SECURANCE CONSULTING

the advantage of insight

BIT BY BITCOIN: CYBERSECURITY RISKS OF CRYPTOCURRENCY

www.securanceconsulting.com

BIT BY BITCOIN: CYBERSECURITY RISKS OF CRYPTOCURRENCY

Investors appreciate cryptocurrency, or crypto, for its decentralization, transparency, and flexibility. Organizations use the blockchain technology on which crypto relies to execute automatic replication across ledgers and increase privacy. Even formal banking institutions have adopted blockchain-based platforms to create faster and less costly transactions among small to medium-sized businesses. Crypto has advantages for enterprises and individuals alike.

Benefits of Crypto

- **Decentralized**
- **Transparent**
- **Flexible**
- **Private**
- **Accessible**
- **Faster transactions**
- **Less costly transaction fees**

Meanwhile, the same distinctions between orthodox finance and crypto that entice investors to crypto can also come with potential risks. For example, conventional bank transactions are reversible, while those on a blockchain are not.[1] While this thwarts criminals from removing transactions or tampering with a ledger, it also makes it more difficult to rectify a fraudulent or accidental transaction.

Cybercriminals profit from the exploding value and relevancy of crypto. They defraud crypto exchange users, employ crypto-mining malware, or pilfer funds, sensitive information, and credentials. This whitepaper will explore the most common risks associated with crypto, including standard cybersecurity issues in the blockchain environment and situations unique to crypto platforms.

> "Cybercriminals profit from the exploding value and relevancy of crypto. They defraud crypto exchange users, employ crypto-mining malware, or pilfer funds, sensitive information, and credentials."

UNIVERSAL CYBERSECURITY RISKS

Cybersecurity is as much about people, policies, and procedures as it is about technology. Unsurprisingly, traditional cyber threats, such as phishing and malware, also affect crypto. While they may take distinctive forms due to blockchain's structure, the outcome for cybercriminals is the same.

