*A Secure Network with **Anonymous Transaction Capability***

White-Paper

Core Team:
Mandica (*project manager*)
Tek (*lead developer*)
Helix (*developer*)
Mammix2 (*developer*)
Ahmed (*developer*)
Beachguy (*community manager*)
RKh (*marketing manager*)

August 2018
Version 1.0

Table of Contents

Abstract

Cryptocurrencies permit their users to securely send money (*cryptographic coins*) without trusting any intermediary or any other centralised third party to verify the transactions. This trust-less nature is also provided for by the transparency of the public ledgers (*blockchains*) that are accessible to the public and verifiable to anyone with the required knowledge. The public nature of the blockchains however, comes at a cost to privacy. Even though the pseudonymous users are not associated with their real-world identities, every transaction among these pseudonyms is potentially traceable. In this white-paper, we present **Spectrecoin**; a cryptocurrency that uses a range of dual-key stealth address and cryptographic techniques to achieve un-linkable and un-traceable anonymous transactions on its blockchain and also protects the user's online identity by integrating Tor (The Onion Router). Spectrecoin also retains the ability to conduct '*open*' public transactions that may serve certain use cases and blockchain audit. We present the current functionality of Spectrecoin to the common reader with some experience and knowledge of blockchain and cryptocurrencies. We also discuss how we achieve anonymous transactions and where we go next and what Spectrecoin will achieve in the future. Further references are included at the end of the document for interested parties.

Acknowledgements

Spectrecoin would not have been possible without the foundations laid by what came before and in particular the Bitcoin, Blackcoin and ShadowCash developers and the work by the authors of the CryptoNote and Zerocoin protocol that provided inspiration for some of the technologies developed for Spectrecoin. Although the Spectrecoin lineage can be traced back through previous projects, open source software provides inspiration for innovation and Spectrecoin has taken a particular direction to improve and enhance the unique privacy technology inherent in its code base and produce a functional anonymous cryptocurrency that will serve its particular community.

Notes

Spectrecoin employs well known technology albeit used in creative ways and some parts of the white-paper is to a large degree referencing already published material from various sources. There is no scope in this document to discuss cryptography or mathematics and the author is neither a cryptographer nor a mathematician. The descriptions of cryptographic functions are taken from the relevant source documents that are referenced throughout this document and if you are so inclined you can read up on the details. This is not meant as an academic paper or as a reference document but rather as a brief description of the Spectrecoin network. This document does not intend to contribute to the debate about anonymity or privacy and this discussion is beyond the scope of this document. We simply believe that we have an absolute right to privacy in our financial affairs online as we do in the real world and so our ideology is also simple; to provide real decentralised resilient privacy and anonymity on the blockchain and offer provable anonymous transactions for users.

Commonly Used Terms

Blockchain: A shared, immutable ledger for recording the history of transactions in blocks.
Block: A defined data structure that contains a record of transaction data and other values.
XSPEC: The symbol (*ticker*) for Spectrecoin and also the name of the public coins on the blockchain.
SPECTRE: The name used for the anonymous coins on the Spectrecoin blockchain.
UTXO: Unspent Transaction Output that can be spent as an input in a new transaction.
ATXO: UTXO that can be spent as in input in an anonymous transaction using a ring signature.
Keyimage: A unique value associated with a specific ATXO calculated using a private key.
Spent (UTXO): A UTXO is spent when it has been '*consumed*' as an input in a new transaction.
Spent (ATXO): An ATXO is spent when the corresponding '*keyimage*' has been included in a valid ring signature.
Hash function: A mathematical one-way function that generates fixed size data from an arbitrary input.
Hash value: A numeric **value** of a fixed length that uniquely identifies the data input in a hash function.
Mixin: A chaff or dummy ATXO not being spent in a current transaction, used in a ring signature.
TOR: The Onion Router. A layered network that attempts to hide your IP address.

Introduction

Spectrecoin strives to provide real-world anonymous transactions that will withstand any kind of blockchain analysis by the most hostile and determined attacker. We will achieve this through constantly working to test and audit the source code and seek to improve the anonymity of our transactions. In this context it is important to understand and appreciate that any cryptocurrency aiming for anonymous transactions will be up against increasingly sophisticated ways to analyse the blockchain and increasingly sophisticated analytical tools. It is in fact an arms race and we must therefore not sit back and claim that our anonymity is forever unbreakable, but we must conduct an honest and fearless audit of the algorithms and methods behind the anonymous transactions and discover our own weaknesses and vulnerabilities. We then need to work to improve our code to stay at the front of the arms race. We will then become a trusted and functional cryptocurrency with real-world anonymity, one of the few out there, beyond just the hype. We understand that the Spectrecoin network is protecting your money and your identity and we take that seriously. It is therefore also important that our users understand what is real and what is not when it comes to online privacy.

