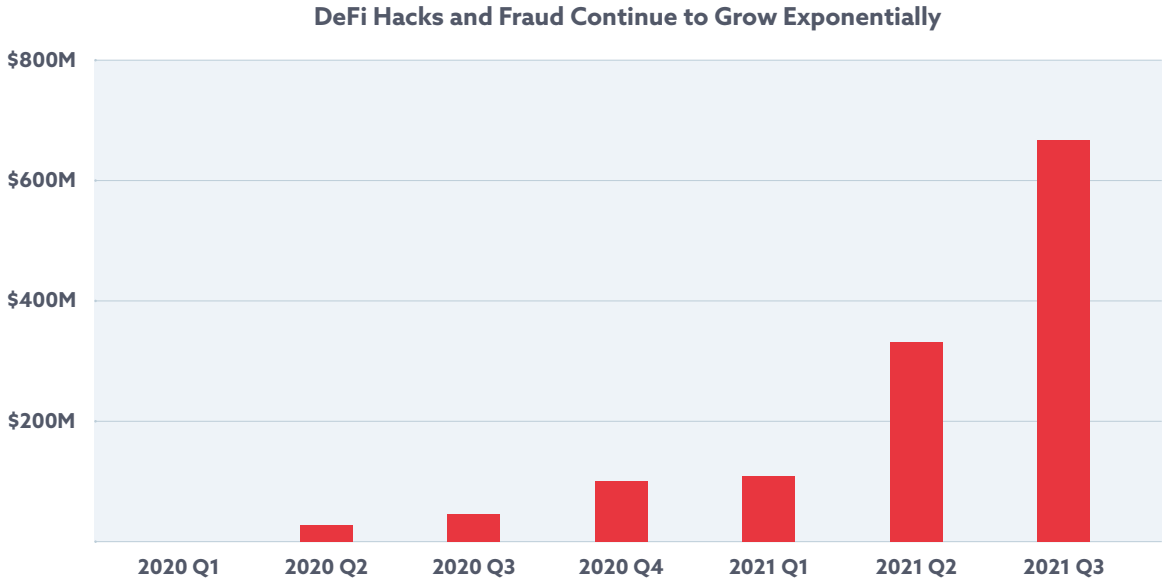
In an "evil contract" exploit, an attacker tricks a smart contract into thinking its "evil contract" has the proper access or permissions. In the Rari Capital hack, the exploit caused the HomoraBank contract to make the incorrect assumption that the hacker was setting up an ibETH pool on the platform. The attacker used flash loan ETH from decentralized cryptocurrency exchange dYdX to repeatedly fund deposits into the liquidity pool—thereby artificially inflating the value—and withdraw more ETH than initially deposited due to the inflation.

While Rari's integration of Alpha was audited, the exploit was not detected during the audit.

According to CipherTrace research, at the time of this report, losses from DeFi hacks totaled $994 million for the year—90% of all of 2021's total cryptocurrency hack volume. This increase in DeFi-related hacks and fraud demonstrate a clear uptrend towards DeFi-related crime, as demonstrated in the charts below:



Source: CipherTrace Cryptocurrency Intelligence



Source: CipherTrace Cryptocurrency Intelligence

Case Study

On August 10, Poly Network suffered a $612 million hack—the largest crypto-related hack to date. The typical DeFi hack is against specific DeFi instruments, resulting in much smaller losses. This attack was against Poly Network's infrastructure, focusing on the DeFi platform itself and targeting control of the decentralized exchange's (DEX) smart contracts. As a result, the main cross-chain contract became completely controlled by the hacker, allowing the hacker to unlock tokens that were supposed to be locked within the contract, send the tokens to addresses under their control, and then repeat the attack across multiple chains.

The hacker returned nearly all the funds within days of the initial hack. However, at the time of this report, a large portion of the returned funds—about $235 million—remain in a multisig wallet under the

control of Poly Network and the hacker. This means that Poly Network cannot move the funds out of this wallet without the hacker's private keys. The hacker has thus far refused to release his private key.

This record-breaking hack exemplifies the importance of smart contract security and audit standards to assure quality and reduce vulnerabilities in the code. As DeFi hacks and fraud continue to grow exponentially quarter over quarter, the future of DeFi crime appears grim. If DeFi crimes continue to grow more sophisticated, smart contracts are likely to be increasingly targeted for larger scale attacks.

Notable DeFi Hacks in the Last Three Years

Date	Protocol	Amount
2020 Q1	bZX	$318,000
2020 Q1	bZX	$636,000
2020 Q2	Bancor	$135,229
2020 Q2	Bisq	$250,000
2020 Q2	UniSwap	$300,000
2020 Q2	Lendf.me	$25 million
2020 Q3	Balancer	$500,000
2020 Q3	Yearn Finance (emmence)	$15 million
2020 Q3	Opyn	$371,000
2020 Q3	bZX	$8.1 million
2020 Q4	Cover Protocol	$4.4 million
2020 Q4	Cover Protocol	$4 million
2020 Q4	Value: DeFi	$6 million
2020 Q4	Axion	$500,000
2020 Q4	Warp Finance	$7.7 million
2020 Q4	wLEO	$42,000
2020 Q4	Cheese Bank	$3.3 million
2020 Q4	Origin Protocol	$7.0 million
2020 Q4	Pickle Finance	$19.7 million
2020 Q4	Akropolis	$2.0 million
2020 Q4	Harvest Finance	$24.0 million
2021 Q1	Roll (WHALE, RARE, and PICA)	$5.7 million

