Why Crypto Needs a TeaParty

By SteveJay

April 5th 2023

To anyone familiar with crypto, the names FTX and Sam Bankman Freid may send shivers down the spine. As a result of criminal activity by FTX executives, customers were left unable to access their funds. Unfortunately, there's a high likelihood that many will never see those funds again.

When you place your crypto onto an exchange you no longer have control over how those funds are used. Although you have a deposit address for your funds, what usually happens is all the deposits of a particular coin are lumped together in a liquidity pool. A portion of that liquidity pool is then often used in various ways by exchange operators attempting to make more money. This is very similar to how traditional banks operate – an assumption is made that not everyone will want to withdraw their currency at the same time, so they only hold enough in reserve to meet the anticipated withdrawal requests.

The problem for customers in this model of operating is that if everyone *does* want their funds at the same time it will not be there. All it takes are a few rumors of the exchange being in trouble and everyone (quite rightly) tries to get their money out. As the exchange cannot meet these demands, the only solution they have is to halt withdrawals. They may, or may not, turn them on again in the future.

Meanwhile, you can't get your funds out. That perfect moment you had been waiting for to buy crypto X is gone, or by the time withdrawals are re-enabled your coins are worth 20% less than they were, or any number of other scenarios exist where you lose out.

In the end, the reason is that the people you entrusted with your money were using *your money* to try to enrich themselves. They can dress it up any way they like but that really is the

bottom line. To be fair, there is very little difference between this and how traditional banks operate – "It's just the way things are done." How comforting.

The other problem with CEX and DEX setups is that all those funds concentrated in one place make them a highly attractive target for criminals. Chainalysis reported in February that an eye-watering $3.8 billion was stolen by hackers in 2022 alone, mostly from DEX systems.

The only alternative to CEX and DEX trades are "over the counter," or OTC trades. These involve two people agreeing a private sale on a social media channel, no CEX or DEX involved. However, this way also carries a high level of risk. There is no way to ensure that both traders are acting in good faith. One will always be the first to send their half of the trade to the target wallet, which gives the other the chance to just take the funds and run. There are a lot of scammers creeping around on those channels and they have a huge bag of dirty tricks they use to separate you from your coin.

So, there are two main vulnerabilities that need to be overcome. The first is the liquidity pool, because *not your keys, not your coins* should be the guiding light of anyone involved in crypto, and the second is the level of blind faith involved in OTC trading.

Enter TeaParty, a trading platform that does *not* utilize liquidity pools and does *not* require blind faith on the part of the traders. No mismanagement or misuse of customer funds, no juicy target for hackers, no reliance on the other side of your trade being a genuine, trustworthy person. Any funds used for trades remain in the customers' private wallets for the maximum time possible, and are only handled by TeaParty for the minimum time possible. At no point do the people running TeaParty have access to customer funds, so no chance for them to use customers' money to make money for themselves.

At its most basic level, the way it works is this:

Jack wants to sell 10 Redcoin (RED) for 20 Bluecoin (BLUE). Jack places a sell order using TeaParty, which advertises the order in the marketplace. Mishka is looking to buy 10 RED and decides that 20 BLUE is a fair price, so she responds to the order and offers to fill. Jack accepts, and they agree a time limit of one hour to complete the trade which is then entered into TeaParty.

TeaParty then creates 2 wallets – one for the seller on REDchain and one for the buyer on BLUEchain. It sends the PUBLIC address for the RED wallet to Jack and the PUBLIC address of the BLUE wallet to Mishka. The moment it does this the clock starts ticking.

Jack sends his 10 RED to the RED wallet, and Mishka send her 20 BLUE to the BLUE wallet. Once TeaParty has confirmed both accounts have received the correct funds it initiates the exchange. This entails sending the PRIVATE key (with randomly generated password) for the RED wallet to Mishka, and the PRIVATE key (with password) for the BLUE wallet to Jack. Each can then retrieve their new wallet and withdraw their funds as they wish. The coins themselves do not move - instead, the keys are given to the relevant party.

If the trade is *not* completed within the allotted time, any funds deposited by either party are automatically returned and Jack's sell order is returned to the marketplace. Whether or not the deal goes through, TeaParty *does not store the private keys!* Those keys are written to the devices on which Jack and Mishka made the trade, and then they are securely and permanently deleted from the TeaParty database.

Both buyer and sellers can still place market and limit orders. Trades can also be made privately, without listing on the marketplace. The movement of coins will still be recorded by the relevant blockchains so nothing will be hidden but the trade will not be advertised. The fees for using TeaParty is paid with GRAMS, the native layer 1 coin of PartyChain.

The advantages are huge. Your funds remain in your private wallets until the moment of the trade. Neither side can lose their funds through being scammed by the other: the process is

automated and unless both sides of the deal are present the transaction will not occur. There are no liquidity pools required, so no opportunity for misuse of those funds from within. And as each trade is carried out independently of any other, in such a small time period, there is no juicy target for bad actors to focus on. You decide how long you leave your funds on TeaParty and there are no withdrawal costs beyond the blockchain gas fee.

This is what TeaParty has to offer from the outset, and there are plenty of plans for expanding services in the future. Its central philosophy is YKYC – Your Keys, Your Crypto. No more FTX type scandals, no multimillion dollar hacks, no more using your funds to enrich others, no more praying that the next exchange to collapse isn't the one your money is on, just fast, safe and secure trading.