PointPay

Technical Paper[1]

Draft version 1.01 - 29.05.2019

Abstract. Cryptocurrencies are a fast-developing asset class in the financial markets. Because of the speed of development and innovative features, there variety amongst them and each cryptocurrency require a special way of working with it. Most of them have their own client and API endpoints for working with, different cryptography mechanics and different ideology. But common trait among this set is that one user can transfer money to another user.
However there is a problem even for the most technically savvy people - it is not easy to manage several cryptocurrencies: one must protect their private keys, check for vulnerabilities in different clients for saving money, etc. Also, the user must remember the specific mechanics of different cryptocurrencies. The absence of a hassle-free way to manage your cryptocurrencies is the main reason why their adoption has been low amongst not technically savvy users.
This is where PointPay comes in. It is an all-in-one platform which encompasses the full circle of services around cryptocurrencies. The focal point is providing banking capabilities to crypto holders (which is still a major gap in the crypto world) with conventional tools such as deposits, debit and credit cards, collateralized loans and cryptocurrency wallets. On the other hand, the platform will also enable businesses and traders via its exchange platform, offering advanced capabilities such as asset tokenisations and Initial Exchange Offerings (IEOs). All services will be payable by the platform's own native token - PointPay (PXP). The token will also serve as a governance tool for the platform itself.

[1] By Hristo Piyankov (hpiyankov@gmail.com) @ https://www.tokenomics-help.com/

Glossary

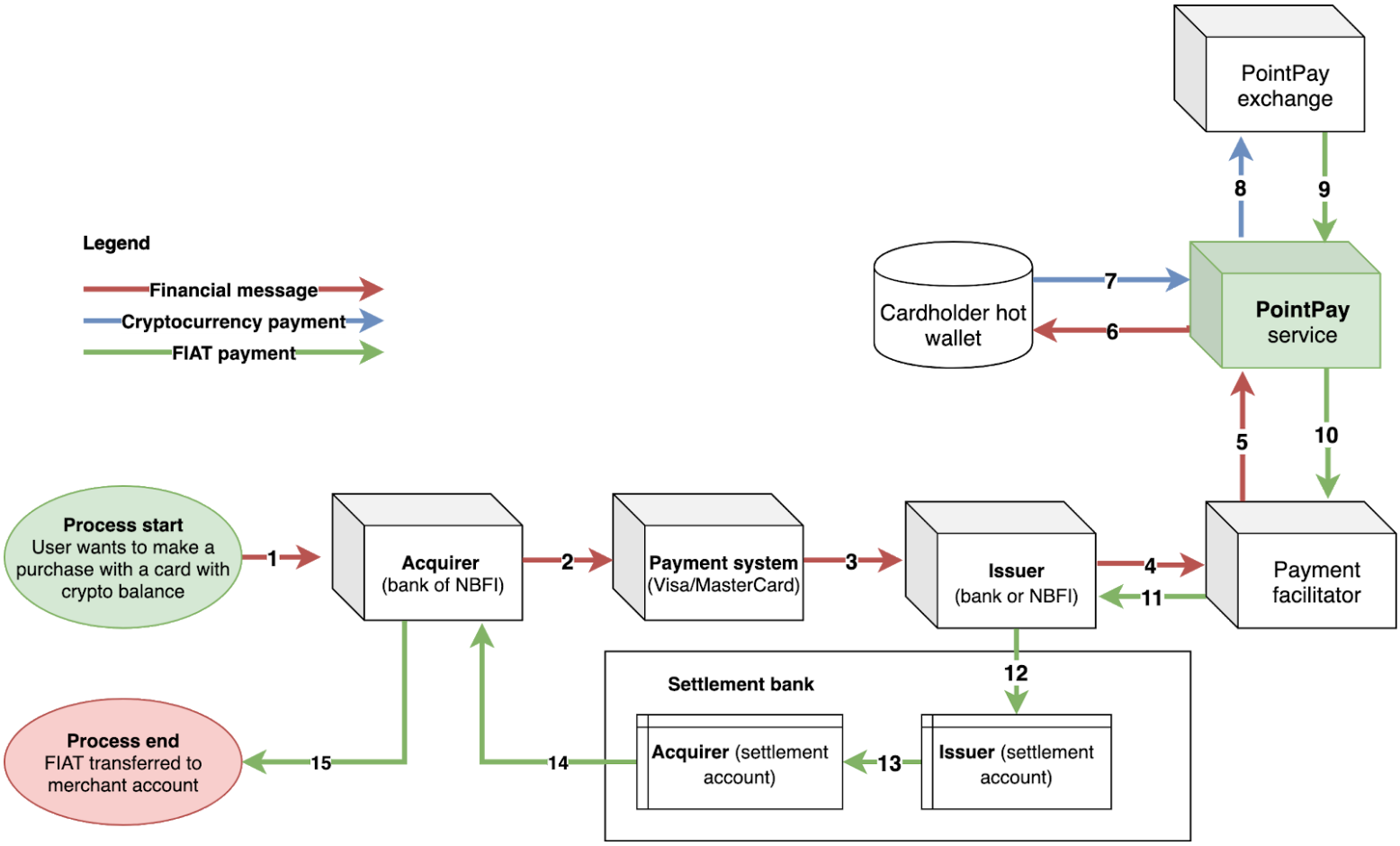
Before we move to the technical details of the system, we would first like to clarify several terms which are commonly encountered throughout this document:

- **PPW** - PointPay Wallet.
- **PPPS** - PointPay Payment System.
- **HS** - Hot Storage. Storage, where a small amount of funds are kept. Used for fast real-time transactions.
- **HSFP** - Hot Storage Fraud Policy.
- **CS** - Cold Storage. Extra-Secure storage, where the majority of the funds are kept.
- **SV** - Supervisor. This is the PPW admin. Controls money flow.
- **SESA** - Special Extra Secure Accounts - secure accounts, which protect the funds, even if the whole system is hacked.
- **PPM** - PointPay Mirroring - PointPay Comfort-Security technology.
- **PPMS** - PointPay Mirroring Storage. Cold storage, that stores payment passwords and additional SESA information.
- **PG** - Payment Gateway. Service, that processes transactions.
- **FIAT** - currency without intrinsic value that has been established as money, often by government regulation.[2]
- **NBFI** - non-banking financial institution.
- **Acquirer** - an acquiring bank or NBFI (also known simply as an acquirer) is a bank or financial institution that processes credit or debit card payments on behalf of a merchant.[3]
- **Issuer** - An issuing bank is a bank (or NBFI) that offers card association branded payment cards directly to consumers.[4]

[2] https://en.wikipedia.org/wiki/Fiat_money
[3] https://en.wikipedia.org/wiki/Acquiring_bank
[4] https://en.wikipedia.org/wiki/Issuing_bank

The PointPay Payment system

The PointPay Payment System (**PPPS**) aims to solve one of the most pressing issues in the cryptocurrency space - liquidity of crypto assets. While they are normally intended as payment methods, actually spending cryptocurrency is no easy task, especially when the vendors accept only FIAT payments. PPPS solves this by integrating with payment providers and leveraging its own cryptocurrency exchange service.



What happens behind the scenes when you swipe your card or touch the point of sale terminal with your phone while buying goods?[5]

[5] This process might be subject to change as the system is currently under development

1. You link your card previously issued by a fully licensed and PCI DSS[6] compliant bank (selected and approved as a PointPay payment partner) to the crypto asset of your choice using our app[7]
2. Information goes from the merchant to a bank that is providing payment services to that particular merchant
3. That bank is called Acquirer and his servers know what payment system is used at the moment so it routes information to the correct payment system
4. The payment system knows what bank issued your card and the information flows to it
5. This bank checks if you have enough funds and then send positive or negative response backwards

So this is how it works in general. We will add just one more simple step for you to this sequence and you will be able to use your crypto assets in brick and mortar stores, ATMs and even at online shops!

The PointPay Wallet

A cryptocurrency wallet is a software program that stores private and public keys and interacts with various blockchain to enable users to send and receive digital currency and monitor their balance. If you want to use Bitcoin or any other cryptocurrency, you will need to have a digital wallet.[8]

Comfort of usage

The PointPay Wallet (PPW) is a cryptocurrency wallet following all established and proven best practices. It has the following features:

- Easy transfer of funds to another user by some identification (email, phone and user-defined id).
- Support of all currencies on the PointPay platform.
- Easy overview of the user's crypto holding and transactions.
- Can facilitate transfers to both PPW and non-PPW-users.
- Multi-platform support.