2021 Q1	DODO DEX	$3.8 million
2021 Q1	PAID Network	$3.16 million
2021 Q1	Furucombo (iouCOMBO)	$14 million
2021 Q1	CREAM Finance + Alpha Finance (Alpha Homora)	$37.5 million
2021 Q1	Year.Finance	$11 million
2021 Q2	EasyFi	$81 million
2021 Q2	Eleven.Finance	$4.5 million
2021 Q2	Alchemix	$6.5 million
2021 Q2	Bogged Finance	$3 million
2021 Q2	Belt Finance	$6.2 million
2021 Q2	Rari Capital	$10 million
2021 Q2	Value.Defi (governance RecoverUnsupported())	$10 million
2021 Q2	Value.Defi (vSwap AMM vSwap pools)	$11 million
2021 Q2	bEarn	$11 million
2021 Q2	Xtoken	$24.5 million
2021 Q2	Pancake Bunny	$45 million
2021 Q2	Spartan Protocol	$30.5 million
2021 Q2	Burger Swap	$7.2 million
2021 Q3	Chainswap	$800,000
2021 Q3	Chainswap	$8 million
2021 Q3	ThorChain	$5 million
2021 Q3	ThorChain	$8 million
2021 Q3	AnySwap	$7.9 million
2021 Q3	Bondly	$5.9 million
2021 Q3	Levyathen	$1.5 million
2021 Q3	Popsicle Finance	$20 million
2021 Q3	Poly Network	$611 million

3. 51% Attack

A 51% attack is an attack on a proof of work blockchain where a group of miners controlling more than 50% of the network's mining hash use this power to prevent new transactions from being confirmed or to reverse transactions that were completed under their control, leading to a double-spend attack. Once this happens, there is often nothing written into the blockchain technology that can stop the attack. The biggest cost resulting from a 51% attack is loss of confidence in the blockchain.

Notable 51% attacks have affected:

- Krypton
- Shift
- MonaCoin
- Bitcoin gold
- Zencash
- Litecoin Cash
- Feathercoin
- Vertcoin
- Bitcoin Gold
- Ethereum Classic
- Verge
- Bitcoin SV

Case Study

In August 2020, ETC experienced a 51% attack that caused a reorganization of over 7,000 blocks, corresponding to roughly two mining days. Four major exchanges were affected by the double-spend, resulting in $4.6 million in losses.

Mitigating a 51% Attack

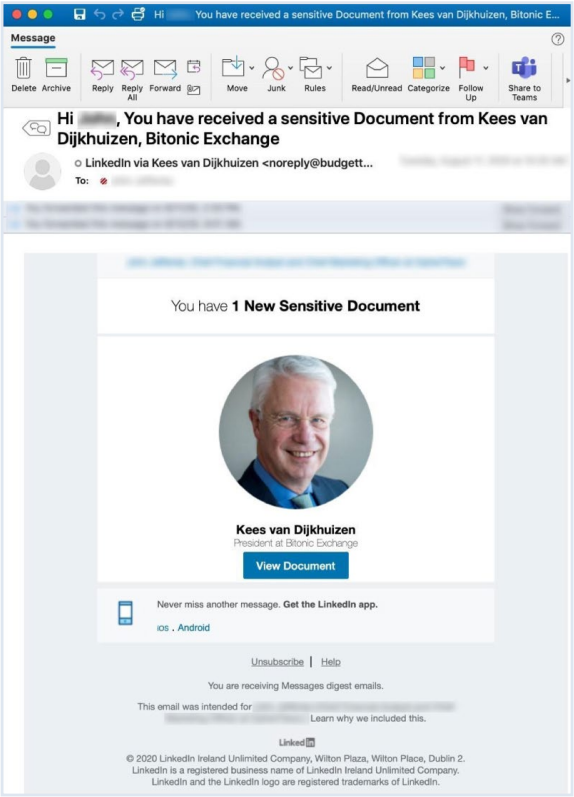
Double-spends resulting from 51% attacks present security and confidence issues in blockchains. One way of improving security protocols and controls may be accomplished through exchanges. Some exchanges wait for a block depth of six confirmations before allowing the coins to be used, and this may be extended to a block depth of 30 or more confirmations once the blockchain informs the exchange that an attack is in progress. Its goal is to allow more time for the minority 49% of miners to regain the hash power of the blockchain and thwart theattack. This benefits the exchange as well—they won't lose coins to double-spending.

4. Phishing

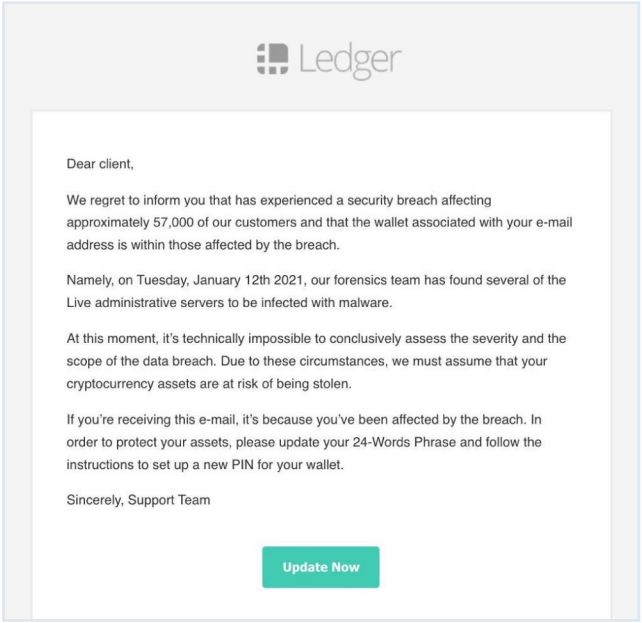
Phishing attacks are all too common in and outside of the blockchain economy. In a traditional phishing attack, criminals will "fish" for targets by casting a wide net and mass-emailing potential victims, posing as a legitimate institution to trick the reader into providing sensitive data such as usernames, passwords, banking and credit card details, and other personally identifiable information. Phishing has evolved beyond email to include phone calls, text messages, and social media platforms.

Increasingly common in the crypto-space are very targeted spear-phishing attacks. In these types of attacks, the criminal has additional details on a victim that they can use to customize their attacks and often appear to come from much more trusted sources.

