DERO PROJECT

White Paper

Build it,They will come.

DERO

Author:
DERO Community

Supervisor:
DERO Dev Team

October 2, 2018

Contents

1 SUMMARY

The Dero Project has written a unique new blockchain technology that is based on the DAG and CryptoNote protocol with double spend protection. DERO is a new, experimental blockchain technology written in Golang with a focus on enhanced Privacy and Smart Contracts while maintaining the transparency and security of the blockchain.

The goal is to create a unique state of the art blockchain technology with enhanced Reliability, Privacy, Security, Usability, and Portability by bringing together some of the best proven technologies like CryptoNote Protocol and Smart Contracts, thereby allowing for the creation of Private Smart Contracts.

Blockchain is an open, distributed ledger that can record transactions between two parties efficiently, and in a verifiable and permanent way.

CryptoNote Protocol uses a distributed public ledger that records all balances and transactions of its in-built currency like Bitcoin. Unlike Bitcoin, CryptoNote's transactions cannot be followed through the blockchain in a way that reveals who sent or received coins. The only people with access to the whole set of data about a transaction are the sender or receiver of the transaction.

A smart Contract is a protocol intended to facilitate, verify, and enforce the negotiation or execution of a digital contract. Smart contracts allow for direct contract execution without a third party. These transactions are trackable and irreversible. Smart contracts were first proposed by Nick Szabo in 1994.

For more details about Blockchain, CryptoNote Protocol, and Smart Contract see:

- Blockchain
- CryptoNote
- CryptoNote Specs
- Smart Contract

Some brief examples of what a smart contract is capable of managing without third-party intervention include: access authorization to a physical object like a building or internet-of-things (IoT) devices, asset management,

trading, ticket purchasing, or share distribution. In some instances, an individual or organization would prefer not to reveal the details of the transaction or contract (i.e. participants, amounts, and contract terms) to the rest of the world. Dero brings true privacy to smart contracts for the first time on any blockchain.

Truly private smart contracts are a unique feature offered by DERO that other projects to date (October 2, 2018) do not offer. Dero accomplishes this by keeping all aspects of the transaction, smart contract, and users details private on the original blockchain without the need to trust sensitive or otherwise private information to second layer or off-chain solutions.

2 CHALLENGES

2.1 Identification and know-your-client (KYC)

Having briefly touched upon the need for privacy on the blockchain we must also address the need for some degree of transparency in certain limited situations. Dero will allow thoroughly verified and publicly known certifying authorities to add their signature to individual wallets, and only for those who have applied. This signature serves as confirmation that your identity has been verified by a certifying authority such as a Government, Bank, telecom operator, Visa, Mastercard, or other organizations as required.

When a service provider require verification of your KYC details, similar to what weve seen with exchanges, the process can now be made as simple as using a wallet with the appropriate certification. The service provider, vendor, or payment gateway will only get to see a basic signature that confirms it is authorized to use their services. No personal details are available in these situations. Only certifying authorities will have personal information for individual wallets and only with those who have submitted an application.

In places where KYC compliance is at its most stringent levels, trades would not be possible without pre-authorization from the appropriate authorities. On an individual level, you can choose whom you certify your wallet with, at your discretion. Given the need for robust privacy and security, DERO blockchain has been designed to allow full integration of hardware wallets with biometric protection.

2.2 Voting using safe, secure, and transparent smart contracts

Any organization may use DERO blockchain for a safe, secure, and transparent voting process that also keeps the identities of all voters anonymous in the eyes of the public. This is achieved through a type of private voting smart contract that is only made possible today on DERO blockchain. Aside from Dero, current voting solutions to date operate on public ledgers with public smart contracts that dont obfuscate or shroud your network traffic from identification. Some workaround solutions have been proposed, such as off-chain computations and second layer solutions; however, these solutions leave a number of fundamental flaws that needlessly complicate wide scale adoption of blockchain technology for private voting processes.

