The Usability of Bitcoin's Cryptography

Levi R. Seibert

Athens State University

ITE 523: Cryptography and Network Security

Dr. Yahia Fadllala

April 9, 2023

The Usability of Bitcoin's Cryptography

Since their inception in 2009, and especially in recent months and years, cryptocurrencies have surged in popularity. Bitcoin was the first cryptocurrency and was introduced by "Satoshi Nakamoto", a pseudonym, in January of 2009. Ever since then, Bitcoin has remained the most popular cryptocurrency in the world (Pinkerton & Davis, 2023). One of the important factors of Bitcoin, at least from a cryptographic standpoint, is that transactions are ultimately just implementations of public key, or asymmetric, cryptography signing interactions on a ledger. Since this currency system is built upon the backbone of keys, proper key management configurations need to be in place in order to protect the integrity of the currency.

Introduction to Cryptocurrencies and Bitcoin

Cryptocurrency

With the U.S. economy in despair and the recent issues with banking facilities, people are turning to cryptocurrency to hold their monetary belongings. Cryptocurrencies do not have any physical presence, and this is alarming to many who do not fully accept cryptocurrency as being a suitable use of financial exchange. Crypto is indeed dangerous; who can trust an Internet-based protocol to hold their riches, especially when their values fluctuate constantly? In many cases, trust should not be placed in the Internet; however, the important factor is whether or not the protocols are established and proved effective. Some cryptocurrencies are simply not safe, but others, like Bitcoin, have been reviewed and proven to be reputable. Cryptocurrencies aren't for everyone, but many people find great benefit from them, both in terms of a form of currency, as well as a means of investment.

Blockchain

Many cryptocurrencies are built on a concept known as the blockchain. While this is a confusing concept for most individuals, especially those without a computer science background, in reality, the blockchain is not incredibly complex. According to Investopedia, it is a large digital database or ledger

that keeps track of interactions between different computers on a large network. The blockchain separates data (or transactions) into blocks, and each block is connected, or chained, to other blocks. Every block is given a timestamp and is unmodifiable (Hayes, 2022). In addition, other computers on the blockchain verify the authenticity of a block before it is added to the chain. Therefore, cryptocurrencies can use the blockchain to keep track of user transactions in such a way that transactions cannot be repudiated.

Bitcoin

Bitcoin is the most popular cryptocurrency available today. Unfortunately, many of Bitcoin users' have little to no understanding of how the currency actually works. Its foundational use of the blockchain allows it to be completely free from centralization. While this may be considered a risk by some, the decentralization of Bitcoin is what protects it from interference by a financial entity. Bitcoin utilizes the blockchain to verify its transactions and to keep a record of all interactions that take place.

The common understanding of Bitcoin is technically inaccurate. This is at least in part due to the fact that the process is somewhat complex and revolves around cryptographic concepts, in particular public key cryptography. Bitcoin users are provided "wallets" that hold sets of keys. The reasoning for having multiple sets of keys will become apparent momentarily. For now, know that the user has access to pairs of cryptographic random, or pseudo-random, values. In each of these pairs, there is a public key, which is allowed to be shared publicly and is used as a receiving address for transactions. The other key, the private key, is the opposite. It must not be shared with anyone, as access to this key gives access to the funds available in the wallet. The private keys are used to verify transactions and to prove ownership (George, 2022).

Whenever two users wish to exchange Bitcoins (usually, parts of Bitcoins, as they are very expensive), they are really just posting data on the blockchain. No money is flowing across the Internet highway. This may be a concern to some, however the important thing to keep in mind is that the

blockchain is backing up and verifying every transaction that occurs and ensures that any issues that do take place are traceable. The more accurate way of viewing Bitcoin is understanding that the "currency" owned by an individual is really just data on a ledger that is protected by private keys. Through the use of a currency exchange application, the information protected by the private keys can be exchanged for fiat currency.

When a user sends "funds", or ownership of blockchain data, to another user, they actually send all the funds they have available. The receiver then sends back the unused portion on the funds, called change, to the sender and the currency is stored with a brand-new key pair.

Bitcoin Key Management

Because the Bitcoin protocol relies so heavily upon public and private keys, some mechanism of key management has to be implemented in order for Bitcoin to remain safe. Shayan Eskandari, David Barrera, Elizabeth Stobert, and Jeremy Clark, in their paper on "A First Look at the Usability of Bitcoin Key Management", consider several approaches to key management for Bitcoin. They take a detailed look at the most common methodologies and evaluate them based on several criteria. Their work shows the strengthens of the cryptography behind Bitcoin, but also discusses some points where they believe the design could be lacking, at least in the applications they considered (Eskandari et al., 2015).

