UNIVERSITY of NICOSIA

Session:

Digital Wallet Security and Privacy

12 Week Schedule

We are here

Session	Session Name	Professor
1	Introduction to Blockchain and Web3	George Giaglis
2	Bitcoin and Digital Money	Garrick Hileman
3	Ethereum and Programmable Blockchains	Apostolos Kourtis
4	Digital Wallet Security and Privacy	Charles Guillemet **(Ledger)**
5	Decentralized Finance (DeFi)	Lambis Dionysopoulos
6	Prediction Markets	Apostolos Kourtis & Lambis Dionysopoulos
7	The Geopolitics of Cryptocurrency	Garrick Hileman
8	Tokenization and Stablecoins	Lambis Dionysopoulos & Lauren Berta **(Ripple)**
Advanced Track & MSc Students		
9	NFTs and Digital Ownership	Punk6529 & Mohsen El-Sayed **(Ledger)**
10	Regulation and Policy of Digital Assets	Jeff Bandman
11	Advanced Topics in Web3	Apostolos Kourtis
12	The Future: Convergence of Blockchain, AI, and IoT	George Giaglis

Session Objectives

- Understand the role and function of crypto wallets in blockchain systems.
- Explain the relationship between private keys, public keys, and addresses.
- Describe how seed phrases work and how wallets can be recovered.
- Identify common crypto security threats and risks.
- Apply best practices to securely store and protect digital assets.

Agenda

1. Understanding Crypto Wallets
2. Key Concepts in Crypto Wallets
3. Cryptographic Keys, Addresses, and Seed Phrases
4. Wallet Security and Asset Protection
5. Conclusions
6. Further Reading

Session: Digital Wallet Security and Privacy

1. Understanding Crypto Wallets

What are cryptocurrency wallets?

- Cryptocurrency wallets are **interfaces** for managing crypto assets on blockchain network
- They enable storing of **private keys**, sending, receiving, and balance/history checking.
- Wallets **do not** store cryptocurrencies physically, they are a key management software.
- They can be thought of as “fancy” password managers, for your crypto.
- Various wallet types provide different tradeoffs when it comes to security, accessibility, and convenience

Types of crypto wallets

- **Mobile Wallets:** Apps for smartphones, combining portability with QR code scanning for transactions. They balance convenience with security.
- **Hardware Wallets:** Dedicated devices for offline cryptocurrency storage, providing high security against online threats. Ideal for storing substantial cryptocurrency amounts.
- **Web Wallets:** Accessible online via web browsers. Convenient for quick access, but more vulnerable to online threats and dependent on third-party security measures.
- **Desktop Wallets:** Installed on personal computers, these offer better security than web wallets by storing private keys on the user's device.
- **Paper Wallets** (Obsolete)**:** Physical documents with public and private keys, often as QR codes. Secure against online threats but at risk of physical damage and challenging to manage**.**

Choosing the right crypto wallet

Wallets and clients can be selected based on several important factors:

- Amount of cryptocurrency you plan to store or use
- Technical experience level (beginner, intermediate, or expert)
- Device type (mobile, desktop, or hardware wallet)
- Usage frequency (occasional transactions vs. daily use)
- Security and privacy needs
- Transaction type and complexity

Find the wallet that’s right for you

- Bitcoin Wallets
- Ethereum Wallets

Wallet types and their trade-offs

Wallet Type	Accessibility	Security	Convenience	Suitability
Paper Wallet	Low	High	Very Low	Not recommended
Web Wallet	Very High	Low	Very High	Frequent, small transactions
Desktop Wallet	Medium	Medium- High	Medium	Balance security and access
Mobile Wallet	High	Medium	High	Daily transactions
Hardware Wallet	Low	Very High	Low	Long-term storage; large sums

Mobile wallets

Installed on a mobile device, usually operate as a lightweight or web client.

Pros

- ✓ Portable, easy, and convenient. Smartphone cameras enable QR code scanning for payments.
- ✓ Suitable for everyday transactions
- ✓ Funds are recoverable if the device is lost or stolen. Requires a secure backup, typically a 12-word recovery phrase.

