Adversary Tactics and Techniques specific to Cryptocurrency Scams

Andrea Horch[1], Christian H. Schunck[2] and Christopher Ruff[3]

Abstract: At the end of the year 2020, there was a steep uptrend of the cryptocurrency market. The global market capitalization of cryptocurrencies climbed from 350 billion US$ in October 2020 to almost 2.5 trillion US$ in May 2021 and reached 3 trillion US$ in November 2021. Currently, there are more than 17,600 cryptocurrencies listed on CoinMarketCap. The ample amount of money within the market attracts investors as well as scammers and hackers. Recent incidents like the BadgerDAO hack have shown how easy it is to steal cryptocurrencies. While all the standard scamming and hacking techniques such as identity theft, social engineering and web application hacking are successfully employed by attackers, new scams very specific to cryptocurrencies emerged, which are the focus of this paper.

Keywords: cryptocurrency, scam, distributed ledger technology, blockchain, digital wallet, digital identities

1 Introduction

The charts of Bitcoin and altcoins (all other coins, which offer an alternative to Bitcoin) on CoinMarketCap show two huge continous uptrends (bullruns). The first very steep uptrend took place in 2017/2018, the other one started at the end of 2020 and is still ongoing. Even though scammers have always been active in cryptocurrency the amount of scams and hacks have increased sinificantly with the global marketcap. According to [Sta20] the value of cryptocurrencies lost to security threats increased nine-fold between 2020 and 2021. This paper gives an overview novel kind of scams, which are very specific to the cryptocurrency ecosystem. In the following we give a brief overview of the literature, introduce cryptocurrency specific terminology, present factors that make attacks cryptocurrency specific and give examples of such attacks and then discuss the results in the conclusion.

Fraunhofer IAO, Fraunhofer Institute for Industrial Engineering IAO, Nobelstrasse 12, 70569 Stuttgart, Germany, firstname.lastname@iao.fraunhofer.de

[1] https://orcid.org/0000-0001-9384-316X

[2] https://orcid.org/0000-0002-7917-8180

[3] https://orcid.org/0000-0003-0484-4131

cbe doi:18.18420/OID2022-10

2 Literature Review

Security problems, hacks and scams related to cryptocurrencies and relevant tools have been reported in several papers. The earliest classification of scams in the context of bitcoin was carried out in [VM15] where scam have been classified into four main categories: high yield investment programs (HYIPs) or Ponzi schemes, mining scams, scam wallets and exchange scams. The authors of [Ba21] provide a more recent overview of scams and present a fairly broad taxonomy, which does not fulfil rigorous requirements such as proposed in [NVM13]. Some of the identified scams have only a loose link to cryptocurrencies. For example, typical ransomware attacks are included in the taxonomy, where the role of cryptocurrency is limited to being a means for ransom payment. Other work closely investigate smart contracts which are very deeply linked to the technologies underlying cryptocurrencies: attackers both exploit vulnerabilities in existing smart contracts [ABC17] and engineer apparently vulnerable smart contracts with hidden traps as honeypots [TSS19]. The study presented in [Tr22] reviews the current state of knowledge on kinds of existing cryptocurrency fraud. It provides a raw classification scheme and definitions of the frauds identified, but does not give any hints on the cryptocurrency-specific attributes of the presented frauds.

3 Terminology

Coins, Tokens, NFTs: According to [Le22] a cryptocurrency is a digital measure of value that can be tracked and transferred without the need of an intermediate authority (e.g. bank or government). Cryptocurrencies are built on and exist on a network called blockchain. A blockchain is an unbounded and immutable (append-only) digital ledger, which stores the information on every transaction made on a network in the form of linked blocks [Fo22]. The native cryptocurrency of a blockchain is called “coin”. Other currencies, which are not the native currency of a blockchain, but built on it, are called “tokens”. A non-fungible token (NFT) is a digital asset on a blockchain. The use of a blockchain allows to prove the authenticity and ownership of the NFT [Ri21]. An NFT is not a currency as currencies are not unique, e.g. all Bitcoins have the same value. NFTs are unique and e.g. used for artwork, where every artwork is unique and has a different value [Ri21].

Digital Wallets: Digital wallets are software applications used to interact with a cryptocurrency or blockchain. Wallets allow viewing balances, making transactions and other interactions with the underlying blockchain (i.e. staking, using smart contracts, etc.) [SSB20]. Digital wallets are a concept to more easily interact with the public key cryptography (PKC) functionality that is the basis of most blockchains and digital ledgers and store the key pair required to access and transfer the funds on a blockchain. The public key serves as an address whereas the private key is used as a password and should never be shared with anyone. Wallets facilitate the pairing of private and public keys and allow users to sign transactions using their private keys. The cryptographic function for building the key pairs allows to generate a public key from a private key, but not vice versa.