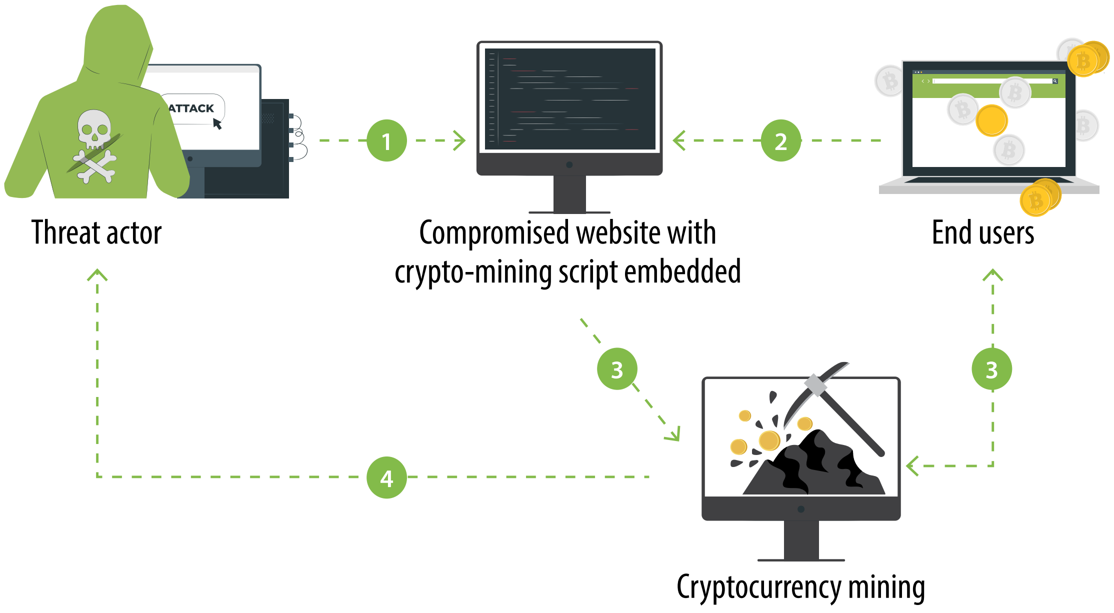
Phishing Attacks

Phishing attacks are a pervasive threat to all technologies, and crypto is no exception. Just as in traditional email phishing, cybercriminals may present as a reputable company, such as a trading platform, and coerce victims into supplying their credentials or clicking on a malicious link. Crypto phishing tactics include spear phishing, DNS hacking, phishing bots, and fake browser extensions.[2] No matter the method, the attacker's goal is to gain access to a victim's private keys and digital assets.

Malware

Crypto-mining malware is attackers' primary tool for hacking crypto. Cybercriminals use crypto-malware to mine a server by deceiving victims into installing malicious code using phishing tactics, or by injecting malicious code into websites.

Hackers use crypto-malware to hijack systems by exploiting crypto-mining.[3] Crypto-mining is the process that creates new crypto coins. It works by awarding crypto coins to data processors that authenticate the legitimacy of Bitcoin transactions on blockchain. Crypto-mining demands a massive quantity of processing power and energy[4]. Cybercriminals use malware to hijack these resources, then swipe the profits,.



1 The threat actor compromises a website

2 Users connect to the compromised website, and the crypto-mining script executes

3 Users unknowingly start mining crypto on behalf of the threat actor

4 Upon successfully adding a new block to the blockchain, the threat actor receives a reward in cryptocurrency coins

Source : ENISA

CRYPTO MANAGEMENT RISKS

Managing crypto as a digital asset comes with cybersecurity risks, as well. Crypto users access their digital assets using complex passwords called private keys. Hackers can steal private keys, like any other data. Unlike with conventional investments, however, crypto investors have sole responsibility for securing their keys. The techniques used to protect this information can introduce risks if not thoroughly understood.

Third-Party Applications

Crypto investors often use third-party applications to manage digital assets for tax reporting, key management, general accounting, and portfolio details. These applications also allow traders to watch crypto prices and calculate the potential returns of a trade. Personal and portfolio information sharing presents unique risks. Hackers can access this data through phishing, malware, or other attack vectors to which the application is vulnerable. For example, a cybercriminal swiped the data of more than 1,000 Cryptotrader.Tax (now Coin Ledger) users by phishing an employee's account and using the credentials to access sensitive customer information.[5]

> Personal and portfolio information sharing presents unique risks. Hackers can access this data through phishing, malware, or other attack vectors to which the application is vulnerable."

Key Management

Like any private key management, crypto key management requires understanding security threats to confidential data, such as phishing or malware. However, crypto transactions are irreversible, and crypto users have sole responsibility for their keys. If a hacker uses a stolen crypto key to access coins, there is no way to retrieve the funds. Hardware wallets, USB devices that generate and store crypto keys, may thwart attackers from accessing private keys.[6] In addition, using a smart multisig contract wallet requires multiple owners to sign off on all transactions—and cybercriminals to compromise more than one person to pilfer the wallet's contents.[7]

ISSUES WITH CRYPTO PLATFORMS

Crypto platforms function as exchanges for buying and selling digital currencies. While platforms have earned investors' trust, fraudulent sites posing as platforms have also challenged the market. Further, while decentralization is essential to crypto, it introduces unique security risks.

Advanced Training Required

Traditional training in cybersecurity best practices is not enough for crypto users. The browser plugins and tools involved in blockchain vary from those used in conventional finance and e-commerce activities. Likewise, each platform manages transactions uniquely[8] and may require a different approach to managing risk. For this reason, a firm grasp of potential threats and vulnerabilities and a regular security review and assessment of the systems involved are essential.