Spectrecoin background and basic properties

The best way to understand what make up the **Spectrecoin** network today is to think of **Bitcoin Core** + **Proof-of-Stake.v3** + **anonymous transactions** (*using dual-key stealth technology and ring signatures*) + **Tor** to hide your IP (*all Spectrecoin nodes run as hidden services*).

Specifications

Live: Block 1 mined on 20/11/2016
Distribution: Low value ICO that raised 16 BTC w/ subsequent distribution in early 2017
Initial supply: 20,000,000
Ticker: XSPEC
Consensus: Proof-of-Stake v.3 (*based on Blackcoin*)
Difficulty retarget: every block
Block time: 60 second target
Block reward: 5% annual inflation based on total supply
Max supply: No max supply(*)

Idealised inflation projection

Year 1: 21,000,000 XSPEC
Time of writing (13/08/18): 21,689,376 XSPEC
Year 2: 22,050,000 XSPEC
Year 3: 23,152,500 XSPEC
Year 4: 24,310,125 XSPEC
Year 5: 25,525,631 XSPEC
Year 10: 32,577,892 XSPEC

Block explorer allows you to explore the Spectrecoin blockchain: https://chainz.cryptoid.info/xspec/

(*)*A note on inflation; Spectrecoin differs from Bitcoin and some other cryptos in that we have no inflation reduction scheme in place at this time. It is beyond the scope of this paper to have an in-depth discussion about inflation and money supply and the nature of money and currencies. At this point in time, we consider Spectrecoin to fulfil only one (of three) criteria for being considered a real currency. Spectrecoin can be seen as a 'medium of exchange' and the hope is that Spectrecoin will be used to buy/sell goods and other fiat currency in its intended use in future cash transfers. Economists discuss and debate this point but some level of inflation appears to be beneficial for long term adoption and will prevent Spectrecoin from the potential dangers of entering a 'deflationary spiral' relaying on fees alone to sustain the Spectrecoin ecosystem. The level of inflation could be considered in the future but we do not believe that a 5% annual inflation rate has any negative impact on value for investors and might in fact help Spectrecoin to be adopted as a currency.*

Proof-of-Stake vs. PoW

Spectrecoin uses a modern Proof-of-Stake v.3 (PoSv3) algorithm to keep the network consensus and to secure and confirm transactions. PoSv3 seems a more resilient system against various attacks that could be instigated against a Proof-of-Work (PoW) system like Bitcoin and DASH. It is well known that large PoW driven networks expend huge amounts of energy and appears to lead to some level of centralisation of mining power due to the huge expense involved in mining new blocks. It is also known that PoW systems are susceptible to so called 51% attacks where a sufficiently funded and motivated attacker can "*take control*" over the network and generate double spend transactions for example. Please have a look at this rather interesting website tracking the theoretical cost of a 51% attack on various well-known cryptocurrency networks like Bitcoin and DASH, https://www.crypto51.app/. It is more difficult to attack a PoS system in this way as it would be infeasible to acquire the majority of Spectrecoin in circulation and doing so would undermine the value. So, in summary, PoSv3 is potentially more secure, more energy efficient and provides for better decentralisation. It is beyond the scope of this paper to discuss this further and there are various discussions around the internet if you are interested in the PoW vs. PoS debate. If you are interested in further details around PoSv3 please see the below links.

Spectrecoin Anonymising Features

Before we go on to explain some of the features and technologies of Spectrecoin in more detail, we will give a short overview of the privacy technology used. The Spectrecoin blockchain is a '*dual-coin*' system or a system where two distinct types of UTXOs can exist in the same block. Both non-anonymous coins or standard UTXOs (*hereafter referred to as public coins or **XSPEC***) and anonymous coins or ATXOs (*hereafter referred to as private coins or **SPECTRE***) exists side by side. Transactions can be carried out with both public and private coins and they are interchangeable. We introduce the terms ***XSPEC*** for the public coins spent in standard UTXO based transactions and ***SPECTRE*** for the private coins spent in anonymous ATXO based transactions using ring signatures.