Approaches

There are six common approaches to managing the keys for Bitcoin, each with multiple available applications. The first popular option is to store keys in local storage. In this approach, a file or database on a user's computer is used to store the key pairs belonging to that user. Advantages to this methodology include the reduction of mental burden on the user, the practically infinite capacity for holding key pairs, and the automation of key generation and transaction creations. On the other hand, the local storage approach also has some dangers. Any malware on the user's computer could infiltrate the key management file. A good end-device anti-virus should prevent this from happening, but there is

always the potential. It should also go without saying, but sharing access to some key folder on a user's device will allow someone else to have access to the information needed to steal the user's Bitcoin.

The second popular method is to use password-protected (encrypted) wallets. These are similar to locally-stored wallets, with the major difference being that the wallet files are protected by a user-chosen password or passphrase. This remediates the chances of physical theft of the keys, so that if the device holding the keys was stolen, the only way of accessing the keys would be through brute-forcing the password. This methodology does not address digital theft, in that if malware were to be loaded on the user's computer, a keylogger could potentially make the password protection useless. The advantages of using password-protected local storage are similar to those of using non-password-protected local storage, with the major difference being that the passwords provide physical protection, while also causing threats to usability in the case that the user forgets the password. Since Bitcoin is decentralized, there is no password-resetting capabilities when using a local system. It is also important to note that the password does not provide access to the keys, rather, it just protects the file that includes the keys. The keys cannot be accessed without having access to the file containing them, even if the password is known.

Another common approach to key management is that of storing the keys offline. The wallet is stored on portable media, like a thumb drive. The major benefit of this method is that it protects the keys from malware attacks, which was one of the disadvantages of the password-protected local storage option. One of the main issues with the offline key storage method; however, is that wallets are inaccessible unless the external device is present and usable. One unique application of this methodology is the use of paper wallets. These paper wallets have the private keys printed onto them, usually in the form of something like a QR code. Using this methodology, a user can read the key by just scanning the code with their smartphone. One disadvantage with this specific application is that the

paper wallets can be stolen or the code for the keys could be observed, and therefore they require special physical protection.

The fourth common key management methodology is to use air-gapped key storage. This is similar to offline key storage in that the wallet is stored on a secondary device; however, with the air-gapped method, this secondary device can also generate, sign, and export transactions, but is never connected to a network. The transactions are created on this device and then the signed outputs are sent (via portable media) to the primary computer that is connected to the Internet. This primary device transmits the transactions on the Bitcoin network. This architecture protects the security of the keys by never allowing a private key to be on a Internet-facing device, however, there is still a potential for attack as the portable device used to carry transactions between the secondary and primary devices may be infected with malware.

An alternative option to the previous four is that of deriving the cryptographic keys from a password, rather than keeping track of the keys themselves. Some type of mathematical operation is performed on the password that is entered by the user in order to generate a private and public key pair. Unfortunately, this design only allows for one keypair for each password, so every time a new keypair is needed, the user must select a new password. That being said, these password-derived keys have a great advantage: the user can re-generate their wallet but just reentering their password. On the other hand, if they forget the password, all their funds will be lost.

The final, and one of the most popular, approaches to Bitcoin key management is the use of third-party web services to host and maintain the keys in a wallet. These services allow a user to access an online application to view their funds and perform transaction, much like an online banking program. This makes currency exchanges with fiat currencies much easier. Users have to entrust these third-party services with their currencies, and have faith that they will be protected against theft. In response to some of the threats associated with hosted wallets, some users store only a small portion of their funds

online (this is known as hot storage) and keep the rest offline (in cold storage). The downside to this is that it requires the user to have to move data whenever the hot storage is depleted. Alternatively, a hybrid hosted wallet can be used to encrypt all private keys and personal data and only uses the web service for transactions and displaying the user's balance (Eskandari et al., 2015).

Evaluation

The authors of "A First Look at the Usability of Bitcoin Key Management" selected ten criteria to evaluate the six key management approaches described above, with the hosted option being split into hot, cold, and hybrid. The first test was to check how resilient each methodology was to malware. Because Bitcoin requires the use of the Internet for transactions, none of the evaluated approaches were fully resistant to malware, although the offline, air-gapped, and cold host wallets are all better protected, as they keep their keys private on secure devices and only use the network for transactions. A related factor that was considered was whether keys were stored offline. This is fulfilled by offline, air-gapped, password-derived, and cold hosted wallets, and was partially fulfilled by password-protected and hybrid wallets, as they are Internet-connected but password-protected.