Cons

- ✗ Limited full node capability. Most operate as lightweight clients, though some support full node functionality.
- ✗ Risk of exposure in public environments. PINs and sensitive information may be visible to others or cameras.
- ✗ Vulnerable to mobile-specific attacks. Devices and accounts must be protected against threats such as SIM-swap attacks.

Popular mobile wallets

Metamask

Trust Wallet

Base App
(formerly Coinbase Wallet)

Binance Web3 Wallet

Browser-based (web) wallets

Accessed through a web browser. Private keys are often stored and managed by the service provider.

Pros

- ✓ Accessible from any device with a web browser.
- ✓ Convenient and easy to use.
- ✓ No installation or software updates required.
- ✓ Quick access for transactions and account management

Cons

- ✗ Increased vulnerability due to third-party dependence. Security depends on the provider's software and infrastructure.
- ✗ High risk of phishing attacks through fake websites designed to capture login credentials.
- ✗ Limited user control over private keys.

Popular browser-based (web) wallets

MyEtherWallet (MEW)

Blockchain.com Wallet

Base App
(web version)

Browser extension wallets

Installed as a browser extension. Private keys are stored locally on the device rather than on a remote server.

Pros

- ✓ Private keys are stored locally, providing user control.
- ✓ More secure than web wallets because keys are not stored on centralized servers.
- ✓ Convenient access directly through the web browser.

Cons

- ✗ Vulnerable to browser-based attacks such as malware or malicious extensions.
- ✗ Risk of phishing through fake or impersonated extensions.
- ✗ Security depends on the browser's security and proper extension maintenance.

Popular browser extension wallets

Metamask
(extension)

Base App
(extension)

Trust Wallet
(extension)

Phantom Wallet

Rabby Wallet

Hardware wallets

Installed as a dedicated physical device designed for cryptocurrency key storage.

Pros

- ✓ Private keys are generated and stored on the device, providing user control.
- ✓ High security through isolation. Less complex than general-purpose computers and less vulnerable to common attacks.
- ✓ PIN protection is required to access the wallet and approve transactions.
- ✓ Backup is required during setup. Typically recorded offline as a 12 to 24 word recovery phrase on paper or metal.

Cons

- ✗ More expensive than software wallets.
- ✗ Less convenient for everyday transactions compared to mobile wallets.
- ✗ Loss of both the device and the backup recovery phrase results in permanent loss of access to funds.
- ✗ Security risk if purchased from unauthorized third-party resellers. Devices should be purchased directly from the manufacturer.

Popular hardware wallets

Ledger

Trezor

SafePal

COLDCARD

BitBox

Desktop wallets – lightweight

Installed on a desktop computer. Only block headers are downloaded, and the wallet relies on full nodes for transaction verification and receives only relevant transactions.

Pros

- ✓ Private keys are stored locally, providing user control.
- ✓ Require less storage space and bandwidth than full node wallets.
- ✓ Faster setup and operation compared to full node wallets.

Cons

- ✗ Cannot independently verify all transactions.
- ✗ Depend on third-party nodes for blockchain information.
- ✗ Vulnerable to malware and security threats on general-purpose computers.

Popular desktop wallets (lightweight)

Exodus

Electrum

Atomic Wallet

Guarda Wallet

Desktop wallets – full nodes

Installed on a desktop computer. Full node wallets download and verify the entire blockchain locally and store private keys on the device.

Pros

- ✓ Private keys are stored locally, providing user control.
- ✓ Contribute to the operation and decentralization of the blockchain network.
- ✓ Independently verify all transactions without relying on third parties.
- ✓ Improved privacy compared to wallets that depend on external servers.

Cons

- ✗ Require significant disk space, bandwidth, and time to synchronize.
- ✗ Vulnerable to malware and security threats on general-purpose computers.
- ✗ More complex to install and use, especially for beginners.