After the data leak on cryptocurrency hardware wallet provider Ledger, many buyers received spear-phishing emails that claimed the user needed to update their seed phrases using a provided link. However, doing so resulted in the attacker obtaining a copy of the user's private keys, granting them complete control of all the cryptocurrency held by Ledger.



Example of a spear-phishing attack that appears to come from a contact on LinkedIn, based on a real banking executive's identity



Example of a phishing attack after the Ledger data breach

Common phishing attack vectors targeting cryptocurrency users include:

- Spear-phishing emails posing as wallet providers or exchanges used by the target
- Unique phishing sites posing as legitimate crypto wallet providers and exchanges
- Spear-phishing attacks by fraudulent groups and people on social media (Reddit, Twitter, Telegram) when seeking help

Case Study

While most people may think of phishing attacks as fraudulent emails, crypto hackers have many vectors from which they can phish for private keys. One of the most notable phishing attacks from this past year comes from fraudulent google ads for a common cryptocurrency wallet application.

In early December 2020, CipherTrace analysts noticed an uptick of alerts and comments within the online cryptocurrency community about users' funds being stolen via a Chrome browser extension phishing attack posing as cryptocurrency wallet and browser extension MetaMask. The fraudulent browser extension directed information to maskmeha[.]io, which then subsequently redirected to https[:]//installmetamask[.]com. The phishing site perfectly mirrored the actual true MetaMask site.

The issue was compounded when $WHALE Community published a post on Medium instructing users to send $WHALE funds to MetaMask and referenced the fraudulent https[:]// installmetamask[.]com domain as the MetaMask wallet download page. As the phishing page appeared at the top of any google search because of its status as a google ad, it is likely that the original poster did a quick search and copied the first link they found, highlighting the dangers of these types of phishing attacks as trusted sources lend the website credibility.

5. Rugpull/Exitscam

In the crypto-verse, an exit scam refers to when an exchange disappears with user funds, seemingly out of the blue, leaving customers unable to withdraw from their accounts. This is typically the result of one or more members of the executive team misappropriating user funds and can be either planned from the inception of the exchange or happen suddenly due to inadequate safeguards to prevent embezzlement.

Rug pulls are similar to exit scams; both involve insiders taking off with a majority, if not all, of users' funds. While often used interchangeably, exit scams are more often linked to established entities or projects unexpectedly closing down ("exiting"), taking user funds with them. For example, in November 2020, the DeFi project SharkTron appeared to have conducted an exit scam with $10 million in user funds, closing its website and leaving users in the dark.

A rugpull, on the other hand, is a specific type of exit scam that involves "pulling the rug" out from under investors (users) by selling the majority of the DeFi pool, thereby draining liquidity from a specific token. Rug pulls are often accomplished through intentional back doors written into smart contracts. In the case of DeFi project Compounder.Finance, a hidden backdoor written into the smart contract allowed developers to pull $10.8 million from the project's liquidity pools in November 2020.

DeFi project Unicats performed a similar rug pull in October, draining the entirety of its users' funds. Both scams highlight the importance of users vetting where they decide to hold their funds. Whether in a centralized exchange or decentralized application, users should vet the platform, careful to look for any red flags. Are all of the lead developers anonymous, as was the case with the WhaleFarm rugpull? Has the smart contract been audited and reviewed by the community? Is the whitepaper suspiciously short and vague? Does the platform guarantee rewards that are too good to be true? How credible are the founders or executive team? These are just a few things to think about when vetting a project.

Case Study

In early 2019, the cryptocurrency community was captivated by the implosion of QuadrigaCX, which had been Canada's largest cryptocurrency exchange. On January 14, 2019, QuadrigaCX customers first learned the company's CEO, Gerald Cotten, had died more than a month earlier. His widow posted an announcement on the QuadrigaCX website explaining that Cotten passed away in India while opening an orphanage. It was around the time of Cotten's reported death that customers began reporting trouble getting their cryptocurrency out of the exchange, leading many customers to believe the exchange's funds were gone along with the CEO. On February 9, news broke that Cotten had, in fact, taken the passwords to all the firm's crypto assets with him to the afterlife. QuadrigaCX's customers were stunned to learn their crypto was inaccessible.

In a sworn affidavit filed January 31 with the Nova Scotia Supreme Court, his widow, Jennifer Robertson, said the exchange owes its customers roughly 250 million CAD ($195 million USD) in both cryptocurrency and fiat. QuadrigaCX's customers were outraged to learn that the exchange filed an application for creditor protection in the Nova Scotia Supreme Court, citing issues with locating "very significant cryptocurrency reserves held in cold wallets."

Ernst & Young (EY), the court-appointed monitor in the QuadrigaCX bankruptcy case, released its fifth report in June 2019. According to the report, Cotten had allegedly used customer funds for years to enrich himself and his wife (then girlfriend). Significant volumes of customers' cryptocurrency were transferred off the Quadriga platform and into accounts controlled by Cotten on competitor exchanges. Quadriga customers' cryptocurrencies were then either traded on these exchanges or used as security for a personal margin trading account established by Cotten. Quadriga's cryptocurrency reserves ultimately suffered due to his trading losses as well as incremental fees charged by these competitor exchanges.

Ernst and Young also essentially claimed that Cotten treated Quadriga's user funds like a personal bank account, identifying significant transfers of fiat to Cotten and his wife, Jennifer Robertson. The two took expensive vacations, made use of private jets, and bought numerous properties. The assets they accumulated—including real estate, cash, an airplane, a sailing yacht, luxury vehicles, and gold and silver coins—had a value of approximately $12.0 million CAD.

Finally, the report addressed the significant flaw in Quadriga's operating infrastructure that initially grabbed headlines around the word. "In addition, the Monitor understands passwords were held by a single individual, Mr. Cotten, and it appears that Quadriga failed to ensure adequate safeguard procedures were in place to transfer passwords and other critical operating data to other Quadriga representatives should a critical event materialize (such as the death of key management personnel)."

