DIKO White paper

DIKO is an ERC-20 token facilitating anonymous transactions on the blockchain.

The DIKO token can be used to send and receive money to email address, just like PayPal.

Introduction

Blockchain technology is revolutionary invention capable of transforming the financial lives of millions of people worldwide. Since its invention, the technology has been lauded a force for change due to its ability to transcend borders, governments, censorship, and central control among others. The decentralised governance structure facilitates peer to peer transactions in a trustless manner enabling people to bypass middlemen and organisations such as banks while transacting. This is enabled by the distributed ledger technology with all the transactions recorded publicly and verify by people within the network. For long periods of time, blockchain-based transactions have been thought to be secure, private, and anonymous as there is no central figure and users not required to provide any personal identification information to participate in the public network. All one needs is a string of random numbers that acts as a public key and secretly held private keys used to sign transactions and confirm ownership of coins within the network. However, with time it has been proven that blockchain transactions are not completely anonymous as one's digital footprint such as IP addresses, Wi-Fi connections, and internet activity can be used to link a person to a blockchain address. As such, blockchain transactions are pseudonymous in that one's address on the blockchain is anonymous but their private details can be easily obtained.

Problem

Violation of privacy and personal data has become an issue of concern in the modern digital world. This problem is greatly amplified in the financial world where personal information is of utmost importance in protecting their finances. There is an increase in all manners of financial fraud stemming from personal data security breaches such as identity theft, SIM swaps, and phishing among others.

These have led to billions of dollars in losses to unsuspecting victims.

The finance sector has also become prone to abuse by bad actors engaged in illegal activities like money laundering, drug trafficking, and terrorism among others. In response, several governments across the globe have set up strict laws to regulate the financial sector in an attempt to weed out the bad actors. As such, the finance sector has become synonymous with tough regulations such as Know Your Customer and Anti Money Laundering (KYC/AML). These laws require that individuals and organisations provide proper identification documents for them to carry out any financial transactions. Whereas these regulations have been installed with the best of intentions, they have created a new wave of concern about user data privacy and financial surveillance. Authorities can easily acquire financial data for just about anyone transacting with institutions within their jurisdiction. As such people feel like they are being watched and their freedoms

violated by these laws. Again, the security of the personal information provided to these institutions is questionable with regular breaches occurring repeatedly. The increase in cases of hacking, identity theft, and loss of clients' confidential information not only result in financial losses but are also a cause of concern among customers.

The need for Privacy

The right to privacy is a basic human right across multiple nations around the globe. This right extends to one's financial life with financial institutions required to protect the personal information given to them by their customers.

They are further required to make disclosures and seek the users' permission before sharing such information to third parties or even government institutions. This right has been repeatedly violated and disregarded which has in turn further strengthened the people's need and fight for financial privacy. Sadly, the desire and fight for more financial privacy and protection of one's personal data has been demonised and champions of the cause deemed to have ulterior motives.

In some jurisdictions, this right has even been criminalised with its proponents cast in bad light and thought to be engaged in illegal activities which acts as their primary motivation to champion the cause. Currently, surveillance is at its peak with the government monitoring multiple aspects of its citizen's lives. The practice has been normalised thus allowing acts such as personal finance surveillance to become a normalcy whereas it is a direct violation of one's rights. This persistence government interference in people's lives have given rise to alternative solutions to the conventional systems. As such, the blockchain technology and decentralised systems have come to the fore and serve a critical role in the modern financial world. Their prominence stems from their unique attributes facilitating privacy and shielding their users from the prying eye of governments and other authorities. Moreover, they provide much needed security of funds while serving as fast and cost effective money transfer alternatives in comparison to the existing banking systems. Blockchain based systems also enable instantaneous and permissionless cross-border transactions that help user bypass time, and cost restrictions synonymous with legacy banking institutions.

However, not all blockchains are created equal. Whereas, privacy is a key selling point, not all blockchains can guarantee this as transactions can be traced back to an individual as identity of addresses among many blockchain is pseudononymous. Therefore, there is the need for a blockchain solutions that enable anonymous transactions while at the same time enabling people to send money easily even when they lack technical blockchain knowhow.

