PLUTUS21 CRYPTO

Digital Asset Security.

Securing the assets of the future.

Table of Contents

Executive Summary

The following are headlines from the latest occurencence of crypto being lost/stolen/hacked. The CEO of a major Canadian crypto exchange died in India at the age of 30 and took with him the keys to the digital wallets holding more than $190 million worth of crypto that belonged to customers. It is not the first, or last, time that we will come across news like that.

Bloomberg: "Crypto CEO Dies Holding Only Passwords That Can Unlock Millions in Customer Coins"
Forbes: "A Major Bitcoin Exchange Has A Serious Problem"
Wired: "A CRYPTO EXCHANGE CEO DIES—WITH THE ONLY KEY TO $137 MILLION"

From the outside, these headlines are the very reason that this new system of value exchange cannot be trusted. But from the inside there is nothing different about this occurrence when compared to legacy systems. It is not a flaw of the entire system but mainly the result of user error. With the right knowledge, procedures and training, the risk of such losses can be virtually eliminated.

Poor security practices on the individual or enterprise level cannot be used as an argument to discredit the utility and security of the entire system. Despite these occurrences and all the negative press, the Bitcoin network has proven to be the most secure and robust electronic payments network the world has ever seen.

Our goal with this paper is not to suggest a comprehensive security system for each individual reader or use case but to go over the basic concepts of digital asset security. More than a solution, this paper will provide the reader the basic knowledge to build their independent and customized solution.

“

The main advantage of blockchain technology is supposed to be that it's more secure, but new technologies are generally hard for people to trust, and this paradox can't really be avoided.

-Vitalik Buterin, co-founder of Ethereum

”

Public and Private Addresses

To safely and securely enable cryptocurrency transactions between two accounts, users have both public and private keys to act as verification of identity. Both keys are long sequences of alphanumeric characters that are unique to each account. This is an integral part of the cryptocurrency market, because it allows instantaneous verification and the potential for an unprecedented level of security in the modern era.

These keys are also important because they allow for cryptography, or the encryption of transaction data, to take place. Cryptography is a central feature of cryptocurrencies and other cryptoassets. Cryptography refers to a process of encryption, in which the sender's public key essentially hides the message or data and sends it to the receiver of the message. Once the receiver has the message, it is then decrypted to the original message. This message, in cryptocurrency transactions, is data regarding the transaction that will be published on the blockchain.[1]

When you wish to send someone a message, you may choose to send them an email. Their email address is available to anyone, and it enables them to receive messages from other email accounts, such as yours. However, in order to access your own email account, you must know the password to your account. If you know the password, you can access your account and send messages to other email accounts. Cryptocurrencies work in a very similar fashion. Public keys can be seen as email addresses, while private keys can be seen as the password to an email account.

Public Addresses

A Public Key or Address is a unique address for each account on the blockchain. This public key is information that is available to everyone on the blockchain. The public key is needed to receive cryptocurrencies payments, but one cannot send coins from the address with only

[1] Seth, S. (2018, October 5). Explaining the Crypto in Cryptocurrency. Retrieved February 18, 2019, from https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/

knowledge of the public key. The public key is used to encrypt the data presented in the transaction. The only way to subsequently decrypt the data is with the private key.[2]

Private Addresses

A Private Key or Address is a 64 character code that only the owner of an account has. These private keys act as passwords that are needed to make payments from an account. This is private information, and it is the only information that protects your assets from hackers and nefarious actors. It is important to keep this key private, because if someone obtains a private key to a known public key, he/she will have access to the account and its contents.[3]

[2] Frankenfield, J. (2018, July 30). Public Keys. Retrieved February 15, 2019, from https://www.investopedia.com/terms/p/public-key.asp
[3] Frankenfield, J. (2018, July 30). Private Keys. Retrieved February 15, 2019, from https://www.investopedia.com/terms/p/private-key.asp

Hot and Cold Wallets

To enable the storage of cryptocurrencies and other cryptoassets, the owner of the assets must be in possession of their private key. When someone has possession of a private key, they have possession of the contents of the account. A crypto "wallet" is the term used for any place where these private keys can be stored. There are many different types and features of wallets, but they are mainly put into two categories: hot wallets and cold wallets.