6. Ransomware

In the wake of the Colonial Pipeline and Kaseya hacks, ransomware continues to plague both the public and private sectors around the globe. Ransomware goes beyond simple financial crime, as in recent months these attacks have affected the ability of hospitals to provision lifesaving care and the ability of utilities to reliably meet customer needs for basics like electricity, while government agencies at all levels have suffered incursions that expose sensitive data.

The rapid growth of ransomware-as-a-service operations like REvil, Netwalker, and Darkside has become lucrative business for threat actors. These recent attacks against critical infrastructure prove that ransomware doesn't only impact individuals. On June 3, 2021, the United States Justice Department announced a shift in priorities towards ransomware incidents, classifying them as critical threats to national security. FBI Director Christopher Wray recently compared the bureau's shift to global ransomware threats to the agency's shift to the threat of global terrorism after the 9/11 attacks. According to Wray, the FBI is currently investigating over 100 different software variants used in ransomware attacks.

In order to adequately counter ransomware, information sharing is key. In mid-June, RaaS operator REvil announced it had updated its ethos and its expected behavior for consideration in choosing ransomware victims, including deeming schools and hospitals off-limits for attacks. This updated methodology was most likely an effort to lower the REvil profile so as not to become a priority target for US DOJ.

Ransomware-as-a-Service (RaaS)

In RaaS operation models, the malware developers partner with third-party affiliates (hackers) who are responsible for gaining access to a network, encrypting devices, and negotiating the ransom payment with the victim. As a result of this relatively new model, ransomware can now be easily used by bad actors who lack the technical capability to create the malware themselves but are more than willing and able to infiltrate a target.

Ransom payment are then split between the affiliate and the operator (developer). This split between ransomware operators and the affiliate who caused the infection is often a telltale sign of RaaS models. In most RaaS models, this split is between 15-30% to the operator and 70-85% to the affiliate.

Combating Ransomware

Blockchain analytics provide the critical cryptocurrency intelligence needed to trace ransomware actors. Only by working together through groups like the Ransomware Task Force can cryptocurrency intelligence firms counter these threat actors. It is crucial to not only trace ransomware proceeds to find and stop the operators, but also to harden systems and educate the public on how these compromises occur in order to properly mitigate disruption. Incident response firms and cybersecurity organizations have vast databases of ransom payments from their clients; identifying and tracking these funds can aid in building a full profile of the ransomware group.

Because ransomware actors use public blockchains for receiving payments, all transactions can be viewed on the chain, enabling law enforcement (or anyone) to trace the flow of funds. Utilizing blockchain analytics tools provides additional intelligence to the trace and investigation, such as identifying when the funds have been deposited into an exchange. Once the funds reach a centralized exchange, law enforcement can stop the movement of funds by requesting that the exchange freeze the account and, if users had to undergo a KYC process, it can be possible to identify the individual behind the address.

Best Practices to Minimize Damage

There are several steps that companies can take to minimize the damage from ransomware attacks.

Preventative measures include:

- Prepare an incident response/business continuity plan and have it on hand before an attack occurs.
- Choose an incident response firm that uses effective blockchain analytics and cryptocurrency intelligence software, such as CipherTrace, to track the cryptocurrency payments made to the hackers.
- Consider purchasing cybersecurity insurance.
- Back up your system and test backups.
- Enable logs to ensure you can gather as much information as possible about the hackers and the attack before making the ransom payment.
- Evaluate whether making a ransomware payment qualifies as a sanction violation. Sanctions violations can result in costly civil fines and even prison time for the ransomed party.

Reactive measures include:

- Pay in bitcoin; avoid using anonymity-enhancing technology or privacy coins to pay ransoms. This way investigators can more easily track flow of funds to identify potential off-ramps and aid in seizure of assets.
- Report all ransomware attacks to national law enforcement.

7. SIM Swap

In a SIM-swapping attack, hackers use social engineering—including stolen credentials purchased on dark markets—to deceive a telecom provider into transferring the victim's phone number to a SIM card (physical or virtual) that they control. This has been exasperated by advances in technology that now allow the customer service teams of service providers to quickly move a number to a new SIM. This is typically reserved for cases when a subscriber's phone is lost or stolen. Once cybercriminals receive the phone number, they can use it to reset passwords and break into the victim's accounts, including accounts on cryptocurrency exchanges. Large cryptocurrency investors are increasingly targets of this attack, which typically starts with the hacker gathering information about the victim through phishing emails or purchasing it off the dark web.

How a SIM Swap Works

The attack is often initiated through social engineering or by compromising an insider, often at a retail location. Lieutenant John Rose of the Silicon Valley REACT Task Force said, "If you're working at a mobile phone store and making $12 an hour and suddenly someone offers you $400 to do a single SIM swap, that can seem like a pretty sweet deal."

Using the stolen identity, the hacker contacts the victim's mobile service provider and asks the provider to port the victim's phone number to the scammer's SIM.

By using SIM swapping, the hacker can suppress security alerts or notifications because, once their phone numbers are switched to the hacker's SIM, the victim has no voice, email, or SMS service on their phones. As a result, they is unaware of any highly unusual transfers until the thieves have made off with their funds.

Protecting Against SIM Swapping

Preventing SIM swapping is nearly impossible for users due to the nature of the vulnerability in the business processes of their cell phone company. Users can reduce the impact of a SIM swapping attack by not using their phone numbers for two-factor authentication and two-step verification in which the second factor is an SMS or a call placed to a mobile phone. Where possible, users should use stronger 2FA/MFA factors such as app-based two-factor authentication or even hardware wallets.