To register for the voting process, an individual must apply to the certifying authority with their public Dero address and documentation as required. In this instance, the authority in charge will validate your wallet and allow for one (1) vote or more as defined by the smart contract. The details of such a contract should theoretically be public, transparent, and fully available in any democratic process.

A smart contract of this nature will, of course, require flexibility, and the ability to be reprogrammed to suit the needs of any party that chooses to utilize a private smart voting contract. To that end, the Dero development team is working to keep as much flexibility in the system as possible.

2.3 Asset management: PRIVATE AND AUDITABLE

With Dero, assets can be recorded, distributed, or traded on the blockchain. Perhaps the most critical issue today facing asset management on the blockchain is privacy. Consider for a moment how assets are recorded today. Most assets are recorded in a private or centralized database like you may find at the Department of Motor Vehicles. Organizations or departments often have limited hours, cumbersome access to information policies, and substantial overhead costs. Bringing asset management to DERO blockchain will allow individuals unrestricted use of their own data, by allowing 24/7 access to anything they have stored on DERO blockchain while simultaneously offering unparalleled privacy.

Any individual or organization that choose DERO blockchain for asset management will benefit from the highest levels of privacy by utilizing the

CryptoNote protocol and complete SSL implementation across the entire network, among other critical features. For audits or tax purposes, all you have to do is provide a simple and convenient viewkey that will list all relevant history from the wallet. This view key can be easily programmed into tax software to reduce cost and human error, while insuring accuracy. Its important to note that all details of wallets are entirely hidden from the rest of the network. As such, it is the individual wallet holders responsibility to make their relevant tax information known as required.

2.4 2-Factor authentication: Secure password management and access

Dero plans to integrate one-time password (OTP) authenticators and passphrases. Subaddresses could be used as the username to keep public address information private, and, if required, an OTP will appear in the wallet. An application programming interface (API) and software development kits (SDK) will be freely distributed to service providers for facilitate integration of their existing infrastructure with the Dero blockchain. This will create a significantly more secure environment for the users on a particular service or platform.

2.5 Integration with telecom gateways

DERO blockchain is built in such a way as to allow integration with telecommunication gateways, to send and receive short message service (SMS a.k.a. text) messages. Once your wallet is certified with a telecom operator, you will be able to send text messages that take advantage of the privacy features from the CryptoNote protocol. For example, ring CT signatures are just one of many features used to hide your data. One-time password verified SMS data will be relayed to the appropriate wallet and held completely privately for only the recipient.

3 DERO KEY FEATURES

3.1 CryptoNote privacy

CryptoNote currencies use a distributed public ledger that records all balances and transactions of its in-built currency like Bitcoin. Unlike Bitcoin,

CryptoNotes transactions cannot be followed through the blockchain in a way that reveals who sent or received coins. Dero utilizes all aspects of the CryptoNote protocols privacy features in its new blockchain technology to protect the identities of all parties involved in a transaction.

3.2 Completely SSL/TLS encrypted network

DERO is the first blockchain to have complete SSL in the P2P layer.

The Dero development team has implemented complete TLS across the Dero network which is a first on any blockchain. This encrypts the entirety of our network traffic, which greatly reduces our attack surface, while simultaneously preventing ISPs or other users from analyzing DERO network traffic.

3.3 Scalability and security

DERO is the first CryptoNote blockchain to have 75 transactions per second on its native blockchain without any lightning networks, validators or off-blockchain solutions.

Currently(October 2, 2018),DERO achieved 12 seconds blocktime and 2 minutes confirmation time by using Dero DAG technology introduced in Dero Atlantis mainnet:

DERO-DAG(Directed Acyclic Graph) DERO Atlantis is DERO-DAG based. DERO-DAG is mineable, POW based, fully linear with same level of security as blockchain.No orphans, scalability limits defined by resources(Compute, Network, Storage etc.)

