NAZA

WhitePaper/EN
Version 0.1.2

Contents

- What is Naza?
- Specifications
- Technology Overview
- Our Mission & Vision
- Roadmap
- Contacts

What is Naza?

- Naza is Naza coin, which is a digital cash For highly-confidential transactions, of which sending and receiving addresses are encrypted and transacted amounts are obfuscated.
- The name of “NAZA” comes from a surname of a person, c.f. https://en.wikipedia.org/wiki/Naza_(disambiguation)
- Not to be confused with NASA and others. They don't matter.

About Naza

- NAZA is created with a high level of privacy in mind, setting Ring Confidential Transactions to conceal sources/amounts transferred and make it high resistance to blockchain analysis.
- NAZA is untraceable; sending and receiving addresses are encrypted, transacted amounts are obfuscated by default.
- It is possible to mine NAZA in its own wallet, facilitating mining for beginners in the world of cryptocurrency. It is worth pointing out that it was not made pre-mining or any ICO.
- Since 08/10/2018, 5% of the coins mined by the official and community pools will be for sponsorship of research of computer science, another 5% finance exchange listing, the development and evolution of cryptocurrency.

Specifications

- Name: NAZA
- Ticker: NAZA
- Algorithm of PoW: CryptoNight V7 Lite
- Difficulty Algorithm: LWMA-2
- Coins supply: 1.8447 billion
- Block target time: 60 seconds
- Address Prefix: "N"

Technology Overview

- CryptoNight V7 Lite
- Ring Signature
- CryptoNight Transaction
- Proof-of-Work
- Difficulty algorithm: LWMA-2
- SendProof Signature
- ChaCha8
- Levin Protocol