Additionally, customers can call their phone providers and enable a separate PIN. For example: "All T-Mobile accounts are assigned a 6-15 digit PIN. All accounts have this protection and a customer's number cannot be ported without verification of that PIN. We also use this PIN to authenticate customers when they call Care."[1]

Case Studies

In early 2018, a hacker used this technique to allegedly steal $23.8 million from a wealthy investor who, incidentally, is suing AT&T for the millions in stolen loot along with an additional $200 million in punitive damages. By the Fall 2018, hackers used SIM swapping to break into CrowdMachine, a California-based cryptocurrency startup, and steal all of its reserve coins, worth $14 million. In July 2018, Bulgarian police arrested three suspects on suspicion of stealing $5 million via SIM swapping. In the same month, California police charged a 20-year-old college student with stealing $5 million. In November 2018, the Silicon Valley REACT team arrested a 21-year-old who allegedly stole $1 million using the same technique.

In February 2021, the European law enforcement agency Europol arrested ten people for their role in a series of SIM swapping attacks targeting thousands of victims throughout 2020, including famous internet influencers, sport stars, musicians, and their families. The attackers are estimated to have stolen $100 million worth of cryptocurrencies.

---

[1] Jacinto, P. (2020, July 7). *How T-Mobile Helps Customers Fight Account Takeover Fraud.* T-Mobile Newsroom. https://www.t-mobile.com/news/press/how-to-fight-account-takeover-fraud

SIM swaps usually come in three major flavors:

1. Social engineering
   Example: "Hi I lost my phone and I have an emergency and I need to transfer my phone number to a new phone asap because I'm expecting a very important call. Why yes, I do know my social security number, home address and cats name."[2]
2. Breaking into the computer of an entity (e.g., a cell phone kiosk at the mall) that has privileged access to port phone numbers. This has been done using phishing, physical attacks, etc.
3. Insiders at cell phone companies simply selling SIM swaps to attackers.

Additional useful advice on avoiding SIM swaps is available at the University of British Columbia's Privacy Matters website.

8. Investment Scam

Investment scams are old scams simply dressed up in new clothing—Bitconnect is a good example. It's simple: you buy Bitconnect coins (BCC) and then invest the Bitconnect coin via a hosted lending platform (Bitconnect.co). Other people borrow the Bitconnect coins, do something, and pay back the loan. On its surface, this does not sound overly fraudulent to the inexperienced investor.

Bitconnect claimed to return 1% per day, an impossibly high consistent return. This also indicated that anyone borrowing Bitconnect would need to pay at least 1% a day, which should be an immediate red flag—either you're borrowing money from a loan shark or your investment risk is so high that you probably should not be borrowing money to engage in that high-risk activity.

Not surprisingly Bitconnect turned out to be a Ponzi scheme (early investors are simply paid out from later investors). As long as investments increase the Ponzi scheme will work, but at some point the pool of available investors will dry up or someone will determine it's a Ponzi scheme (destroying investor confidence). In January 2018, two weeks after the Texas State Securities Board issued a cease-and-desist to the company calling it a Ponzi scheme due to its failings in user earnings transparency and misleading statements, Bitconnect shut down and the price of the Bitconnect coin crashed.

There were subsequent follow-up scams: a secondary coin called Bitconnect X (BCCX) and an attempt at an initial coin offering (ICO). Although various courts issued cease-and-desist orders it's not clear that there was any legal entity (e.g., corporation) against which to actually apply the order. One person was subsequently arrested in India, but no funds were recovered and later-stage investors of course lost most or all of their money (in addition to the people who bought Bitconnect (BCC) coins and did not lend them out due to the value of BCC crashing).

More than three years later, in May 2021, the Securities and Exchange Commission (SEC) filed a civil lawsuit in federal court in Manhattan against five promoters of the virtual asset BitConnect. The lawsuit alleges that the five failed to register themselves as brokers—as required by law—before promoting the sale of unregistered securities, raising over $2 billion from retail investors.

[2] Franceschi-Bicchierai, L. (2019, May 13). *AT&T Contractors and a Verizon Employee Charged With Helping SIM Swapping Criminal Ring.* Vice. https://www.vice.com/en/article/d3n3am/att-and-verizon-employees-charged-simswapping-criminal-ring

This is not the first time the SEC has charged virtual currency promoters for defrauding retail investors. Those looking to promote virtual currencies should proceed with caution as such actions may constitute a sale of a security. The fact that BitConnect was defunct for over three years before the SEC filed this lawsuit shows their willingness to pursue violations of the Securities Act, no matter when they were conducted.

9. High-Profile Doubler Scam

Bitcoin doubler scams are simple and commonly propagated over social media by criminals. Doubler scams promise new investors—typically under the guise of a prominent, high-profile individual—that by simply sending funds to a specific address they will be sent back double the funds they initially invested. These scams are typically time-sensitive, prompting a sense of urgency in its victims in hopes that they are less likely to think critically about the offer.

These scams typically target users that are less familiar with cryptocurrency and scammers will typically pose as high-net worth individuals such as Bill Gates or Elon Musk under the guise that they are trying to give back to the community. This is typically done through shared screen shots of doctored social media posts or altered videos of past live-streams with newly embedded messages urging people to send funds to a specific address. These scams are sometimes given an extra sense of legitimacy through the use of vanity addresses that contain the high-profile individual's name.

These scams are often easy to identify because they are broadcast by new accounts with no ties to the high-profile individual they claim to be linked to. However, in July 2020, multiple trusted accounts on Twitter fell victim to a hack. The hacker was then able to proliferate a high-profile doubler scam across the globe—the largest of its kind. Ultimately, the Twitter hacker was able to steal $125,000 from over 430 victims—most of which came after many high-profile, noncrypto- related accounts were compromised.

