NightTrader:
A Decentralized Multisignature Electronic Cash Wallet and Exchange Whitepaper

Alec Hahn and others
alec@bitcoin42.com
NightTrader.org

Table of Content

Abstract

Among decentralized exchanges, there are currently no fast, low cost, Bitcoin based exchanges with full order books(with bid and ask) that are actually truly safe and decentralized. In this paper we will highlight the reason and need for a decentralized multisignature exchange using threshold signatures and explore its features and services and how it compares to existing solutions. We will show how it is accomplished with signature hashes, 2 of 2 or 3 of 3 multisig with threshold keys on a decentralized backend. We will also explain the use of force majeure backup strategies using checklocktimeverify. Finally we will explain how users and hosting providers are incentivized to support this DEFI infrastructure while maintaining privacy measures and not prone to hacks. The conclusion will show how this system is a superior method for exchanging digital cash and more.

Introduction

When it comes to exchanges there is a rampant problem of hacks, data breaches, inside jobs and exit scams due to centralization. The most known was in 2014 when the Mt.Gox exchange, which handled about 70% of the entire market volume, got “hacked”. As a result it crashed the Bitcoin price and about 7% of all the Bitcoins at that time were lost. It was clear that centralized exchanges can’t be a long term solution for the decentralized nature of Blockchain technologies and for the most part these exchanges can not be trusted under any circumstances. Up until today it is estimated that at least 20% of all Bitcoin in circulation are lost forever or have been stolen most often by centralized exchanges and exit scams or “hacks” by insiders. Besides, it was the fact that Bitcoin is ownerless and decentralized that let it thrive in the first place! So NightTrader should seek to mirror this success in the form of a decentralized exchange.

Current Solutions and Reason to Evolve:

Decentralized exchanges have emerged but other than the success of "automated market makers"[1]the traditional bid and ask style exchange could not yet gain significant market share. This is mainly because they are slow, complicated to run or only work with so-called “middle coins” or other blockchain “ecosystems” which are not truly decentralized exchange solutions, but more a sort of bridge. Ethereum has had wild success with exchanges such as UniSwap however these exchanges although being wonderful have some downsides. One of them is that there is no ability to bid, there is impermanent loss for liquidity providers, users can suffer from "rug pulls", they pay high gas fees for small trades and so forth. Although gas fees

may reduce with zk-sync[2] and rollups[3], there are still the other mentioned drawbacks. Some systems such as BitShares[4] pioneered a sort of middle coin solution although this wasn't actually truly decentralized because there was always risk where the coins were held. Then there are systems such as Blocknet[5] or Komodo[6] or various "atomic swap" solutions and wallets. These are the "perfect" solutions cryptographically. However practically they have not caught on because of the high costs of doing every single transaction on the blockchain. This can be a hindrance because it doesn't offer the fast, high volume trades which are so popular with users. We wish that they would catch on, however demand and liquidity are important for users to reduce cost of trading with a better spread.

Nighttrader changes this paradigm by utilizing the built in signature hashes which were most likely intended for these types of applications since Bitcoins inception. To us it comes as a surprise that this solution was not used already. However perhaps it is because things such as "Shamir's secret sharing"[7] and threshold signatures[8] had not risen to popularity yet, so signature hashes in a multisig alone would at best form a green address unless combined with other methods. Still, why Coinbase or Binance hasn't implemented such a simple feature of giving a user 50% control over the account appears to be almost borderline negligence considering the volumes they get and money they make... whatever happened to putting the customer first?! What many don’t understand is that Bitcoin came with some built in contracting abilities. So NightTrader uses the combination of signature hashes, multisignature and threshold keys to achieve the most secure exchange possible.

