Cypherock: Building the World's Safest Mobile Crypto Wallet

Rohan Agarwal, Vipul Saini

cypherock.com

May 23, 2018

Abstract

Hardware wallets are the safest way to store a private key. The hardware wallet digitally signs the blockchain transaction offline in a dedicated tamper resistant hardware which makes it immune to physical and remote malware attacks. Cypherock is building a design layer over the existing hardware wallets to offer a seamless and secure mobile blockchain transactions.

Contents

1. Introduction

The world is moving towards a decentralised economy. Blockchains with its inception in 2009 introduced digital scarcity in the world in a decentralised arrangement. Digital scarcity allowed protocols like Bitcoin to provide value to its stakeholders in the ecosystem. In order to access the funds, a user needs to prove ownership of the funds. A private key in asymmetric cryptography is used to prove a user's authenticity through digital signature. By the virtue of digital signature, Bitcoin protocol allows users to claim ownership of the funds. Built on top of principles of Cypherpunk Manifesto, cryptocurrencies have privacy built into them. Due to the pseudo-anonymous nature of the cryptocurrencies, it is near impossible to trace the hacker who manages to steal a user's private keys. Hence the ownership of a particular private key poses significant burden on the common user to secure it.

There are a number of ways that people resort to when storing a private key. The most secure way to do so is through a hardware wallet [2]. A hardware wallet is a dedicated hardware disconnected from the internet. The master private key is generated inside the hardware offline. It is never exposed to the internet. Additionally, the private key never leaves the device. The digital signature happens inside the hardware. Since it is a mathematical operation, it does not require connection to the blockchain. The secure process of signature of the hardware wallets is the reason why funds are yet to be stolen from them.

2. Need

Asia accounts for almost 36% of the total participants in the cryptocurrency domain, highest among the continents. Hardware wallets arrive in India and other Asiatic regions at about 50-60% premium cost wise. There exists approximately 23 million blockchain wallets which is going to grow exponentially over the next 5 years. Hackers have stolen approximately 14% of the total funds invested in the cryptocurrency market which amounts to roughly $15 Billion in today's worth. No wonder it is a $250 million dollar a year industry now and hence there needs to be enough players in the market to cater to the need of securing user's digital assets.

Mobile Security implementations today, protect passwords and sensitive information like credit card details. Passwords can be reset using recovery emails whereas credit card transactions are

insured and reversible even if a fraudulent transaction takes place. A transaction on the blockchain on the other hand is irreversible and has a single point of failure.

Mobile Software Wallets today have been forced to go closed sourced [10] (specifically for their Android codebase) due to existence of clones on the Google playstore and phishing attacks through them. Close sourcing the codebase introduces trust into the system which was what blockchain intended to remove.

Android is a fragmented market. Unlike Apple, a lot of power lies with the hands of the manufactures. And hence they offer their customers ease of use and features without adequate security scrutiny [13].

Data is the new oil. Understanding consumer behaviour through embedded consumer analytics (spyware software) becomes a recurring ad revenue stream for the companies and hence it causes sensitive information to potentially come into public domain [14].

3. Product Vision

The current computer networks rely on a centralised architecture. The centralised server acts as a master and the user's device as a slave. The requests are always routed from the server. The server is responsible to maintain consistency and security of user's funds. Hence, the server becomes a single point of failure in the ecosystem. If the ease of use is taken into account, the user has the ability to access a single wallet instance from any smart device.

On a Blockchain based networks, the system is decentralised. Since the networks itself are secure, humans become the weakest link in the ecosystem. The availability of the funds rely upon the peers connectivity to the wallet. Hence it is not advisable to access a single wallet instance on multiple smart devices [16]. Since a single wallet is not permitted in this ecosystem, it is of utmost importance to either secure funds of every single smart device in the ecosystem or allow the user to port the secure storage onto the different ecosystems. A user today typically holds three different smart devices - PC, smartphone and smartband. So, Cypherock envisions a hardware wallet portable across the three smart devices to secure the decentralised ecosystem.

