DAN

Internet without limits for everybody

VIEW WHITEPAPER

Intro

Privacy - most people think that this is a given life, but behind the scenes, there is a race, whose participants are secretly trying to penetrate into the privacy of the user as far as possible. Today, Internet users are limited in the use of services and applications due to censorship. It comes to us in many forms. National states are constantly monitoring the Internet traffic to be able to form political profiles of their citizens. In this paradigm, dissent becomes dangerous, and honest political discord in some places is impossible. Similarly, content providers and ISPs have been able to control, track and profile every user on the Internet. Each user's daily Internet activity, communications and habits consolidated and sold to advertisers and, in general, to any willing buyer. These transactions take place with little or no user's conscious consent and with complete disregard for any notion of personal privacy. Access to content is restricted by content providers in certain areas due to intellectual property restrictions or simply because users from those specific locations have low ratings. Today there is still a lack of investment in research, implementation and maintenance of tools capable of restoring the confidentiality of Internet users. These circumstances create a need for protective measures aimed at preserving the open and unhindered nature of the Internet. With the invention and maturity of powerful peer-to-peer computing technologies, such as Ethereum and Bitcoin, it becomes possible to use Blockchain technology in developing mechanisms for evading restrictions. The DECENTRALIZED ANONYMOUS NETWORK team believes and seeks to build a future that respects the privacy of any user, leading to the destruction of existing industries and the creation of new ones in the digital connection in the near and long term. Looking ahead, we expect the DECENTRALIZED ANONYMOUS NETWORK networking platform to be the foundation for a world of open access to content and applications for all citizens of this planet without fear of censorship or someone secretly looking over our shoulder.

Motivation of DECENTRALIZED ANONYMOUS NETWORK

Mission of the company

"Our mission is to build a distributed, reliable and sustainable network that provides open access and privacy to all Internet users.

The Internet in its current state is neither open nor private. At DECENTRALIZED ANONYMOUS NETWORK, we believe that censorship and espionage are unethical and unnecessary forms of intimidation and social control that hinder technological and social progress.

There is a belief that if you need encryption, you must hide something, assuming it is something illegal. Here is a short list of six frequently used and very legitimate uses where strong encryption is a proven solution:

1. Travelers visiting places where their personal email and social network accounts are censored or blocked by local authorities;

2. 2. Reports in your private life about your political, religious, gender/orientation, entertainment preferences that may lead to discrimination or reprisals against you;

3. 3. Businesses that need confidentiality to avoid corporate espionage;

4. Journalists communicating with informants, especially when the source is inside the government or corporation itself;

5. Dissidents and activists need to organize rallies and protests;

6. Protesters and journalists who need to send reports on human rights violations. Ask for help or inform the outside world with the confidence that local authorities will actively try to suppress all forms of communication.

Motivation of DECENTRALIZED ANONYMOUS NETWORK

Mission of the company

In this way, we intend to develop the DECENTRALIZED ANONYMOUS NETWORK as an open and distributed peer-to-peer platform embedded in sustainable incentive protocols, while at the same time taking advantage of the constantly evolving mechanisms for evading censorship developed by the community. Once it developed and released, DECENTRALIZED ANONYMOUS NETWORK technology will allow anyone around the world to both provide and gain access to content and privacy, eliminating censorship imposed by third parties. We have spent a lot of time discussing the ethics of creating DECENTRALIZED ANONYMOUS NETWORK tools to avoid censorship. We believe that the cost of content censorship is not worth the perceived benefits (perceived reduction in crime, increased profits for certain corporations, increased political power, etc.), as these goals can be achieved by other, more ethical means.

Main tasks

Phase I: the development of the decentralized VPN node

Our first goal is complete decentralization of VPN network nodes, using technologies such as VPN and proxy protocols, Blockchain, smart contracts, decentralized databases, token privacy and other tools. We will achieve this goal throughout the development of phase I. At the end of this phase, we will release a fully decentralized and open VPN network with all decentralized functions.

Phase II: the development of DECENTRALIZED ANONYMOUS NETWORK

Our first goal is complete decentralization of VPN network nodes, using technologies such as VPN and proxy protocols, Blockchain, smart contracts, decentralized databases, token privacy and other tools. We will achieve this goal throughout the deOur first goal is to create a protocol capable of "dissolving" user data and sending it deep into the network of DECENTRALIZED ANONYMOUS NETWORK nodes without traceability or censorship. The network will take care of sending this shredded and encrypted data in an unrecognizable form to the receiving end, where DECENTRALIZED ANONYMOUS NETWORK protocol will ensure that this user data reassembled. DECENTRALIZED ANONYMOUS NETWORK protocol will eventually become a combination of different elements, combined into a complete system. Once completed, this protocol ensures that it is not possible to capture user data by third parties.