Methodology

1. Multisignature Wallet, Transactions and Trades

Nighttrader uses throughout its entire site 2 of 2 or 3 of 3 signatures to perform any operation. The users signature is generated client side in the browser and cached for example based on an email and password combination for user friendliness. Any requests they make are signed and sent to nodes. The 2nd signature is actually generated by a group of nodes like a giant multisignature. The public key is generated by splitting the elliptical curve ECDSA signature into "shares". The parameters of the curve can be set up so that you need to pass a certain threshold for it to be valid. For example it can be set up where 70% of all nodes must agree in order to construct a valid signature. This technique is used for signing without the need to construct a private key and this is called a "threshold signature". The utility of this threshold public key is that a single node does not have full control over the account, spreading the risk among multiple parties. It emulates multisignature using a single key. The motive behind this is to increase the privacy of the nodes and also to dramatically reduce the fees to signing transactions. The p2sh script therefore has a threshold multisignature key inside of it and the users key. This means the user has 50% control of the account to begin with so unlike the issue of "wrapped" tokens such as REN[9] (which uses threshold signatures), the user actually has to provide specific authorization for a specific trade. This is accomplished using the old-school signature hashes already built into Bitcoin. Bitcoin originally was designed to give an authorization for a specific input for a specific amount. This is similar to ERC-20 authorizations called "allowances". Basically if a user has 10 BTC in their account but only wants to authorize to spend 2 BTC they only need to sign that 10 BTC with "sighash single" which can spend their change of 8 BTC into the adjacent output. This means the remaining 2 BTC has not been accounted for yet. So the 2nd key holder (the nodes) can now redirect this 2 BTC however they see fit. It can be thought of as an IOU. This can in theory be a drawback in the sense that if left to a single user the funds can be compromised however because there are a lot of nodes they can agree to spend it to the person owed. Compare this to traditional exchanges where the entire 10 BTC is at risk. In the case of the above example only 2 BTC is at risk and it is an extremely low risk because there is a large consortium of nodes who form a consensus about where it goes.

2. IOU System

The user may find themselves signing some of all of the amount of coins within certain inputs. If they sign away all of the inputs funds then "sighash none" can be used. Once the nodes get this transaction they will then keep track of who is owed for that trade. However it will not be reported to the blockchain. This gives the opportunity to dramatically cut down on fees! This is because that debt is constantly routed to other users as volumes increase. This debt can be kept open until a withdrawal is made or until the debts are cleared. This is particularly useful to day traders who constantly move back and forth between pairs which would make atomic trading totally not feasible. The user can pretty much trust that the trades will be properly routed because the nodes on the back are all checking the transaction under the exact same criteria so unless all of them find each other and conspire there would be almost no chance of loss otherwise. And even in such an event of nodes colluding it is highly unlikely because the number of nodes can easily be a few hundred nodes without having any significant impact on performance.

3. Debt Clearance and Withdraws

The debts of course need to be eventually paid and when that happens it restores the accounts of the users to have absolutely nothing pending and this dramatically increases their security because then they can hold the funds on the exchange almost as safely as they can on a private wallet because they are in control of their key. There are two ways where a debt is paid. The first way is simply a user who is owed or owes another user withdrawals. This causes the funds to be unavailable to trade for the recipient until the proper number of confirmations are completed. This is similar to a new deposit in that sense. The exchange itself chooses these intervals of when to process withdrawals and user feedback would be an important part of timing that properly. The other way debts are cleared is when the entire exchange goes into "debt clearance". This event can happen daily or weekly depending on the volumes. If there is a high volume (which can bring down the fees) it may happen more often. However to avoid too much down time it is ideal to do this every few days or once a week. Again, user feedback and the feedback of the Bitcoin community as a whole would be useful in this regard. During the debt clearance some of the users owed might see some of their bids temporarily paused if those bids had funds which used an input which was partially sold. This is okay though because they can decide how to proceed if they want to keep the order open or cancel it and post it again once the deposit confirms. The exchange should be patient and give lots of time for properly pausing orders and waiting for sufficient confirmations.