The DIKO Solution

DIKO is a privacy focused blockchain that facilitates anonymous transactions on the blockchain. The blockchain will have its own cryptocurrency named DIKO coin that can be used to send and receive money to email address, just like PayPal. At the moment, the DIKO blockchain and coin are in development and set to be launched soon. As such, the DIKO project is currently being run using and Ethereum-based ERC-20 token named DIKO token that serves similar purpose as the native token. DIKO is a private digital currency for secure payment which will be completely decentralized and open for use by anybody from anywhere in the globe. The token seeks to address some openly glaring vulnerabilities among cryptocurrencies in modern times subsequently creating the most secure payment and transaction network. One of the most critical problem that DIKO seeks to address is the lack of confidentiality currently plaguing a host of blockchains. This is of great importance as regulators usually exploit this loophole to pry on the financial transactions of its citizenry. This has become quite prevalent recently as blockchains transactions data is available publicly. DIKO will employ advanced technology that obscures the transaction data thus eliminating the possibility of tracing payments and transactions conducted on the network. DIKO will also feature high level encryption as well as bundling of transaction data to further raise the difficulty of traceability. This is critical so as to facilitate anonymous transactions in a seamless and a highly effective manner.

DIKO is also focused on addressing the insecurity problem that is plaguing some blockchains. We believes that people are entitled to financial sovereignty and sole control over their funds. The DIKO project therefore seeks to create a fair payment system where the users serve as the decision makers in all matters related to their money.

The platform will feature a privacy centred technology enabling the shuffling the details of each transaction such that one cannot identify the source and destination of any payment occurring on the blockchain. This feature will be available for use to all users thus giving them the choice to exercise their sovereignty. Each transaction uses multiple cryptographic signatures controlling multiple outputs to mix with the outputs of the sender. An observer cannot tell which outputs are controlled by which party providing untraceability for everyone included in the ring signature. This will make all transactions anonymous by default thus restoring the users' confidentiality which enables them to spend their funds as they wish. It also removes the complexity involved in making anonymous transactions on most blockchains. This means, a user can display his receiving address publicly yet all payments made to this address cannot be linked to it. This is accomplished with the use of one time use stealth addresses for every single transaction.

Technical application

The DIKO blockchain will use the zero knowledge proof system as the underlying infrastructure to support anonymous transactions. This blockchain architecture is a tried, tested and proven foundation for privacy based coins. Of the different technologies for trusted computation, zero knowledge proof is the most utilized in production. It is the underlying technology for the popular privacy focused coin, Zcash, with its zkSNARK infrastructure running zero knowledge proof based transactions since October 2016. The technology has proven itself as well as its capability to facilitate anonymous transactions as evidenced by the stability of Zcash. So much so that the technology has grown in popularity with several

projects popping up recently from academia, business world and even startups to apply it in their applications.

The zero knowledge proof technology has also been used on layer 2 solutions on the Ethereum network further solidifying its usefulness and viability for privacy based blockchain solutions. Therefore, DIKO will deploy zero knowledge proof system as the foundation for its blockchain. Zero Knowledge Proof systems allow for sharing of encrypted private state to everyone. Parties can submit transactions which include information (encrypted) to transition current state to new private state (encrypted) along with a proof which verifies that such state transition was a valid one.

The DIKO blockchain will process transactions in batches. Batches provide protection against front-running and replay types of attacks. A transfer or a burn proof can be successfully verified only in the same batch that the proof is generated for. To prevent the problem of failed transactions, all transfers will usually be put into pending state for each batch and will only be processed in a future batch whenever the account is trying to spend the funds. This will ensure the security of the entire system and protect users against losses while at the same time preventing any potential double spending of coins.

Token details

Name: DIKO

Token Ticker: DIKO

Total Supply: 20,000,000

Ethereum Based ERC-20 Tokens

ICO Start: April 1, 2020 00:00 UTC

ICO End: November 1, 2020 00:00 UTC

ICO Tokens: 10,500,000

Minimal Goal to start: 2000 ETH

Accepting: ETH, BTC, Fiat

Exchange Rate: 100 DIKO - 1 ETH

Fiat Exchange Rate: 1 DIKO - $2.62