DECENTRALIZED ANONYMOUS NETWORK aims to be a fully decentralized, peer-to-peer and serverless node network designed to provide methods to restore privacy to its users with financial incentives from its providers (nodes). Once the steps are complete, the network will protect the privacy of users and their data, allowing everyone to share free Internet access with those who need it in exchange for financial compensation in the form of DECENTRALIZED ANONYMOUS NETWORK tokens.

The DECENTRALIZED ANONYMOUS NETWORK network will act as a decentralized market between suppliers and consumers involved in the creation and maintenance of this infrastructure. Consumers will pay for the costs of providers using DECENTRALIZED ANONYMOUS NETWORK tokens. The development of the technology, its capabilities and functionality will take place in several stages to minimize risk, learn from early experiences and benefit from the development of additional technologies.

Main tasks

Phase II: the development of DECENTRALIZED ANONYMOUS NETWORK

We will achieve the decentralization of all functions that ensure network performance by the end of the phase. Participants in the sale of DECENTRALIZED ANONYMOUS NETWORK tokens will have access to tokens that will form the basis for all transactions occurring within the network. The network we create will have opportunities for different levels of development by entrepreneurs and communities after its deployment. The network will also be open to applications that will make censorship less efficient, ways to make payments easier and more efficient, and new network services related to the reuse of infrastructure and protocols developed by our team.

The DECENTRALIZED ANONYMOUS NETWORK market model will lead to the creation of a VPN service that is both competitive and almost infinitely scalable, allowing other entities (e.g. other VPN vendors or application developers) to buy a VPN service from the network by integrating it into their solutions. This competitiveness comes from the open nature of the network and the ease with which anyone can make money by joining it as a VPN provider. Further improvements and new applications will follow at later stages and we will reach a full decentralization by the end of phase 3.

Dynamic of market

Every day bigger and bigger part of our lives transferred to the network, which inevitably creates more opportunities to steal, crack, filter or abuse our data. Research shows that increased data vulnerability is one of the main forces driving the expansion of the Internet privacy and security solutions market:

State law

There is a noticeable tendency for governments to invade privacy. As more and more information about the lives of users is on the Internet, this invasion will only increase.

Western countries get used to VPN services

Currently, the main countries using VPN are in Asia. However, after recent changes in Western governments' policies, the number of people looking for Internet privacy solutions is growing rapidly in the Western world.

The risk of cyberthreats

The number of cyberthreats increases with each year, followed by an understanding of the need for countermeasures. Companies and individuals tend to invest and change their online behavior in response to cyberattacks, leading to a rapid expansion of the VPN market.

The need for freelancers, who securely connect to corporate servers

Nowadays, freelancers done more and more work. Secure connection to corporate servers is becoming more and more important. Small businesses also need a secure connection, but creating their own VPN can be a financial challenge.

Keeping in mind the current world situation and visible trends, people are becoming more and more concerned about their personal life. According to one study, the use of advertising blockers has increased by more than 40% (184 million active users per month). According to the report of Market Research Future project: "The global VPN market is expected to reach $106 billion by the end of 2022, with a compound annual growth rate of 13%.

VPN’s can be used to secure both private and public networks such as Wi-Fi access points and the Internet. Organizations working in the healthcare and telecommunications industries deal with sensitive information that needs constant protection. Hackers are mainly targeting these industries because of the very high price of data on the black market.

Dynamic of market

The need for freelancers, who securely connect to corporate servers

The same study shows that "the world is currently undergoing more than half a million attacks every minute, which will grow due to the spread of high technology. Given these trends (growing demand following changes in privacy policies in many countries, increasing cybercrime and growing dependence on online services), the need to restore online privacy is becoming essential to counter a serious threat to both personal freedom and business security.

Privacy recovery has become a visible global trend around the world. With the development of DECENTRALIZED ANONYMOUS NETWORK will help its users to restore their privacy, ensuring freedom of speech and peace of mind in their personal and business life.

Tokenization

The need for freelancers, who securely connect to corporate servers

DECENTRALIZED ANONYMOUS NETWORK protocol is based on DAN token. At the first and only tokenization of DAN will be created once and in a limited supply, and therefore the total stock of DAN is fixed. DAN will become an integral part of the DECENTRALIZED ANONYMOUS NETWORK network, where service fees will be charged to VPN customers. The largest part of these fees will go to the owner of the VPN code (service provider), and the rest will be dedicated to protocol development and support. These fees will be initially nominated in the DAN, which may be changed in the future. As it mentioned above, the owners of the node will get rewards for their network support. Thus, the node owner will essentially act as a miner and the reward will come in the form of a DAN token. Unlike typical Bluxxaips, the maintainer will get rewards not for his processing power (proof of work) but for sharing his bandwidth. The DECENTRALIZED ANONYMOUS NETWORK Foundation will seek to allow DAN holders to benefit by receiving a commission for each transaction on the DECENTRALIZED ANONYMOUS NETWORK Network with payments made in currencies other than DAN.