- For the phone, it will be placed inside the mobile case.
- For the desktop, the case with the wallet will work as a traditional hardware wallet.
- For the smartband, it will be attached to a bluetooth enabled smartband.

As banking becomes more personalised through decentralization, it will mark the shift from an enterprise culture towards storage of assets to more consumer focused. Hence, a customer would prefer a choices in design over a universal design of the device which the company intends to focus on.

We envision digital networks to shift towards a blockchain based architecture in the next 10 years. If we unify the networks (both public and permissioned) through BIP 32 implementation, our single device could support infinite different networks through a single keychain. This will act as a single secure key to different IOT based locks and replace every NFC based payment cards (metro cards, plastic cards etc).

4. Alternate Designs & Their Problems

VISA backed Debit Cards

Payment processors such as Bitpay offers merchants to accept cryptocurrencies for their products and services from the consumers and facilitates conversion from cryptocurrencies to national currencies to be deposited into the merchant's bank accounts. The problem in this model is the introduction of the middlemen into a peer to peer payment architecture and delegation of control to the payment processors which tends to get misused often.

Blockchain Phone

A blockchain phone introduces key security features into the android ecosystem to facilitate secure blockchain transactions, however there are inherent problems with such a step. Firstly, they are expensive. Secondly, different users have different preferences when it comes to choosing a smartphone. A blockchain phone forces a user to use a particular phone. Thirdly, integrating other advanced features such as micro resource sharing into the phone along with the cold storage may enable new opportunities for attackers to compromise it [17]. Lastly and most importantly, they use the same screen as the phone to confirm user's transaction which is not a true trusted display and hence a security loophole.

Plug & Play Device

Plug and play devices connected directly through a micro USB to the phone offers the portability that the traditional hardware wallet fails to provide. However, the aesthetics of the product becomes such that it behaves as an external device to the phone. The problem in such a scenario

is that the tendency to lose such a device increases exponentially, hence causing monetary loss to the user.

Debit Card Shaped Hardware Wallet

A debit card shaped hardware wallet increases portability across devices. However, they tend to have same tendency of getting lost as a plug & play device. A bank debit card is worthless and could be issued again from the bank but a debit card shaped hardware wallet is expensive which causes monetary loss. Additionally, it requires battery as a source of energy for bluetooth which becomes an overhead for the user.

SmartBand as Hardware Wallet

A smartband makes sense when one considers the loss tendency of a phone as compared to a wearable, and hence explains why Cypherock enables porting to a smartband. But it forces a user to wear an external device and needs bluetooth to work. Moreover, until localised payments through cryptocurrencies goes mainstream, there isn't a need for such.

TEE Based Wallets on Smartphones

TEE or Trusted Execution Environment [1] is a virtual OS implementation on newer smartphones. The apps run on them are trusted with isolated implementation from the normal OS. They offer a great long term solution to integrated cryptocurrency wallet on a smartphone [4]. However there are issues in the implementation currently. Firstly, they are limited to only certain smartphones currently. Secondly, they have an issue of trusted display since they use the same display of the smartphone and hence are vulnerable to an attack. Various solutions have been proposed for local attestation [3], but none of them has reached market adoption. And lastly, they do not implement a hardware-backed monotonic counter [18] and hence the attacker can physically brute force the PIN. It trades some level of security that a secure element offers to run complete applications in its environment.

5. Product Overview

As the mass adoption of cryptocurrencies draws nearer, it is essential to keep the digital assets handy on the go. Cypherock wallets ensures that your assets are extraordinarily safe and secured.

CY1

CY1 is the main detachable part that act as a hardware wallet. This could be ported to different mobile case and wrist bands. Built over CC certified EAL6+ secure element, wallet will provide best in class hardware security available in the market. It will be BIP 32, 39 and 44 complaint.

Scratch resistant touch screen display will provide ultimate ease of use to the user. The wallet will be water & dust resistant to provide seamless trading experience at any weather condition. It offers unparalleled security since the information exchange takes place at the application layer. The device will be work fine even if the smartphone is filled with malware. It will support all the major coins (including ERC20 & ERC721 token support) and the support will increase over time for other cryptocurrencies.