4. Decentralized Nodes

The nodes are one of the most important parts of the infrastructure. First of all, they are incentivized to follow protocols because of the trading fees. Also, they are all holding a part of the secret. During the issuance of new keys the user addresses can either be occasionally rotated as new nodes join or broken into pieces from the beginning depending on how many join initially. Nodes can also choose to break their own elliptical parameters into additional parts. Nodes are volunteers who simply choose to be part of the infrastructure. NightTrader does want nodes who are actually invested into the platform in some way so there is some sort of vested interest so it is possible the nodes might either be trusted members of the crypto community, investors or liquidity providers. However, it is not the desire of NT to issue another coin, at least not in the initial release. This is to avoid creating more "bag holders" and avoid creating "another coin". If there is community demand for such a thing it can be considered. Instead most likely, an internal accounting token that is not intended to be traded can be issued just for accounting purposes. This token will give an idea of how many shares that user has and make it easy for the front end to pay them fairly. The nodes have to manage a good amount of data. So actually that data is held by a master node so the exchange can benefit from the fast paced trading most exchanges have. However every single node will be encouraged to have a similar setup to support the same demand the current master node is having. They will also mirror the database of the node. Users can check with the other nodes to ensure the integrity of the master nodes orderbook. Because the other nodes are running the same software they will immediately be able to detect if the master node is misbehaving and if so they will change over the management to the next node in line. It is also possible to slash a deposit to incentivize honesty among the nodes. In the meantime other decentralized backends will be explored as well. However for the launch this is the current proposed architecture.

5. Threshold Keys

Keys can be generated using decentralized secret sharing and then issued to new nodes in the pool. Once new nodes join the change address can be changed for the users to eventually update to accommodate the new participants. In the beginning it is guessed that NightTrader could have up to 40 pieces to an elliptical curve and this can be increased gradually. The specific threshold is not yet decided however the target is for at least 70%. If for whatever reason too many nodes go offline there are already provisions in place for this with the backup options. Once it comes time to sign all of the nodes should have perfectly identical order books. If for whatever reason one or two nodes falls behind they will have a lot of time to catch up because the clearing days and withdrawal times are properly spaced out. The spacing out of withdrawal and clearance times cuts down on fees for the users and

reduces downtime while waiting for new deposits. This might also make DDOS slightly more difficult. If for whatever reason a node drops out of the pool that's also okay as a new key can be generated for the back end as volumes increase. Also users can be asked to submit a transaction or trade essentially moving funds to update to the new key.

6. Security features and Backup Options

A good security system and backup option also needs to be user friendly. Traditional logins via email and password generate the private key with the requirement of a very long password. This gives the familiarity users would have with typical systems. Other key options may also be made available over time. The two factor authentication and confirmation emails give a simple buffer although somewhat superficial because the bulk of the security relies on the user not giving away their private key. Still it is like a traditional website because a token won't be generated allowing them to trade without completing authorization. This means a hacker would still need to login to make a withdrawal or trade so it is possible that the key alone will not be enough to compromise the account. The user will be encouraged various backup strategies as well during login. Strategies like choosing their own security questions and sending themselves an encrypted email and other traditional backup methods are to be explored. If for whatever reason the exchange goes down or many nodes vanish the user is at almost no risk whatsoever. This is because all accounts for applicable coins use checklocktimeverify [10]. Most Bitcoin derived coins support checklocktimeverify and the NightTrader selection process for the first coins to be integrated will focus on projects that have this feature. Therefore if the nodes disappear then after one year or however long the locktime is set for, the account automatically reverts to the user. The exchange will make sure a user is nowhere near this time limit before allowing a trade to avoid situations where the exchange is taken offline for prolonged periods. So if a user has been inactive for 6 months they might need to update their inputs to the new locktime. This is totally fine anyways because more nodes may come into the network making it convenient to change keys. The one risk to nodes going offline permanently is that some trades might not get completed. If that happens it is very unlikely to end in loss because the half signed trades would not be broadcasted. However there could be losses in profits from some of the trades. Evidence of the script is also extremely important so it should be burned into the blockchain during any significant changes to an account or the script should be generated in a very obvious and deterministic manner. A user could decline to change anything without burning evidence of the change or seeing evidence of that change published somewhere. Alternatively the exchange can burn these changes (for example this change might be seen on a token history on Etherscan if the internal accounting token goes this route). The locktimes should be at a predictable timestamp modulus so the updated scripts can be searched for by brute force. All of this is because a Bitcoin

