SECURE CASH WHITEPAPER V1.0

RESUME

Secure Cash (SCSX) is a reserve currency for the upcoming world economic crisis. In addition to making anonymous transactions like any other coin, secure coin will be used as reserve currency, as well as gold, secure cash will also value much more during a global economic crisis.

HIGH EMISSION LINE

the emission line is responsible for the calculation of the reward per block mined, a high emission line means there will be fewer coins per block, this means that few have coins and consequently, there will be few coins in circulation favoring the appreciation of the price of coin.

EXTREMELY LOW SUPPLY

For greater profit and appreciation in the market for Crypto-currencies, the maximum coin supply of this blockchain is 300,000 coins, along with the high emission line and rewards per block of 0.13 scsx, Secure Cash has everything to appreciate quickly when there is buying power.

SPECIFICATIONS

Name Secure Cash
Ticker SCSX
Algorithm Cryptonight Lite V1 (Variant 1)
Genisis Block
01/15/2019 11:55 pm
Minig Protocol Proof of Work (POW)
Total Supply 300,000
Premine 45,000
Premine Destinantion
Social and Sustainable Destination 1,000
Giveaways 2,500
Reward per Block 0.011 SCSX and decreasing
Block Time 120
Difficulty Adjustment Varied
Emission Curve 22
Maturation Time 10 Blocks
Transaction Fee 0.00000100 SCSX

INTRODUCTION

With a number of cryptocurrency projects around the world say that ring signature transaction anonymity is groundbreaking or that the crypto night Lite V1 (Variant 1) algorithm technology is a solution would be a lie, many cryptocurrencies uses this technology and all its codifications are opened for all users consulting. Thinking about this issue and analyzing the current Cryptocurrency market we see Big Named Projects like Bitcoin, Ethereum, Monero, Litecoin, among others that had their initial project changed over time.

Many Cryptocurrencies have promised to offer a means of payment function but have failed to achieve the goal, failures such as delays between transactions, high rates or high market buoyancy. Other cryptocurrencies sought to decentralize their Project and ended up in a few individuals or companies hands, thus ceasing to be decentralized.

Secure Cash has come up to solve several problems at once which are: Low Transaction Cost (0.00000100 SCSX), Transaction Time (1 transaction block every 2 minutes), User Anonymity through Cryptonight Algorithm Lite and Full Project Decentralization through Voting Campaigns conducted by SCSX Users. Beyond all these points that will be addressed in this Document, 10% of Secure Cash Total Available Inventory will be destined for Social and Sustainable Causes

ROADMAP

Q1 - 2019

- Wallets development -OK
- Genesis Block: 01/15/2019 11:55 pm - OK
- Create Windows wallet GUI and CLI - OK
- Create Linux wallet CLI - OK
- Create Paper Wallet - OK
- Web-miner – Mining via web browser, compatible with mobile phones and tablets - OK
- Block Explorer - OK
- Open mining for general public - OK
- Website - OK
- Social media and communication platforms: Twitter, Discord, Telegram - OK
- Publish SCSX code on GITHUB - OK
- Promote SCSX on BITCOINTALK – OK

Q2 - 2019

- Listing on Letsdocoinz exchange - OK
- Listing on Finexbox exchange - OK

Q3 - 2019

- Listing on Nanu.exchange - OK

Q4 - 2019

- Airdrop campaign - OK
- Listing on Gokuex exchange - OK

Q1 - 2020

- Second airdrop campaign - OK
- Security update for Wallets

Q3 - 2020

- Third airdrop campaign - OK
- Security update for Wallets

Q4 - 2020
- Publish Whitepaper - OK

2021
- Add SCSX in at least one big Exchange
- Release of the mobile wallet
- Release of the MAC OS wallet

CAPITAL FOR SOCIAL PURPOSES

The Secure Cash Project is based on a Sustainable Social Bank where 1.5% of the total available cryptocurrency stock will be earmarked for donations, the more the user mine the more they help these social entities.

All capital will be directed to a portfolio and will be available for withdrawal for the purposes due per voting process.

MINING

We chose to develop a Cryptocurrency where mining is virtually viable for any user with a computer or even a mobile phone. Because the Cryptonight Lite V7 algorithm is a ASIC resistant, only CPUs and GPUs can be mined. As an alternative for non-computing users, SCSX will offer its own airdrop sites on social networks.

TRANSACTIONS AND ANONIMATE

Seeking improved usability of cryptocurrency transactions we offer an extremely low transaction rate of 0.00000100 SCSX, complete transaction anonymity through the Cryptonight Lite V1 (Variant 1) algorithm. In addition to these factors we have a particularity that the amount of transactions per block is unlimited, helping to improve the performance and speed of transactions.

FINAL CONSIDERATIONS

As the purpose of the Secure Cash Project is to develop a Cryptocurrency where all participants are key parts of the process, everyone should benefit from performing their duties; miners, investors, social and sustainable funds, and developers having the same importance within the Project. Any users who are interested in supporting Secure Cash are welcome. Become a financial exponential and let Secure Cash do for you what no other currency does: make you a partner in a company without patrons, just members with equal powers.

al powers.