CY Case

CY Case is the mobile case to which CY 1 could be attached. Built over cutting edge design elements, case will provide ultimate protection to your phone courtesy of high impact material used inside. Case will be available for major smartphones in the market including IPhone X, IPhone 8 IPhone 7, IPhone 6, Samsung Galaxy s9 and Note 8 phones initially.

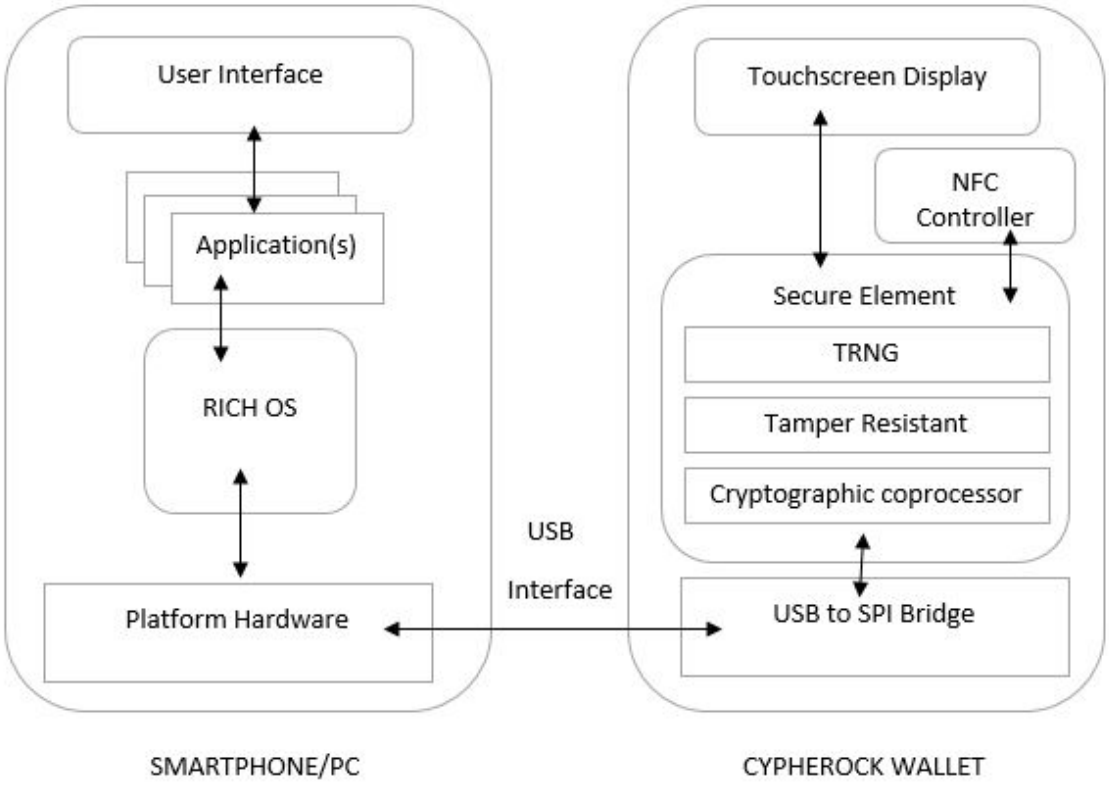
Client Application

An open source client side library will be developed to allow other software wallets to extend hardware support. Along with the library, client side application will be developed by Cypherock which will offer DEx support, integrations with Changelly & Shapeshift, Segwit support and multisig support both for Android & IOS. Cypherock will be running a full node to support the SPV clients.

6. Applications

- **Trade**: Device will support all major coins like Bitcoin, Bitcoin Cash, Ethereum, ERC20 Tokens.
- **U2F**: Our devices will support the FIDO Universal Second Factor (U2F) standard that simplifies the authentication process on compatible online services such as Gmail, Dashlane, Dropbox or GitHub.
- **Exchange**: User will be able to transact through decentralized exchanges.
- **Encrypt/Decrypt**: User can encrypt or decrypt any file to securely share data over untrusted channels.
- **Digital Signature**: User can digitally sign any data using their private key secured inside the wallet.