Dual Coin System

The Spectrecoin '*dual-coin*' system is currently necessary for staking (*PoSv3*) and for confirming new blocks and validating transactions for both **XSPEC** and **SPECTRE.** When the Spectrecoin blockchain was created the genesis transaction which created the first 20,000,000 XSPEC was a standard UTXO transaction and the blockchain was built around a PoSv3 mechanism based on the work of the Blackcoin developers. It is only recently that the Spectrecoin development team has been able to create a new forthcoming Proof-of-Stealth algorithm that we will explain later in this paper and **that will make it possible to transition to a fully anonymous system** at some point in the future.

The anonymous coin '*subsystem*' was inspired by the principles of the Zerocoin protocol which can be summarised as '*Anonymity by destruction / creation of basecoins*', i.e. destroy / consume one baseunit, create an anonymous token and create a proof that the user owns it and the system later agrees to re-create one basecoin from that proof when requested. The Zerocoin protocol utilises a so called *zero-knowledge proof* (ZKP) to create the anonymous coins and to prove ownership. Zerocoin is computationally intense and requires a trusted setup and can be subject to certain attacks.

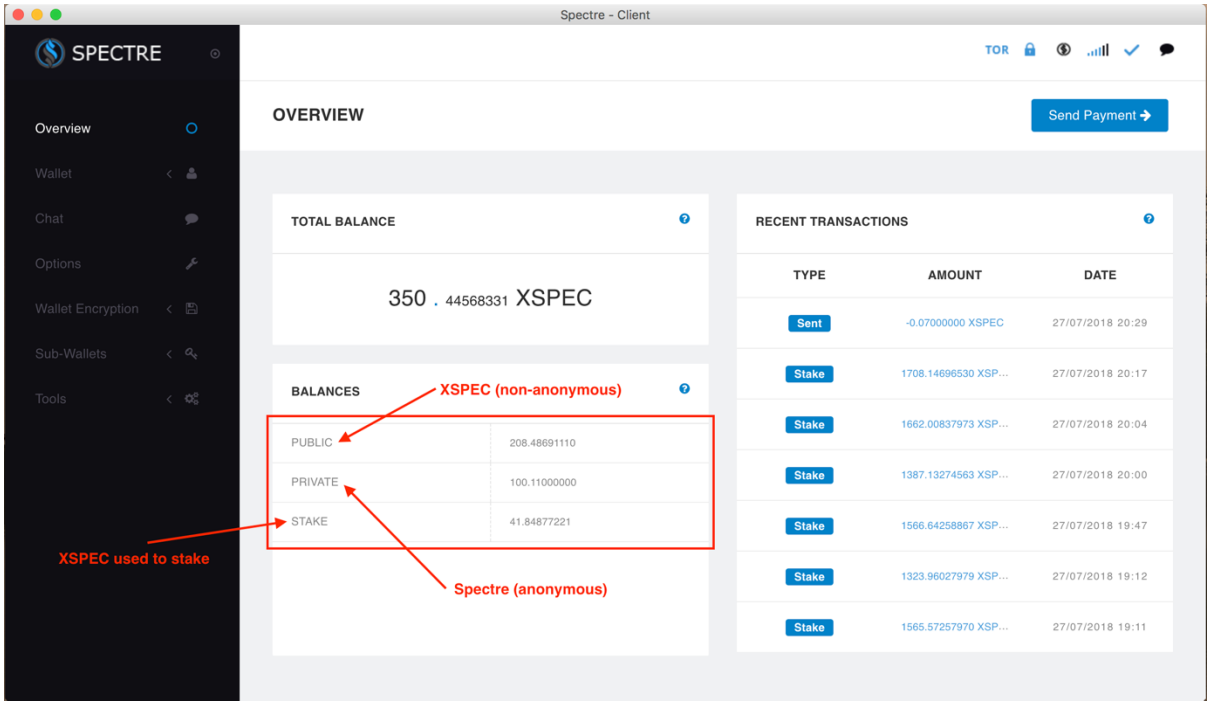
The Spectrecoin network instead employs dual-key stealth address cryptography to facilitate the creation of anonymous **SPECTRE** coins on the blockchain whilst consuming **XSPEC**. This is done without the trusted setup required for Zerocoin and without using the computationally intense Zerocoin cryptographic methods. Where the Zerocoin protocol use ZKP to anonymise the transactions, the Spectrecoin network use ring signatures.