Cryptocurrencies use 256bit numbers as private keys, which are up to 77 figures long and cannot be easily remembered by humans. A wallet software often provides 12 to 24 word key phrases called "seed phrases” generated out of 2,048 words of a dictionary [Me22] which can be used to reconstruct public keys. However, once a private key is inaccessible it cannot be recovered and the corresponding funds become inaccessible as well. Since digital wallets can additionally hold digital attributes and certificates, the novel scam techniques are also relevant in the context of securing self-sovereign and decentralized identities based identity management schemes.

Smart Contracts: A smart contract is machine readable code stored on a blockchain network or distributed ledger. The contracts are self-verifying, self-executing and tamper resistant. Storage, execution, computation and documentation are handled by the underlying network, removing the need for a single trusted third party. Thus, smart contracts allow one or more parties to enter agreements or agree on certain actions defined by the contract in a transparent and “trustless” way. There are numerous use cases for smart contracts, such as transparent autonomous supply chain documentation, financial services or real estate transactions and documentation [MPJ18].

Decentralized Exchanges: In contrast to centralized exchanges (CEX), Decentralized Exchanges (DEX) don’t rely on a central authority that has custody of the transacted funds, tokens or coins but instead allows users to (mostly anonymously) transact peer-to-peer using smart contracts, while still having control of their private keys. The benefit of having full control over the funds often comes with trade-offs like scalability, low liquidity, high transaction fees, price slippage, front running and missing regulatory compliance [Ts20].

Decentralized Finance: Decentralized Finance (DeFi) is a generic term describing financial technologies and services based on distributed ledgers (e.g. blockchains) and smart contracts. DeFi cuts out the middleman (i.e. financial institutions) and instead provides said services based on smart contracts stored on an immutable distributed ledger. Depending on the services, this can eliminate fees, shorten processing times and does not require approval from third parties such as banks.

Airdrops: Airdrops involve the distribution of tokens or coins to wallets or addresses for free. This is often used for marketing and promotion purposes, to increase visibility and usage of a coin, or an underlying platform. To be eligible for an airdrop, users often have to complete certain tasks, such as following or sharing a project on social media or using a certain platform while some airdrops do not require any user interaction.

4 Novel scams using cryptocurrency-specific approaches

We analysed hundreds of recent cryptocurrency scams and attacks and identified important factors, which make an attack or scam cryptocurrency-specific: these scams use functionalities of a blockchain (1) to distribute coins/tokens (e.g. airdrop scams), (2) to move coins/token on the blockchain (e.g. honeypot to drain wallets) or (3) to manipulate trades on the blockchain (e.g. Sandwich Attack). There are attacks and scams using blockchain technologies such as smart contracts (e.g. exit scams). We still regard these scams to be cryptocurrency specific but note that the blockchain-specific part could be substituted with a not blockchain-specific technology and thus the scam could also work outside of the cryptocurrency ecosystem.

Airdrop Scams: Airdrop scams are phishing tokens airdropped to random wallets of a blockchain in order to lure the wallet owners to phishing websites of fake exchanges by showing a high conversion rate for the airdropped token [Tu22]. In August 2021 the scammers airdropped $SHIB tokens on Binance Smart Chain (BSC) to random users showing up in their wallets to be worth around 1,000 USD. Wallet owners who visited the scam website were asked to approve their wallets to swap the tokens. Approving the smart contract gave the scammers access to drain the wallets and the funds were stolen [Bs21].

Scam Tokens: Decentralized exchange platforms like Uniswap (https://uniswap.org/) allow an open and free listing of new tokens, which benefits new projects to launch fast, and at low costs. These advantages for new projects also help scammers to run fake coins and scam projects with low efforts [Ma21]. Scammers use different approaches to get the cryptocurrencies of victims. A very popular way is the creation of fake token imitations where the scammers search for new legitimate tokens on decentralized exchanges and create a similar token listing, e.g. $SHIB and $SH1B.

Smart Contract-based Scams: An example for a smart contract based scam is a smart contract-based honeypot where scammers post private keys or seed phrases in chatrooms (e.g. on telegram). The post looks like a mistake by an unexperienced user, but it was posted on purpose by a scammer. Honeypot wallets hold a significant number of tokens, which can only be moved by paying a fee using a corresponding “gas” token (e.g. $ETH on Ethereum). The victims who decide to exploit the ostensible user’s mistake are thus lured into spending gas tokens in order to move the user’s tokens to their own wallet. But an underlying smart contract foresees that the gas tokens sent will be instantly moved to a wallet owned by the attacker who created the smart contract behind the honeypot [Mc18].

Sandwich Attacks: Bots of malignant traders search for pending large trading transaction of other traders on the blockchain. A bot sniffs out a transaction and front-runs the victim trader by purchasing the same asset as the victim. The front-run is possible by paying a higher gas fee, which gives a higher priority in the transaction queue. By placing the front-run trade the attacker manipulates the price of the asset and the victim suffers a higher slippage (price difference between the point in time a transaction was submitted and the time the transaction is confirmed) for its transaction and pays a higher price for the purchase. The attacker now back-runs the victim’s transaction and then gets a higher price for selling the asset. The attack is called sandwich attack because the attacker front-runs and back-runs the original pending transaction, which is sandwiched in between [Da21].