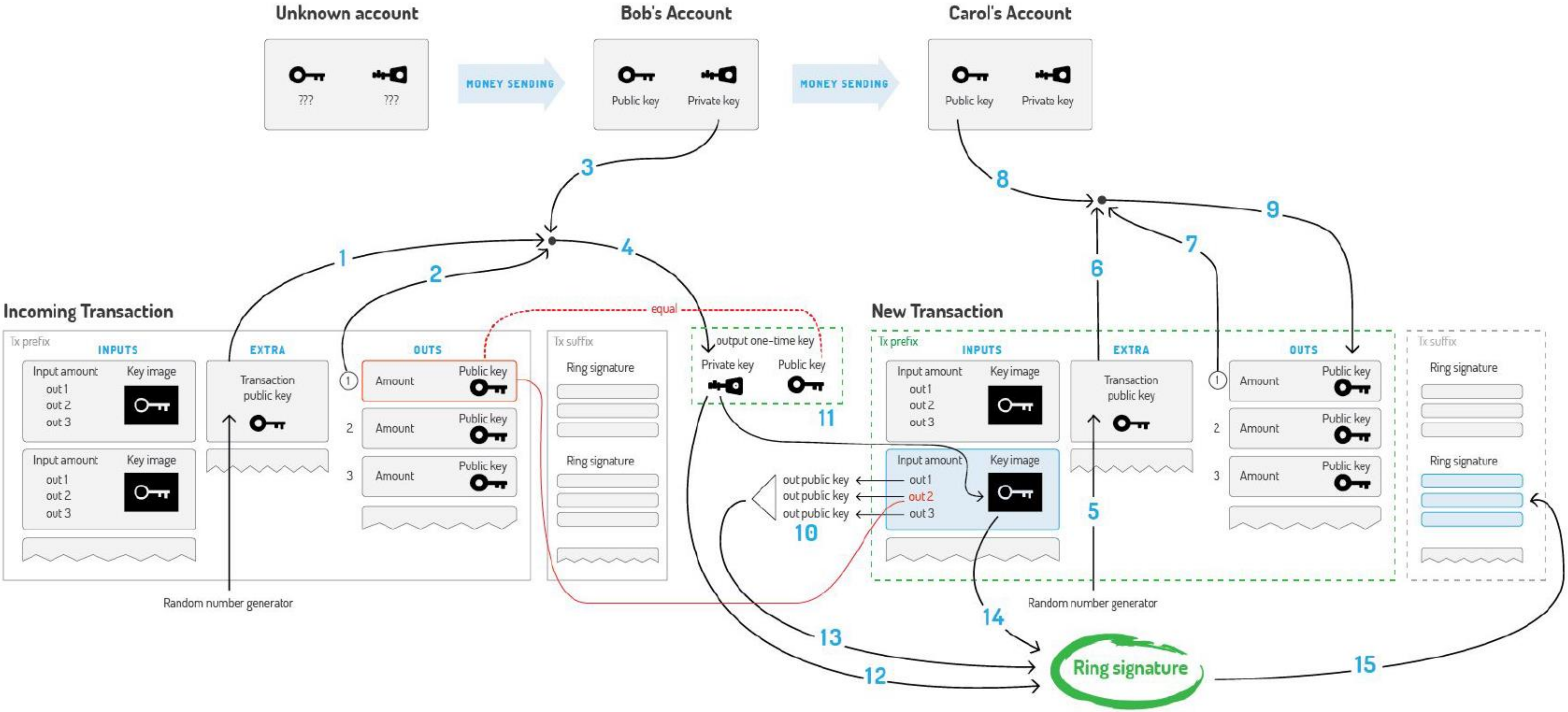
CryptoNight V7 Lite

- CryptoNight V7 Lite is a proof-of-work algorithm. It is designed to be suitable for ordinary PC CPUs, but currently no special purpose devices for mining are available. Therefore, CryptoNight V7 Lite can only be CPU-mined for the time being. CryptoNight V7 Lite was originally implemented in the CryptoNote codebase.
- CryptoNight V7 Lite relies on random access to the slow memory and emphasizes latency dependence. Each new block depends on all the previous blocks (unlike, for example, scrypt).

Ring Signature

- Ring signatures work by constructing a ring of possible signers to a transaction, where only one of the signers is the actual sender. Ring signatures will be mandatory for all transactions (excluding block reward transactions) with an enforced ring size of five. This means that for any transaction there are at least five possible signers, including the true signer. A modified method is used for choosing ring signature mixins, to further obfuscate output distributions.

CryptoNight Transaction

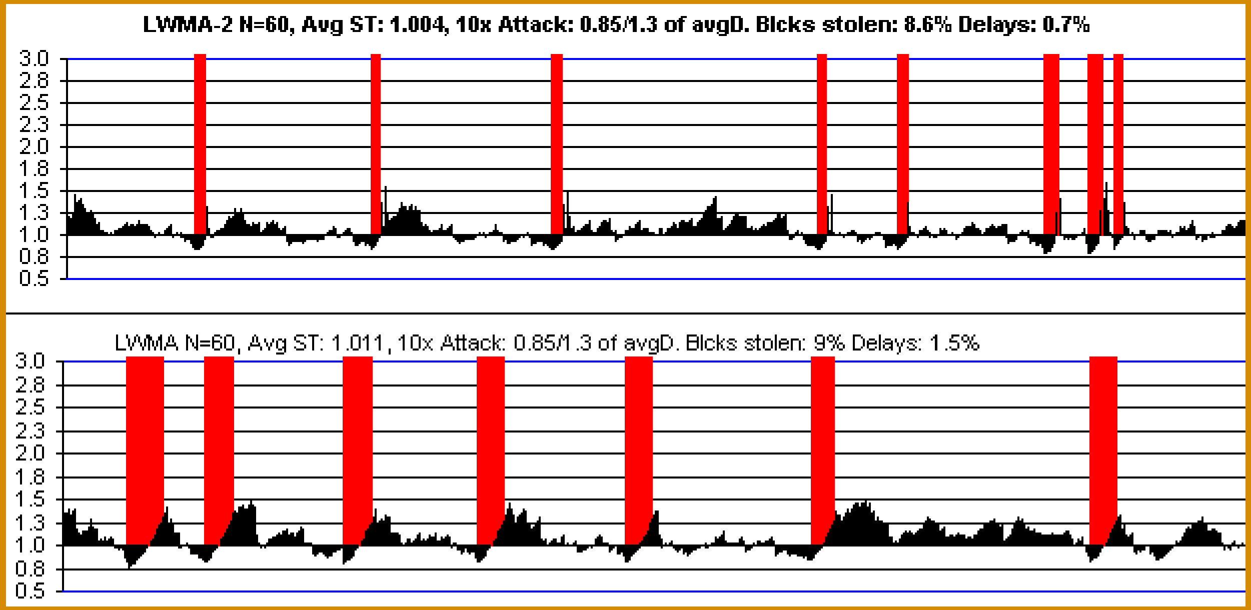


Proof-of-Work

- The proof-of-work mechanism is actually a voting system.
- Users vote on the correct order of transactions, to allow new features in the protocol and for honest distribution of money supply.