7. Architecture



8. Security Aspects

Due to decentralized nature of crypto economy, you are in control of your own assets but the price to pay is that you are the sole in charge of your own security. Most of the widely used wallets today runs on internet connected devices like PC or smartphone on which the potential attack surface is quite enormous. While the wallet app may be secure and open source, this does not help if you have already been tricked into downloading into a piece of malware that may anomalously record your screen and keystrokes or may even swap the recipient public address just before the signing process.

Hence considering the attack vectors possible (detailed below) it is advisable to use a completely standalone and proven wallet solutions known as hardware wallets for maximum security.

Attack Name	Description	Solution
ATTACKS ON BLOCKCHAIN		
Finny attack (or similar)	Mining a block that contains a double spend, then buying a service, then broadcasting the block.	It is advisable that the wallet should spend or accept only those transactions that have 6+ confirmations.
51% attack	If an attacker can control your connections to the Bitcoin network, they can prevent you from seeing newly found legitimate blocks and mine their own invalid block containing a bad transaction.	It is advisable to use only decentralised blockchain networks.
ATTACKS ON WALLETS RUNNING ON INTERNET CONNECTED DEVICES.		
Spyware Attacks	There could be number of background application running anomalously [11] that may access internal files or track your screen, key strokes, mic audio, geographical location, camera etc. This becomes even severe if the device is rooted.	Use a standalone device like hardware wallets.

Man in the middle attack	Pre-installed malware may swap the actual recipient public address at the source point or just before the start of signing process.	The attack surface on mobile phones and PCs is quite enormous, hence a dedicated standalone hardware wallets should be used for signing transactions.
Supply chain attack/Phishing	Hacker can publish fake trading app to buy assets on crypto-exchange, but you may be trading nowhere, instead just sending money to hackers account. Additionally, android allows installation of applications from untrusted sources without review, which further puts device security at risk.	The end device should have a unique identification code (or company's private key) known "only" to the trusted software provider for secure updates.
Lack of App Sandboxing	Android lacks the sandboxing of apps [7]. It is easy to create a keylogging application on Android using Accessibility services.	Digital assets need to be away from an internet connected device at any cost, specifically android. Use dedicated hardware devices.
Zero Day Attacks	IOS is completely closed sourced. Hence, the users will need to trust the OS for the security. Due to lack of openness, it increases likeliness for zero day attacks [8][9]. Graykey [12] is one of the examples.	Even if the firmware is closed-sourced, at least use applications which are open sourced to have greater fault avoidance.

PHYSICAL ATTACKS		
Side channel attack	Reverse engineering and analysis of power consumption, EM radiation etc. could be responsible for leakage of sensitive data.	Use secured tamper resistant processors.
Perturbation attack	Manipulations on clock or code execution sequence [15].	Use secured tamper resistant processors.
Brute Force Attack	The attacker brute forces the PIN to get access to the wallet.	Use hardware based counters and erase private keys on consecutive tries on the wallet.
Master Key Signing Theft	The attacker may hack wallet server to get hold of the master signing key and push malicious firmware update.	The signing will be initiated through 3 out of 5 multisignature architecture.
COLD STORAGE ATTACKS		
Address Display	Current hardware wallets due to screen size shows limited address string which opens to hacker generating same address string as displayed, but different address in reality [5].	Display complete address on the hardware wallet screen and save frequent addresses on hardware wallet for quicker transaction confirmation by the user.
USB Firmware	There have been successful attempts to use the device Firmware Update	Use tamper proof secure element to store the private keys.

	function on generic microcontrollers to dump their memory remotely [6].	
CUSTODY SPECIFIC RISKS		
Data Backup	Data is regularly backed on centralised clouds which opens attacks on brute forcing the external storage if it stores the private keys/seed.	Use dedicated manually backed up hardware cold storage.
Data Storage	IOS only allows its own set of credentials (for eg - private keys of Apple Pay) to be stored in secured element.	Secure Element should be used to store private keys. Hence, hardware wallets are utmost necessary for digital assets.