5 Discussion and Conclusion

In this paper we presented a number of recent attacks schemes specific to cryptocurrencies. The field develops very quickly, and new scams emerge almost daily. Therefore this analysis is only preliminary and cannot be regarded as comprehensive and complete. Furthermore cryptocurrencies facilitate many conventional fraud schemes and scams due to the difficulty of tracing cryptocurrencies. Our medium-term goal is to use an approach similar to ATT&CK matrices to comprehensively present and analyse all the tactics used in attacks on cryptocurrencies in a web-based format so that it can be extended and updated as new techniques emerge and tactics become more elaborate.

6 Acknowledgments

This work was partially supported by the project ONCE (01MN21003F, once-identity.de), funded by the German Federal Ministry for Economic Affairs and Climate Action.

Bibliography

[ABC17] Atzei, N.; Bartoletti, M; Cimoli, T.: A Survey of Attacks on Ethereum Smart Contracts SoK, Berlin, Heidelberg, vol. 10204, pp. 164–186, 2017.

[Ba21] Bartoletti, M. et.al.: Cryptocurrency Scams: Analysis and Perspectives. In: IEEE Access, vol. 9, pp. 148353–148373, 2021.

[Bs21] BSCScan.com: BSCScan SHIB Scam, https://bscscan.com/token/0xab57aef3601cad382aa499a6ae2018a69aad9cf0#comments, accessed: 21/02/2022.

[Da21] Das, A.: DEFI Sandwich Attack Explain. https://medium.com/coinmonks/defi-sandwich-attack-explain-776f6f43b2fd, 2021, accessed: 18/02/2022.

[Fo22] Fool.com: "What Are Crypto Tokens? https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/crypto-tokens/, accessed: 21/02/2022.

[Le22] Ledger.com: WHAT IS CRYPTOCURRENCY? https://www.ledger.com/academy/basic-basics/about-crypto/what-is-cryptocurrency, accessed: 21/02/2022.

[Ma21] Maksimenka, I.: How to Identify and Avoid Uniswap Scams. https://coinmarketcap.com/alexandria/article/how-to-identify-and-avoid-uniswap-scams, 2021, accessed: 18/02/2022.

[Mc18] McIntosh, R.: Hack the Hackers: 'Honeypot' Crypto Scam Targets Would-Be Coin Thieves. https://www.financemagnates.com/cryptocurrency/news/hack-

hackers-honeypot-crypto-scam-targets-coin-thieves/, 2018, accessed: 18/02/2022.

[Me22] Medium.com: The ultimate guide to private keys and recovery seed phrases. https://medium.com/coinmonks/the-ultimate-guide-to-crypto-private-keys-and-recovery-seed-phrases-556ae60e59e7, 2022.

[MPJ18] Mohanta, B. K.; Panda, S. S.; Jena, D.: An Overview of Smart Contract and Use Cases in Blockchain Technology. In: 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1–4, 2018.

[NVM13] Nickerson, R.C.; Varshney, U.; Muntermann, J.: A method for taxonomy development and its application in information systems. In: European Journal of Information Systems, vol. 22, no. 3, pp. 336–359, 2013.

[Ri21] Rizvi, S.: A Complete Beginner's Guide to NFTs, https://trustwallet.com/blog/a-complete-beginners-guide-to-nfts, 2021, accessed: 21/02/2022.

[SSB20] Suratkar, S.; Shirole, M.; Bhirud, S.: Cryptocurrency Wallet: A Review. In: 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), pp. 1–7, 2020.

[Sta20] Statista.com: Total value of cryptocurrency lost to and recovered from theft and other attacks between March 2020 and February 2022. https://www.statista.com/statistics/1285057/crypto-theft-size/, accessed: 21/02/2022.

[Tr22] Trozze, A. et.al.: Cryptocurrencies and future financial crime. In: Crime Science 11, BioMed Central Ltd, article no. 1, 2022.

[Ts20] Tsai, W. -T. et.al.: Decentralized Digital-Asset Exchanges: Issues and Evaluation. In: Proceedings of the 2020 3rd International Conference on Smart BlockChain (SmartBlock), pp. 1–6, 2020.

[TSS19] Torres, C. F.; Steichen, M.; State, R.: The Art of the Scam: Demystifying Honeypots in Ethereum Smart Contracts. In: Proceedings of the 28th USENIX Conference on Security Symposium, USA, pp. 1591–1607, 2019.

[Tu22] Tunny, J.: What are Scam Airdrop Tokens on Binance Smart Chain and Why Are They So Prevalent? https://www.bsc.news/post/what-are-scam-airdrop-tokens-on-binance-smart-chain-and-why-are-they-so-prevalent, accessed: 18/02/2022.

[VM15] Vasek, M; Moore T.: There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. In (Böhme, R., Okamoto, T. ed.): Financial Cryptography and Data Security, FC 2015, Lecture Notes in Computer Science, Springer, Berlin, , vol. 8975, pp. 44-61, 2015.