Hot Wallets

Hot wallets are stores of private keys that are connected to the internet. Since these wallets are connected to the internet, they are vulnerable to hackers and regulation. This makes hot wallets much less safe than cold or offline wallets. However, hot wallets tend to be much more accessible than cold wallets. When selecting a wallet with which to store cryptoassets, one may choose a hot wallet if they value accessibility or liquidity over safety or security. Most investors keep only small amounts of crypto currency in hot wallets.[4] The various types of hot wallets include:

- Web Wallets: Typically used by online exchanges, these wallets store private key information for its accounts on a cloud. These accounts may be accessed from any device, but are the most at risk for hacking. Furthermore, users are not in control of their private keys. Web wallets are relatively easy to access and the assets are easier to trade, but security is sacrificed to achieve accessibility.[5]
- Desktop Wallets: Also referred to as "warm" wallets, desktop wallets are applications downloaded to a computer that can only be accessed by that computer. They allow users to be in control of their private keys, but if your computer is compromised, then your assets may be stolen. These wallets are still relatively accessible, but a connection to the internet will still leave your account vulnerable to hackers.

[4] King, Ray. (2019, January 15). Best Cold Wallet Available. Retrieved February 20, 2019, from https://www.bitdegree.org/tutorials/cold-wallet/

[5] Jovanovic, Lazar. (2018, July 26). All You Need to Know About Cryptocurrency Wallets. Retrieved February 20, 2019, from https://medium.com/market-protocol/all-you-need-to-know-about-cryptocurrency-wallets

- Mobile Wallets: These wallets are similar to desktop wallets, but they are less complex and accessed only from the mobile device on which it is downloaded. Like a desktop wallet, they are secure until your phone gets hacked, and they are more secure if the application does not connect to the internet.

Cold Wallets

Cold wallets hold private keys to access crypto assets but are not connected to the internet. Since they are not connected to the internet, they are less vulnerable to digital attacks. Cold wallets, like paper and hardware wallets, are at risk of physical harm instead of a hacking threat. If you lose or damage a paper or hardware wallet, you may not be able to recover your assets.

- Hardware Wallets: Hardware wallets are physical devices resembling a large thumb-drive that isolate the private keys from the computer. These are considered the most secure as they significantly reduce the risk of hacking. Hardware wallets, such as the Ledger Nano S, must be stored in a safe location to minimize the risk of theft. Hardware wallet prices range from $60 to over $200.
- Paper Wallets: Like hardware wallets, paper wallets are offline and extremely safe. Using a paper wallet does however come at the risk of losing or damaging the physical paper that holds the private key and currency address info.

Exchange Hacks

Bitcoin (BTC) itself is virtually impossible to hack due to the technology behind it. Cryptocurrencies in general, however, are still exposed to hacking risks at various stages of the transaction. There have been several examples of cryptocurrency exchanges being hacked since the inception of Bitcoin. There is a risk of hacking whenever someone uses an online exchange to process a transaction or to hold assets. There are three layers to crypto security: protocol, personal wallets and exchanges. Protocol is complex and harder to hack. Personal wallets are too distributed. Exchanges are usually the most vulnerable part that hackers tend to attack. All the crypto exchanges have weaknesses in the architecture because they were not designed in cryptocurrency protocols. Any crypto exchange is based on centralized web applications, exposing it to risks that plague any other web application.[6]

The most famous crypto hack in history is the Mt. Gox hack. Mt. Gox was a Tokyo-based exchange that was launched in 2010 and went bankrupt in 2014. This exchange was once responsible for more than 70% of the Bitcoin transactions, 6% of total Bitcoin in circulation. In June 2011, Mt. Gox was hacked for the first time. 2,609 BTC were stolen due to a compromised computer belonging to an employee of the firm. In spite of the 2011 hack, Mt. Gox rebuilt trust and established itself to be the world's largest exchange[7]. In February 2014, the company experienced a fatal attack. The company suspended the exchange, claiming that they discovered suspicious activities involved with its digital wallet. Later, the company discovered that more than 650,000 BTC (around $450 million) were missing from the exchange. Mt. Gox filed for bankruptcy in Tokyo and was ordered to liquidate in April 2014[8].