script is not known in advance until it is spent from and a user would not want to send to an address that they are a participant of without knowing the script. So all of these things are considered and this is what gives NightTrader world class top notch security. Users should know how to anticipate their scripts without much assistance from the exchange.

7. Incentives; DEFI, yield farming, LPs and Orderbook Maintenance Fee

Various incentives have been discussed and explored. First of all the nodes get a small part of the commissions and this takes away from a centralized conglomerate taking the fees. However, NightTrader wants to support some of the liquidity providers of the first coins to be part of the exchange by supporting those coins using yield farming strategies. One strategy is staking for the fees. As a liquidity provider not only takes a risk, they provide a service by trading, it is a good strategy to find ways to let them get some of the fees. So one proposed plan is to let users who have placed a signed bid to buy to run the possibility to take some fees for that round. The thing is when the exchange goes into clearance mode for the debts it needs to take care to not pay excessive amounts of outputs if there are not enough fees to pay for a large transaction. Also it wants to be sure these transactions will be broadcasted and not backlogged. So the proper way to distribute fees is to actually pay groups of recipients randomly based on their weight in the system. The randomness can come from various places, for example basing it off of a recent Bitcoin block hash. The system will still select multiple recipients for winning the fees for that round. This actually gives a nice incentive to a small investor because they run a small chance of winning a bigger payout. Although like staking it should be determined based on the amount of liquidity risked and for the amount of time it was risked. This type of promotion may not be released in the initial exchange however it will be considered. Similar methods can be used by paying the "top 500" holders of a certain coin based on occasional snapshots. This is being considered for coins such as Bitcoin or Ethereum or BitBay. Coins like this are considered for their technical genius and others may also be considered. This method may also require the participation of whales in those communities to at least sign up and place some orders actively. Liquidity is key to a successful exchange as traders go where there is the tightest spread. This is why NightTrader may also investigate other services such as AMM style trading because it is so easy to issue those contracts and NightTrader may follow market trends to on board more users. Either way, the exchange will maintain its position as an ownerless decentralized exchange and the fees will ultimately only exist to support the nodes on the back end. Also referrals which gain percentages of trading fees of recruited members are a great way to incentivize more users.

8. Privacy and code security

To prevent identity theft and big data mining, we simply don’t do it. NightTrader only collects the minimal to ensure a reliable and secure experience. User data can also be encrypted with their private keys. The code can also be verified on github where the front end is hosted. Also because the entire exchange is open source, a user can even download the JavaScript and run it from their computer without the need to visit the webpage directly. This should be easy to accomplish without needing to install any packages.

9. Simplified Optional KYC Verification

Even though NightTrader is autonomous, if the exchange is somehow forced to stop trading activity of a user that absolutely would not stop the flow of funds indefinitely because of checklocktimeverify protections. We retain the right to ask for KYC information, which we would collect on a dedicated platform to further prevent the risk of identity theft or other forms of personal information abuses. This also helps NightTrader to be protected and stay in business. Trading limits may exist beyond a certain volume although most likely being decentralized it would be hard to enforce. As it is seen Uniswap surely doesn't have such limits and never will because it is from a decentralized nature. All user data is encrypted protecting their privacy.

