Walltime Zero

Crypto assets negotiation without crypto custody.

Felipe Micaroni Lalli <micaroni@gmail.com>
Igor Hjelmstron Vinhas Ribeiro <igorhvr@iasylum.net>

v 1.0, April 1st 2020

Abstract

Walltime Zero defines itself as a "Blockchain observer" that validates public transactions and performs certain actions if they occur. This document proposes a model for trading crypto assets (such as Bitcoin and Litecoin) involving fiat currency (such as Real and Dollar) without the need for centralized custody of crypto assets through the concept of "Outbound Oracle", completely eliminating all the risks related to custody for both users of the service and the custodian. Not outsourcing crypto custody has numerous advantages for all parties involved and for the entire ecosystem. Unlike a traditional exchange, instead of receiving cryptocurrencies and fiat currencies from the interested parties and keeping them until the trade process is complete (which can take months or years), this intermediary receives fiat currencies from only one of the parties. The party willing to trade cryptocurrencies for fiat currencies ("selling" party) sends the cryptos directly to the other party interested in exchanging fiat currency ("buying" party). After that, it is checked whether the transfer actually occurred on the Blockchain and, once it is confirmed, fiat money is transferred from the buying party's bank account to the selling party's account.

1 Motivation

Since the creation of Bitcoin, centralizing the of crypto assets has proven to be a fiasco for several reasons [10]. Bitcoin is not linked with the well-known moto "Be Your Own Bank" for no reason. Walltime Zero's proposal is in line with this principle of Bitcoin and as a result we avoid separating the crypto owner from the crypto custody.

1.1 The risk of crypto custody

The process of outsourcing crypto custody is quite risky. Some of the risks are: simply losing private keys [8], the death of private key managers [7], fraud, theft, insolvency, hacking and mismanagement of funds. In 2019, numerous cases like these took place in Brazil [9]. The risks apply both to the user, who has his funds lost irreversibly, and to the custodian who — unless he is the scammer himself — may be threatened or have his reputation destroyed forever. There are many risks to be taken into consideration (especially if the custodian himself is dishonest) even with security techniques to mitigate them, such as the use of cold wallets, multi-signatures and timelock, among others. Crypto theft is very attractive to criminals because it is irreversible and leaves little or no trace. When custodians collapse, it is difficult to know for sure whether the reason was incompetence in managing the funds, virtual or physical attacks or whether the custodians were scammers themselves.

Figure 1: Bitcoin magazine from August 2012 showing one of the first disasters resulting from centralized crypto custody - Bitcoinica bankruptcy caused a huge price crash at the time.

Moreover, it is almost impossible to actually prove the solvency of crypto assets. Even sophisticated techniques specifically designed for this purpose face meaningful limitations [13]. For example, a custodian can always borrow crypto assets and use them during an audit.

1.2 Centralization and artificial inflation

Centralizing a crypto asset can be harmful for the asset itself because it may result in "artificial inflation" when custodians become big and insolvent, undermining its market price. Imagine an almost completely insolvent exchange platform operating with millions of crypto assets: in the eyes of the market, those assets does not exist until they are withdrawn from the platform. Now, picture many platforms doing just the same: a scenario like this can easily make the total number of "virtual" (inexistent) crypto assets in circulation much higher than the number of real assets (artificial increase in supply). Of course, it all could be exposed when custodians collapse, but the asset's price would devalue until then.