Fraudulent Platforms

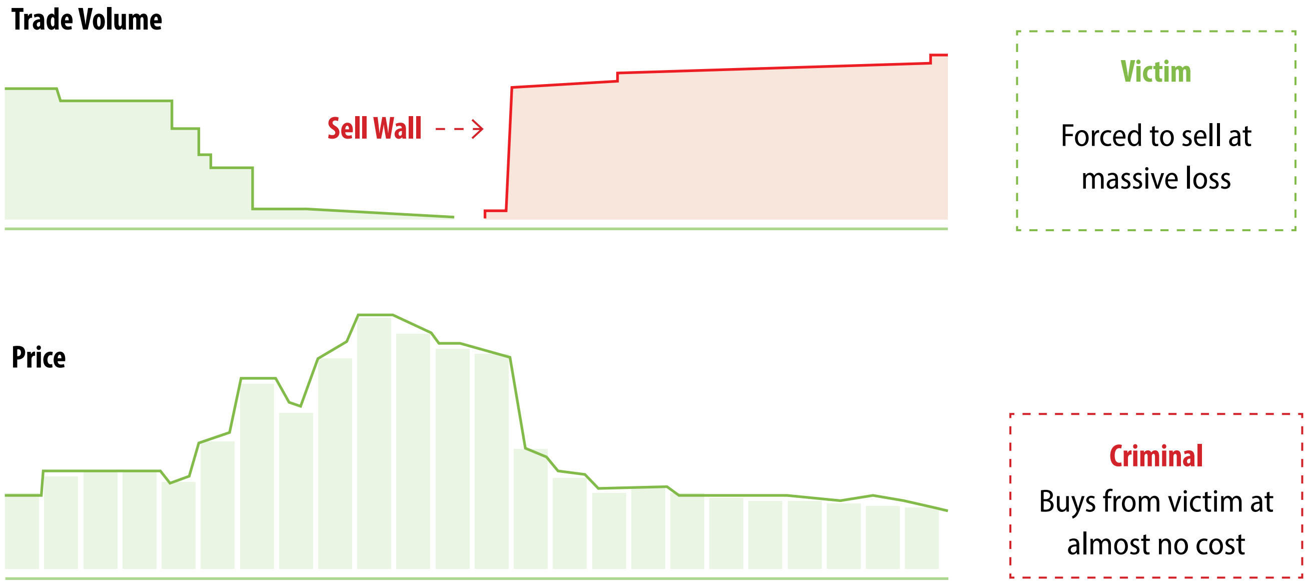
As new trading platforms appear, so do scams. Unfortunately, fraud can be as costly as a hack or data breach. For example, a bogus crypto company called OneCoin lured investors by disguising a multi-level marketing con as a legitimate currency system.[9] While the company sold courses on cryptocurrencies as their primary business, they falsely claimed that OneCoin mining worked like crypto. No blockchain model or payment system backed it up. The scheme defrauded investors of $4 billion.

API Interrupted

A cybercriminal can steal API keys from the trading platform and use this proprietary code to make trades and withdraw funds over time. CyberNews found that hackers exploit APIs to steal crypto from victims' accounts without withdrawal permissions, malware, or spyware by automating trades with their bots. These trades drain victims' wallets.[10]

The diagram below illustrates a sell wall, a manipulation method that involves creating artificial sell orders to lower crypto prices and buy them up cheaply. Attackers deploy bots to open thousands of orders far below market value. They then authorize those orders via stolen API keys and continue the cycle for millions of dollars' worth of transactions.