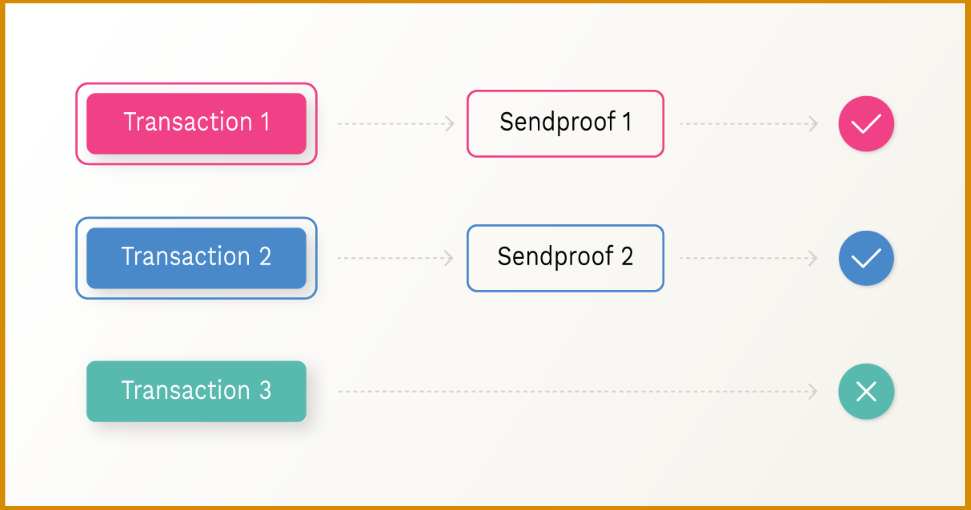
Difficulty Algorithm: LWMA-2

- **Copyright (c) 2017-2018 Zawy, MIT License**
- **https://github.com/zawy12/difficulty-algorithms/issues/3**
- *“LWMA-2 verses LWMA if there is a 10x attack. There's not any difference for smaller attacks. See further below for LWMA compared to other algos.”*



SendProof Signature

- **SendProof Protocol was first implemented by Bytecoin (SendProof Protocol v1.0, July 31, 2018)**
- *"The SendProof signature can be generated by the sender selectively for any subset of recipients without compromising in any way the anonymity of other recipients or other transactions."*



ChaCha8

- **Naza Wallet file is encrypted with ChaCha8 algorithm (Daniel J. Bernstein, 2008).**

- *“ChaCha8 is a 256-bit stream cipher based on the 8-round cipher Salsa20/8. The changes from Salsa20/8 to ChaCha8 are designed to improve diffusion per round, conjecturally increasing resistance to cryptanalysis, while preserving—and often improving—time per round. ChaCha12 and ChaCha20 are analogous modifications of the 12-round and 20-round ciphers Salsa20/12 and Salsa20/20.”*

Levin Protocol

- *By Andrey N. Sabelnikov, https://github.com/sabelnikov/epee*
- *“For the network, we use abstract tcp server, which in turn runs on boost.asio. This server is template class, parameterized with a simple binary protocol LEVIN. The operation of this protocol is organized through the exchange of packets, which are conventionally called the "command" and "notification". "Command" assumes synchronous response, while the "notification" does not imply any synchronous response.”*
- *“An interesting feature of this protocol is that it is bi-directional, i.e. both parties are simultaneously acts as client and as server. At any time, either party can make an command request or notification to the other side. Using of this component looks like RPC - you just invoke remote command and get result.”*

Our Mission & Vision

- Payment for Game, E-Shopping, Publication, Online Video.
- Integration with Anonymous IM, Online Video, Online Music, Copyright of Designs.
- Research Awards Fund for Cryptography, P2P, Protocol, and so forth.

Roadmap

- Naza launch.
- Naza Gui Wallet (Windows, Linux, Mac)
- Mining Pool.
- Block Explorer
- List on Exchange
- Web Wallet
- Mobile Wallet
- Faucet
- Integration with E-Shoping
- Integration with Anonymous IM, Online Video, Online Music.
- Research Awards Fund

Contacts

- Website: https://naza.io
- Email: info@naza.io
- Bitcointalk Thread: https://bitcointalk.org/index.php?topic=4582673
- Twitter: https://twitter.com/AdamJacoby6
- Reddit: https://www.reddit.com/user/nazacoin
- Facebook: https://www.facebook.com/jacoby.adam
- Pinterest: https://www.pinterest.com/aj282/
- Telegram: https://t.me/nazacoin
- Discord: https://discord.gg/QKZ3FGY

NAZA

https://naza.io/

WhitePaper/EN
Version 0.1.2