CRYPTONOTE STANDARD 009 Brandon Hawking
Category: Main Track Pacific_skyline
Yggdrasil
Johannes Meier
CryptoNote
August 2013

CryptoNote Technology

Abstract

This document is part of the CryptoNote Standards describing a peer-to-peer anonymous payment system. It defines the core concepts of the CryptoNote technology and surveys the whole system's workflow. All transactions are public data and are stored by every peer, yet none of the private information is revealed. Payments cannot be unambiguously traced to senders; transfers can only be interlinked by their owners. Peers validate all the data and rely on proof of work to reach a consensus. The proof-of-work function guarantees egalitarian voting, so that none of the participants can utilize special purpose devices to obtain an excessive voting advantage.

Copyright and License Notice

Table of Contents

1. Introduction

CryptoNote is a technology that allows anonymous, unlinkable and untraceable peer-to-peer payments.

The system is based on Satoshi Nakamoto's Bitcoin [BITCOIN] concept: a distributed public ledger (blockchain) of transactions (ordered records of money transfers). Each peer stores a local copy of blockchain and verifies every new transaction. Hash-based proof of work [POW] is the solution to "the problem of determining representation in majority decision making", when some of the data was missed by an offline peer. If there are multiple conflicting versions, peers choose the one with more work presented. All data is sent on the best-effort basis.

2. Definitions

alternative branch: a blockchain branch that includes blocks that are not on the main branch

block: a dataset (payload) with a block header

blockchain: a tree structure of blocks

blockchain fork: a situation when there are two such peers that the main branch for each of them is an alternative one for the other peer

double-spending: the result of successfully spending an amount of money more than once

main branch: the set of blocks that represents the current state of the distributed ledger

nonce: a field in a block header that peers change as part of the proof-of-work scheme

peer: a participant in the p2p (peer-to-peer) CryptoNote network

proof of work (PoW): a way for a computer system to demonstrate that it expended a certain amount of computational resources in support of a particular decision

ring signature: a class of schemes that allow a user to sign a message on behalf of a group, making his identity indistinguishable from the other members of the group

transaction: a single record of assets ownership transfer

3. CryptoNote Protocol

This section describes the principles of the CryptoNote technology.

3.1 Transactions

Each user possesses several unique secret keys, each associated with a certain amount of money. A key gives user the ability to spend the money, lock, or even destroy it. At any moment there is a definite many-to-one mapping between all currency units and keys.

User can divide his funds into smaller pieces or merge several amounts into one by reassigning ownership from his old keys to new ones. Each set of such transfers forms a new transaction that will be stored in the blockchain. Each key (old or new one) belongs to a sender or to some other user (i.e. there might be several senders and addressees in a single transaction). See [CNS004] for details.

After a transaction has been created and sent to other peers, it exists in one of the four possible states:

1. Unconfirmed: every peer is aware of the transaction, but it is not included in the blockchain yet.

2. Confirmed: the transaction is now a part of the blockchain. In case of a blockchain fork, newly confirmed transactions may become unconfirmed again.

3. Irreversible: the transaction has stayed confirmed for some time. The probability of an irreversible transaction becoming unconfirmed is negligible.

4. Rejected: the transaction is not included into the blockchain, since a contradicting one (involving the same funds) has been confirmed. These transactions cannot be stored in the same blockchain branch, therefore any rejected transaction should be abandoned.

The users' privacy depends on how the transactions are constructed. The properties described below are integral parts of the CryptoNote anonymous transactions technology:

1. Untraceability: it is impossible to determine the exact sender of a transaction.

2. Unlinkability: it is impossible to determine whether any two

transactions are sent to the same address.

3.1.1 Transaction Untraceability

The untraceability requirement can be fulfilled through ring signatures [TRS]. Any signature is, in fact, a proof of the user's knowledge of the secret key that allows spending the corresponding amount of money. Regular digital signature schemes ((EC)DSA or similar) reveal the signer's identity, since they use only one public key for the verification procedure.

Unlike regular digital signature schemes, a ring signature is a much more sophisticated scheme that allows a user to sign his message on behalf of a group. A verifier is able to see that the message was signed by someone within the group of signers, but he is not able to determine the exact signer. All public keys required for verification are indistinguishable in that sense.

To prove the ownership of the money the user randomly chooses public keys of other users and then adds his key to produce a ring signature that must be verified with all these keys. The owner of one of those keys may produce his own ring signature with the same set of public keys (making his own transaction), and there will still be no way (better than guessing with 1/n probability) to determine from which particular key the money was reassigned.

There are several ring signature schemes. An implementor should use a scheme, which is not completely anonymous, but allows to check whether two signatures were made under the same secret key. Every peer should be able to perform this check to prevent double-spending. One possible algorithm is described in [TRS].

See [CNS002] for details.

3.1.2 Transaction Unlinkability

Usually a person has a public address that unambiguously identifies him. However, none of his incoming transactions should expose the connection with this address.

This can be achieved through generating a unique key for each transfer with the modified Diffie-Hellman protocol [DH]. The original scheme allows two parties to produce a common secret by exchanging data via open channels. In CryptoNote, public keys are generated in such a way that only the recipient can link them to his account, while even the sender cannot recover the corresponding secret key.