Sell Wall Via Stolen API Keys

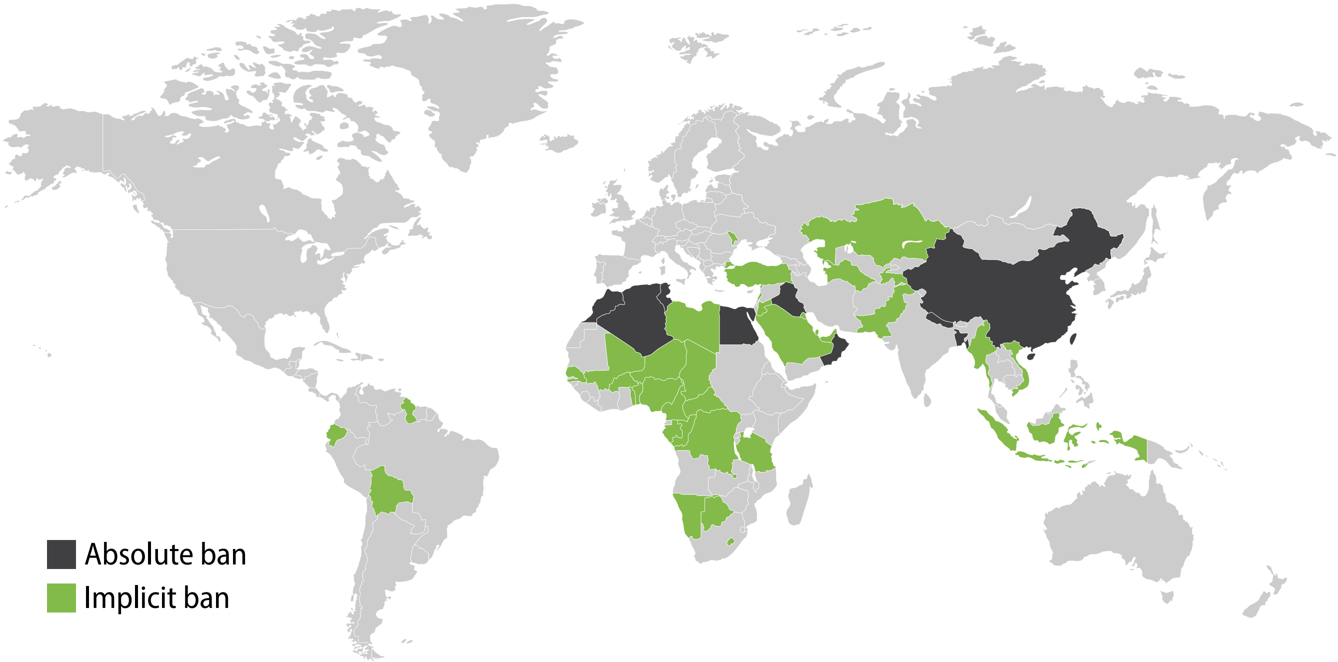


Source : cybernews.com

> "Hardware wallets, USB devices that generate and store crypto keys, may thwart attackers from accessing private keys."

Unregulated Exchanges

No governing body or agency directs the creation or trading of cryptocurrencies. This absence of regulation draws traders but also entices fraud artists, hackers, and cybercriminals. Governments worldwide have realized the dangers of crypto and are enacting laws, even outlawing transactions entirely.[11] Nine countries have banned crypto worldwide, while 42 more have implicitly banned it with banking restrictions.[12]



Countries Where Crypto is Directly Banned:

- China
- Tunisia
- Algeria
- Bangladesh
- Iraq
- Morocco
- Nepal
- Qatar
- Egypt