[6] Novikov, Ivon. (2018, Sep. 17). Forbes Technology Council. Retrieved February 15, 2019, from https://www.forbes.com/sites/forbestechcouncil/2018/09/17/why-are-crypto-exchanges-are-hacked-so-often/#6fa18d734214.
[7] Norry, Andrew. (2018, Nov. 19). Blockonomi. Retrieved February 15,2019, from https://blockonomi.com/mt-gox-hack/.
[8] Frankenfield, Jake. (2018, July. 5). Investopedia. Retrieved February 16, 2019, from https://www.investopedia.com/terms/m/mt-gox.asp.

Our Approach

One of the many value additions for our team is the security solution that we provide to our partners. We developed a robust in-house system to secure the digital assets that we invest in. Our system is based on the principles of redundancy, geographic dispersion, multi-signature access, physical security, and other industry best practices. Additionally, operational security, particularly with asset security, is a key factor in our portfolio management and investment strategy. Finally, we have a business continuity and recovery plan in case one or more necessary people are unable to perform their duties.

We currently store the vast majority of our digital assets in company-controlled cold storage solutions, using dedicated hardware or paper wallets that never touch the internet. Multiple people are required to be physically present in order to move funds from a hardware wallet.

A small portion of our assets may be stored in warm or hot wallets (i.e. on exchanges) for short periods of time in order to facilitate trading. Additionally, we may hold a few assets with exchanges when there are not well-tested cold storage or custody solutions available for them. We strive to store all assets securely while minimizing counterparty risk. This is why following transactions with our exchange and OTC partners, we transfer assets to cold storage.

In the near future we will transition to storing a substantial portion of our assets with one or more U.S.-regulated, third-party, crypto custodians that employ similar cold storage solutions. This change will enhance the attractiveness of our fund, particularly for institutional investors, that may require third-party custody.

Even with a third-party custodian, for the foreseeable future we will likely need to continue maintaining our internal digital asset custody solution, as some of our positions are not currently supported by custodians. We specialize in identifying emerging projects early on so we need to have systems in place to secure these assets while waiting for the industry security infrastructure to support them.

Our strategy was designed with security in mind so we favor long investment horizons and a thesis driven approach as it minimizes the need for assets to be exposed to the internet, being held at exchanges or in hot or warm wallets. Our average investment hold period is around 2-3 years so the assets can be securely stored on cold wallets or with custodians for the vast

majority of that time, reducing the risk of hacking. We also mitigate digital asset security risk by sizing positions according to the availability of security infrastructure and our confidence in our ability or our custodian's ability to effectively secure the assets.

While cold storage and custody solutions help prevent hacks of digital assets, we also take the security of personal, company, and investor information seriously. All of our accounts are secured with strong passwords and whenever possible, 2-factor authentication (preferably non-SMS) apps such as Google Authenticator that require physical access to a cell phone or other dedicated device in order to gain access. We make regular backups of our data to secure physical storage devices. Lastly and perhaps most importantly, we have a business continuity plan that uses bank security deposit boxes to store information needed to recover funds and operate the business.

While there are unique challenges to this space, with proper planning and execution, investors can greatly benefit from exposure to this asset class.