The '*dual-coin*' system can be seen as a feature allowing for complete transparent transactions and network audit functions if needed but without any privacy indebted overhead such as resource intensive calculations. Anonymous **SPECTRE** can ONLY be created by consuming **XSPEC** at this time and the total supply on the network will always be transparent.

The transparent '*layer*' of normal UTXO transactions involving **XSPEC** do not in turn interfere with the '*subsystem*' of anonymous ATXO transactions involving **SPECTRE** so long as we can secure enough entropy in the system in terms of available anonymous outputs. We will elaborate on this concept as we go along. It is also important to remember that we may not need to or desire to keep the Spectrecoin network as a '*dual-coin*' system in the future. With the new technology we are working on it is conceivable that the Spectrecoin network could transition to an anonymous only system at some point in the future.

XSPEC / SPECTRE Conversion

Each user can convert (*non-anonymous*) ***XSPEC*** coins into (*anonymous*) coins, ***SPECTRE***. Users can then send ***SPECTRE*** to other users, and split or merge the ***SPECTRE*** they own in any way that preserves the total value. Users can also convert ***SPECTRE*** back into ***XSPEC***, though in principle this is not necessary: all transactions can be made in terms of ***SPECTRE***.



In the wallet your public coins balance in **XSPEC** is shown on top and underneath the private balance of anonymous coins in **SPECTRE** is shown.

The core anonymising technology used for **Spectrecoin** is:

Recipient privacy: Stealth addresses are used to protect the recipient's privacy.

Sender privacy: Ring Signatures are used to protect the sender's privacy.

IP address privacy: All Spectrecoin nodes run as Tor hidden services to protect users IP addresses.

Un-traceability: for each incoming transaction all possible senders are equiprobable.

Un-linkability: for any two outgoing transactions it is impossible to prove they were sent to the same person.

Now let's have a look at the different features in some more detail…

Stealth Addresses

Before we go on to explain what stealth technology is and how it is used in Spectrecoin we need to get some background and some knowledge about how standard UTXO transactions might be de-anonymised and why stealth technology came to be used to counter this issue. It will also become apparent why stealth address technology in itself is not sufficient to provide reasonable anonymity.

The Spectrecoin blockchain is based on the design from Bitcoin Core (*except the consensus mechanism*) and in both systems there are $1.46 * 10^{48}$ possible receiving addresses(*). This is an extremely large number and it would give every person on Earth $2.05 * 10^{38}$ different receiving addresses to use. The fact that it is possible to re-use an address more than once can be considered a fluke and is not by design.

First, let's have a quick look at how a UTXO blockchain might be deanonymized. The three major factors that can reduce privacy for the user and are exploitable through transaction graph analysis are *address re-use* , *change addresses* and *the merging of outputs*.

Address re-use is treating XSPEC addresses like a bank account where a single address is used for multiple transactions. XSPEC addresses are not designed to be used in this way. There are in fact no restrictions on the number of XSPEC addresses one person can use and for each transaction a new XSPEC address should be created.

When addresses are re-used, all other transactions performed by that address can be seen by examining the blockchain. If you are aware of a transaction made by a person of interest and that transaction comes from the same address by which this person receives all their payments, then their balances can easily be determined. You will also be able to look back at the history of that address, following the chains of transactions, to ascertain what other information can be extracted.

Address re-use also weakens the security of the coins stored in those addresses. Transaction signing requires 256 bytes of random data (*r-value*) so that the private key cannot be reverse engineered. If the *r-value* is not truly random then the private key can be determined, which can be used to sign other transactions for that particular address. This attack can be negated by not re-using addresses, as once a transaction is signed from an address, it remains empty.

Furthermore, each input in a standard transaction must be a full UTXO from a previous transaction as UTXO's cannot be partially spent. This means that if you spend / send less than a full UTXO you will generate an output that is your change address. Therefore, an attacker examining the blockchain may generally assume that one output in any transaction belongs to the creator of the transaction.

Also, if a transaction is generated where two or more UTXOs are pooled together to create the total input required an assumption can be made that the addresses merged together belongs to the same person.