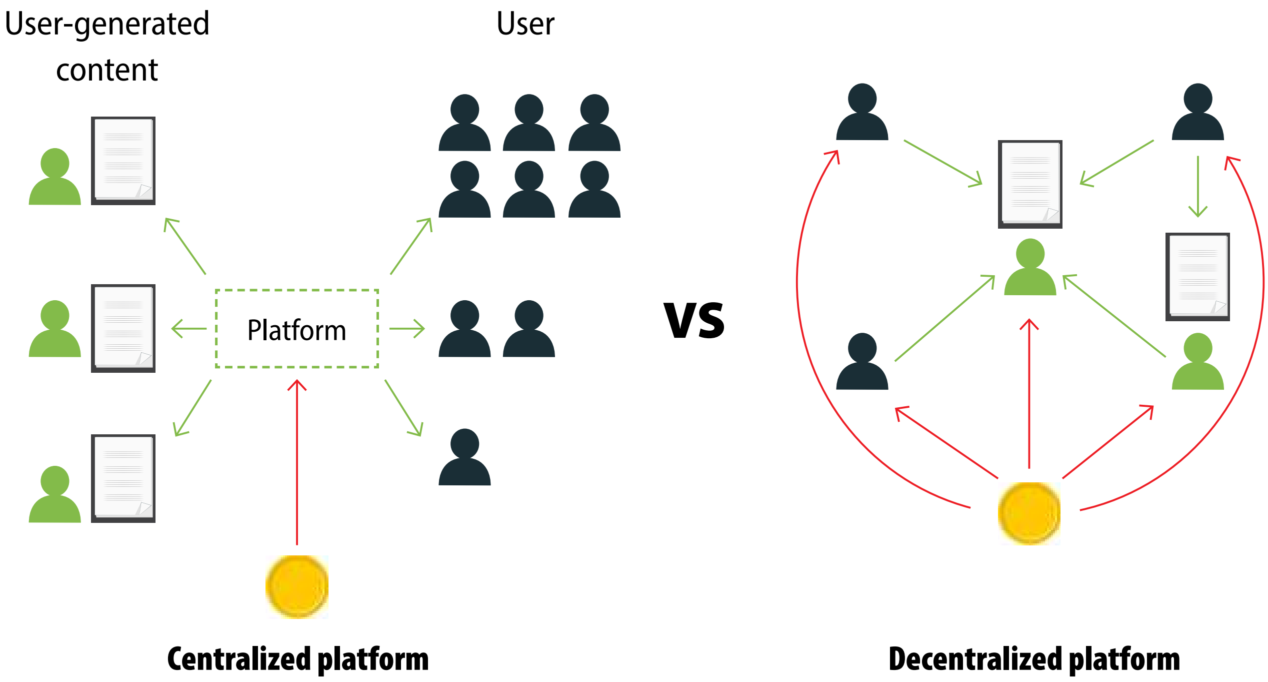
Countries Where Crypto is Implicitly Banned:

- Bahrain
- Benin
- Bolivia
- Burkina Faso
- Burundi
- Cameroon
- Central African Republic
- Chad
- Côte d'Ivoire
- Democratic Republic of the Congo
- Ecuador
- Gabon
- Georgia
- Guyana
- Indonesia
- Jordan
- Kazakhstan
- Kuwait
- Lebanon
- Lesotho
- Libya
- Macao
- Maldives
- Mali
- Moldova
- Namibia
- Niger
- Nigeria
- Oman
- Pakistan
- Palau
- Republic of the Congo
- Saudi Arabia
- Senegal
- Tajikistan
- Tanzania
- Togo
- Turkey
- Turkmenistan
- United Arab Emirates
- Vietnam
- Zimbabwe

Source: Susan Taylor, Law Library of Congress

Marketplace Security Risks

Centralization is the process of concentrating control and authority with a central entity; within an organization, this is typically senior management. Alternatively, decentralization within a system refers to the distribution of authority at various management levels. A centralized platform based on blockchain technology makes it easier for users to interact with digital assets. However, centralized marketplaces also inherit vulnerabilities that decentralized platforms avoid. For instance, while less challenging to implement, centralized platforms require centralized governance. Consequently, their transactions are slower, with fewer sources to verify the authenticity of records. While implementing a decentralized platform requires sufficient time and effort to safeguard against attacks, it increases both control and the speed of decision-making.[13]