9. Hardware

Need for a Trusted User Interface

A ‘trusted user interface’ (trusted UI) is defined as a specific mode in which the device is controlled by the secured microcontroller unit(MCU), enabling it to check that the information displayed on the screen comes from an approved trusted application (TA) and is isolated from the rich OS on smartphone. The trusted UI enables the information to be securely configured by the end user and securely controlled by the MCU by verifying the user interface the device. When a user makes a transaction, a summary of the transaction is displayed on the screen by the MCU, ensuring that any non-secure applications stored in the rich OS on smartphone cannot tamper with the payment details. The end user is able to sign exactly what is shown on the screen and authenticate themselves by entering a PIN or password. As this authentication is carried by separate secured MCU, the activity is isolated from the handset and protected from unauthorized viewing.

Once an end user has entered a PIN on the trusted UI to authenticate themselves to the service or application, the trusted UI ensures that there is a protected mode in which only a specific TA is able to exchange information with the buttons and screen. i.e. a $1 transaction entered into a key is equal to a $1 transaction in the secure area of the device.

Secure Microcontroller Unit

A hardware wallet should have a hardware based root of trust (e.g., secure microcontroller, secure element, hardware security module, etc.) to securely store private keys and process transactions. These security components are dedicatedly designed to protect sensitive information against a wide range of physical attacks.
A Secure Element (SE) is a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities.

Secure Element used inside the Cypherock wallet is based on SecurCore®SC300™ 32-bit RISC core which is built on the Cortex®-M3 core with additional security features to help to protect against advanced forms of attacks.

The entropy source of the seed used to generate the random number is an integrated analog noise generator circuit. The verification of the randomness of the random number generator was done through NIST(National Institute of Standards and Technology) Statistical Test Suite SP800-22b.

10. Specific Features

Address Storage

Since the device will be frequently used, it is important to reduce the time a user will take to verify address on the screen. Commonly used addresses could be saved by the users on the secure element with an alias to enable faster confirmation of transactions, thus minimising phishing attacks.

Touchscreen

The user will require faster actions for transactions through the hardware wallet. Tasks like entering PIN and navigation are cumbersome with physical buttons. Hence the screen will need to be a capacitive touchscreen.

Portability

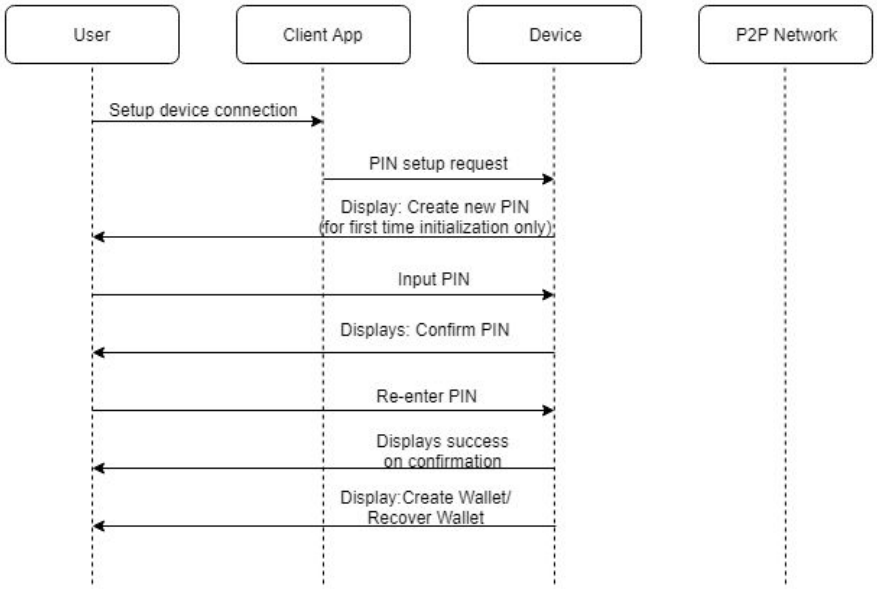
There are users who wish to change smartphones frequently and hence it is not economically viable to purchase a new hardware wallet for a new smartphone. Therefore, the hardware wallet will be a separate entity from the mobile case. If a user buys a new smartphone, he would only need to purchase a new phone case to use the old hardware wallet thereby cutting down the costs significantly.