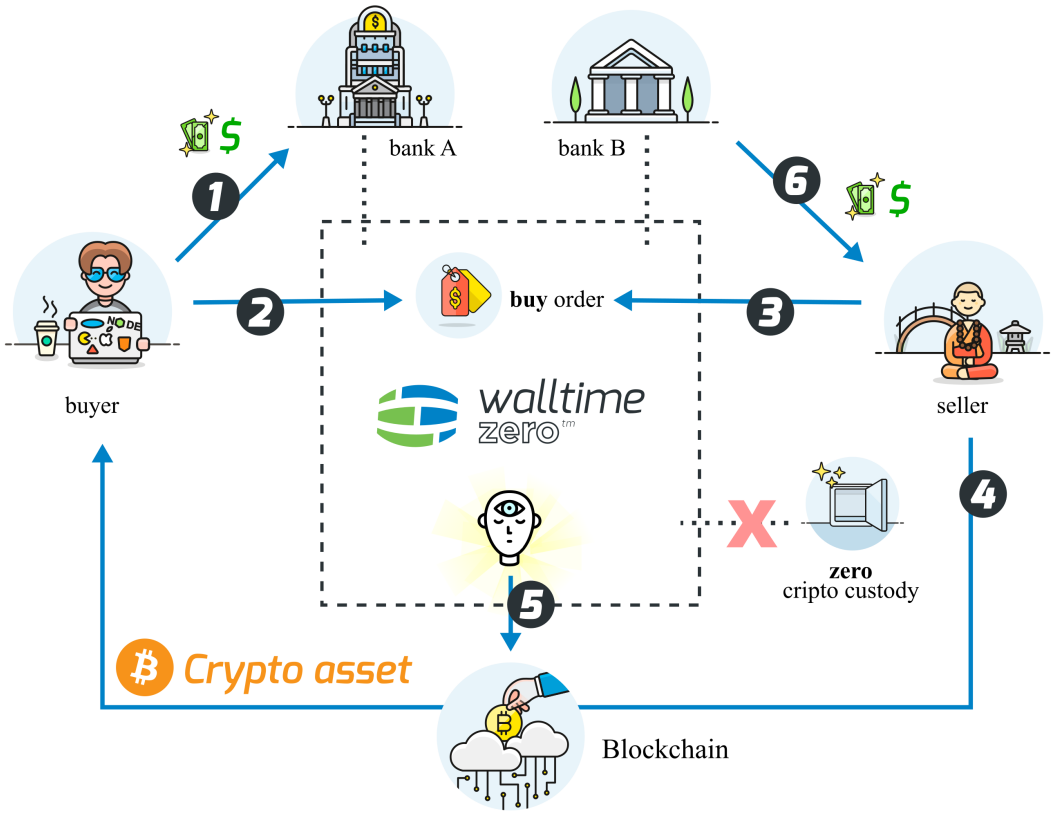
"Fake papers" are relatively common in the gold market [11] and in the precious metal market in general, mainly because this type of asset is not very portable and therefore it is necessary to trust its storage to a centralized entity. Crypto assets, on the other hand, have the advantage of being quite portable and "Plausibly Deniable" [12], which makes them much more propitious to being held by its owner and to decentralization than precious metals. Why not take advantage of these features of crypto assets and avoid centralized custody as much as possible?

1.3 Conclusion

Due to the reasons discussed above and aiming to eliminate crypto custody risks and to avoid the centralization of crypto assets, the authors of this proposal created **Walltime Zero**, an innovative and lean mechanism for trading cryptos without the need to store them.

2 Specification

To sum up the concept, **Walltime Zero** is a "Blockchain observer" (Oracle outbound or Outbound Oracle [6]) that validates public transactions and performs certain actions once a transaction is made on the Blockchain.



2.1 Step by step of a semi-decentralized negotiation

1. Buyer deposits fiat currency in one of the **WZ** bank accounts and specifies the crypto asset's address, price and quantity.
2. **WZ** publicly displays it in the **buy order book** on its website.
3. The seller chooses one of the available buy orders and makes a reservation.
4. The address of the buyer's crypto asset is shown to the seller and then he transfers cryptos **directly** to the buyer without going through **WZ**.
5. **WZ observes** the transference on the Blockchain and confirms its validity.
6. **WZ** makes a bank transfer in the corresponding amount to the seller.

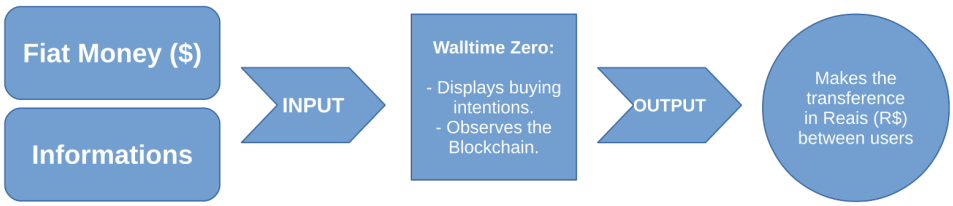
2.2 Some important considerations

- For large amounts of money, the lawfulness of the origin of the fiat currency deposited by the buyer into a **Walltime Zero** bank account must be checked, that is, whether the buyer has financial capacity compatible with the volume.
- Likewise, **Walltime Zero** can only make a bank transfer to the seller if he proves his financial capacity.
- There are some operational risks better described in section

3.2.