Case Study

On July 15, 2020, Twitter accounts for multiple high-profile cryptocurrency exchanges, public figures, and various entities were taken over by hackers promoting a Bitcoin doubler scam. The Twitter accounts of popular cryptocurrency-related users AngeloBTC, Binance, Binance CEO Changpeng Zhao, CoinDesk, Coinbase, Gemini, Kucoin, and Tron Founder Justin Sun were hacked. Each of these accounts posted or retweeted the following:

The website claims to be running a 5,000 BTC giveaway under the condition that if an individual sends 0.1 BTC to 20 BTC to the contribution address, then CryptoForHealth will send twice the amount back.

After the initial wave of Tweets, multiple other accounts were compromised including Jeff Bezos, Uber, Barack Obama, Joe Biden, and Elon Musk. These compromised accounts reference the Bitcoin doubler scam directly and included the BTC deposit address rather than redirecting victims to a website. As a result, the amount of Bitcoin in the provided address started to skyrocket.

Screenshot from U.S. President Joe Biden's compromised Twitter account, promoting the scam

Mitigating Doubler Scams

While the exploitation of trust markers like multiple verified Twitter accounts was an attempt to fool users into thinking the Bitcoin Doubler scam was legitimate, the amount the hacker pocketed was minuscule when compared to the vast reach of the compromised accounts. This could be attributed to two main factors: proper AML practices at exchanges prevented new users from sending their coins to the hackers while the scam was at its peak, and crypto users are becoming more informed when it comes to common crypto scams.

It is likely that most victims of the scam already had accounts open at crypto exchanges because it would be nearly impossible to open an account at a reputable exchange and deposit and transfer funds in one day, even through ACH transfers. Exchanges where users could open accounts more quickly would typically request fiat deposits in wires, not ACH. These accounts would not be able to trade any crypto until the wires clear, which could take up to three days. This likely prevented the hacker from exploiting those that were not already holding cryptocurrency or maintaining accounts at exchanges.

10. Extortion

Online extortion attempts have increased dramatically since the wider adoption of cryptocurrency. One flavor, in particular, is especially common—"sextortion." Criminals are able to personalize their communications using data derived from breaches at Yahoo!, Experian, and Facebook to dupe email recipients into believing they have been recorded watching online pornography or involved in other compromising activities. In one example, the extortionist threatens to publicize a split screen video with one half showing the recipients in the act while the other half displays the video they had been watching at the time. The "sextortionist" offers to let the victims off the hook if they send payment to a bitcoin address.

Sometimes, the extortionist claims to have infected a porn site with malware that used the victims' computers to record keystrokes in order to gain access to the display screen and webcam. The extortion email shows a real password from some point in the past; however, these are acquired through data leaks and not through infected sites. These spear -phishing attacks add a layer of authenticity to the email, increasing the likelihood of a payout.

The scammers further claim to have collected the victims' contacts and threaten to send the video to the list if the ransom, typically anywhere from a few hundred to a little over a thousand dollars' worth of bitcoin, is not received. A CipherTrace analysis of online extortion payment addresses has determined that most of these online extortion emails are fraudulent, but the emails are intimidating enough that even innocent victims may pay out of fear.

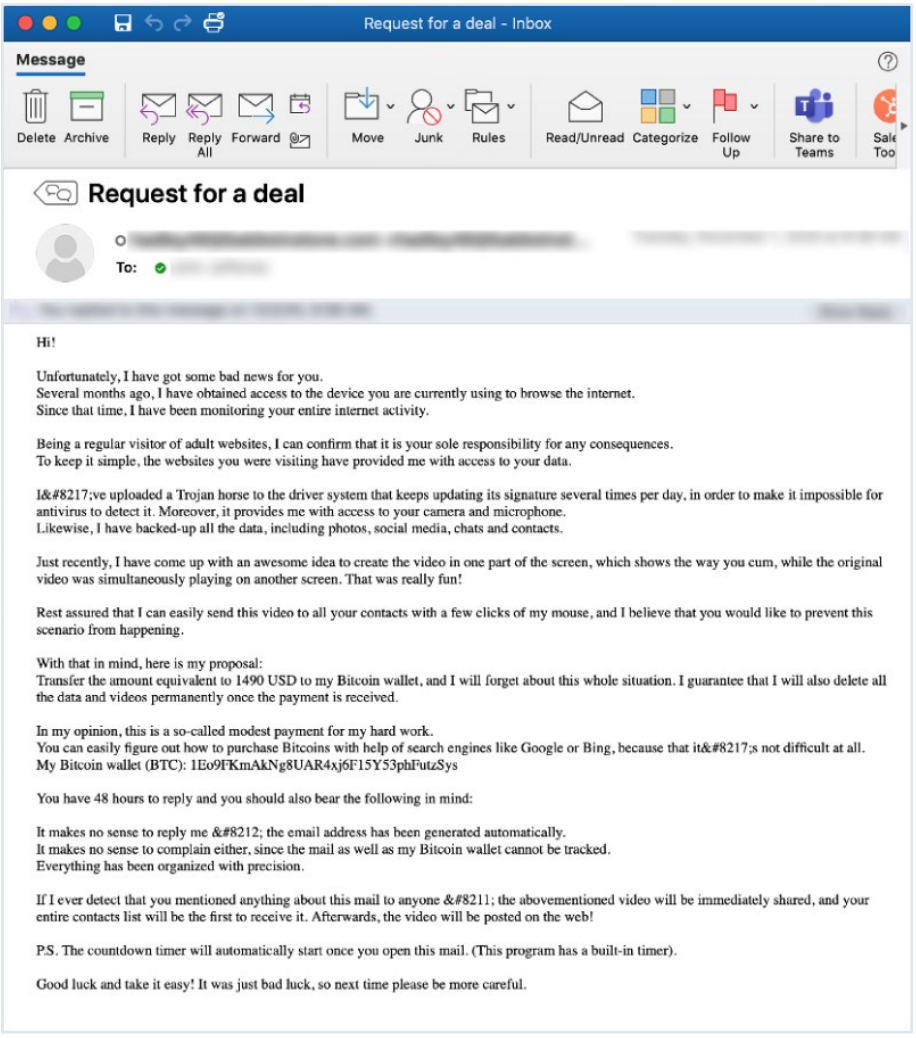
Preventing Extortion Attacks

More often than not, these extortion scams are fake—meaning paying or not will result in the same outcome: nothing. It is recommended not to pay extortions or reply to these emails.

