OfflineCoin Protocol

A cryptocurrency protocol which works with and without internet-connection, as convenient like paper money and credit card put together.

Condensed Draft Version (0.1.4)

Nearly all public cryptocurrencies today rely on fast and unaltered access to the global internet. They are basically useless in situation were access to the internet is not available, which is the case for many people and many situations.

The OfflineCoin protocol has the ability to work between at least two devices (smart-phone, computer, etc) without the need of an internet connection.
But when available it use the internet to get the transactions faster across the globe.

Typical use-cases:

- A situation where it would normally be possible to pay with paper-money, this could be as simple as fetching a soda from the vending-machine. Here we get instant, valid payment, without internet access.

- One wants to buy or sell something via the internet. Here we have internet available, and need a valid payment within a reasonable short time, but is does not have to be instant.

- One just wants to send or receive some money, like the monthly pay-check, or you want to send money to some relative who is on vacation on some island. In this case both parties may or may not have an internet connection, and usually a certain delay is tolerable.

Typically the bigger the payments, more time is available to get the transaction done.(For example: when buying a new car, the delivery usually takes weeks.) On the other hand the smaller and direct the payment are, the more instant they have to be. Eg. Buying a slice of pizza at a fast-food stand.

The technology behind it:

To make the OfflineCoin Protocol work independently of an internet connection, it transmits additional data during any payment, thereby building an offline peer-to-peer network, which is a mesh based network.

An example:
Alice without internet wants to sent 5 Offline-Coins to Bob

Alice opens her wallet and sends 5 coins to bob.
--- The wallet formulates the transaction and stores it.

Alice goes to the bakery and buys a bread for 0.05 OfflineCoins.
--- During that payment the transaction to bob gets transmitted to the baker.

A bit later Carl also goes to the bakery to buy something, and pays.
--- During that payment the transaction form Alice to Bob moves to Carl's smart-phone.

Carl travels to the next town and buys something at the cafeteria.
--- The 5 coin transaction from Alice to Bob make their way to the wallet of the cafeteria.
--- This wallet is connected to the internet, now every wallet within the internet get this transaction.

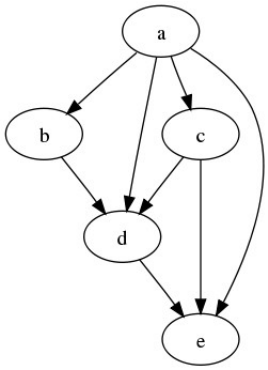
If Bob does any coin exchange with anybody who was connected to the internet he will automatically receive this transaction, and like in all cryptocurrencies, Bob is the only one how can use it.

In case in that cafeteria internet would not have been available, the information form this transaction would have been transmitted to every costumer after Bob. And those would then carry them to other towns and city's with shops and cafeterias with again would spread this transaction further over the globe.

Within a few day most of the OfflineCoin Wallets around the world including Bob should have gotten the transaction. Thereby enabling a slow internet like communication.

Even after not using his wallet for a month, upon making a fresh transaction with any other wallet, Bobs wallet is immediately updated to use the funds he has waiting.

The OfflineCoin Protocoll is based on a Directed Acyclic Graph (DAG), like the cryptocurrency IOTA and Byteball. This is an evolution of the Block-Chain technology used by Bitcoin.



See:
https://en.wikipedia.org/wiki/Directed_acyclic_graph
https://iota.org/IOTA_Whitepaper.pdf
https://byteball.org/Byteball.pdf
https://Bitcoin.org/Bitcoin.pdf
https://en.wikipedia.org/wiki/Blockchain

The main focus in the OfflineCoin Protocoll is that every wallet has to maintain a flawless and linear history of transactions, and has to be able to prove that to every other wallet.

There are also miners in the network, who compile blocks of information, which are provided to the wallets to enable them to quickly verify any payment for themselves without the help of an internet connection and without storing the history of every transaction ever made. These blocks are not connected in a Block-Chain like manner, but also in a Directed Acyclic Graph, creating a Block-DAG.

Thereby there is no limit of transactions per time possible on the network.

The miners second purpose is to merge and correct seemingly conflicting payments. There may happen certain situations in which conventional cryptocurrencys seem to work but do not:

The national Firewall -Problem:

A nation decides to install a national firewall which blocks for any Bitcoin related traffic. This would result in the situation that the Bitcoin wallet in that country would still behave normally, so one could receive and send Bitcoin within that country.

But as soon as any Bitcoin-protocol communication to the rest of the internet is re-established, all transactions in that country during that period are undone, as if they had never existed.
In case that country would house more than half of the miners in the world, it would undo all transaction of the rest of the world.

