FTS Coin: A Peer-To-Peer Electronic Private Transaction System

Project FTS
whitepaper@ftscoin.xyz
www.ftscoin.xyz

Abstract. While electronic peer-to-peer cash systems have been a growing part of the evolving economic paradigm the past 10 years, emerging as we embrace a new age of technology, there is still much room for improvement with this new software. FTS Coin hopes to address some of these areas for improvement, including but not limited to; Privacy, POW centralization, slow transaction times, high transaction fees, confusing transaction systems, and the loss of seed phrases. By addressing these issues and offering solutions to them, and using FTS Coin to help spread mass adoption through our POB distributions, we hope to help drive cryptocurrency towards mass adoption!

1. Introduction

Over the past decade cryptocurrency has cemented it's place in global society as a means of storing value and conducting transactions easily over borders. While Bitcoin, the original cryptocurrency, laid the way for the variations of this technology, it had shortcomings that have become clear over it's decade of use in society. FTS Coin hopes to address these issues, while also leveraging part of a small premine, from it's 25,000,000 total coin supply, to help create incentive for people to teach new businesses about cryptocurrency.

The most apparent issue existing with Bitcoin is privacy; Once a transaction has been made with a bitcoin wallet and other people know the wallet address they can track all the financial dealings of that wallet. If that wallet can then be connected to an individual all transactions by that individual have just become public information. Since privacy coins have tackled this problem well already FTS is a later generation fork of the Cryptonote technology. Cryptonote uses a form of unlinkable payments to ensure privacy; Information about Cryptonote technology can be found in the Cryptonote Whitepaper.

Another problem we found troubling about Bitcoin was the ability for one person or entity to centralize the POW mining power of the coin by creating large ASIC mining farms, or buying hash power from a hash renting service. A cryptocurrency network works best if the distribution is as widely spread as possible and a large number of people are invested in the zero sum POW competition for block rewards. The over-centralization of POW hash power deters this natural and beneficial network growth, and its ability to attract new people to cryptocurrency.

Bitcoin is also subject to slow transaction times, though most of the "clog" in Bitcoin happens within the bitcoin mempool, another issue is the block time itself. We greatly reduced standard block time to something that averages close to 2 minutes a block. This increased block speed, and our reduced transaction fees, help transactions move in a timely manner, allowing the system to be easily utilized for exchanging goods.

Confusing software systems are also common in the world of cryptocurrency. Since most of the people initially attracted to cryptocurrency, the currency of the internet, are regular computer users this is the group this software has been tailored to so far. This is not conducive of global adoption by the people of crpytocurrency; The global adoption of any new technology is fueled in part by it's ease of use compared to other systems. As FTS Coin moves forward with future development this goal will be kept front and center at all times, and we will approach all endeavors in hopes that they will some day be used by everyone.

A part of the confusion surrounding cryptocurrency is the management, and often times loss, of the origination seed for the wallets funds are stored with. Though this problem wouldn't exist if people were careful with their wallet seeds, and treated them like cash, we believe we have come up with a solution that will allow for people to have their wallet seeds on them at all times, without creating a security risk. By allowing a user selected combination of bio-metric data to replace the words that represent the standard wallet seed, we hope to bridge the gap lost by not having a bank teller; With funds always just a scan away from being generated off the blockchain.

FTS Coin will offer both POW and POS options in the near future, but will be launching with a POW set up for block rewards, with an additional POB earning system. The POB earning system, a unique design linked to this coin, involves giving people incentive for helping spread the mass adoption of cryptocurrency. This POB system will be managed through the FTSMothership.info web site and paid out of a portion of the FTS Coin premine.

For the sake of growth and development, a small premine of FTS Coin was conducted during the launch of the coin. FTS Coin has a total coin supply of 25,000,000 coins, set to distribute slowly over a century, 2,000,000 of which were premined. That means that 8% of the FTS Coin supply was pre-mined, with 92%, or 23,000,000, left to become available over the next 100 years. The use of this premine will be outlined for transparency later in this whitepaper.