Popular desktop full node wallet clients

Bitcoin Core

go-ethereum (Geth)

Session: Digital Wallet Security and Privacy

2. Key Concepts in Crypto Wallets

Hot vs Cold storage

Hot Storage: Wallets connected to the internet, such as Web, Desktop, and Mobile wallets.

- Designed for ease of use, facilitating frequent transactions and quick access.
- More susceptible to cyber attacks, phishing, and malware due to internet connectivity.
- Suitable for small to medium holdings for daily transactions and active trading.
- Examples: Rabby, Metamask, Coinbase Wallet, Trust Wallet.

Cold Storage: Wallets not connected to the internet, such as Hardware and Paper wallets.

- Offers higher security, protecting against online threats.
- Less convenient for frequent transactions, requiring physical interaction.
- Ideal for storing significant amounts of cryptocurrencies over long periods.
- Examples: Ledger Trezor, ColdCard.

Examples of cold storage

- USB drive or other digital storage kept offline
- Paper wallet with keys printed or written down
- Physical bearer item that stores the private key
- Encrypted online file with the key kept offline
- Hardware wallet that stays offline when not in use

Hierarchical Deterministic (HD) wallets

Before HD wallets:

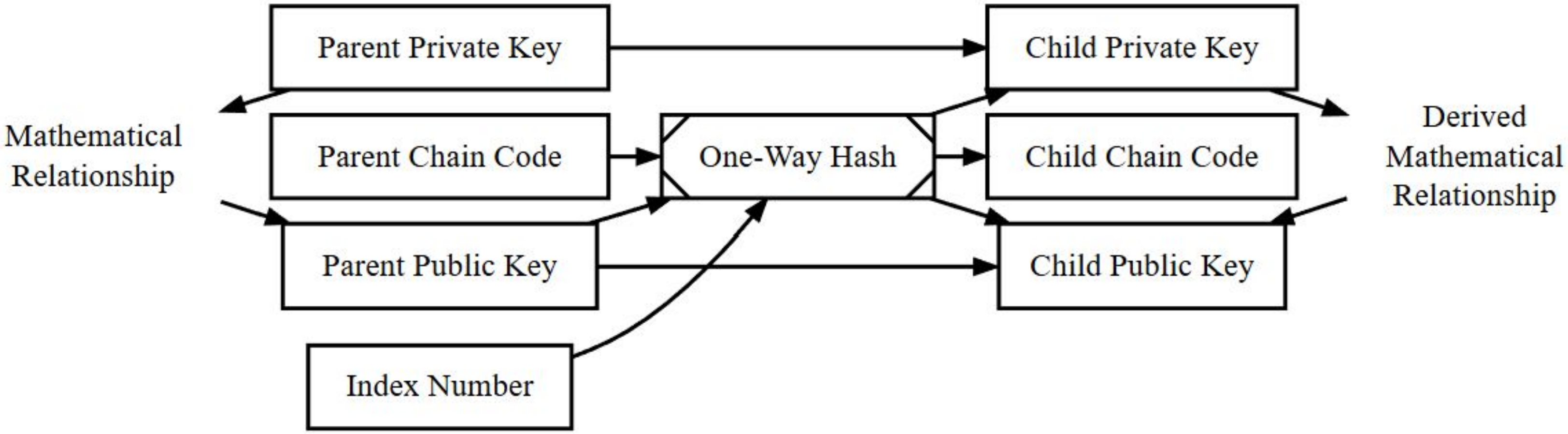
- Users had to generate and back up a new key pair for each transaction to maintain privacy
- Managing many private keys was difficult and increased the risk of loss
- Seed phrases (12 or 24 words) were introduced to represent a master private key in human-readable form

HD wallets today:

- Based on Bitcoin Improvement Proposal 32 (BIP 32), HD wallets generate all keys from a single seed phrase.
- The seed phrase can restore all private keys and addresses in the wallet
- HD wallets generate many new addresses, improving privacy by reducing address reuse
- This is the **gold standard for modern crypto wallets**, used by most wallets today.