- The concept proposed by **Walltime Zero** is only possible for crypto assets whose transferences can be observed externally.
- There are only **crypto assets buy orders**. This can negatively impact the user's experience because the buyer is always the "maker" (he cannot place taker orders) while the seller can only place taker orders, failing to express his intention to sell in the order book.
- Every order must be executed **in full**. There is no concept of partial orders and if the seller wants to negotiate a very high volume it is necessary to make several transfers to different wallets, which can negatively impact the user's experience. Creating some minimum or incremental restrictions could optimize this procedure. For example: allowing orders for predetermined amounts such as 0.1, 0.5, 1 and 5 BTC to be created. In this case, a user who wants to buy 4.6 BTC can place 4 orders for 1 BTC, 1 order for 0.5 BTC and another order for 0.1 BTC. On the other hand, if the buyer creates orders for high quantities (5 BTC, for example) he will need to wait for a seller who wants to execute the order as a whole. To increase the chances of execution and decrease the waiting time, the buyer should create orders for small quantities.
- Cancelling an order can be difficult for a buyer, as the seller can reserve an order for a time period in which cancellation is unavailable. Keep in mind that, despite that, the seller must go through with the selling process in case he had reserved the order and if he doesnt he may receive a penalty for it. One way to minimize this negative impact on the user's experience is to provide the possibility to create "dynamic orders", that is, orders whose purchase prices are automatically updated based on some external indicator. Example: "exchange price XYZ + 5%". That way, the price would vary and would be worth the price at the time of consolidation of the transfer in crypto.

2.3 Transformation model



Notice that crypto assets do not go through **Walltime Zero**.

3 Risks

3.1 Legal risks

Legal risks comprehend bank account freezing, governmental requests to provide personal information about clients and receiving illicit money from buyers. All of these risks are common to traditional exchange platforms and one way to minimize them is through compliance and KYC.

3.2 Operational risks

3.2.1 Possible conflicts and mediation

1. Accidental transference by a seller

   One of the greatest risks for a seller is making an **accidental transference** to the buyer. A seller could make three kinds of mistakes:

   (a) transfer an amount *higher* than the one specified in the order.

   (b) transfer the amount *after* the transference window is closed (transference expiration). In this case, the order could be reopened and be available to another user meanwhile.

   (c) transfer to an old buyer's address (out of any negotiation context).

   In these three cases above, the only way to recover the amount sent is through the buyer's *goodwill*. Thus, in this scenario, the **Walltime Zero** system limits itself to detecting and confirming that the accident

occurred and trying to mediate the case as far as possible. **Walltime Zero** will give the buyer a deadline to return the exceeding amount to the seller and, if it is not met, his data will be informed to the seller so that he can file a complaint to the competent authorities and sue the dishonest buyer. The *privacy policy* makes it clear from the beginning that in cases of conflicts like these, the data can be handed over to the other party so that he can take appropriate legal measures.

The seller could also transfer an amount *lower* than the specified in the order. In that case, **Walltime Zero** would take no action until the seller transfers the remaining amount. Because it could harm the buyer temporarily, some type of sanction could be applied to the seller, such as a red flag that prevents him from reserving orders for a period of time or indefinitely.

2. Slow transference(inadequate fee)

   Another case of conflict can occur if the seller transfers the crypto to the buyer with an inadequate network fee (smaller than what is suggested by the system), causing the maximum acceptable waiting time for the buyer to be exceeded. In this case, **Walltime Zero** will try to mediate the conflict and suggest that one of the parties use the CPFP technique (for Bitcoin purchases and other techniques for other cryptos purchases). In this scenario, the seller would also receive a penalty.

3.2.2 Abuse from the seller by reserving numerous buy orders

This kind of abuse has a meaningful impact because reserved orders are invisible to other sellers and unavailable for cancellation during the entire reservation period (transference window), which could last for a few minutes. In a scenario of high volatility, not going through with a reservation could be damaging for the buyer as he has his order frozen during this time period. For this reason, similarly to trading systems such as Mercado Livre or e-Bay, when a seller reserves an order, he is obliged to honor his commitment under the penalty of paying a pre-defined fine that will be divided between **Walltime Zero** and the buyer as a form of compensation.

3.2.3 Risk of fiat custody

Despite not taking crypto custody risks, the **Walltime Zero** model still takes fiat custody risks just like any traditional exchange. The risk is less than that of storing crypto assets, since all transfers in fiat currency are controlled by the traditional banking system, nominal, reversible and also have strict limits, in contrast to crypto assets, which are anonymous, irreversible and unlimited - therefore, much more attractive to attackers. Another important point is that, as soon as an order is executed, the value in fiat currency can be automatically transferred to the other party without the need for a withdrawal request made by the seller. This results in the custodian amount being actually reduced.