10. Privacy coins and Solidity protocols

Some coins lack a full scripting or contracting system such as Monero. This prevents Monero from being traded on most decentralized exchanges. Furthermore, it makes it hard to create a trustworthy bridge to trade Monero on Solidity since Monero does not even support p2sh or multisignature. NightTrader also proposes a solution for Monero as well. The revolutionary innovation proposed is to include the user in the threshold signature scheme. This helps establish the multisignature account. However, how can a user control 50% of the account and yet "sign" a blank check for debt to be routed? Is there anything that can simulate sighashes? In order to emulate "sighash none" a user simply has different parameters for each input resulting in a different address for each input and then the user publishes their parameters to the other nodes in the threshold group. This is the same as relinquishing their control over that input without actually signing anything. Their parameters of course are as important as private keys so the user should know how to generate them deterministically. Another challenge is that Monero does not support checklocktimeverify. However, there is a solution to this as well using Moneros "unlock_time" feature. How this works is the user creates some small shard transactions with an unlock_time to become available to spend after so many months. They could in theory

prepare many of these to last them for years after they set up their account. Then the nodes in the threshold sign a redemption transaction including all of the inputs and the shard transaction repaying all of the funds to the user. Even though the shard transaction exists, it cannot be published until the unlock_time passes. Also if any of the inputs get spent the transaction is no longer valid and the nodes can create a new one including the shard with the correct amount of time for the new time lock. Coins such as Ethreum and all of the ERC tokens would also need to support a way to route transactions off chain in a multisignature with methods similar to signature hashes and time locks. Fortunately Solidity makes this easy to implement. The method used here is to take advantage of the ecrecover function to validate a users signature. Then the user can sign their intentions off chain for that specific nonce or interval. The nodes can use one or multiple signatures which may also include threshold signatures and the nodes can route debt how they deem necessary. The security and methods of the contract can be audited by reviewing the source code on the blockchain and on github.

Conclusion

This design really is unequaled. It has the speed of top notch exchanges, it is lower cost for small traders who are unable to use AMM exchanges for daily trades and useful for users who want to bid/ask. It doesn't require complex collateral like “lightning network”(which is not as viable for large trading platforms). NightTrader has no middle coins, is many times cheaper than atomic trading, gives the user a key to control their account unlike wrapped tokens, and it utilizes the most simple design possible. The use of signature hashes, 2/2 or 3/3 multisig, threshold accounts and checklocktimeverify makes for a complete system for the best a DEX can currently be. And NightTrader is also an enthusiast of things like rollups and atomic trading although those options are currently too high cost, may not support legacy coins like Bitcoin or Monero, are not fully developed and/or not fast enough yet. Although NightTrader does believe those systems are the future of exchanges and is therefore excited to explore more options as things develop to stay on the cutting edge. NightTrader did not deploy a coin on it's release and instead chose to give fees to the dedicated participants/nodes and possibly liquidity providers. Also remember the old adage "not your keys, not your crypto" which is exactly why the users of the platform have a key and control over their account. NightTrader is created for a single purpose and that is to give users a safe place to trade.

References

[1] Mohsen Pourpouneh, Kurt Nielsen, Omri Ross, "Automated Market Makers," https://okonomi.foi.dk/workingpapers/WPpdf/WP2020/IFRO_WP_2020_08.pdf

[2] Alex Gluchowski, "Introducing zkSync: the missing link to mass adoption of Ethereum," https://medium.com/matter-labs/introducing-zk-sync-the-missing-link-to-mass-adoption-of-ethereum-14c9cea83f58

[3] DappRader, "Ethereum Rollups: A simple explanation," https://dappradar.com/blog/ethereum-rollups-a-simple-explanation

[4] https://docs.bitshares.build/docs/get-started/bitshares-whitepaper/

[5] https://blockdx.com/#features

[6] https://komodoplatform.com/en/wallets.html

[7] https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing

[8] Hartwig Mayer, "What are the Benefits of Threshold Signatures for Crypto Wallets?," https://blog.coinfabrik.com/what-are-the-benefits-of-threshold-signatures-for-crypto-wallets/

[9] https://renproject.io/

[10] https://en.bitcoin.it/wiki/Timelock