Let's then introduce **Stealth Address techniques** which allow public keys appearing in the blockchain to be fully disconnected from "*stealth*" public keys which can be publicised by a payee. The public "*stealth*" keys publicised serve as a "*master public key*" from which "*ephemeral public keys*" are derived. The "*stealth*" public key is never recorded in the blockchain. This enables the payee to receive infinite un-linkable payments by publicising only one stealth address. The problem of address re-use is therefore solved.

A Stealth address therefore is an anonymity technique that protects the privacy of the recipient. The first stealth address technique was invented by a user known as 'bytecoin' in 2011 in the Bitcointalk forum. Later improvements to stealth tech were proposed by van Saberhagen in 2013/14 and by Peter Todd in 2014.

The original stealth tech had various problems (*very technical but I have linked to a relevant paper*) and on 02/08/2014 one of the ShadowCash developers known as '*rynomster*' announced a first fully working implementation of stealth address tech that is known as dual-key stealth addresses that solved some of the issues in previous proposals. A "*dual-key stealth address*" has two public keys and solves certain problems associated with previous schemes. For a full and in-depth explanation of stealth addresses, see: http://www.scitepress.org/Papers/2017/62700/62700.pdf

(Courtois N. and Mercer R. (2017). **Stealth Address and Key Management Techniques in Blockchain Systems.** In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy* ISBN 978-989-758-209-7, pages 559-566. DOI: 10.5220/0006270005590566)

The use of dual-key stealth addresses provide privacy for the receiver of funds and introduces various forms of un-linkability (1) *It is hard to link different public keys/addresses of the same user*, (2) *It is hard to link different transactions of the same user*, (3) *It is hard to link the sender to the recipient*.

Limitations of Stealth Addresses

As mentioned above, stealth addresses generate a new standard address for every payment but If you receive for example 10 transactions using your stealth address you will have 10 UTXOs available to form further transactions. If you then use some or all of the UTXOs to form a transaction an observer will be able to link the UTXOs together and assume that they all belong to one user (*merging of outputs*). Furthermore, an attacker could create a number of dust transactions with a stealth address and then monitor the blockchain to see if the user ever joins those UTXOs together or with others, in order to make an input to a higher value transaction in the future. Blockchain analysis can easily link this. **This is the reason why any cryptocurrency that rely on stealth addresses ONLY is not private.**

Anonymous Spectrecoin creation

Dual-key Stealth technology is used in the process to create anonymous **SPECTRE** by consuming the equivalent value of **XSPEC**. The creation of **SPECTRE** involves the creation of an ATXO with a bundled one-time key-pair that will allow that ATXO to be '*spent*' by providing a valid ring signature using your remaining public key corresponding to the ATXO you previously created and the corresponding '*keyimage*'. The fact that an ATXO has been '*spent*' is only known to the sender and an observer cannot determine if the ATXO has been '*spent*'.

Keyimage

The '*keyImage*' is the result of a cryptographic one-way function derived from a user's one-time keypair. The '*keyimage*' is unique to the ATXO contributing the value to the new ATXO being created in an anonymous transaction. The '*keyimage*' is then recorded in the blockchain to prevent double spends, but without revealing which ATXO is the value-contributing member in the ring signature. Although the '*keyimage*' is recorded in the blockchain it cannot be reverse engineered due to the one-wayness of the cryptographic function that generated it. The calculation of the '*keyimage*' includes the users private key associated with the ATXO being '*spent*'. Hence, if the user tries to spend the same ATXO again the same '*keyimage*' will be generated and the system will reject the transaction as that '*keyimage*' has been seen before.

The following SPECTRE denominations are possible; 10,000, 5000, 4000, 3000, 1000, 500, 400, 300, 100, 50, 50, 30, 10, 5, 4, 3, 1, 0.5, 0.4, 0.3, 0.1, 0.0(000000)5, 0.0(000000)4, 0.0(000000)3, 0.0(000000)1

We are currently improving this system with updated algorithms around ATXO creation and selection. We will introduce a ATXO denomination balancer algorithm that will ensure sufficient supply of ATXO to ensure the necessary entropy in transactions.

We have seen how the use of stealth address tech can be used to solve the problem of address re-use and to create un-linkable transactions. Now, we still have the problem of ATXOs being linked together in future transactions. To resolve this issue Spectrecoin employs the use of ring signatures in transactions formed by **SPECTRE** ATXO outputs.