BLOCKCHAIN RISKS

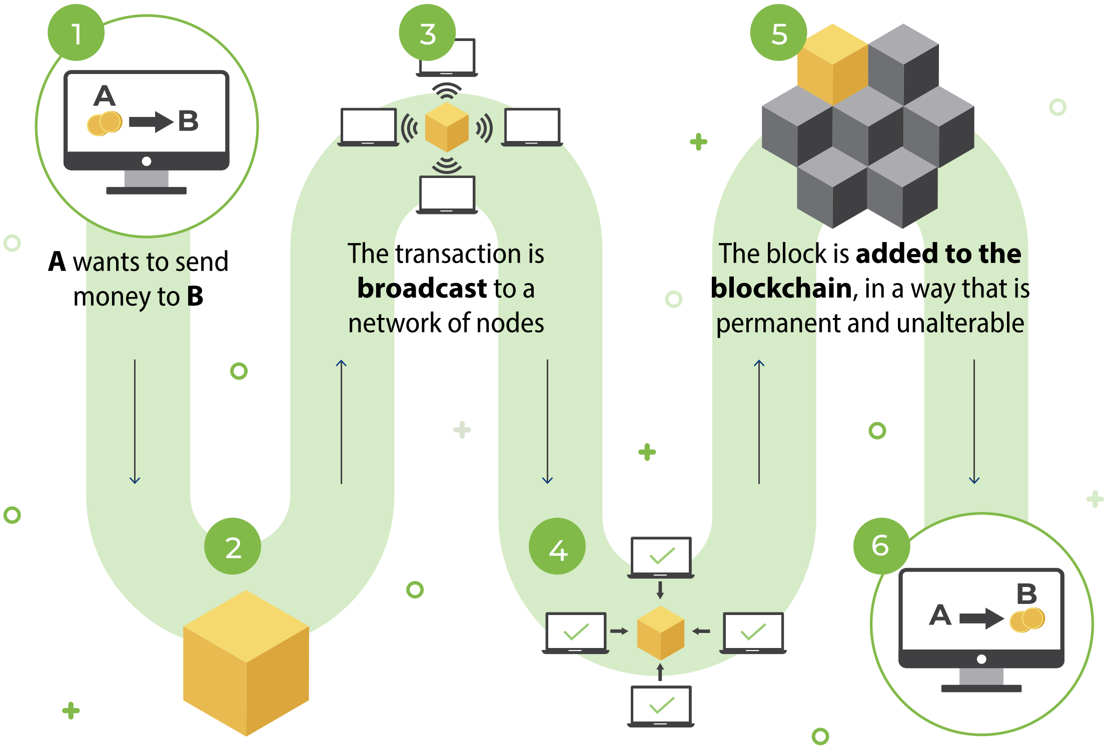
Traditional security methods often rely on a single trusted authority to verify information or store encrypted data. Hackers can target a sole mark to perpetrate denial of service attacks, inject malicious code, and extort data. In contrast, blockchain relies on consensus mechanisms to substantiate transactions. Each node has a complete copy of the same data and can secure the group more efficiently than one centralized authority. However, blockchain still has vulnerabilities connected to exploiting these consensus mechanisms, vulnerabilities in the code, and protocols.

Blockchain Protocols

A blockchain protocol is the rule set that must be agreed upon by all the nodes, or peers, in the network. These rules decide who can make a transaction or govern the distributed ledger. They also contain the blueprint for communicating between nodes on the network, outline how the network agrees on the next block in the chain, and determine what behavior will result from a transaction. It can be complex to integrate a mature and fitting protocol. Incorporating the technology may come with the choice between downtime and security risks or steeper transaction fees. A protocol may fit the preferred use case, such as allowing payments, but lack adequate support and require specialized service providers. Still, a survey from Deloitte found that 53 percent of respondents think that blockchain technology is a critical priority for their organizations.[14]

Blockchain-based projects require security resources during adoption, implementation, and beyond. To avoid managing the added security risks, IT departments traditionally phase out products when they are at the end of their life or are no longer supported by the vendor. Companies who take on blockchain projects must support them forever, or the assets no longer hold value.