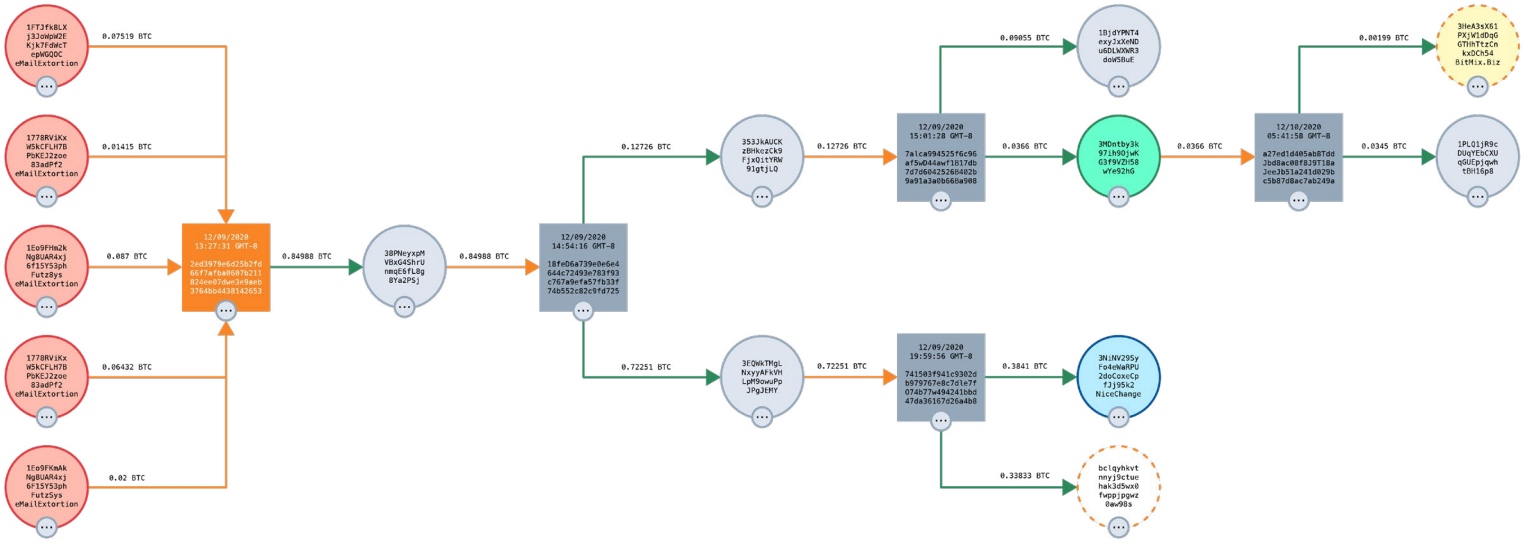
Extortion scams are often given a façade of legitimacy through spear-phishing. One thing people can do to protect themselves from this type of attack is to freeze all credit bureau accounts such as Equifax, Experian, Transunion, Innovis, and NCTUE (owned by Equifax). The APWG Crypto Currency Working Group also recommends consumers opt out of pre-approved credit offers by calling 1-888-5-OPT-OUT (1-888-567-8688) or visiting OptOutPrescreen.com, and opt out of the of the major data brokers, including Lexus Nexis (https://optout.lexisnexis.com/) and Acxiom (www.aboutthedata.com).

Case Study

Below is actual text from a real extortion email:



Blockchain analysis of this address, 1Eo9FKmAkNg8UAR4xj6F15Y53phFutzSys, revealed a total of 20 victims fell for the extortion scam. As seen in the trace below, in laundering the proceeds the scammer moved the consolidated funds into mixing services to obfuscate the flow of funds, in order to make it more difficult to identify which cryptocurrency exchanges they were using as an off-ramp. Cryptocurrency exchanges are typically used to convert cryptocurrency into fiat currency for use in the real world; however, many now collect KYC information that could identify the scammer if investigators were able to follow the crypto there.



Source: CipherTrace Cryptocurrency Intelligence

11. Bonus: Wallet Security

Fake Software Wallets

Creating a mobile application and getting it into the Apple or Google Play app stores requires work, but it is of course not impossible. As of the time of this report, there are 1.96 million apps in the Apple app store and 2.87 million in the Google Play app store. While both companies make an effort to ensure that malicious apps do not enter the store, it is of course impossible to prevent all such malicious applications due to the sheer volume of applications.

A number of malicious software wallets have been distributed via both app stores. The economics of it are simple; building a "fake" app and getting it into the app store can be done for a few thousand dollars. If even a single user falls prey to the scam, the attacker can easily make a profit.[3]

It is especially difficult for users to determine if an application is "real" or "fake" due to the ability of an organization to create professional-looking applications and websites and populate positive application ratings (Google "buy app ratings" and you'll see a huge number of ads for companies). Picking one software wallet at random resulted in finding:

1. A legitimate-looking application and business name
2. A business name and developer company name in the app that did not match up exactly
3. An allegedly Ukrainian CEO
4. An alleged US based corporation with approximately 12 employees
5. No corporate records found in searches
6. A single five star review of the application in the Apple app store, and almost 2000 reviews in the Google Play app store

[3] Albergotti, R. (2021, March 30). *He believed Apple's App Store was safe. Then a fake app stole his life savings in bitcoin.* Washington Post. https://www.washingtonpost.com/technology/2021/03/30/trezor -scam-bitcoin-1-million/

The lack of reviews (a single review only in the Apple app store versus almost 2,000 in the Google Play app store) combined with the inability to track down the company (beyond a website) indicates this may be a scam. The single application review is odd—a scammer would typically spend some money on getting fake positive reviews for the Apple app store. Additionally, the developer responds to any negative review in the Google Play app store, so either this is a long-term scam or the developer focuses mostly on the Android market and not the Apple market.