DERO DAG implementation builds outs a main chain from the DAG network of blocks which refers to main blocks (100% reward) and side blocks (8% rewards). Side blocks contribute to chain PoW security and traditional 51% attacks are not possible on DERO network. If DERO network finds more blocks at the same height, instead of choosing one, DERO include all blocks. Thus, rendering the 51% attack futile.

Traditional Blockchains process **blocks as single unit of computation**(if a double-spend tx occurs within the block, entire block is rejected). However DERO network accepts such blocks since DERO blockchain considers **transaction as a single unit of computation**.DERO blocks may contain duplicate or double-spend transactions which are filtered by client

protocol and ignored by the network. DERO DAG processes transactions atomically one transaction at a time.

Client Protocol It handles same transactions mined by two different miners in different blocks mostly due to luck/Network lag.

Optimized Bulletproofs Secure and fast crypto is the basic necessity of this project and adequate amount of time has been devoted to develop/study/implement/audit it. Most of the crypto such as ring signatures have been studied by various researchers and are in production by number of projects. As far as the Bulletproofs are considered, since DERO is the first one to implement/deploy, they have been given a more detailed look.

First, a bare bones bulletproofs was implemented, then implementations in development were studied (Benedict Bunz,XMR, Dalek Bulletproofs) and thus improving our own implementation.Some new improvements were discovered and implemented (There are number of other improvements which are not explained here).

Major improvements are in the Double-Base Double-Scalar Multiplication while validating bulletproofs. A typical bulletproof takes 15-17 ms to verify. Optimized bulletproofs takes 1 to 2 ms(simple bulletproof, no aggregate/batching). Since, in the case of bulletproofs the bases are fixed, we can use precomputed table to convert 64*2 Base Scalar multiplication into doublings and additions [1]. This time can be again easily decreased to .5 ms with some more optimizations.

With batching and aggregation, 5000 range-proofs (2500 TX) can be easily verified on even a laptop. The implementation for bulletproofs is in `https://github.com/deroproject/derosuite/crypto/ringct/bulletproof.go` , optimized version is in `https://github.com/deroproject/derosuite/crypto/ringct/bulletproof_ultrafast.go`.

There are other optimizations such as base-scalar multiplication could be done in less than a microsecond.Some of these optimizations are not yet deployed and may be deployed at a later stage.

Further research/studies/optimizations are in-progress to further improve DERO network.

[1] We do not use Bos-Coster/Pippienger methods

Ultra Compact Blocks Faster block propagation times and low network usage.

3.4 Smart contracts

A smart contract is a digital self-executing contract that is capable of enforcing the terms laid out by all participants in the contract. The goal of smart contracts is to significantly increase contract security while simultaneously reducing costs associated with traditional contracts.

3.5 Atomic swaps

Atomic swaps make the exchange of one cryptocurrency for another possible without the need for a trusted third-party. To prevent one party from failing to send their coins, atomic swaps use something called hash time-locked contracts (HTLCs)[2] to enable a trustless trading system.

3.6 Mobile and offline wallets

As with any currency, multiple forms of storage and varying degrees of financial availability are required. Dero is bringing a complete spectrum of wallet storage options to users by providing solutions that range from mobile wallets on mobile devices to offline 2FA (Two Factor Authentication) biometric identification protected hardware wallets.

3.7 Lightweight wallet

Instead of downloading the entire blockchain, a lightweight wallet connects to randomly selected decentralized nodes to utilize the data stored there. This dramatically reduces the amount of data required to transact on the network while maintaining the security of your private keys on your device, not the node the device is connected to.

3.8 Subaddresses

This technology allows for the creation of additional public addresses for one wallet. This allows a user to differentiate where payments are coming from

[2]https://en.bitcoin.it/wiki/Hashed_Timelock_Contracts

while preventing privacy loss caused by linking transactions to one public address.