How HD wallets work

1. A seed phrase is generated when the wallet is created
2. The seed phrase creates a master private key
3. The master key generates many child private keys and addresses
4. Only the seed phrase needs to be backed up to recover all funds



Normal Hierarchical Deterministic (HD) Key Derivation (BIP32)

Source: https://developer.bitcoin.org/reference/wallets.html

Air-gapped wallets (deep cold storage)

- Air-gapped devices are used for “deep” cold storage and are never connected to the internet or wireless connections (Wi-Fi, Bluetooth, NFC)
- Private keys are generated, stored, and transactions are signed entirely offline.
- Transaction data is transferred using QR codes or micro-SD cards, keeping private keys isolated
- Provides very high security against online attacks but requires careful handling and is best suited for long-term storage

Custodial vs Non-Custodial wallets

Crypto custody: the possession and control of the private keys that allow access to and management of cryptocurrency.

Custodial Wallets: A third party (such as an exchange) stores and manages the user's private keys and funds on their behalf.

- ✓ Simple to use, especially for beginners
- ✓ Account recovery and customer support available
- ✗ Limited control over funds
- ✗ Security depends on the provider

Non-Custodial Wallets: The user stores and manages their own private keys, giving them full control over their funds.

- ✓ Full ownership and control
- ✓ Independent of third parties
- ✗ Funds cannot be recovered if keys are lost
- ✗ Requires careful key management

Multisignature wallets

- Multisignature **(multisig)** wallets **require more than one signature** to authorize a transaction, enhancing security over single-signature wallets
- They operate on a **n-of-m**, where transactions must be signed by at least **n** out of **m** participants. Common schemes include 2-of-3, 3-of-5.
- Any mix of cold/hot wallets can be used to facilitate mutlisig, including Shamir’s Secret Sharing seeds (explained later).
  - **Use cases:** shared account management for organizations, added security, escrow, non-custodial wallet recovery services

✓ Increased security from multiple approvals and reduced risk of single point of failure.

✗ complexity in setup and use, slower transaction initiation processes due to the need for multiple signatories.

Shamir’s Secret Sharing

- A technique that enhances security by dividing a private key into multiple shares.
- Shares are stored in separate secure locations or given to trusted parties.
- The private key can be recovered only when a **predefined threshold of shares is combined** (e.g., 2 of 3).
- Individual shares are non-functional on their own, preventing compromise from a single point of failure.
- Protects against loss, theft, or damage, and enables secure key recovery.
- Useful for inheritance, backup, and shared custody scenarios.
- **Different from Multisig** which requires multiple signatures to authorize transactions rather than reconstructing a key.

Source: https://www.ledger.com/academy/topics/security/shamirs-secret-sharing

Social recovery

- **Social recovery** allows wallet access to be restored through a trusted group of **Guardians,** reducing reliance on seed phrase backups.
- It lowers the risk of permanent asset loss if keys are lost, devices are replaced, or access credentials are forgotten.
- Recovery is authorized through **a threshold approval process (e.g., 3 of 5 Guardians)**, ensuring secure recovery without giving any single Guardian control over the wallet.
- Guardians do not have access to the private key or funds. They only approve a **recovery request**, which allows the wallet owner to assign a new key and regain access.
- This approach improves both security and usability, making self-custody safer and easier for individuals.
- **Social wallet examples:** Ready, Loopring Smart Wallet

Session: Digital Wallet Security and Privacy

3. Cryptographic Keys, Addresses, and Seed Phrases

Some important terms

- **Private Key:** Comparable to a bank account password, used to access and manage your crypto. It must remain confidential to ensure security.
- **Public Key:** Mathematically derived from the private key. It’s nearly impossible to deduce the private key from the public key.
- **Public Address:** A hashed version of the public key, used to receive cryptocurrency. It uniquely identifies participants in a transaction on the blockchain.
- **Digital Signature:** Generated using the private key to authenticate a transaction. Its verification ensures the transaction is authorized by the private key holder.