2. Transaction Privacy**

****Section 2 has been borrowed word for word from the Cryptonote whitepaper!**

We propose a (privacy) solution allowing a user to publish a single address and receive unconditional unlinkable payments. The destination of each CryptoNote output (by default) is a public key,derived from recipient's address and sender's random data. The main advantage against Bitcoin is that every destination key is unique by default (unless the sender uses the same data for each of his transactions to the same recipient). Hence, there is no such issue as "address reuse" by design and no observer can determine if any transactions were sent to a specific address or link two addresses together.

First, the sender performs a Diffie-Hellman exchange to get a shared secret from his data and half of the recipient's address. Then he computes a one-time destination key, using the shared secret and the second half of the address. Two different ec-keys are required from the recipient for these two steps, so a standard CryptoNote address is nearly twice as large as a Bitcoin wallet address. The receiver also performs a Diffie-Hellman exchange to recover the corresponding secret key.

A standard transaction sequence goes as follows:

1. Alice wants to send a payment to Bob, who has published his standard address. Sheunpacks the address and gets Bob's public key (A,B).
2. Alice generates a randomr$\in[1,l-1]$ and computes a one-time public key$P=H_s(rA)G+B$.

3. Alice usesPas a destination key for the output and also packs valueR=rG(as a partof the Diffie-Hellman exchange) somewhere into the transaction. Note that she can create other outputs with unique public keys: different recipients' keys (A_i,B_i) imply different P_i even with the same r.
4. Alice sends the transaction.
5. Bob checks every passing transaction with his private key (a,b), and computes $P=H_s(aR)G+B$. If Alice's transaction for with Bob as the recipient was among them,then$aR=arG=rA$and$P'=P$.
6. Bob can recover the corresponding one-time private key:$x=H_s(aR)+b$, so as$P=xG$. He can spend this output at any time by signing a transaction with x.

As a result Bob gets incoming payments, associated with one-time public keys which are unlinkable for a spectator. Some additional notes:
•When Bob "recognizes" his transactions (see step 5) he practically uses only half of his private information: (a,B). This pair, also known as the tracking key, can be passed to a third party (Carol). Bob can delegate her the processing of new transactions. Bob doesn't need to explicitly trust Carol, because she can't recover the one-time secret key p without Bob's full private key (a,b). This approach is useful when Bob lacks band width or computation power (smartphones, hardware wallets etc.).
•In case Alice wants to prove she sent a transaction to Bob's address she can either disclose ror use any kind of zero-knowledge protocol to prove she knows r(for example by signing the transaction with r).
•If Bob wants to have an audit compatible address where all incoming transaction are linkable, he can either publish his tracking key or use a truncated address. That address represent only one public ec-keyB, and the remaining part required by the protocol is derived from it as follows:$a=H_s(B)$ and $A=H_s(B)G$. In both cases every person is able to "recognize" all of Bob's incoming transaction, but, of course, none can spend the funds enclosed within them without the secret key b.

3. The Premine

FTS had an 8% premine that was released from block zero, this premine of 2,000,000 coins is being used to further the coin and support the POB system. The distribution of these 2,000,000 coins will be laid out in this section with as much detail as is possible.

500,000 of this premine will be used towards tech bounties for further development. As the coin develops, and the community using it grows, it will be common place for the FTS Coin team to release bounties available for coders and developers that can accomplish certain tasks. These bounties will be based on the need for, and difficulty of, the work being sought out.

500,000 of this premine will be used toward marketing and promotion. This will include a combination of promotional air drops, rewards for IRL promotional activities, rewards for social media promotion, as well as any other advertising or promotion the FTS team feels will help move the coin forward.

500,000 of this premine will be used toward the POB system. The POB system will offer individuals FTS coin for teaching businesses about cryptocurrency, and getting them to start accepting any cryptocurrency currently on the market. More details will be available on the POB system later in this whitepaper.

50,000 of this premine will be used for ecosystem development, in any form that may take; Including FTS only crypto stores, services soley funded by FTS coin, or any

other activity that will help support the value of FTS coin.

The remaining 450,000 FTS coins is being used toward initial development fees.

4. The Tech Road Map

FTS Coin will be launching in its initial forms as a Cryptonote forked privacy coin, with a total supply of 25,000,000 coins. This distribution of 25,000,000 coins should complete after 100 years with the reward for each block steadily decreasing over time. This is the roadmap for our current plans with the technology; Though it is likely we may add items to this agenda, it is highly unlikely we will take any of these items out of our future plans.