4 Glossary

- **Blockchain** is an immutable registration technology. This concept first appeared in Bitcoins white paper[3].
- **Buyer** is the person interested in exchanging fiat currency for crypto currency. Although the term is ambiguous (it is also possible to say that someone wants to "buy" reais using Bitcoin, for example), its meaning has been previously specified in this document.
- **Crypto asset** is a purely digital commodity such as Bitcoin [3].
- **Crypto custody** is defined as the custody of crypto assets, that is, the temporary centralized storage of digital assets where the user does not own the private key to these assets, which are under the custodian's responsibility.
- **Exchange** [1] is the service of intermediating two parties interested in exchanging cryptocurrencies and fiat currencies. This third party receives assets from the other two parties and then, once the transaction is consolidated, it exchanges between them. That way, none of the parties needs to trust each other, they only need to trust the exchange during the trade process. **Walltime Zero** does not define itself as an "exchange" because at no time does it receive or store crypto assets. The service is limited to observing whether two parties comply with the agreement between them and, if so, it takes another action (in this case, the transference of fiat currency from one party to the other).
- **KYC** (Know Your Customer) comprises client identification and customer due diligence (also known as KYCs requests), implying that companies that are active in the financial services industry must perform customer due diligence in order to prevent identity theft, fraud, money laundering and terrorist financing. Laws and strict regulations imposed by governments from all over the world forced companies to take a closer look into their operations and into the relationships they promote in order to proactively manage risk exposition. National and international regulations on money laundering (Anti-Money Laundering - AML) such as the Alternative Investment Fund Managers Directive (AIFMD), the Foreign Account Tax Compliance Act (FATCA) and the Common Reporting Standard (CRS) impose KYC obligations that affects companies world wide.
- **Fiat currency** [2] is a state currency (such as Real, Dollar, Euro, etc.) issued and controlled by government agencies. This kind of currency is usually not backed by any commodity.
- **Outbound Oracle** - An "Oracle" [4] connects the "real world" and the "Blockchain". Entry Oracles are the most common, they feed smarts contracts [5] with observations from real-world events (for example: ambient temperature or the result of a presidential election) so that a certain pre-programmed behavior happens and the result is consolidated on the blockchain. An "Outgoing Oracle" [6] does the opposite: it uses the Blockchain as information source (payment for a particular wallet, for example) and executes actions in the real world. **Walltime Zero** does just that: it checks whether a particular payment has been made to a particular wallet and, if so, performs an action in the real world which is the transference of fiat currency from one bank account to another as specified in a previously signed contract.
- **Order** represents a user's intention to buy or sell.
- **Maker order** represents an order in the order book awaiting an offer.
- **Order taker** represents an order that is executed immediately without awaiting in the order book because it has an attractive price.
- **Socketpuppet** is the creation of a fake identity used for fraudulent purposes on the internet.
- **CPFP Technique (Child Pays For Parent)** is an elementary concept that means that the child transaction is paying and compensating for the parent transaction so that both can be confirmed soon.
- **Seller** is a person who is interested in trading cryptos for fiat currency. Although the term is ambiguous (because we could also say that a person wants to "sell" reais for bitcoin, for example) its meaning has been previously specified in this document.

5 References

- [1] J. Frankenfield, Bitcoin Exchange Investopedia Definition (archived), 2019.
- [2] L. Mises, The Theory of Money and Credit, 1912.
- [3] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (archived), 2008.
- [4] B. Curran, What are Oracles? Smart Contracts, Chainlink & "The Oracle Problem" (archived), 2019.
- [5] N. Szabo, Smart Contracts: Building Blocks for Digital Markets (archived), 1996.
- [6] S. Voshmgir, Blockchain Oracles (archived), 2019.
- [7] Quadriga: The cryptocurrency exchange that lost $135m (archived), 2019.
- [8] Cryptocurrency exchange CEO 'loses' private key to user funds — claims it doesn't really matter (archived), 2019.
- [9] Crypto and Blockchain News From Brazil: Oct. 6–12 in Review (archived), 2019.
- [10] The Bitcoinica Hack (archived), 2012.
- [11] B. Saelensminde, There's Something Fishy Going On In The Gold Market, 2014.
- [12] Plausible Deniability (archived).
- [13] Kraken Proof-of-Reserves Audit Process (archived), 2019.