CRYPTONIGHT / CRYPTONOTE TECHNOLOGY

The CryptoNote Technology Now that we have covered the limitations of the Bitcoin technology, we will concentrate on presenting the features of CryptoNote.

Untraceable Transactions

In this section we propose a scheme of fully anonymous transactions satisfying both untraceability and unlinkability conditions. An important feature of our solution is its autonomy: the sender is not required to cooperate with other users or a trusted third party to make his transactions; hence each participant produces a cover traffic independently.

Literature review

Our scheme relies on the cryptographic primitive called a group signature. First presented by D. Chaum and E. van Heyst [19], it allows a user to sign his message on behalf of the group. After signing the message the user provides (for verification purposes) not his own single public 1This is so-called "soft limit" — the reference client restriction for creating new blocks. Hard maximum of possible blocksize was 1 MB

key, but the keys of all the users of his group. A verifier is convinced that the real signer is a member of the group, but cannot exclusively identify the signer. The original protocol required a trusted third party (called the Group Manager), and he was the only one who could trace the signer. The next version called a ring signature, introduced by Rivest et al. in [34], was an autonomous scheme without Group Manager and anonymity revocation. Various modifications of this scheme appeared later: linkable ring signature [26, 27, 17] allowed to determine if two signatures were produced by the same group member, traceable ring signature [24, 23] limited excessive anonymity by providing possibility to trace the signer of two messages with respect to the same metainformation (or "tag" in terms of [24]). A similar cryptographic construction is also known as a ad-hoc group signature [16, 38]. It emphasizes the arbitrary group formation, whereas group/ring signature schemes rather imply a fixed set of members. For the most part, our solution is based on the work "Traceable ring signature" by E. Fujisaki and K. Suzuki [24]. In order to distinguish the original algorithm and our modification we will call the latter a one-time ring signature, stressing the user's capability to produce only one valid signature under his private key. We weakened the traceability property and kept the linkability only to provide one-timeness: the public key may appear in many foreign verifying sets and the private key can be used for generating a unique anonymous signature. In case of a double spend attempt these two signatures will be linked together, but revealing the signer is not necessary for our purposes.

Unlinkable payments

Classic Bitcoin addresses, once being published, become unambiguous identifier for incoming payments, linking them together and tying to the recipient's pseudonyms. If someone wants to receive an "untied" transaction, he should convey his address to the sender by a private channel. If he wants to receive different transactions which cannot be proven to belong to the same owner he should generate all the different addresses and never publish them in his own pseudonym.

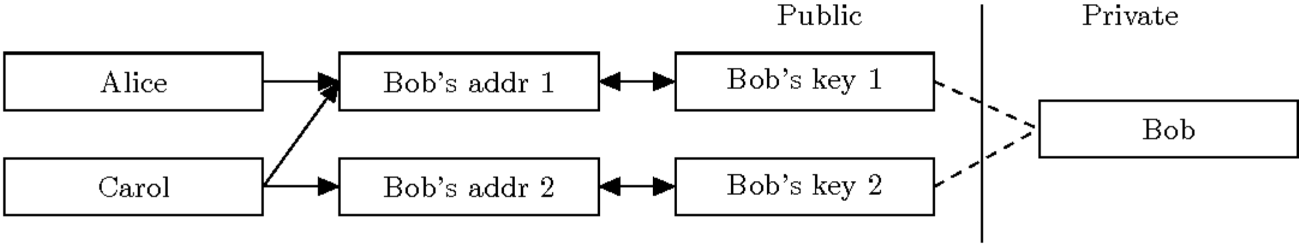


Fig. 2. Traditional Bitcoin keys/transactions model.

We propose a 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.