4.1 Phase 1-Genisis

The blocks average just under 2 minutes each with transactions being handled privately as detailed above, and blocks being mined with an ASIC resistant POW algorithm. The coin will be launching with CPU mining options and terminal wallets, as well as easy to use GUI wallets for Windows, Linux and Mac.

4.2 Phase 2-Pool Mining and Phone Wallets

At this stage FTS Coin will be adding Pool Mining and android and/or IOS wallets for the coin. These added options will help expand both the miner, and user, base for the coin. Adding phone wallets will become a crucial piece of stage 4.5

4.3 Phase 3-Easy Mining, Messages & Exchange

Phase 3 of FTS Coin will involve adding an easy “mine now” button to the GUI wallets, as well as adding the ability to send private messages from the wallet.

We hope to implement the easy “mine now” button as a part of our effort to spread cryptocurrency mass adoption. We feel an ASIC resistant system that easily provides the ability for people to be engaged in the network and help contribute to its security, not only provides a more decentralized and solid network, it also provides a platform for new people to become invested in the system of cryptocurrency itself by engaging in the competition for block rewards.

By providing a means for people to send encrypted messages, with a timed self destruct mechanism, over a secured network that also allows for private transactions; We hope to provide a means for complete private business interactions in the field of legal and medical consultations. This will be extremely useful for people that wish to interact with lawyers or medical professionals remotely, and privately, while streamlining both payment and the consultations being paid for under one software mechanism.

At this point we will also be buying our way onto an exchange if one hasn’t become available to the coin, for free, from the crypto community.

4.4 Phase 4-POS/POW Hybrid

Proof of Stake will be coming at this stage. In order to help create incentive for people to hodl their FTS Coin we will be conducting a hard fork of the system to add on POS options. Thus allowing people to obtain FTS Coin by holding onto it, providing POW to help network security, or introducing new businesses to FTS Coin with our POB system on www.ftsmothership.info

4.5 Phase 5- Biometric Seed Integration

The fifth and final stage of the planned tech road map for the FTS Coin software involves adding a secondary means for wallet generation. People at this point will be able to generate a standard legacy address with a word seed, as is currently common in cryptocurrency. Alternatively they will be able to start using the camera and fingerprint

scanners on their phone to choose a combination of bio-metric data to be used in connection with an algorithm that translates this information into the seed for your SHA 256 algorithm. Through this method people will be ensured that as long as they still have key body parts they will have the seed itself for their wallet, and should be able to use any phone to download the wallet software and recover their funds.

5. Proof Of Business

500,000 FTS from the premine will be going towards the Proof Of Business mechanism, or the POB. People will be able to turn over a 10 second + video of a business owner saying they now accept cryptocurrency thanks to the recorder, and the person that sends in the video will receive FTS Coin in compensation.

The first 2,000 submissions will receive 50 FTS coin each for submitting these videos on www.ftsmothership.info after the information has been verified. The next 4,000 submissions will receive 25 FTS coin for their submission. The amount of FTS Coin received for a submission will continue to half like this every 100,000 FTS coin until 50,000 FTS Coin is left in the POB fund. At the point the FTS POB Fund wallet only has 50,000 FTS Coin left people will receive 1 FTS for every business they submit.

For the FTS POB Submissions; It is not necessary the business started accepting FTS Coin. The only thing that matters is that they started accepting any form of cryptocurrency at all, and were willing to take a video thanking you for teaching them about it. The point of this is to support cryptocurrency mass adoption, not just FTS adoption!

6. Conclusion

We have proposed a series of improvements to the current cryptocurrency systems that will both enhance the cryptocurrency ecosystem as a whole, and provide a cryptocurrency designed to be easily adopted and used by the public at large. The current cryptocurrency systems, including Bitcoin, paved the way for all modern border-less peer-to-peer cash systems, but this decade of beta testing has made the faults in the current systems very clear. We hope to fix these problems by providing a combination of technical and ideological shifts that will aid in the continued adoption of this incredible technology.