Blockchain addresses (1/2)

“Like email addresses, Bitcoin addresses can be shared with other Bitcoin users who can use them to send bitcoins directly to your wallet. Unlike email addresses, you can create new addresses as often as you like, all of which will direct funds to your wallet.

A wallet is simply a collection of addresses and the keys that unlock the funds within. There is practically no limit to the number of addresses a user can create.”

Antonopoulos, A. M., "Mastering Bitcoin Second Edition: Programming the Open Blockchain" (2018), https://github.com/bitcoinbook/bitcoinbook

Source: https://aantonop.com/about/

Blockchain addresses (2/2)

- **Every blockchain address is generated along with two related pieces of information:**
    - the private key, and
    - the public key.

- These keys allow you to control the cryptocurrency **corresponding to that particular blockchain address** and receive crypto from other people.
- To understand a private key, it is also important to understand its relationship with its public counterpart.

Public and Private keys

What Is a Public Key?

- A public key is a public receiving address that enables you to receive crypto.
- Any user on the blockchain can send funds to your address using your public key.
- The public key is similar to your bank account number such as IBAN or SWIFT.
- Anyone can send you money using your bank account number but they cannot control the funds with it.
- In the same way, a public key does not give others access to the crypto at your blockchain address, it is purely an address that receives assets.

What Is a Private Key?

- A private key grants users access to manage the crypto funds at a specific address.
- While the public key is like your bank account number, the private key is more like a PIN number or password.
- It gives you access to your blockchain address and your funds.
- However, whoever has access to it can control and spend the cryptocurrencies at your address. Thus, keeping it away from prying eyes is imperative.

What do Private Keys look like?

- A blockchain private key is a randomly generated number with hundreds of digits.
- For simplicity, they are represented as a string of alphanumeric characters.
- The private and public keys of Bitcoin wallets and Ethereum are generated using an algorithm called the **Elliptic Curve Digital Signature Algorithm**.

Bitcoin	Ethereum
uses a 256-bit number that can be represented in several ways.	uses a private key made up of 64 hexadecimal characters.
E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA33262	**afdfd9c3d2095ef696594f6cedcae59e72dcd697e2a7521b1578140422a4f890**

ECC in cryptocurrency: Foundation for secure transactions

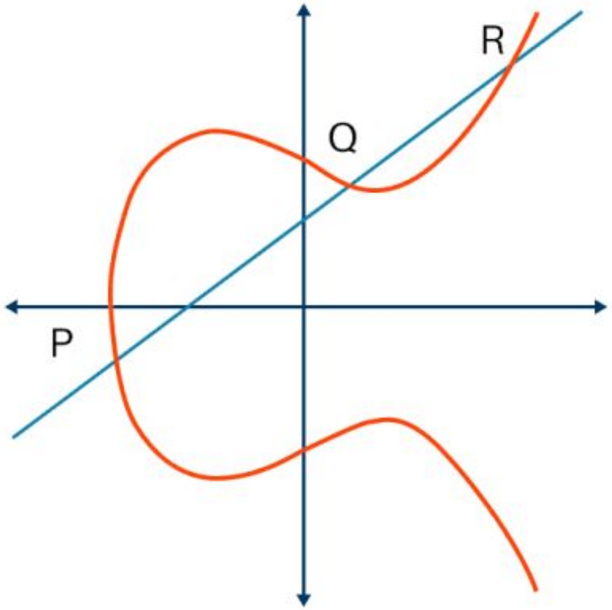
- **Elliptic Curve Cryptography (ECC)** is important for cryptographic security in various applications, including cryptocurrency systems.
- ECC is based on the properties of elliptic curves, which typically have an equation of the form

$$y^2 = x^3 + ax + b.$$

- A key feature in ECC is **Scalar Multiplication**: Multiplying a point P on the curve by an integer k gives a new point

$$Q = k \times P.$$

- This property is used for creating key pairs in cryptographic systems.



