CUT tokens: CryptoNote Tokens (CNT-1)

Cutcoin Team
email info@cutcoin.org

July 16, 2020

Abstract

A distributed ledger made up of privacy-by-design protection could allow for a single global database that records any state of deals, agreements, and acts as a settlement system between individuals and organizations, without compromising sensitive information about them. Such a system can be used for accounting, voting, financial markets, insurance, and more. By leveraging CryptoNote-inspired cryptocurrency CUTcoin and using redesigned transaction processing we propose a privacy-preserving tokenization protocol.

I Introduction

CUTcoin[1] has been developed since 2018 as the first CryptoNote coin with the Proof of Stake consensus algorithm. This achievement is difficult to be underrated as many parties benefit from it: CUTcoin users get an attack-resistant protocol with exceptional privacy level inherited from Monero while being able to participate in the consensus with lowered costs, thus saving electricity and the planet. That was the first stage of development when we created the technological basement for fast, reliable, energy-efficient, and privacy-focused cryptocurrency.

Now we present the first CryptoNote-based tokens. Regular tokens (e.g. ERC20) are a useful tool that can represent valuable assets. Privacy tokens obviously play a similar role but preserve the privacy of their owners and confidentiality of the transaction details.

II CryptoNote Tokens: CNT-1

Technology highlights

CUTcoin has a standard CryptoNote mechanics of the funds' circulation[2]. Network layer includes peer to peer nodes that permanently establish consensus on the state of blockchain, the distributed database, where all transactions are stored. Each node runs daemon, the core software that maintains connections with other daemons, validates incoming transactions, and adds consistent records to the blockchain.

The money supply is presented as a collection of unspent transaction outputs (UTXO) stored on the blockchain, which are effectively pairs of the public and private key. Different UTXOs may belong to the same or different users and have different amounts of coins. The private key is needed if somebody wants to transfer funds to another user, so only the owner knows it.

CryptoNote protocol relies on elliptic curves (EC) cryptography. Elliptic curves have specific algebra, supporting several operations similar to real values operations: addition, subtraction, multiplication. The most important property of them is that the division (opposite to multiplication) is hard to be evaluated and belongs to so-called hard problems. In other words, if k is a secret key and G is a known EC point the corresponding public key $K = kG$ can be easily found. At the same time, for a known K the secret key k cannot be found by no means except for brute force matching.

Key pairs are broadly used in CryptoNote (and CUTcoin) and lay in the basement of more complicated cryptography constructions[3]. In the vast majority of cases, a single EC point is used for commitments, it is defined as $H = nG$ (n is unknown) and referenced as the base point. From the practical point of view, it's a matter of convention which one to use, so in CNT-1 each token uses its own base point. Token's base point has a deterministic, pseudo random relation to its token id (name), so for a given token id its base point can be easily evaluated.

Since tokens appear in CUTcoin each input and output in a transaction contains a corresponding token id. It is used for commitments and signatures and also allows a daemon to check that the token being sent has been already created.

Starting from CryptoNote protocol v.4, when RingCT technology was implemented, the exact amounts of funds being transferred in a transaction are hidden. It might be a problem for the daemons that prove incoming transactions as they need to verify that the sum of input amounts equals

to the sum of output amounts. This challenge was resolved by using bulletproofs. It's a cryptography construction allowing the verifier to check that:

(1) amounts of a transaction inputs are positive and belong to allowed range,

(2) sum of all transaction inputs is equal to the sum of the outputs + fees.

Technical realization of the range commitment (1) is quite complicated[4], therefore we don't look at it in detail. The latter statement (2) is checked more simply.

Suppose a transaction has inputs with amounts $a_1, ..., a_n$ and outputs with amounts $b_1, ..., b_m$. For each input we can construct the commitment $C_i = x_i G + a_i H$. x_i is a blinding factor (mask) chosen randomly, G and H are specific EC points, as discussed before. Same commitments can be written for outputs: $C_j = y_j G + b_j H$. Keeping in mind that EC points have additivity property, we can note that $\sum_i C_i = \sum_j C_j$ is enough for a verifier to be confident that the sum of input amounts is equal to the sum of output amounts without revealing of them. In this case a transaction contains just commitments C_i and C_j.

When we have tokens of different types in a single transaction things become more complicated as a verifier should be confident that the sums of inputs and outputs are equal for all tokens separately. Fortunately, we can use different base points B_t for different tokens, deriving them from the token ids in transaction's inputs and outputs. Then form similar commitments:

$$C_{ti} = x_i G + a_i B_t, C_{tj} = y_j G + b_j B_t, \text{ and claim} \tag{1}$$

$$\sum_{t,i}(C_{ti}) = \sum_{t,j}(C_{tj}). \tag{2}$$

This example illustrates how token-specific base points help in preserving the same level of consistency and privacy for tokens as coins themselves have. These changes also affect RCT signatures, one-time addresses etc.