One factor that users often care about is the absence of a trusted third party for signing authority. All of the management tools except for hot and cold hosted wallets at least partially meet this criterion. The authors also checked for certain resistance factors, in particular, resistance to physical theft and resistance to physical observation. In terms of physical theft, password-protected and password-derived wallets partially meet the resistance factors, but do not do so fully as their passwords are often weak and allow for brute forcing. In regards to resistance to physical observations, local storage, air-gapped storage, and password-protected wallets all meet the requirements.

Resilience to password loss is met by all methods except for password-protected wallets and password-derived keys, and resilience to key churn (meaning that funds aren't lost when the initial keypool is exhausted) is met by all except offline storage. Cold hosted wallets, offline storage, and air-

gapped storage do allow for immediate access to funds, while all other methodologies do not. Password-derived keys, and hot/cold/hybrid hosted wallets are cross-device portable (as is offline storage) and do not require new user software.

When all of the methodologies are considered using these criteria, no one approach necessarily stands as being the best, although the data may indicate that the use of a third-party hosting service may be the most secure option. That being said, this can be considered to be contrary to one of the foundations of Bitcoin: a decentralized currency. A third-party controlling one's currency is in a way centralization, but in return, it provides extra protections that may make it worth the tradeoff. The authors suggest that the best advice for cryptocurrency is to keep small amounts available for spending, in a hosted wallet for example, while keeping larger amounts secure in an offline or air-gapped storage mechanism, similar to a savings account (Eskandari et al., 2015).

Application Walkthroughs

The authors also used cognitive walkthroughs of six different Bitcoin applications to evaluate their usability, in terms of key management. They chose Bitcoin Core to represent keys in local storage, Multi-Bit for a password-protected wallet, Bitaddress for offline storage, Bitcoin Armory for air-gapped storage, Brainwallet for password-derived keys, and Blockchain.info for a hosted wallet. They performed four tasks on each of these clients: configuring a new Bitcoin address and obtaining its balance, spending Bitcoin, spending Bitcoin on a secondary device, and recovering from the loss of the main credential. The evaluations were based on eight guidelines that indicated usability concepts, such as the user's awareness of steps to perform, the user's knowledge of successfully completing a core task, and the user's inability to make dangerous errors. Each of the applications had their own advantages and disadvantages, and some faired better in the evaluation then others, but it does appear that the air-gapped key storage and the hosted wallet seemed to surpass the others in achieving the guidelines. This

further points to the conclusion made by the authors that a combination of multiple methodologies might be best for security and usability purposes.

In addition, the authors discuss some of the pros and cons of the metaphor of Bitcoin being a traditional currency. While it does often make Bitcoin easier to understand, it can at times give false impressions and add confusion to users. Also, several of the evaluated Bitcoin clients struggled with some abstractions that may cause misunderstandings by users, as well as technical language that was not defined for users that may lead to further confusion. This is not to say the key managements are unusable, just that they need to address some specific usability issues (Eskandari et al., 2015).

Conclusion

The work done by Eskandari, Barrera, Stobert, and Clark proves that there are multiple applications for using Bitcoin, all with various levels of usability and practicality, especially in terms of key management. Because of the cryptographic nature of Bitcoin, the currency system itself should be considered safe and secure. It has survived the test of time, and while it does fluctuate drastically in value, its cryptography has not weakened. Bitcoin is a secure and usable alternative to fiat currencies.

References

Eskandari, S., Barrera, D., Stobert, E., & Clark, J. (2015). A first look at the usability of Bitcoin Key Management. *Proceedings 2015 Workshop on Usable Security*. https://doi.org/10.14722/usec.2015.23015

George, B. (2022, August 5). *A crypto must-know: Public vs. private keys*. CoinDesk Latest Headlines RSS. Retrieved April 9, 2023, from https://www.coindesk.com/learn/a-crypto-must-know-public-vs-private-keys/

Hayes, A. (2022, December 19). *Blockchain facts: What is it, how it works, and how it can be used*. Investopedia. Retrieved April 9, 2023, from https://www.investopedia.com/terms/b/blockchain.asp

Pinkerton, J. (2023, February 27). *The History of Bitcoin, the First Cryptocurrency*. U.S. News. Retrieved April 9, 2023, from https://money.usnews.com/investing/articles/the-history-of-bitcoin