Example of an EEC

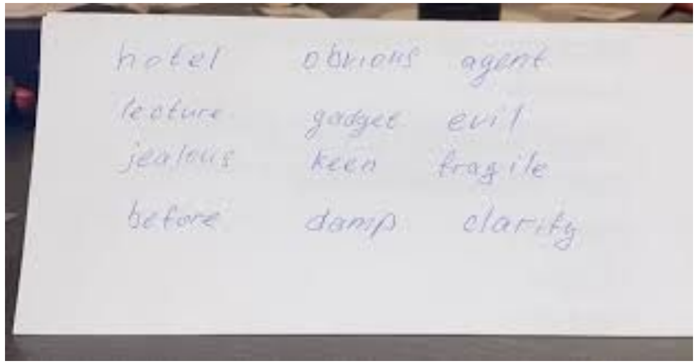
Source: https://crypto.com/university/custodial-vs-non-custodial-wallets

Key Pair generation and security properties

- In ECC-based cryptocurrencies, key pairs are generated as follows:
  - The **private key (k)** is a randomly selected integer from a predefined range.
  - The **public key (Q)** is computed as **Q = k × P**, where **P** is a predefined base point on the elliptic curve.
- The public address in cryptocurrencies is derived by applying a **hash function** to the public key (Q), resulting in a shorter, **unique identifier**.
- Security in ECC relies on the infeasibility of solving the **Elliptic Curve Discrete Logarithm Problem (ECDLP)**, which is the challenge of deducing the private key (k) given the public key (Q) and base point (P).

What is a seed phrase?

- **A seed phrase, also known as a Secret Recovery Phrase (SRP) or mnemonic**, is simply a collection of words that allows you to restore your entire crypto wallet.
- It's those 12-24 English words that your wallet presented you with while setting it up.
- This simple sequence is **similar to a master key for your private keys**. Your wallet uses it to generate private keys for multiple networks and accounts.
- This is how you can restore the entire wallet with that single seed phrase.



hotel	obvious	agent
lecture	gadget	evil
jealous	keen	fragile
before	damp	clarity

Seed phrase (Source: https://en.bitcoin.it/wiki/Seed_phrase)

Why seed phrases are important

- A seed phrase **acts as a backup to recover your wallet** if your device is lost, stolen, or damaged.
- It allows you to restore your wallet on another device or compatible wallet software.
- **Your crypto remains on the blockchain**, while the seed phrase restores access to your private keys that control it.
- It ensures continued access to your funds independently of any wallet provider.

How do seed phrases work?

- A seed phrase is a human-readable version of a long random number called **entropy**.
- BIP-39 introduced a standardized method to translate that long number into something more easily recorded by a human.
- The standard uses a fixed list of 2048 English words to generate seed phrases.
- The security of a seed phrase **depends on the randomness and length of the entropy**.
- Entropy of 128 bits or more is considered secure and practically impossible to guess.

Session: Digital Wallet Security and Privacy

4. Wallet Security and Asset Protection

You responsibilities in digital ownership

- **Safeguard Your Secret Recovery Phrase:** This is your most important asset. Store it offline and in a secure location. Never share it with anyone. Never store it digitally, or type it on an internet-connected device.
- **Verify transaction details:** Always double-check the address you're sending to and the amount before confirming a transaction on your device. Never blindly approve a transaction.
- **Be aware of scams:** Phishing attacks and other scams are common. Never give out your seed phrase or private keys, and be skeptical of any unexpected requests for information.
- **Understand smart contracts:** When interacting with decentralized applications (dApps), understand what permissions you are granting.

How can you acquire cryptocurrency?

- **Exchanges (most popular):** Cryptocurrency exchanges like Coinbase, Binance, and Kraken allow you to deposit traditional currency and buy cryptocurrencies.
- **Peer-to-Peer:** Platforms like Binance P2P enable buying cryptocurrency directly from other individuals using various payment methods.
- **Earn it:** Earn cryptocurrency through freelance work, services, tasks, or by receiving your salary in crypto.
- **Mining or staking (advanced):** Earn cryptocurrency by mining or staking if you have sufficient technical knowledge and resources.
- **Ask a friend to get started:** Friends can send you cryptocurrency and help you set up a wallet and learn the basics.