Multipurpose Design

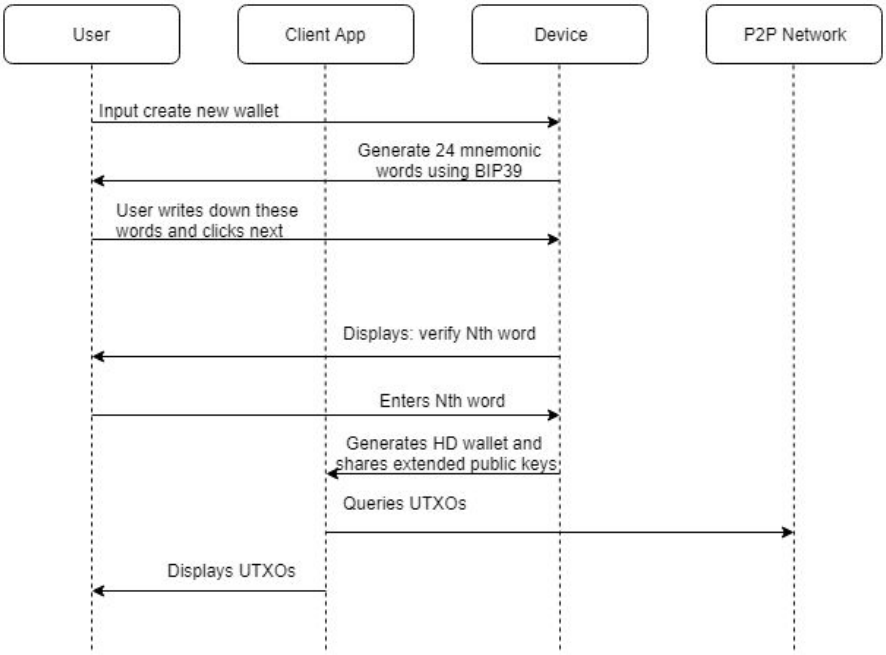
Most of the hardware wallets in the market are designed keeping in mind a single device (either a smartphone or a desktop) they address to. We intend to create the hardware wallet such that it could be used with any smart devices without compromising security and ease of use.