Bitcoin was not designed to handle this kind of situation. If everything goes well those transactions can be rescued, ending up in Bitcoins Mempool again.
However the miners would try to process them, but unfortunately not in the right order. Thereby trying to send money for an account which was not received jet, resulting in invalid transactions.

There could be a solution with some human intervention, but in the meantime some would resend some “refunded” Bitcoins, some would spend them otherwise. In the end resulting again in an ugly situation.

In the OfflineCoin network the miners do not expect to receive transactions in the correct order, and do not abandon other blocks but rather incorporate the information, and merge available information to a consistent state. Therefore the state of the network is always improved when yet unknown transactions or blocks from other miners become available.

Double-spending Attack:

There are several mechanism to prevent a double-spending of occurring:
Every wallet software can determine a “limit-value” based on its database, and on the situation (offline or not), the counter-party and some further factors.

It is always safe to accept an instant transaction below this “limit-value”, without any further confirmations.
If the payment is just a bit above that value, the wallet determine a short time for both parties to wait until the payment is valid.

For payments which are way above that threshold (one wants to buy a new car or a house) both parties simply have to wait for enough confirmations. In the case that one of them has internet-connection it will take just a short time.
In an offline context, depending on the situation, collecting the confirmations may take form few hours up to a few days.

When double-spending attack is detected by any member on the network, the account which did it gets frozen. The possible “limit-value” determined by the algorithms make sure that a loss for the wrong-doer in that situation is higher than the possible gain from the double spending.

A double-spending is easy to detect and to prove since the same base point of an account history was used for two different transactions and was tamper-prove signed. This cannot happen by accident.

Further, all parties which are potentially victims of the attack get informed to be able to file a legal charge against the payee.
In offline situations especially when higher amounts are involved one usually knows who the counter-party is.
The miners make sure that the money from frozen account is distributed correctly. Nobody who acted correctly loses money, but at the same time it is made sure that no additional money is created in an improper way.

Miners do not necessarily have to be connected to the internet, it also would be sufficient if one has a good wallet-connection to some shops. It is enough for a miner to get a relevant amount of transactions and have the means to provide the resulting blocks effectively.

The OfflineCoin can keep working without any miners at all. The consequence is only that over a longer period of time the devices have to carry bigger databases in order to function properly. Instant payments may slow down because more data has to be transmitted each time.

Incentives:

The accounts which are mainly involved in distributing many transactions can claim parts of the transaction-fees involved. This helps to keeps the offline mesh network fast.

Miners get rewarded for their effort to merge and compile blocks, having stored a huge history and being very available (maybe online). Merging itself is a huge computational effort. This is in itself a partially Proof-of-work.
Since the mining algorithms are constantly improving, a conventional computer is the most appropriate machine to accomplish that task.

The advantage: Even in remote locations without stable internet-connection with only a few inhabitants, a few people there could be happy to provide this mining-service with their computers or high end smartphones to the local environment.

There are further incentives behaviours that help to evolve and stabilise the network:
eg: Wallet-programmers, for those who detect bugs in those wallets (bugbountys), VPN-tunnels, core-programmers, those who improve the math behind protocol, anonymizing, etc.

Value-Stability and Cold-Storage Parking

With the offline coin protocol it is possible to keep coins in ones account in a less liquid state and receive interest on those parked coins with the trade-off of having to wait a short while when converting them back into the normal liquid state for online and offline use.

The interest rate during “parking” varies and is depends on the amount of coins “cold stored” (or Proof-of-stake).

Usually, when a currency is gaining value, people store the money because it is getting more valuable just by waiting, thereby the available amount of money in circulation decreases, this then further increases the value.

In the other case when a currency is losing value, people tend to not store it, thereby increasing availability, which further pushes down the value.

Since a currency should be stable, this is prevented in OfflineCoin from happening: the interest rate compensates this behaviour.

If many coins are stored the interest rate gets low, thereby people get motivated to store less.
If few coins are stored the interest rate gets high, thereby people get motivated to store more.

This is quite similar to how central banks would regulate interest rates to stabilise the value of a paper currency, but in this case it is automatically determined by algorithms depending on the amount of coins that are cold-stored in the global network.

Outlook:

Since this is an early condensed version, there is more to come.

Do not hesitate to give suggestions or ask questions via email: protocol@offlinecoin.net

I will directly answer and improve this document accordingly in upcoming versions

Links:

Secure Wallet-Assisted Offline Bitcoin Payments with Double-Spender Revocation
https://en.wikipedia.org/wiki/Directed_acyclic_graph
https://iota.org/IOTA_Whitepaper.pdf
https://byteball.org/Byteball.pdf
https://Bitcoin.org/Bitcoin.pdf
http://www.jbonneau.com/doc/BM14-SPW-fawkescoin.pdf