---

[6] The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes - https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

[7] This part might be changed in the future depending on the final system architecture

[8] https://blockgeeks.com/guides/cryptocurrency-wallet-guide/

Security

Cryptocurrency transactions occur all the time. Most of those transactions are done in small amounts (such as small purchases and payments to merchants). On the other hand, large money transfers are a lot more seldom and require better security and validation.

This is where the concepts of Hot and Cold wallets in the cryptocurrency space come from.

- **Hot Wallets or Hot Storage (HS)** are wallets which are constantly connected to the internet which makes them less secure. They, however, offer a higher speed of execution and availability. In the PointPay system, only a small amount of funds will be kept in HS. Users will be able to operate with funds within the HS without the approval of the PointPay supervisors (**SV**). Regardless of this fact, this does not mean that the funds in those wallets will not be monitored. They will be under PointPay's Hot Storage Fraud Policy (HSFP) which automatically detects fraud patterns and alerts the SV.
- **Cold wallets or Cold Storage (CS)** are air-gapped[9] wallets which are considered state of the art in cryptocurrency security. They are not constantly connected to a network and require an SV interaction with the cold storage in order to approve a transaction. For example, let's assume that Bob wants to send Alice 1000 ETH. After he clicks the "Send" button, SV is notified about the large transaction. The transaction remains in "Waiting for moderation" status until the SV approves the transaction. After he checks the transaction for validity, the SV transfers ETH to Alice using CS. After a blockchain confirmation is received, the transaction's status is changed to "Done".

Using HS requires extra commissions and makes large-amount transactions slow and not user-friendly. What happens if the user wants to manage his money in a fast and secure way, even without supervision? In this case, the SESA and PPM technologies used.

PointPay Mirroring and Special Extra Secure Accounts

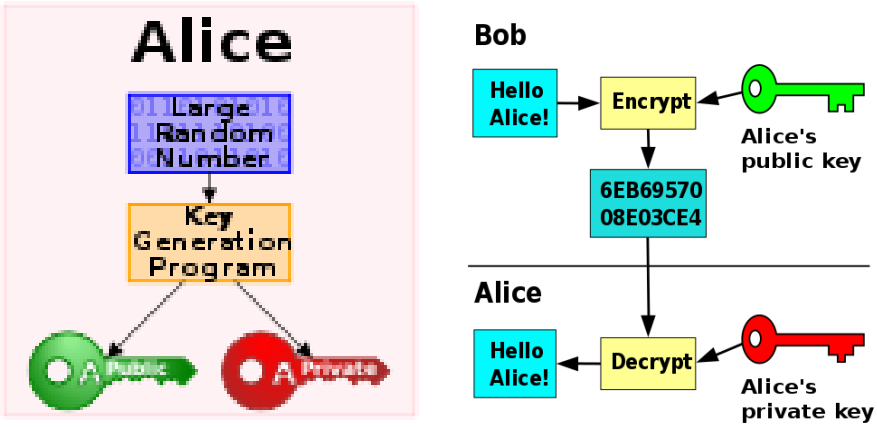
Any user can enable Special Extra Secure Accounts (SESA) as an option. If this is done, every transaction afterwards must be confirmed with a special payment password. All of the user's secure-sensitive data will be encrypted with this

[9] https://en.wikipedia.org/wiki/Air_gap_(networking)

password. Even if another person has full access to the PointPay system, they still cannot decrypt this data.

In the event where the user loses his payment password, it will be recoverable, by passing an extended verification procedure. This is possible due to PointPay Mirroring (PPM), that includes asymmetric cryptography and PointPay Mirroring Storage (PPMS).

So what is PPM? When a user enables SESA and sets his Payment Password, this information is sent to PPMS in encrypted form. The encrypted form is produced using public/private key cryptography.



Private key from this public key is stored in cold storage, access to which granted only to SV. User can disable Mirroring when enabling SESA, but in this case, they will not be able to restore the data if Payment Password lost.

As an additional security measure, the user can choose to enable 2FA[10] (two-factor authentication) checks for SESA, that will make checks in PG.

[10] https://en.wikipedia.org/wiki/Multi-factor_authentication