11. Working

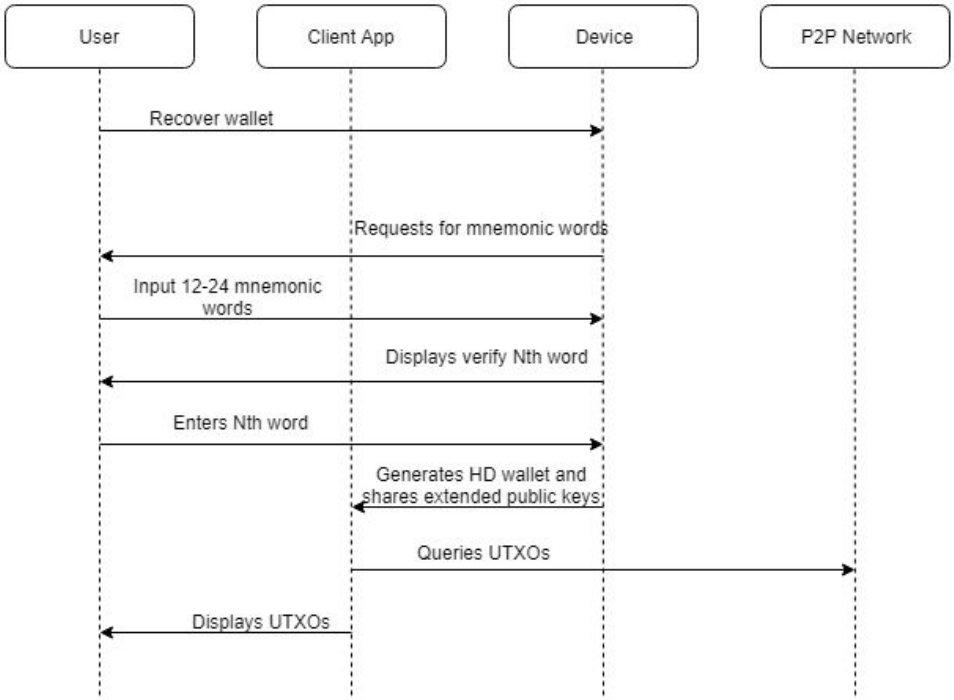
11.1 Wallet Initialization



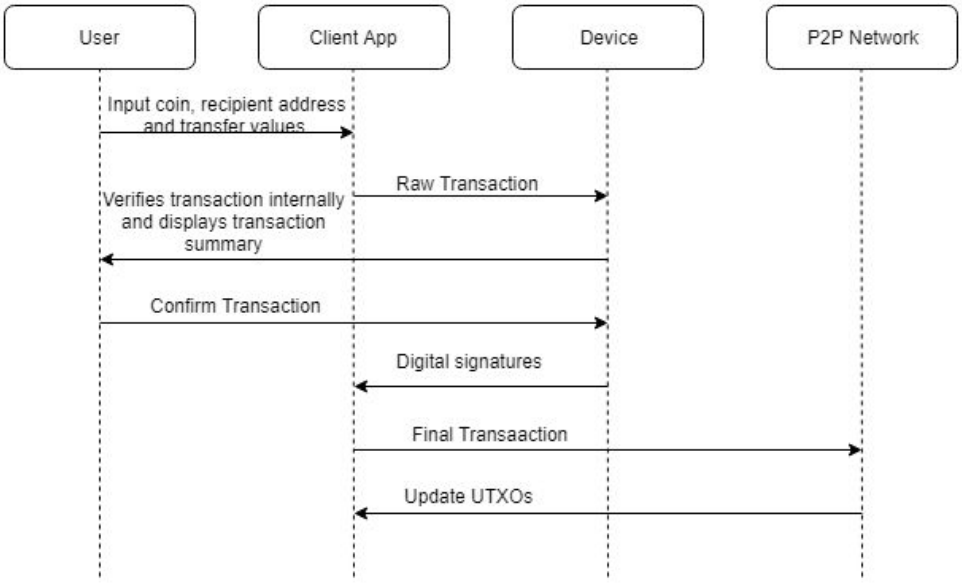
11.2 New Wallet Creation



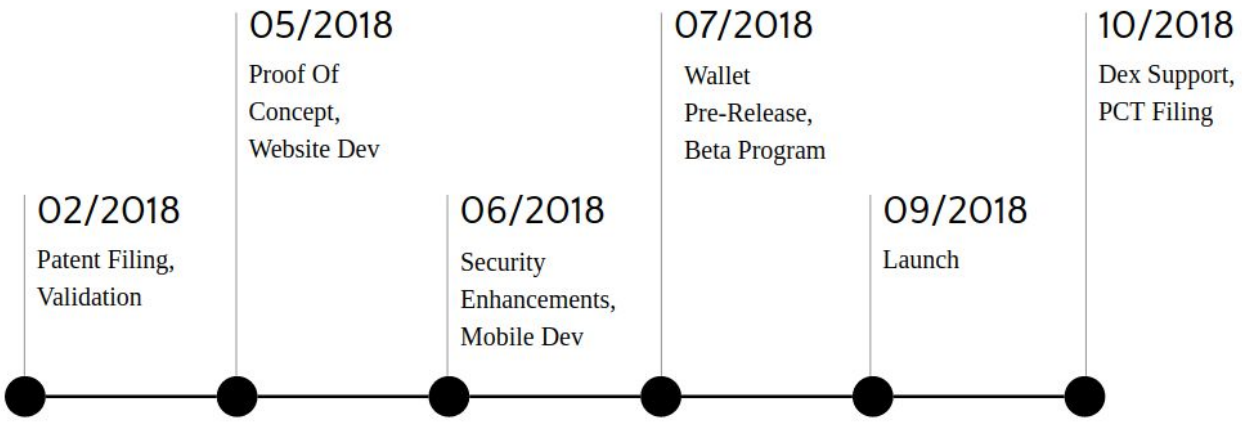
11.3 Old Wallet Recovery



11.4 Transaction Sequence



12. Roadmap


02/2018
Patent Filing, Validation
05/2018
Proof Of Concept, Website Dev
06/2018
Security Enhancements, Mobile Dev
07/2018
Wallet Pre-Release, Beta Program
09/2018
Launch
10/2018
Dex Support, PCT Filing

13. References

[1] TEE https://www.cs.ru.nl/E.Poll/papers/TEE.pdf Accessed: 2018-05-15

[2] Hardware Wallet
https://hackernoon.com/secure-cryptocurrency-hardware-wallets-71a6c65247be Accessed: 2018-05-15

[3] Local Attestation https://patents.google.com/patent/US8479022 Accessed: 2018-05-15

[4] TEE Based Hardware Wallet
https://www.ledger.fr/2015/04/30/leveraging-trusted-execution-environments-for-trustless-bitcoin-applications/ Accessed: 2018-05-15

[5] Security Risks
https://blog.hacken.io/hardware-wallets-the-illusion-of-total-safety-f2f44f6124d2 Accessed: 2018-05-15

[6] Hardware wallet vulnerabilities
https://blog.gridplus.io/hardware-wallet-vulnerabilities-f20688361b88 Accessed: 2018-05-15

[7] Android Security http://www.ru.nl/publish/pages/769526/scriptie_tim_cooijmans.pdf
Accessed: 2018-05-27

[8] IOS encryption
https://www.washingtonpost.com/world/national-security/johns-hopkins-researchers-discovered-encryption-flaw-in-apples-imessage/2016/03/20/a323f9a0-eca7-11e5-a6f3-21ccdbc5f74e_story.html?noredirect=on&utm_term=.f61eb866c0a4 Accessed: 2018-05-27