Ring Signatures

In a standard UTXO transaction the sender signs the transactions using his/her private key and the signatory can be explicitly determined and identified. In cryptography, a **ring signature** is a type of digital signature that can be performed by any member of a defined group of users that each have the required keys. A distinctive **ring signature** is produced through a process that combines the keys of all possible signers and other values and which are then subject to a hash function.

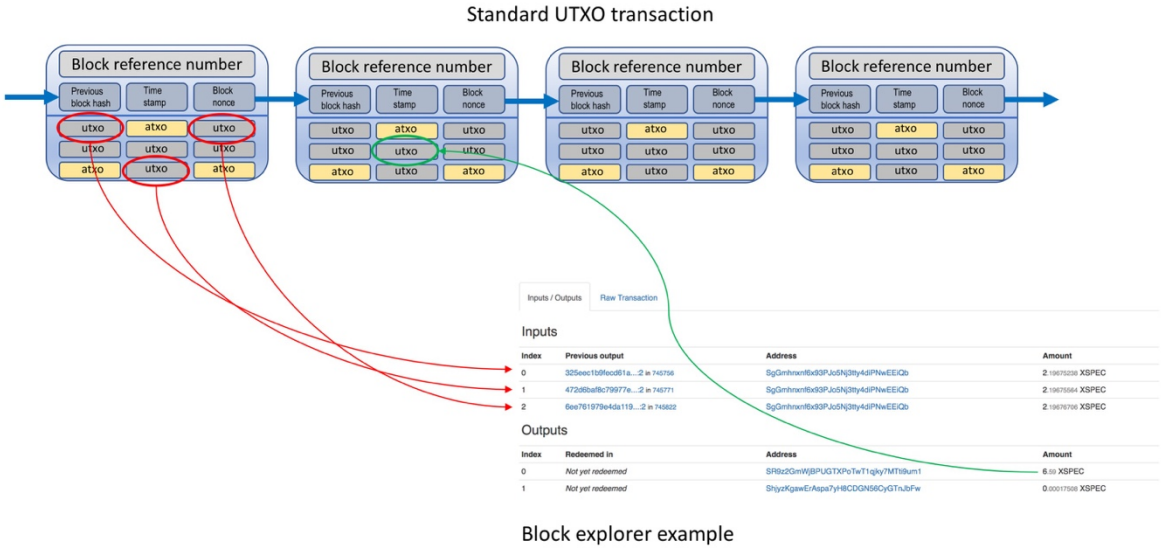
In cryptography a ring signature is a form of a *non-interactive zero knowledge proof*. In layman's terms, what this means is simply that you can prove the correctness of a statement/transaction to a verifier without leaking any additional information by just using a shared common reference string (*public key*). This system must include cryptographic completeness, soundness and zero-knowledge.

Completeness means that if the statement is correct, then the verifier will always accept. Soundness is a property of such a system that requires that no prover can make the verifier accept a false or incorrect statement. If the statement is incorrect or false, then the verifier will always reject. The last part is zero knowledge. It is not possible to gain any extra information from the proof itself except for the correctness of the statement for any malicious verifier.

This offers a group member a level of anonymity not attainable through generic digital signature schemes. This is a property known as '*plausible deniability*', or anonymity with respect to an anonymity set. With a ring size of 8 for example there are 8 possible signatories, i.e. 8 public keys and an observer cannot determine which one corresponds to the **SPECTRE** spent in the transaction. This is only know to the sender. This protects the privacy of the sender. With every transaction using a ring signature the system entropy increases and it becomes very hard to link input/output on the blockchain.