Key characteristics

CNT-1 is a named entity that represents a specific value. Once created, a token can be owned or sent to another owner. No token duplicates (tokens with the same names) are allowed.

To create a token user needs to issue a special token genesis transaction. The price for token creation is 100 CUT, it is fixed and paid once from the user account.

Token supply is specified at the moment of token creation. It can vary from 1 up to 200,000,000. Once created, tokens experience neither inflation nor deflation, though for the purpose of artificial scarcity tokens can be sent to a coinburn address.

Token name is specified once and must consist of A-Z letters and 0-9 digits. The maximum name length is 8 signs. Token id is generated automatically from the token name. Token id 0 corresponds to CUTcoin. As we mentioned, CNT-1 token names are unique. At the moment of token creation its name is being checked and it is created only if another token with the requested name doesn't exist.

Transactions with tokens are just regular CUTcoin transactions with the standard fees that depend on their size. Current limitations imply no tokens with different names can be transferred in a single transaction. Tokens have the same default spendable age (10 blocks) as CUTcoin, so they can be transferred in approximately 20 minutes after they were received or after their creation.

CUTcoin account may have different tokens at the same time. The user can list all tokens in his account and output their balances.

III Use cases

A privacy-preserving voting

An online voting system has long been a hot topic in the literature: many multi-party voting algorithms have been proposed over the years to preserve the secrecy of voting information and, therefore, the integrity of voting in an online format.

For sure, electronic voting is already here for some time. However, there are three typical problems with it:

- security problems (electronic systems can be hacked, often scandals are associated with it);
- problems with verification of election results (as opposed to paper ballots that can be counted);
- the possibility of incorrect system operation due to software errors.

Before the invention of blockchain, it was clear that the privacy of a vote may be preserved in two ways[5]: by encrypting the vote or by sending the vote through an anonymous communication channel. Both ways have drawbacks; in the first case, it seems impractical due to the amount of communication needed to validate the vote; in the second case, central authority is required to tally the votes, let alone the chance of ballot collision.

The idea of using blockchain in voting systems suggests itself: blockchain allows replacing ancient voting technology by transferring someone's voice expressed by a physical object (a ball of the desired color, a paper ballot, etc.) to a digital token. It also enables trusted results, i.e. confidence in the election results is formed not at the expense of a centralized authority, but as a result of confidence in the technology.

However, a privacy problem arises since most blockchain platforms are public ledgers, i.e. any token transfer can be easily attributed to the specific users, and this is a violation of secret ballot principle, or a voting method in which a voter's choices in an election or a referendum are anonymous, forestalling attempts to influence the voter by intimidation, blackmailing, and potential vote-buying.

That's pretty much where privacy-preserving tokens can be used. We do not limit the possible usage of CNT-1 to voting, though it seems like a good match to start with. There might be different mechanics of token distribution:

- new series made to the upcoming elections;
- a limited amount of tokens created and distributed among community members;
- tokens can be delegated to special electoral college (like in indirect elections) and so on.

One particular case is the board of directors voting. Because corporations depend on their boards to make vital decisions that impact their company's future, it's crucial for the board of director voting procedures to be accurate, efficient, transparent, and secure.

Besides, similar mechanics can be used in various scenarios like community governance and distribution of limited resources (as an alternative to auctions), share holding, transferring, and accumulation.

Commodities digitalization

Essentially, tokenization is a process of turning things (physical goods, property rights etc.) into digital assets. Thus, a token is a digital print of possessing rights towards a specific product, or piece of the product (take painting as an example). Tokenization of assets is already disrupting not only the financial industry, but also real-estate, precious metals, sports teams, energy, luxury goods and more.

The specific thing about tokens built on the CUTcoin infrastructure is a privacy-centric approach – though the total number of tokens of particular kind can be identified from the blockchain, the number of "circulating" tokens, the amount any particular user possesses, amount sent and received by users – all that being concealed.

Securitization of artworks

In the art market, authenticity is largely determined by evaluating a limited circle of experts, and experts are also people who can make mistakes / bribe, and besides, their work is expensive, so if the history of an object becomes opaque, then questions immediately arise about its authenticity when it reappears. And the owners often just do not want to be public and therefore the objects of art after the sale disappear from sight.

Here's how, merely from a technological perspective but with plans to bootstrap the full value chain, the above mentioned inefficiency can be solved by using CUT tokens. Steps to securitize a new artwork:

- an owner or creator of an artwork expresses his intention to securitize;
- the artwork is evaluated by several experts;
- tokens with limited supply are created;
- these tokens are listed at the dedicated platform, where the investors can buy and store them in the CUT wallet.

Counterfeit Protection

Common problems for the industry of luxurious goods are the opacity of supply chains and the associated fragmentation of information, as well as the lack of common incentives between market participants and, as a result, opportunistic behavior due to which all participants suffer. And this applies not only to jewelry, but to clothing, cosmetics, and many more goods.