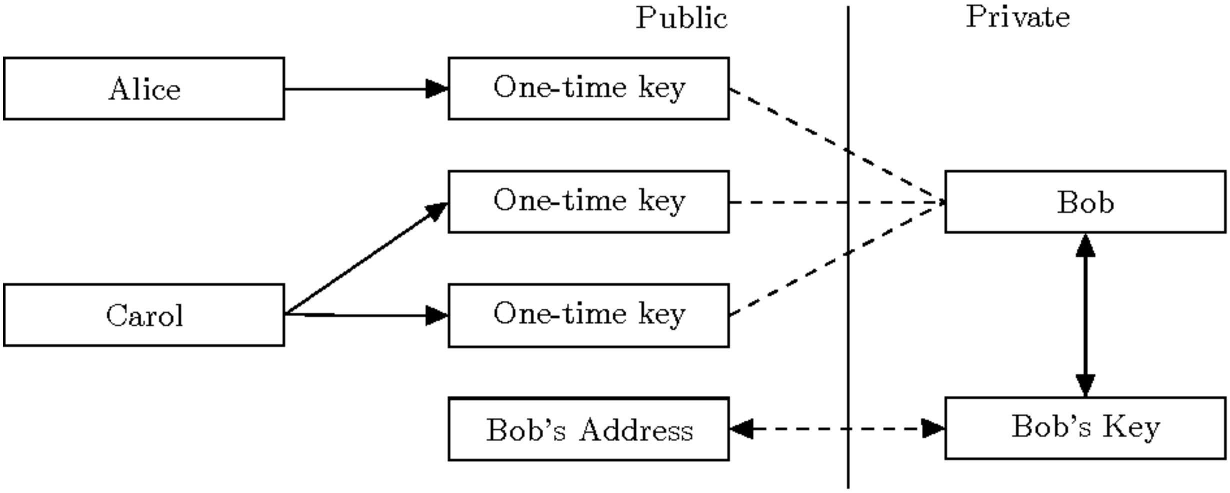


Fig. 3. CryptoNote keys/transactions model.

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

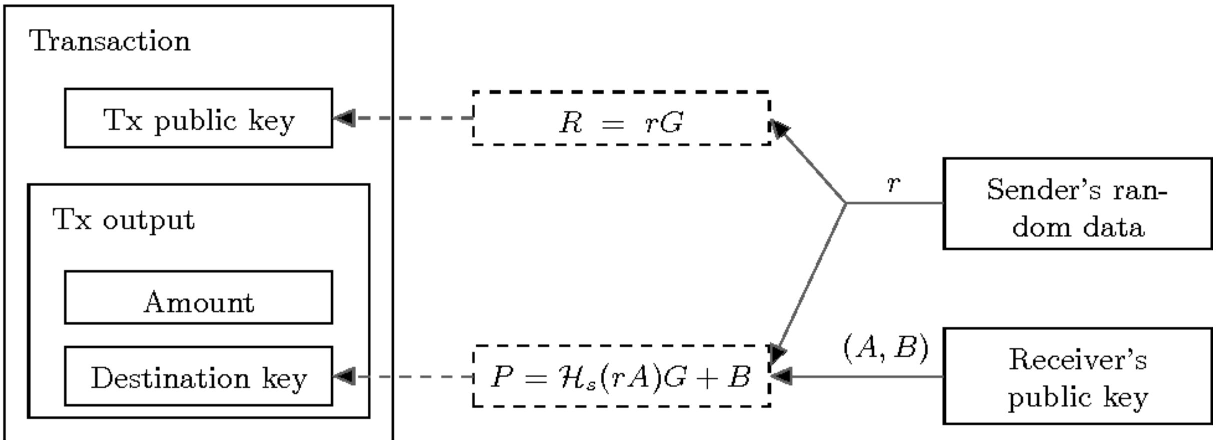
address. The receiver also performs a Diffie-Hellman exchange to recover the corresponding secret key. A standard transaction sequence goes as follows:

1. Alice wants to send a payment to Bob, who has published his standard address. She unpacks the address and gets Bob’s public key (A, B).

2. Alice generates a random r □ [1, l−1] and computes a one-time public key P = Hs(rA)G+ B.

3. Alice uses P as a destination key for the output and also packs value R = rG (as a part of the Diffie-Hellman exchange) somewhere into the transaction. Note that she can create other outputs with unique public keys: different recipients’ keys (Ai , Bi) imply different Pi even with the same r.

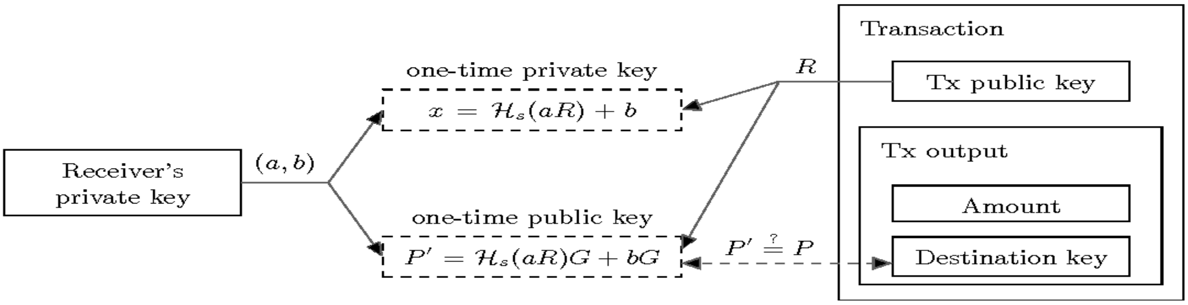
even with the same r.



4. Alice sends the transaction.

5. Bob checks every passing transaction with his private key (a, b), and computes P 0 = Hs(aR)G + B. If Alice's transaction for with Bob as the recipient was among them, then aR = arG = rA and P 0 = P.

6. Bob can recover the corresponding one-time private key: x = Hs(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 bandwidth 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 r or 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-key B, and the remaining part required by the protocol is derived from it as follows: a = Hs(B) and A = Hs(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.