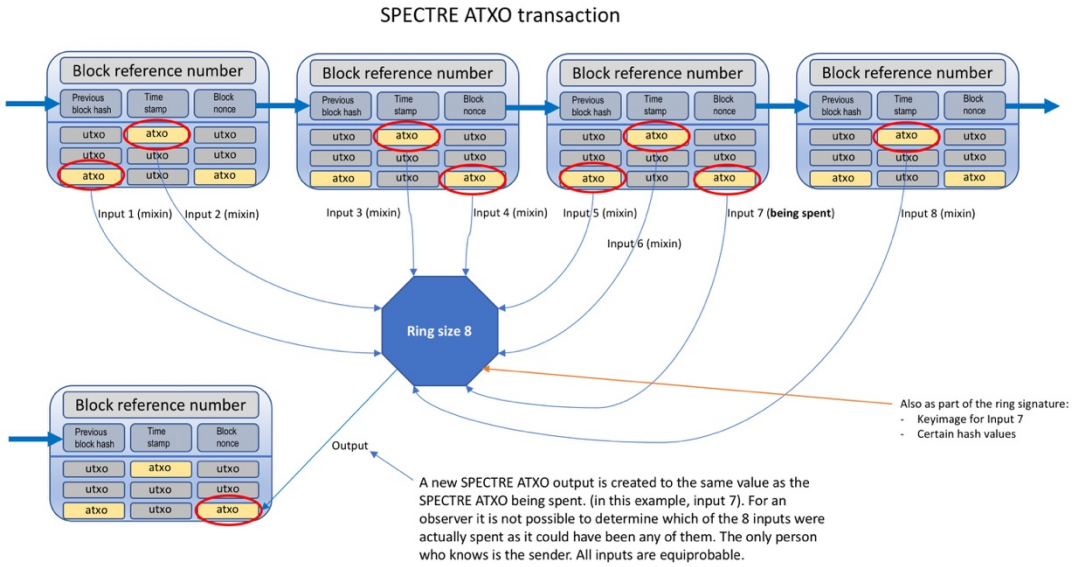
Look at it like this; scattered along the blockchains are ATXOs of various denominations from 10000 to 0.00000001 SPECTRE. These ATXOs may be spent or unspent but this cannot be determined by an observer. The proof of an ATXO being spent is formed on an ad-hoc basis through the creation of a 'keyimage' and there is nothing contained within the data of the ATXO itself or the transaction data that signifies if it has ever been '*spent*'. In a standard UTXO transaction on the other hand an observer can explicitly determine that an UTXO has indeed been spent to create a new UTXO.

Standard UTXO transaction



On the blockchain there is a **direct** correlation between the inputs and the outputs and all the transactions can be traced back to the genesis transactions. This is still the case even if a mixing strategy is used, such as in DASH. There are increasingly sophisticated methods to analyse blockchain data and this is a growth industry. You should consider any standard UTXO transactions to be non-anonymous and public, whether with Spectrecoin or Bitcoin.

Anonymous ATXO transaction



In the Spectrecoin software we talk about ring sizes and this refers to the group or set of possible signers. So, in the example below, we have a ring size of 8 which simply means that amongst the 8 public keys that form part of the digital signature, 7 are so called '*mixins*' or chaff and only 1 is the public key corresponding to the SPECTRE being spent.

When conducting an anonymous transaction, we use ring signatures to hide spent output in a set of the same denomination.

Anonymous transactions in Spectrecoin can be said to have levels of entropy as there is an interface between the '*public*' and the '*anonymous*' coins. Entropy level 0 can be said to be at the interface between XSPEC -> SPECTRE and between SPECTRE -> XSPEC. Once SPECTRE has been created from SPECTRE, i.e. an ATXO used as an input to create a new ATXO we can say that this is entropy level 1 as the freshly created ATXO has no public UTXO origin. Once these ATXOs are used to create further ATXOs this would be entropy level 2 and so on. The entropy increases with every level, IF AND ONLY IF a minimum ring size is used and the ATXOs have not been part of any ring size 1 transaction.

We are planning to introduce a minimum ring size of 8 in the next major release of Spectrecoin.

Spectrecoin is comparable to Monero in terms of transactional privacy at entropy level 1 and beyond. The transaction amounts will still be visible but we are working on strategies to improve on this.

Any ATXO used in a ring size 1 transaction will be marked as '*compromised*' and will not be selected as a 'mixin' in any future ring signature transaction.

We have seen how dual-key stealth address techniques are used to create ATXOs on the Spectrecoin blockchain with bundled one-time key pair that can only be 'spent' by providing a valid ring signature. In this way Spectrecoin protects the privacy of both the sender and the receiver.

TOR (The Onion Router)

TOR aka. The Onion Router is described on the project website (https://www.torproject.org/) "*Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.*"

Tor, in essence, hides your real IP address and instead provides you with a so called *.onion* address that should be extremely difficult to de-anonymise for any attacker. A normal IP might look like this: 123.45.67.8 and an .onion address might look like this: fpzcf23ifxpiucjm.onion. When you broadcast your normal IP address it will be possible to identify you through the internet service provider. If you broadcast a .onion address only this is not possible.