How to source a Hardware wallet

- Risks: **Device tampered with pre-purchase.**
  - Pre-set master keys.
  - Altered random number generators
- Mitigations: **Correct Sourcing**
  - Purchase directly from the manufacturer.
  - Opt for reputable resellers if direct purchase isn't feasible.
- Other Measures: **Inspection and Verification**
  - Inspect packaging for tampering.
  - Check for packaging anomalies (discoloration, sign of re-packaging).
  - Verify device's integrity using manufacturer guidelines.

Notice anything that doesn't look right? Contact the manufacturer for a replacement.

Common crypto security threats

- **Custody risk:** Loss of funds due to lost private keys, lost seed phrase, user error, or failure of a custodial provider (e.g., exchange bankruptcy such as FTX, or exchange hacks such as Mt. Gox).
- **Device hacks:** Malware or hackers access your computer or phone to steal private keys.
- **Phishing attacks:** Fake websites, emails, or links trick users into revealing sensitive information or approving malicious transactions.
- **Social engineering:** Scammers manipulate users into sharing recovery phrases or granting wallet access.
- **Blind signing:** Users approve smart contracts without understanding them, allowing attackers to steal funds.

Bybit hack case study (2025)

On February 21, 2025, **Bybit lost over 400,100 ETH** ($1.4B–$1.5B at the time) in the largest crypto exchange hack.

- Bybit used **Gnosis Safe**, a multi-signature wallet, to manage its cold storage, requiring multiple approvals for transactions.
- Attackers compromised the **Gnosis Safe web interface using malicious JavaScript**, not the underlying smart contract.
- This allowed hackers to **trick signers into approving a malicious transaction**, which gave attackers control of the wallet.
- **Only the transaction proposer was compromised**, allowing attackers to bypass the multi-signature protection.
- Attackers first made a small test transfer, followed by the theft of over 400,000 ETH.

This demonstrates that **cold storage and multi-signature wallets can still be compromised** through interface and **human vulnerabilities**.

Source: https://www.ledgerinsights.com/euroclear-launches-tokenized-collateral-initiative-with-digital-asset/

Secure your wallet, no matter what type it is!

- **Generate private keys locally** on your personal device or hardware wallet, and avoid online key generators.
- **Use different wallets for different purposes**, such as mobile wallets for daily use and hardware wallets for long-term storage.
- **Backup your wallet and seed phrase** and store backups securely offline; periodically test recovery.
- **Protect your wallet with a passphrase** to add an extra layer of security beyond the seed phrase.
- **Do not** split your seed phrase into parts and store them separately, as this increases the risk of accidental loss; instead, use multisig or Shamir's secret sharing scheme (SSSS).

Finally, in general, make sure to use the most up-to-date versions of software on your devices. Otherwise you may miss important security patches!

Session: Digital Wallet Security and Privacy

5. Conclusions

Conclusions

- Crypto wallets provide access to digital assets but do not store the assets themselves.
- Private keys and seed phrases are critical and must be protected to maintain control over funds.
- Loss of private keys or seed phrases can result in permanent loss of cryptocurrency.
- Users are fully responsible for their crypto security due to the lack of central authority.
- Following proper security practices significantly reduces the risk of theft or loss.

Session: Digital Wallet Security and Privacy

6. Further Reading

Further Reading

Ledger Academy:

- What is a Private Key?
- What Is A Crypto Wallet?
- What is a Seed Phrase?
- Crypto Threats: How Crypto Gets Stolen

Wallet security papers:

- Security aspects of cryptocurrency wallets—a systematic literature review
- Security analysis of cryptocurrency wallets in android-based applications
- SoK: Design, vulnerabilities, and security measures of cryptocurrency wallets

UNIVERSITY *of* NICOSIA

Questions?

Contact Us:

Twitter: @mscdigital
Course Support:
digitalcurrency@unic.ac.cy
IT & Live Session Support: dl.it@unic.ac.cy