Token Destribution

IEO 100.000.000 DAN	Staking Pool 60.000.000 DAN
Airdrop 25.000.000 DAN Will be frozen till 31.12.2020	Team 5.000.000 DAN Will be frozen till 01.03.2021

Price: 0.00000010 BTC

Total: 190 000 000 DAN

Levels of the platform

The DECENTRALIZED ANONYMOUS NETWORK network will consist of four main levels:

1) Decentralized databases; 2) Decentralized service infrastructure; 3) Service providers; 4) Customers.

1. Decentralized service infrastructure and all database levels

DECENTRALIZED ANONYMOUS NETWORK decentralized service infrastructure and database levels provide basic smart contracts that allow DECENTRALIZED ANONYMOUS NETWORK nodes to identify themselves in the network, detect each other and send micropayments between nodes.

2. Service providers

The provider's level consists of nodes that act as providers of VPN services. The provider level consists of nodes that act as providers of VPN services.

3. Customers of DECENTRALIZED ANONYMOUS NETWORK

The level consists of DECENTRALIZED ANONYMOUS NETWORK client applications, which will be developed by DECENTRALIZED ANONYMOUS NETWORK as well as third parties that use DECENTRALIZED ANONYMOUS NETWORK as their VPN service provider.

Structure of DECENTRALIZED ANONYMOUS NETWORK

DECENTRALIZED DECENTRALIZED ANONYMOUS NETWORK is still in the phase of intensive development and will continue to be so throughout the project. Some parts of this section are subject to change.

VPN Technical Overview - the customer service finds and pays for the service providers in the DECENTRALIZED ANONYMOUS NETWORK Network using a smart contract built into DECENTRALIZED ANONYMOUS NETWORK based on identification, service detection and payment services. The network itself operates over the Internet and relies on Blockchain to provide uncensored distributed storage and transaction processing. The DECENTRALIZED ANONYMOUS NETWORK network uses registered identity cards to provide a means of building limited trust when interacting with services and payments.

Any person with an identity registered with the DECENTRALIZED ANONYMOUS NETWORK Network may declare the provision of VPN services (compatible with the network's VPN protocols) together with the payment terms on which the services will be available. Other users of the network will be able to find services that match their specific needs (location, price, etc.) and use the search results to connect to selected VPN service providers and use the announced services. The VPN service consumer and VPN service providers exchange multiple messages to agree on payment terms (e.g. details of service measurement) and technical information required to establish a secure VPN session. During these negotiations, the service consumer will give a promise to pay a certain amount for the services that will be received in advance, and the consumer will update this promise each time an extension of the service is required. The VPN service provider will later use this promise to clear payments with smart contracts on Blockchain. If the consumer's balance in the network deposit account is sufficient, the promised amount of DAN tokens will be transferred from the consumer's deposit account to the service provider's account.

Provision of services

When a client (service consumer) needs VPN services provided by VPN providers in the DECENTRALIZED ANONYMOUS NETWORK Network, he must first select a service that meets his needs. After selecting a service, the customer's identity begins a dialogue with the person providing the advertised service. During the dialogue, the transfer of funds may be promised and VPN service sessions prepared. The dialogue can be launched through existing channels of message exchange between nodes or a new channel can be installed. The dialogue ends if one of the partners stops contacting the other party or any party loses contact with the Internet.

Identification service

There are interconnected software agents (identification agent) representing digital certificates. Each Identification Agent acts on behalf of the person controlling the identity. This software agent is a functional part of the application (DECENTRALIZED ANONYMOUS NETWORK network node) used to connect to the DECENTRALIZED ANONYMOUS NETWORK network to provide or use VPN services. Each agent has access to a digital ID presented by the agent's ability to confirm service in a digital way by signing and decrypting all messages using the private key associated with the ID. The node can have access to several identifiers. Generating public and private keys creates the identity. Identity of confirmation by unique identifier received from public key using last 20 bytes of public key hash. It is possible to share this identity to other users of the Network by announcing its existence by calling a smart identity registration contract on Blockchain. The contract must be provided with an identifier and a public key of identification as an argument. Once the identity contract is successfully fulfilled, the public key of the identity card is added to the Blockchain. At that moment, the added ID becomes a registered ID. All DECENTRALIZED ANONYMOUS NETWORK nodes on the network follow the Blockchain to read the newly registered ID transactions and maintain a local copy of the database of all registered users using the data collected from the transactions. Nodes may use the local copy of the registered ID database to search for public keys associated with other IDs. To check whether messages received from other nodes are valid registered IDs and if they are signed in the correct way the database used by nodes.