How Blockchain Works



1 **A** wants to send money to **B**

2 The transaction is represented as a **block**

3 The transaction is **broadcast** to a network of nodes

4 The network **validates** the transaction

5 The block is **added to the blockchain**, in a way that is permanent and unalterable

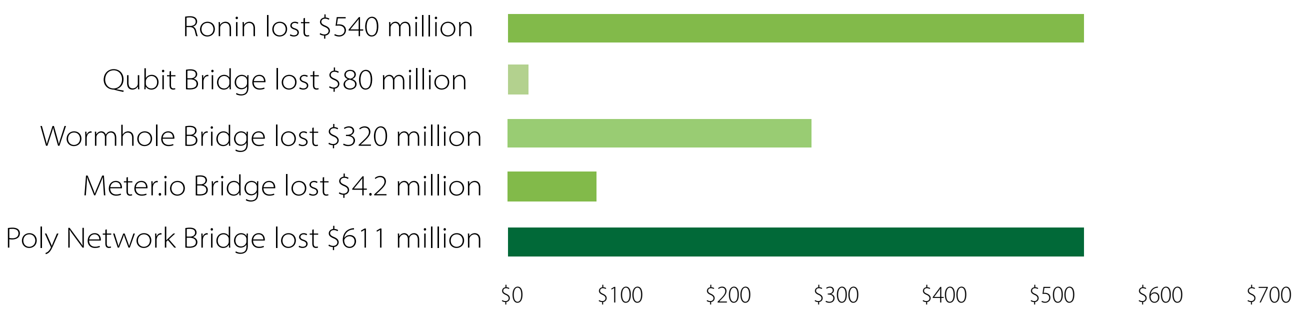
6 The **money moves** from A to B

Blockchain Bridges

A blockchain bridge allows the transfer of assets between two blockchains, despite different coins and rules. blockchain bridges are crucial to the crypto economy because they facilitate the exchange of digital assets from one blockchain to another. On the other hand, blockchain bridges are a desirable target for criminals because they need a reserve of coins to function. Bridges are also susceptible to attacks because any capital in the transfer is vulnerable to exploits targeting the platform.

Some of the biggest crypto hacks have involved blockchain bridges, such as Ronin, Qubit Bridge, and Poly Network.[15] In each event, the attacker found a vulnerability between a bridge and the blockchain. In the Ronin attack, the criminal used an exploit to input malicious data. The hacker exploited access rights between two conflicting rules in the Qubit Bridge event. An attacker may also hack private keys for one or more nodes in the bridge and use them to falsify network withdrawals, as with Poly Network.

> 53% of responding executives say that blockchain is a priority.[14]



51% Attacks

In "51%" attacks, hackers gain control of 51 percent of the computational power or available currency in a blockchain, giving them the consensus to revise transactions or concoct phony trades. Ethereum suffered two successful 51% attacks within five days of each other in 2020, resulting in the loss of millions. In response to the events, Ethereum Classic increased transaction confirmation times by as long as two weeks.[17]

> In **"51%"** attacks, hackers gain control of 51 percent of the computational power or available currency in a blockchain, so they can revise transactions or concoct phony trades.

Code Vulnerabilities

Even if identity verification is strict, cybercriminals can still inject code into registration forms and compromise them to access valuable user information. Cybercriminals can use these personal details to find the next target or create fraudulent accounts. Therefore, development teams responsible for configurations and implementations should conduct thorough testing and code reviews to minimize the likelihood of a security incident.

In one attack, cybercriminals robbed the Decentralized Autonomous Organization (DAO) of more than $50 million in digital currency through the exploitation[18] of smart contracts. A core feature of decentralization, these agreements enforce themselves through programming, rather than human commitment. The purpose of smart contracts is to automate rules and implement impartiality Yet, the programming behind smart contracts is historically prone to flaws[19], of which cybercriminals have taken advantage. Attackers exploit these decision-making tools when there are flaws in the code's logic or misunderstandings of specificity.

> Blockchain-based projects require security resources during adoption, implementation, and beyond.