3.9 Escrow services on the blockchain

Escrow services may take advantage of DERO blockchain technology by using it as the trusted third party. In this instance, a financial instrument or an asset is recorded on the blockchain and held until the appropriate instructions are given, or contractual obligations have been fulfilled.

3.10 Address signing and certifying

Comparable to the way a certifying authority may issue a passport or drivers license, an individual may receive digital signatures and pre-authorizations that are stored on their individual wallet on the blockchain.

3.11 Voting

Through the use of blockchain technology any group or organization may create a safe and transparent voting system that also maintains complete anonymity among voters.

4 DERO VIRTUAL MACHINE

Smart Contracts on the DERO blockchain will run in a DERO Virtual Machine (DVM). DVM is a Turing complete 256-bit Virtual Machine runtime environment for DERO Smart Contracts with CryptoNote Protocol Privacy and additional modifications. DVM is unique in its ability to execute Smart Contracts while maintaining the privacy and fungiblity of the identities involved in the Smart Contracts. DVM will support the Golang language for writing Smart Contracts with the possibility of Solidity in the future. DVM is in the development phase, and several other features and optimizations are planned which may be added in the future.

5 ROADMAP

Dero Project Roadmap

Dec 2017 · Launch of the Dero project.

March 2018 · Implementation of the CryptoNote Protocol in Golang completed.

April 2018 · Dero mainnet migrates to the Golang implementation.

June 2018 · Dero Atlantis development completed and testnet launched.

July 2018 · Mainnet migrates to Atlantis code base with 12 secs block time and Rocket Bulletproofs.

August 2018 · Application for listings on various exchanges. Marketing and expansion starts in parallel.

Q4 2018 · Smartcontracts/Atomic Swaps on testnet.

Before 2019 · Smartcontracts/Atomic Swaps live on mainnet.

6 SPECIFICATIONS

- PoW algorithm: CryptoNight
- Max supply: 18.4 million for first 8 years, Infinite 157,000 DERO/year
- Block reward: Smoothly varying
- Block time: 12 seconds
- Difficulty: Retargets at every block
- Ticker: DERO

7 DERO BLOCKCHAIN DEVELOPMENT

DERO takes a utilitarian approach to development. From real world examples, use cases, community suggestions, it strives to develop a blockchain that can be deployed and widely used for practical applications. DERO welcomes everyone to participate in shaping its roadmap and technology by contributing directly to code development, proposing new ideas, or submitting comments and suggestions.

Dero has no ICO. A premine was deemed to be necessary for the long term development and success of the project.

There are totally 2 million dero premined.

1 million premine for devs are locked and will gets unlocked at 20%, 20%, 30%, 30% respectively in years 1-4.

Devs premine second year wallet viewkey:

fabe3d21316fc1c9a1fdd3526dc3be2c1e4c3da4faa72b280b
f07500481222792e2237737d01c6a1cd9147afdb3552c84e
016ce06d08bd68e66ff27353a7530f

Wallet viewkey of third and fourth year:

4685a4f7d86ecd6f2493291fdb26329f97ea5e7af48629c12
0dcb175df7c62ac09dd096278efec8df52c531298f5cf73aa
9d6ee722d64521efdf97cf69172505

The other 1 million dero is used for marketing/community growth and project develop.

8 AREAS WILL REFINE CONSTANTLY IN THE FUTURE

- Reducing energy consumption of the network
- Reducing block times
- Increasing transactions per second
- Reducing blockchain sync times and resource utilization
- Reducing blockchain size
- Increasing reliability and security of the network
- Secure hardware wallet with biometrics.
- Regular audits and updates of the core cryptography to negate the benefits of quantum computations.

9 DERO PROJECT Foundation:

Plan to incorporate a foundation which will market, develop, maintain, and expand DERO. Foundation would hire more developers, expand the marketing team, add advisors, and would be representing DERO to the world.

Draft Version, This document will be updated based on community inputs.