The sender uses the address and his random data to create a new public key and transfers money to it. The recipient scans all the keys in new transactions and checks if he can recover the corresponding secret key. If he succeeds, he learns that he is the new owner of the money, i.e. the transfer is completed. The keys can only be linked by the receiver, as this requires the knowledge of the secret key corresponding to the address.

See [CNS006] for details.

3.2 Blocks

All transactions are stored in a single distributed ledger that consists of chained blocks. Each block contains a hash reference to its predecessor, several new transactions that have been sent since the previous block, and some additional information, such as a timestamp and nonce (see below). To go along with Nakamoto's notation [BITCOIN], we will call this ledger the blockchain.

A consensus on the state of the blockchain is achieved by a voting mechanism called proof of work. Each block is considered valid only if the value of a special hash function of this block is less than the target value. Peers that choose to participate in the voting alter the block by iterating the value of the nonce field in the header of the block. If the hash of the resulting block meets the above criterion, the block is added to the blockchain. This stochastic process provides a continual supply of new blocks. If two or more blocks with the same predecessor appear simultaneously, a blockchain fork occurs. If this happens, each peer can choose any of the branches as a current one. Eventually one of the branches will outrun the other one, making all peers switch to it.

See [CNS003] for details.

3.3 Proof-of-Work Function

Voting on the state of the blockchain is performed through calculation of a special hash function. The right choice of the function is of fundamental importance.

The main concern is security. The blockchain model is proved by Nakamoto's Bitcoin [BITCOIN] to be safe in case more than 50% of the hashing power is under the control of honest users. Therefore, a potential attacker should not be able to acquire massive hashing power. There should not be a significantly cheaper source of powerful hardware beyond the reach of ordinary users. For this reason memory-bound algorithms are superior to CPU-bound.

Another issue with PoW is the nature of voting. Any public mechanism of a majority decision-making process must satisfy a natural assumption of egalitarianism. There may be several contradictory transactions that result in two or more valid versions of the blockchain (a blockchain fork). Since only one of the versions will win, it must represent the majority of people, i.e. all users must be nearly equal in terms of hashing power to guarantee the "majority rule".

Generally, the hash function must not allow a user to have a significant advantage over another. The most acceptable way of discovering new blocks is to use regular hardware, such as a PC, and utilize uniformly distributed resource (such as fast on-chip memory, not just CPU power [MBOUND]). Special purpose devices may always be possible in theory, but their manufacturing costs should be as high as possible. With the billions of PCs running and millions being produced every day, an emergence of ASICs with a comparable speed/cost ratio is inconceivable.

See [CNS008] for the description of CryptoNote default proof-of-work function.

3.4 Adjustable Parameters

There are many internal parameters in CryptoNote that affect the performance of the system. The size of blocks and transactions is limited in order to prevent a flood attack. The proof-of-work difficulty changes following the hashrate of the whole network to provide nearly constant time between new blocks. Sometimes these parameters need to be changed.

There are two ways of changing the parameters: manual (developers change the parameters with a new software release) or automatic. However, the first option is not suitable for a distributed software, as it is crucial that the values of the parameters are the same for all peers and it is not feasible to make all the peers upgrade simultaneously.

CryptoNote uses adaptive algorithms instead of hardcoded values. New values are computed for each new block on the basis of past data. The values should be adequate to the current state of the system and no one should be able to arbitrarily manipulate these values unless he has the majority of hashrate. Only robust statistics should be used (for example, the median should be used instead of the mean value).

4. Asset Exchange

CryptoNote is an ownership tracking system. It means that the keys can be associated not only with the money but with any digital asset as well. It is possible to create a separate blockchain with its own inner currency and distinct rules. An alternative blockchain can reuse the proof of work from the main one. As a result, both systems will combine their hashing powers for better protection against possible attacks.

Alternatively, a person can use an already existing blockchain as a platform for a public offering. By proving his ownership of some keys and announcing that these keys are now associated with a new type of assets (i.e. company's shares), he can manage these assets within the blockchain. Asset ownership can be transferred privately just like money. The only limitation is that it should not be mixed with another currency or asset; every ring signature must use the keys of the same "color".

The concept of "colors" within a single blockchain can evolve into a system more powerful than just a p2p transactions ledger. By introducing new types of transactions it is possible to create a private decentralized exchange with any type of assets: money, shares, or commodities.

5. References

[BITCOIN] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.

[CNS002] "CryptoNote Signatures", CryptoNote Standard 002, May 2012.

[CNS003] "CryptoNote Blockchain", CryptoNote Standard 003, September 2012.

[CNS004] "CryptoNote Transactions", CryptoNote Standard 004, September 2012.

[CNS006] "CryptoNote One-Time Keys", CryptoNote Standard 006, November 2012.

[CNS008] "CryptoNight Hash Function", CryptoNote Standard 008, March 2013.

[DH] Diffie, W., and M. Hellman, "New Directions in Cryptography", 1976.

[MBOUND] Abadi, M., Burrows, M., Manasse, M., and T. Wobber, "Moderately hard, memory-bound functions", 2005.

[POW] Dwork, C., and M. Naor, "Pricing via Processing, Or, Combatting Junk Mail", 1993.

[TRS] Fujisaki, E., and K. Suzuki, "Traceable Ring Signature", 2007.