Spectrecoin has TOR '*built-in*' and when you start the software you will connect to the TOR network with an .onion address and you will not broadcast your real IP address through the Spectrecoin software for as long as you use the software.

Governance and Funding

The Spectrecoin blockchain will fork on 21/08/2018 @ 2200 hours (GMT) to introduce '*Development Contribution Blocks*' (DCB) to secure a minimum amount of funding for the project. One in six staking block rewards will be designated DCBs and will be sent to the Spectrecoin core team development fund wallet. Currently, @Mandica, @Beachguy and @RKh hold the private keys to this wallet. @Mandica manages the development fund at this time until a final governance structure has been put in place. One in 6 block rewards means that the stake reward from block 1, 6, 12, 18 and so forth are designated DCB regardless of who owns wallet that "won" and signed the contribution block. This means that larger wallets will have a higher probability of donating. It also means that it is possible to "win" two or more stake rewards 6 blocks apart and the owner of the wallet will contribute 2 stake rewards in a row. We believe that this will average out and that on the whole larger wallets will contribute more. This system can be considered transitional system and we are working on an improved version of this.

This fund will ensure a future for Spectrecoin, will enable us to pay for certain services, hire contractors and to pay Spectrecoin core team members in XSPEC/SPECTRE to enable them to work full time on the project. We have some long-term projects and concepts to implement such as a new proof-of-stake algorithm we call Proof-of-Stealth to enable so called "*stealth staking*". These developments depend on a source of steady funding. We believe this will give us the opportunity to produce better software and will create value for investors. We currently have some very skilled developers working for us and we want to keep it that way.

We are aiming to create a Spectrecoin foundation that will maintain the Spectrecoin GitHub repo, manage the development and the development fund and its distribution to developers and collaborators. This will be a legal entity with a stated constitution and rules. Further details will be available in a future updated white paper.

Industry / Outreach

Spectrecoin fully intends to collaborate with industry and specialist providers of software assurance and audit services to improve the quality and security of the cryptography. Spectrecoin will also work with academics and researched to work on improved solutions to our cryptography. Further details also in a future updated white paper.

Development Goals

Below we set out the development goals for the next 12 months. We are primarily focused on improving and optimising the privacy technology and roadmap is will reflect that. We have not set any dates for when we anticipate the roadmap to be completed at this time.

Proof-of-Stealth

We will release a new proof-of-stake mechanism for the ATXO subsystem. This means that your SPECTRE coin balance will be able to stake and you will be paid the stake reward directly in anonymous SPECTRE coins. This will make the staking process totally private and an observer will not be able to determine who is staking, any balances or rewards. Once introduced in Spectrecoin v3 there will be two parallel staking systems, one for standard UTXOs and one for ATXOs.

ATXO denomination balancer

It is vital that the process of selecting mixins for ring signatures is sound and that a sufficient selection of mixins of different denominations are available. We will therefore introduce a process of balancing the ATXO denominations when ATXOs are created to ensure sufficient supply of entropy rich mixins. Spectrecoin already has a concept of 'compromised' ATXOs in the code base and we will improve on this system.

Improved mixin selection algorithms

We will improve the way in which mixins are selected for inclusion in ring signatures.

Minimum ring size

In the next major wallet update we will introduce a min ring size of 8 for all ATXO based transactions.

Docker images and automated building

We are aiming for rapid automated builds when new code is released.

Cryptography audit and research

We will work with industry and academics to audit our cryptographic implementations, to research improvements and propose new solutions to fix vulnerabilities or weaknesses.

Network security

We will work to audit and improve the TOR integration and work towards integrating the TOR pluggable transports. We will also look at proposals such as Dandelion to assess if this can be introduced to enhance Spectrecoin network security.

References

https://bravenewcoin.com/assets/Whitepapers/ShadowCash-Zeroknowledge-Anonymous-Distributed-ECash.pdf

Proof-of-Stake

https://peercoin.net/assets/paper/peercoin-paper.pdf
https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf
http://earlz.net/view/2017/07/27/1904/the-missing-explanation-of-proof-of-stake-version

Stealth Address Technology

http://www.scitepress.org/Papers/2017/62700/62700.pdf
http://www.nicolascourtois.com/bitcoin/paycoin_privacy_monero_6_ICISSP17.pdf

Ring signatures

https://people.csail.mit.edu/rivest/pubs/RST01.pdf
https://arxiv.org/pdf/1612.01188.pdf