MITIGATING RISKS

Crypto traders should follow best practices to mitigate cybersecurity threats. It is essential to use multifactor authentication, evaluate apps and websites for legitimacy, and understand crypto trading consequences. Individuals should also use hardware wallets, instead of storing crypto on platforms that may not be secure. Organizations should collaborate with experts to audit their systems, work with protocols, and develop security strategies rooted in best practices and cybersecurity frameworks.

Mitigating Risks to Individuals

- Understand the consequences and risks.
- Carefully evaluate all websites.
- Read the terms and conditions of all applications.
- Use multi-factor authentication.
- Practice caution with third-party applications.
- Do not use the trading platform as a wallet.
- Consider offline or hardware wallets.

Mitigating Risks to Organizations:

- Understand the consequences and risks.
- Hire a third-party security auditor to help find known vulnerabilities.
- Carefully analyze the maturity and suitability of any protocol.
- Be prepared for limited support by the platforms themselves.
- Before taking on any integrations, consult with an expert in the protocol.
- Have a security strategy grounded in best practices.
- Consider cyber insurance to help reduce the cost of a breach.

IN CONCLUSION

The exploding value and relevance of crypto continue to inspire the adoption of blockchain platforms. Unfortunately, cybercriminals have also entered the arena. They defraud crypto exchange users, use crypto-mining malware, or steal funds, sensitive information, and private keys. More sophisticated attackers may go after code vulnerabilities in platforms or third-party apps, influencing compliance risk and leaving organizations liable.

It is paramount for organizations that use crypto to understand cybersecurity risks. Organizations must defend against vulnerabilities with crypto-specific education, evaluate their system and staff vulnerabilities, follow compliance measures, employ best practices, and monitor potential threats. Businesses that use blockchain technology and related external protocols should have solid security strategies. They should also periodically engage third parties to assess their processes and systems for risks and vulnerabilities. Adequate security resources during adoption, implementation, and beyond are essential to the security of any blockchain-based project.

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://www.ledger.com/academy/crypto/why-decentralization-matters

2. https://101blockchains.com/crypto-phishing-attacks/

3. https://www.investopedia.com/terms/c/cryptojacking.asp

4. https://www.cnet.com/personal-finance/crypto/bitcoin-mining-how-much-electricity-it-takes-and-why-people-are-worried/

5. https://finance.yahoo.com/news/hacker-stole-1-000-traders-211509731.html?guccounter=1

6. https://crypto.com/university/what-is-a-hardware-wallet

7. https://whatincrypto.com/concept/what-is-multi-signature-multi-sig/

8. https://www.tradestation.com/learn/market-basics/cryptocurrencies/what-makes-crypto-unique/how-different-is-one-crypto-from-another/#:~:text=Most%20crypto%20assets%20rely%20on%20blockchain%20technology%2C%20which,and%20scalable%20medium%20of%20exchange%20than%20traditional%20methods. Missing Cryptoqueen: FBI adds Ruja Ignatova to top ten most wanted - BBC News

9. https://www.bbc.com/news/world-us-canada-62005066

10. https://cybernews.com/security/report-how-cybercriminals-abuse-api-keys-to-steal-millions/

11. https://fortune.com/2022/01/04/crypto-banned-china-other-countries/

12. https://tile.loc.gov/storage-services/service/ll/llglrd/2021687419/2021687419.pdf

13. https://code-care.com/blog/how-to-create-a-cryptocurrency-exchange-website/

14. https://www2.deloitte.com/content/dam/insights/us/articles/2019-global-blockchain-survey/DI_2019-global-blockchain-survey.pdf

15. https://www.wired.com/story/blockchain-network-bridge-hacks/

16. https://www.investopedia.com/terms/1/51-attack.asp

17. https://www.newsbtc.com/news/how-51-attacks-ethereum-classic-crypto/

18. https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/

19. https://stacks.org/bringing-clarity-to-8-dangerous-smart-contract-vulnerabilities/

Bit by Bitcoin: Cybersecurity Risks of Cryptocurrency

SECURANCE CONSULTING
the advantage of insight

13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com