Registered value of the identifier

DECENTRALIZED ANONYMOUS NETWORK nodes must attach a predetermined number of values (DAN) to successfully invoke and register an ID registration contract. The amount of value will be automatically adjusted periodically to reflect the DAN value in fiat currencies. In addition, due to the high cost of producing IDs in large quantities, the system limits the impact of several types of trust exploitation. We view registered IDs as something that can be reused for the benefits of the user. By reusing ID for payments, users will have access to their payment history and balances, and their IDs will become more predictable and therefore reliable for service providers.

Service providers who want to provide VPN services and receive compensation for this can announce their services on the network. To announce a service, the provider's node prepares an offer. The offer encodes the format version, the provider's description and the qualitative definition of the service, as well as a list of methods to achieve the node. Then the vendor identification agent signs the offer and the node calls a smart contract to declare the service on Blockchain with the signed offer as an argument. Once the miner launches the contract and adds the offer to the Blockchain, the offer becomes public to all who can read and copy it. The DECENTRALIZED ANONYMOUS NETWORK nodes follow the Blockchain and copy transactions containing the offers from it, marking the Blockchain block number on which they appeared. The nodes then extract the sentences from the transactions and use them to build and locally store a consistent database of all services available on the network.

The nodes may request a locally stored database or a database on other trusted nodes to search for services that match the specific needs of users.

Disclaimer

The information set forth in this Whitepaper may not be exhaustive and does not imply any elements of a contractual relationship. The content of this Whitepaper is not binding for DECENTRALIZED ANONYMOUS NETWORK Group (“Company”) and is subject to change in line with the ongoing research and development of the DECENTRALIZED ANONYMOUS NETWORK Platform (“Platform”) and DECENTRALIZED ANONYMOUS NETWORK Protocol (“Protocol”), hereinafter together referred as “Project”. This Whitepaper does not constitute investment, legal, tax, regulatory, financial, accounting or other advice, and is not intended to provide the sole basis for any evaluation of a transaction on acquisition of DECENTRALIZED ANONYMOUS NETWORK tokens, hereinafter together referred to as “Tokens”. Prior to acquiring the Tokens, a prospective purchaser should consult with his/her own legal, investment, tax, accounting, and other advisors to determine the potential benefits, burdens, and other consequences of such a transaction. Nothing in this Whitepaper shall be deemed to constitute a prospectus of any sort or a solicitation for investment, nor does it in any way pertain to an offering or a solicitation of an offer to buy any securities in any jurisdiction. This document is not composed in accordance with, and is not subject to, the laws or regulations of any jurisdiction which prohibit or in any manner restrict transactions in respect to, or with use of, digital tokens. Certain statements, estimates and financial information contained in this Whitepaper constitute forward-looking statements or information. Such forward-looking statements or information involve known and unknown risks and uncertainties which may cause actual events or results to differ materially from the estimates or the results implied or expressed in such forward-looking statements or information. Tokens are not being offered or distributed to, nor can be resold or otherwise alienated by their holders to, citizens of, natural and legal persons, partnerships, having their habitual residence or domicile, location or their seat of incorporation (i) in the United States of America (including its states and the District of Columbia), Puerto Rico, the Virgin Islands of the United States, or any other possessions of the United States of America, or (ii) in a country or territory where transactions with digital tokens are prohibited or in any manner restricted by applicable laws or regulations. If such a restricted person purchases Tokens, that person has done so on an unlawful, unauthorized and fraudulent basis, and in this regard shall bear any negative consequences.

Disclaimer

The Company doesn't carry on any regulated activity in the Republic of Korea, in the People's Republic of China or in other countries and territories where transactions in respect of, or with use of, digital tokens fall under the restrictive regulations or require from the Company to be registered or licensed with any applicable governmental authorities. Each purchaser of Tokens is reminded that this Whitepaper has been presented to him/her on the basis that he/she is a person to whose attention the document may be lawfully presented in accordance with the laws of the purchaser's jurisdiction. It is the responsibility of each potential purchaser of Tokens to determine if the purchaser can legally purchase Tokens in the purchaser's jurisdiction, and whether the purchaser can then resell the Tokens to another purchaser in any given jurisdiction. This English-language Whitepaper is the primary official source of information about the Project. The information contained herein may from time to time be translated into other languages. In the course of such a translation, some of the information contained herein may be lost, corrupted, or misrepresented. The accuracy of such alternative communications cannot be guaranteed. In the event of any conflicts or inconsistencies between such translations and this official English-language Whitepaper, the provisions of this original document shall prevail.