Upcoming Research Topics

1. Bear Markets in Perspective: long-term investors have won
2. Why Now: why is the opportunity time sensitive and what catalysts could spur growth
3. Liquid Venture Capital: the rise of a new asset class
4. Technology Adoption Curves: where we are and where we are headed in the adoption cycle
5. Peer-to-Peer is the Name of the Game: how peer-to-peer systems have already achieved mainstream adoption and blockchain is just the next phase of that revolution
6. The Rise and Fall of ICOs: how the picks-and-shovels adapt to a change in investment infrastructure
7. The Illusion of Diversification: 100 percent long on government-issued currencies
8. Survival of the Fittest: focus on sustainability in the longest bear market in crypto history
9. A Case for Diversification within Crypto: diversification remains the only free lunch in finance
10. Blockchain: the foundation for the next 100 years
11. The Overhaul of Traditional Finance: millennials demand innovation and prefer control
12. A Textbook Alternative Asset: how crypto fits the definition of an alternative asset
13. Non-Linear Growth: investors have a hard time imagining exponential growth

Research Team

Email: research@plutus21.com
Twitter: @_Plutus21

Richard Raizes: Richard is a General Partner at Plutus21 Crypto Fund I, L.P. Richard heads the research efforts and is the Chair for the Investment Committee for Plutus21 Crypto. Richard is a graduate of the Alternative Asset Management Center at Southern Methodist University and spent the first 4+ years of his career in investment banking focused on diversified financial companies and energy and natural resources.

Email: richard@plutus21.com
Twitter: @richardraizes

Hamiz Mushtaq Awan: Hamiz is the founder of Plutus21 and a General Partner at Plutus21 Crypto Fund I, L.P. Hamiz heads the operations and is the Chair of the Risk Management Committee for Plutus21 Crypto. Hamiz is a graduate of the Alternative Asset Management Center and a recipient of the Don Jackson Fellowship at Southern Methodist University.

Email: hamiz@plutus21.com
Twitter: @hamizawan

Robert Till: Robert is the Head Analyst at Plutus21 Crypto. Robert heads the team of analysts involved in the research efforts. Robert is a Finance and Economics student at Southern Methodist University.

Email: robert@plutus21.com

Kento Orii: Kento is a Research Analyst at Plutus21 Crypto. Kento is a Finance and Japanese student at Southern Methodist University. His past experience includes starting and operating a digital media agency.

Email: kento@plutus21.com

Irene Qiu: Irene is a Research Analyst at Plutus21. Irene is a Finance student at Southern Methodist University.
Email: irene@plutus21.com

Jake Baumli: Jake is a Research Analyst at Plutus21. Jake is a Finance student at Southern Methodist University.
Email: jake@plutus21.com

Gage Baumli: Gage is a Research Analyst at Plutus21. Gage is a Finance student at Southern Methodist University.
Email: gage@plutus21.com

Lauren McCarthy: Lauren is a Marketing and Communications Analyst at Plutus21. Lauren is a Marketing student at Southern Methodist University.
Email: lauren@plutus21.com

Disclaimers

All news, research, commentary and other information ("Information") provided by Plutus21 Crypto Fund I, L.P. ("Plutus21") or its affiliates have been prepared solely for informative purposes and should not be the basis for making investment decisions or be construed as a recommendation to engage in investment transactions or be taken to suggest an investment strategy in respect of any financial instruments or the issuers thereof.

Information has not been prepared in accordance with the legal requirements designed to promote the independence of investment research.

Information is not intended and should not be used or construed as an offer to sell, or a solicitation of any offer to buy, securities of any fund or other investment product in any jurisdiction. No such offer or solicitation may be made prior to the delivery of definitive offering documentation.

Information provided is not related to the provision of advisory services regarding investment, tax, legal, financial, accounting, consulting or any other related services and is not a recommendation to buy, sell, or hold any asset. Information is based on sources considered to be reliable, but not guaranteed, to be accurate or complete. Any opinions or estimates expressed herein reflect a judgment made as of the date of publication and are subject to change without notice.

Trading and investing in digital assets involves significant risks including price volatility and illiquidity and may not be suitable for all investors.

Plutus21 and its affiliates trade and hold positions in digital assets and may now or in the future trade or hold a position in an asset that is the subject of Information provided. As a result, Plutus21 or its affiliates may be subject to certain conflicts of interest in connection with the provision of Information. Plutus21 will not be liable whatsoever for any direct or consequential loss arising from the use of this Information.