Ultimately, it is very difficult to determine the trustworthiness of a mobile application unless it is from a very large, well-known company. Additionally, even if you can verify the application, they may sell the application or the company to a third party; for example, there are documented cases of malicious actors attempting to buy web browser extensions.[4]

Fake Hardware Wallets

There are two kinds of hardware wallets: those that plug into a computer's USB port and essentially behave like a key management service, and those that are effectively a selfcontained computer with a screen and can do data transfer by consuming and displaying QR codes. One simple truth of USB devices is that it is almost impossible for a user to determine if they are safe to plug in to their computer or not.[5] An attacker can, for example, load USB storage with malware that is executed when plugged into the PC, either as an autorun program or by configuring the USB device to send commands to the computer (by pretending to be a keyboard/mouse, for example). A modified device can be spotted if a user disassembles the device and examines it, e.g., if it contains extra wires and chips soldered in after it was manufactured. It should be noted that if an attacker were to create a custom board and manufacture it (which can be done in small batches for under $10 per board) the only way to notice this would be to compare the hardware to a manufacturer's schematic (which are generally not available).

Source: Bitcoin Magazine

[4] *Many temptations of an open-source chrome extension developer · Discussion #670 · extesy/hoverzoom. (n.d.)*. GitHub. Retrieved September 9, 2021, from https://github.com/extesy/hoverzoom/discussions/670

[5] Open Source Security. (April 21, 2019). *Hypothetical security: What if you find a USB flash drive?* Open Source Security Podcast. https://opensourcesecurity.io/2019/04/21/episode-142-hypothetical-security-what-if-you-finda-usb-flash-drive/

In 2020, a data breach occurred at the hardware wallet company Ledger. Subsequently, an attacker mailed out to various customers "new" hardware wallets that had been modified to run malware when plugged into a computer. In 2021, multiple confirmed incidents of users receiving a new, shrink-wrapped hardware wallet along with a letter from the CEO were reported. These hardware wallets had been modified to include aUSB storage chip. Older reports include users buying hardware wallets on Amazon, but the hardware wallet had already been initialized (a step the user is supposed to do in order to ensure it is securely set up). If a user used an already initialized hardware wallet, then the attacker would already have the seed phrase used to initialize it, allowing them to hijack any funds associated with that hardware wallet.[6]

In general, when buying a hardware wallet, it is probably best to buy directly from the company and to ensure that the setup and initialization procedures are followed. Unsolicited hardware, much like unsolicited support or emails from a company, should either be ignored or reported to the company in question. Theoretically, any hardware device could be disassembled and examined for extra wires/chips—but realistically this is not an option for most users, and it is possible for an attacker with sufficient motivation and funding to have a board manufactured that appears identical to the real thing using counterfeit or rebadged chips or real chips loaded with malicious software.

[6] *Ongoing phishing campaigns.* (2021, June 17). Ledger. https://www.ledger.com/phishing-campaigns-status

Conclusion

There is a strong misconception that the immutable properties of DLT systems and the encrypted nature of blockchain technologies make them inherently secure. However, as this paper illustrates, this is far from the case. Unaudited smart contracts can result in massive hacks for DeFi platforms. Smaller blockchains risk 51% attacks if one person or organization is able to amass too much hash power. People new to the space can easily fall victim to common scams and extortion techniques, and phishing attacks will continue to target the human element behind DLT systems, resulting in anything from centralized exchange hacks to loss of personal private keys.

These 10 DLT attack types highlight the most common threat vectors resulting in cryptocurrency losses all around the world:

1. Exchange Hack
2. DeFi Hack
3. 51% Attack
4. Phishing (for private keys)
5. Rug Pull/Exit Scam
6. Ransomware
7. SIM Swap
8. Investment Scam
9. High Profile Doubler Scam
10. Extortion

Many virtual assets can be easily converted into fiat currency, making them both the target and the mechanism of many of these cloud-based crimes. The instant, pseudo-anonymous nature of crypto enables new criminal business models such as ransomware and online extortion. As centralized exchanges have hardened their cloud security controls, attackers have pivoted to targeting human users with social engineering attacks and confidence schemes. Fortunately, because of the open nature of most blockchains, blockchain analytics tools provide unprecedented capabilities to trace virtual assets in order to investigate crypto crimes, seize assets, and prosecute bad actors.

References

Albergotti, R. (2021, March 30). *He believed Apple's App Store was safe. Then a fake app stole his life savings in bitcoin*. Washington Post. https://www.washingtonpost.com/technology/2021/03/30/trezor-scam-bitcoin-1-million/

Franceschi-Bicchierai, L. (2019, May 13). *AT&T Contractors and a Verizon Employee Charged With Helping SIM Swapping Criminal Ring*. Vice. https://www.vice.com/en/article/d3n3am/att-and-verizon-employees-charged-simswapping-criminal-ring

Jacinto, P. (2020, July 7). *How T-Mobile Helps Customers Fight Account Takeover Fraud*. T-Mobile Newsroom. https://www.t-mobile.com/news/press/how-to-fight-account-takeover-fraud

Many temptations of an open-source chrome extension developer · Discussion #670 · extesy/hoverzoom. (n.d.). GitHub. Retrieved September 9, 2021, from https://github.com/extesy/hoverzoom/discussions/670

Ongoing phishing campaigns. (2021, June 17). Ledger. https://www.ledger.com/phishing-campaigns-status

Open Source Security. (April 21, 2019). *Hypothetical security: What if you find a USB flash drive?* Open Source Security Podcast. https://opensourcesecurity.io/2019/04/21/episode-142-hypothetical-security-what-if-you-find-a-usb-flash-drive/