CUT tokens can help to eliminate the risk of counterfeiting by:

- assessment of the authenticity and provenance of luxurious objects (artworks, watches, rare and collectible alcohol etc.);
- recording of evaluation results on the blockchain;
- cataloging;
- safe custody.

Alternative investments

Another possible scenario grasps investment opportunities into alternative asset classes like:

- luxurious watches,
- premium spirit drinks,
- rare coins etc.

These commodities can be tokenized with CNT-1 tokens, and the possessions of rights easily transmitted / traded via decentralized exchange. Given that the very fact of possession of this asset or a part of it remains hidden, it lies behind the privacy-first approach and lets the user be safe from malicious actions of the criminals.

Company rewards

One can imagine an IT-company that wants to be able to reward distinguished employees with bonuses, but turn these bonuses into money only at the end of the year, when the financial results of the company are known. In that case, it's possible to distribute tokenized stock options of the company (if it's public) or stakes of the future income. As with an employee's contract, bonuses are a delicate thing that should remain confidential.

IV Further development

Advanced token functionality

In further development, CNT-1 tokens receive more functionality: one of the features that we expect can be useful is a completely hidden token supply. Such a feature may be necessary when the user issuing tokens wants to keep

their total number a secret – among possible use cases there can be, for example, wills.

Also, there may be scenarios of automated token distribution of one tokens to another. Such a function will allow tokens to act as points in loyalty programs, or serve as a marketing tool to attract new community members to the crypto projects.

Decentralized exchange

We envision the decentralized exchange as the next big step in the CUT ecosystem. A decentralized exchange is useful for private tokens in that one does not need to drag them to a regular exchange, where deanonymization can occur.

DEX eliminates the inherent problems of centralized exchanges, namely security vulnerabilities, centralized control of digital assets, custodian challenges and more. Custody trading service will be a step back against all the efforts made to create a decentralized privacy network – the whole idea behind CUT is about that.

At present, there are lots of decentralized exchanges being developed, but they barely can meet the needs of our users. Problems mainly include:

- the absolute majority of the DEXs are trading platforms for Ethereum and ERC-20 tokens, which is quite an obstacle for UTXO-based tokens;
- low product quality;
- low liquidity levels, low volume;
- inefficient, slow transaction speed, poor UX.

In our initial DEX architecture, the exchange back-end will be developed as a part of our daemon as this seems more feasible than privacy-preserving full-featured smart contracts at this time. At the same time, we invite developers and technically savvy enthusiasts to work together on use cases and specific realization.

Privacy stablecoin

For a long time, various crypto payment systems aimed at replacing fiat money as a mean of payments, unit of account, and store of value. However, existing cryptocurrencies, including stablecoins, provide a very low level of privacy as all the transaction and account balances are stored publicly. In

this regard, cash is essentially anonymous, and that's something we believe might be relevant for people in the coming bright new world. That's why a privacy-centric stablecoin might be built using CUTcoin infrastructure. CNT-enabled stablecoin could become a leading stablecoin contender for cash-like usage such as simple purchases from merchants who should not be able to see the buyer's total cash balance.

On public blockchains, like Bitcoin and Ethereum (and thus on most stablecoins since they are ERC20) it is often possible to view the history of units. Thus, coins stolen in an exchange hack, for instance, are identifiable – and even if a user has no connection to the hack but received these coins, it can cause trouble. This transparency makes coins unexchangeable, violating their fungibility property. At this point we envision creating the needed infrastructure and back-end for algorithmic privacy-preserving stablecoin (like Maker, but with Monero properties).

V Conclusion

In this paper, we described the first specification of CryptoNote tokens which we labeled CNT-1. We then proposed potential use cases for these tokens, like voting, commodities digitalization, counterfeit protection and alternative investments. As the CUTcoin project moves forward, the next big thing to be created is a decentralized exchange that will pour liquidity to tokens. We believe that tokens liquidity will allow attracting and involving broad groups of developers and crypto projects focused on privacy and personal data protection.

References

[1] Cutcoin Team (2019) Cutcoin: a Privacy-Focused Cryptocurrency Based on PoS Consensus Algorithm: https://static.cutcoin.org/cutcoin-whitepaper-v1.0.pdf.

[2] Nicolas van Saberhagen, (2013) CryptoNote v 2.0.

[3] Kurt M. Alonso, (2018) Zero to Monero.

[4] Benedikt Bunz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, Greg Maxwell, Bulletproofs: Short Proofs for Confidential Transactions and More. https://eprint.iacr.org/2017/1066.pdf

[5] A. Fujioka, T. Okamoto, and K. Ohta (1993) A practical secret voting scheme for large scale elections, Advances in Cryptology – AUSCRYPT '92, Berlin, Heidelberg, 1993, pp. 244-251.