[9] Iphone Unlock By FBI
https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/ Accessed: 2018-05-27

[10] Trust Wallet Going Closed Source
https://medium.com/@trustwallet/why-open-sourcing-android-app-could-be-a-harm-to-the-crypto-community-fb3ae1707dc6 Accessed: 2018-05-28

[11] Android Botnet https://thehackernews.com/2018/03/android-botnet-malware.html Accessed: 2018-05-28

[12] Graykey https://motherboard.vice.com/en_us/article/vbxxxd/unlock-iphone-ios11-graykey-grayshift-police Accessed: 2018-05-28

[13] Android Security patches Lies https://www.xda-developers.com/android-oem-lying-security-patches/ Accessed: 2018-05-28

[14] Spyware Software https://cointelegraph.com/news/why-smartphone-wallets-are-insecure-and-how-to-protect-your-bitcoin Accessed: 2018-05-28

[15] Exfiltrate from Air-Gapped Computers https://thehackernews.com/2018/04/bitcoin-wallet-keys.html Accessed: 2018-05-28

[16] Single Wallet on Multiple Computers https://support.exodus.io/article/142-can-i-use-the-same-exodus-wallet-on-multiple-computers Accessed: 2018-05-29

[17] Sirin Labs Whitepaper https://sirinlabs.com/media/SIRINLABS_-_White_Paper.pdf Accessed: 2018-05-29

[18] TEE Software Counter https://www.ledger.fr/2015/04/30/leveraging-trusted-execution-environments-for-trustless-bitcoin-applications/ Accessed: 2018-05-29