# Payment Card Wallet

Bernard Parenteau

bern@floridalogic.com bparente@fit.edu

October 2018

v2 May 2019

## The problem:

If a Bitcoin wallet is compromised and a malicious actor obtains a private key they can immediately spend any coins held by its associated public key addresses. This fact, along with the uncertain security of both common user networks and personal computers and devices, leads to real and perceived vulnerabilities. These vulnerabilities can dissuade many coin owners from using their own private wallets, instead prompting them to effectively outsource security to an exchange. Evidence of this can be seen by the transaction volumes on exchanges. As such, many of Bitcoin’s original design goals, including decentralization, anonymity, and direct peer-to-peer transactions with no intermediaries have been sacrificed by the centralization and KYC/AML requirements of exchanges. (note recent “Proof of Keys” movement to encourage individual wallet ownership)

There are good existing solutions for desktop wallets such as using hardware wallets to complement existing software wallets. But for reasons ranging from perceived complexity to conceptual unfamiliarity to costs, these are not as ubiquitous as they might be.

And there are fewer secure solutions for users that would like to manage their holdings on their mobile devices, though several hardware wallets also have mobile device connectivity.

## A solution:

Most consumers are comfortable with credit cards and many are familiar with smart card authorizations. We combine these common security concepts to create a two factor authorization system for Bitcoin. The second factor will be a key combination stored externally on contactless smart cards with a form factor of a credit card. The payment card will need to be in close proximity to the mobile wallet initiating the transaction to spend Bitcoin that has been received by the Payment Card Wallet.

### Payment Card Wallet

The Payment Card Wallet is initially a customized version of the Electrum open source wallet for mobile devices that can receive and hold Bitcoins with multi-signature transactions (multi-sig in P2SH). And one of those signatures will have to be generated by a key on the card.

A user of the wallet will receive a credit card-sized smart card (the user would probably want multiple copies of the card for backup). The card will contain cryptographic codes on an RFID chip that can be read by the wallet. The payment card must be in physical proximity to the wallet’s mobile device for any coins to be spent.

Unlike some other security schemes, the Payment Card Wallet is more resilient to attacks in which phone service and phone numbers are hijacked, because a physical card is required to spend the coins.

(see the CardWalletDesign.docx document for technical details)

## The Goal:

The goal is to increase decentralization and anonymity via the use of individual wallets, with minimal modifications to existing methodologies. By providing additional security using techniques familiar to most users, such as payment card authorized spending that requires the actual card, it is hoped that more consumers will be encouraged to use their own wallets.

## The Present and the Future:

The initial version is for Bitcoin and uses a 1KB RFID chip in a plastic payment card.

Subsequent functionality is planned to include support for additional cryptocurrencies.

Subsequent functionality is also planned to include a wallet version that uses NFC to communicate with a chip on the card. This would enable the card to act as an ad hoc hardware wallet, potentially providing additional functionality and security.

## RFID vs NFC

While new mobile devices support NFC, most existing mobile devices do not. There have recently been a couple similar payment cards introduced (Cool Wallet S, D’Cent Card Wallet) that use a chip on the card and require the mobile device to have NFC to power the chip. This design also typically requires additional hardware component(s) and subsequently some additional cost.

But given that many existing mobile devices, especially lower-cost devices, do not have NFC capabilities, we chose to develop our initial version with readable RFID chip functionality only. As such, it might be particularly useful in lower income areas, as both the card itself and the mobile device would both be less expensive.