Diamond Guard

A personal device for securing cryptocurrency at rest and in transit with a built-in decentralized VPN

White Paper

(pre-ICO project)

2017

diamondguard.io
info@diamondguard.io

Version 2 from 15/11/17

DIAMOND GUARD

Table of contents

diamondguard.io
info@diamondguard.io

DIAMOND GUARD

LEGAL DISCLAIMER

PLEASE, READ THE CHAPTER BELOW CAREFULLY. IF YOU HAVE ANY DOUBTS AS REGARDS YOUR FUTURE ACTIONS, WE RECOMMEND YOU CONSULT YOUR FINANCIAL, LEGAL OR OTHER PROFESSIONAL ADIVSER(S) FIRST.

Information below may not be complete and does not intend to form a basis for any form of transaction. In this manual we tried to provide as accurate and full an account as possible. Having said that, this technical manual does not qualify as professional consulting. Diamond Guard does not guarantee and cannot be held accountable for the accuracy or completeness of the information in this White Book. We recommend investors and potential GRD crypto tokens buyers seek professional advise first before making any transactions based on the information in this manual. The manual is published for general information purposes only. Diamond Guard crypto tokens – known as GRD tokens - cannot be used as securities in any jurisdiction. This White Paper is not an offer to sell or a solicitation of any offer to buy any securities in any jurisdiction.

Diamond Guard does not provide any legal advice or opinions of any kind, or any advertising or solicitation with regard to buying, selling or any other operations with GRD tokens. The provisions of this White Paper cannot form a basis of any legal agreement or an investment decision. This book does not oblige anyone to conclude any agreements or enter into any commitments that involve

either selling or purchasing of GRD tokens or any other currency, whether digital or otherwise.

IMPORTANT You neither have the right and nor you should purchase GRD tokens if are a US Green Card holder or a citizen or a permanent resident (for tax or any other purposes) of either the United States of America or Singapore, or a private individual of either the US or Singapore. “A private individual of the US or Singapore” usually refers to a private individual who resides on the US territory or Singapore or any legal body created or registered in accordance of either the US or Singapore legal system. Please note that American citizens living abroad may according to certain provisions also meet the definition of “a US private individual”. GRD tokens cannot be sold on the secondary markets (for example, via exchanging them or via a direct transaction) if you are a citizen, a resident (for tax or any other purposes) of either the US or Singapore, or if you are a US green cardholder.

diamondguard.io
info@diamondguard.io

DIAMOND GUARD

diamondguard.io
info@diamondguard.io

DIAMOND GUARD

General Information

Diamond Guard provides secure means of accessing and managing private and corporate resources (including assets stored in crypto wallets). Our personal device utilizes several solutions to ensure the safety of user's information and cryptocurrency. First of all, the device can be used as a hardware crypto wallet, providing secure and encrypted storage of owner's private keys and perianal identifiable and private data. Other means of protecting user's assets and integrity include wireless router mechanism and decentralized Virtual Private Network (VPN).

This White Paper describes key advantages of using the Diamond Guard personal device. It also provides an overview of the company's business-model and token allocation terms. Diamond Guard crypto tokens are distributed among an unlimited number of participants during the emission period.

DIAMOND GUARD

Problem Description

Cybercrime is one of the most salient problems in today's world. According to data collected by Jupiter Research, cybercrime cost the global economy $1.5 trillion in 2015. By 2019 losses due to cyberattacks are projected to reach $2 trillion.

Small and medium businesses are more vulnerable to cybercrime than larger firms. More than 50% of companies employing between 100 and 1.000 people have been victims of cyberattacks. The cost of an average cybercrime is estimated at $879.582.

It is not just corporate users that remain vulnerable to this type of attacks. Regular Internet users, too, do not pay enough heed to cyber risks. Research by Symantec found that 87% of internet users connect to Wi-Fi without using any additional devices. Revealingly, 60% are confident that in doing so they do not endanger their personal data.

Technical progress creates new vulnerabilities, while exposing those that already exist. While the rise of blockchain technology has led to an increase in demand for various cryptocurrencies, a private key is the only element that guarantees the security of owner's assets. Yet private key is usually stored on the owner's personal computer used for everyday activities, including for Internet access. This situation has led to a rapid rise in the attacks on crypto wallets that are stored as usual files on personal computers.

Seen in this context, anonymity, one of cryptocurrencies' core strength, also becomes its principal vulnerability. Cryptocurrency is easy to steal; but it is hard for the victim to prove one's ownership of one's assets. At the start of 2016, the US Federal Trade Commission registered more than 2.600 cases involving cryptocurrency theft. The majority of such incidents actually go unreported. According to Coinbase, a digital currency exchange, the problem of cryptocurrency theft is most widespread in the United States. The number of this kind of cyberattacks grows by 100% every year.

Hackers often launch targeted attacks on users' personal computers to steal authentic data in order to get access to their accounts. It is estimated that antivirus products miss 90% of this type of attacks.

Indeed, some types of malware are almost impossible to trace and 'can' hide on user's device for a long time. But when the user authorizes his or her access to the network via a security token, the virus will quickly overlay a fake transaction page that will lure the victim into providing a digital signature to conduct wrong transaction instead of the one he or she originally intended. The fraudster can also conduct various transactions using owner's assets without it actually appearing on the screen.

Another problem with hard tokens is their inconvenience. For one, hard tokens are not compatible with both stationary and mobile devices. Additionally, they cannot incorporate many important security features like, for example, biometrics or GPS.

DIAMOND GUARD

Finally, many users face mounting difficulties when trying to protect their anonymity on the Web. Many content and Internet providers are becoming too restrictive in their objective to monitor, track and profile every user online.

To sum up, several tasks need to be implemented if working with cryptocurrency is made safe:

1) providing a safe and secure access to crypto wallets;

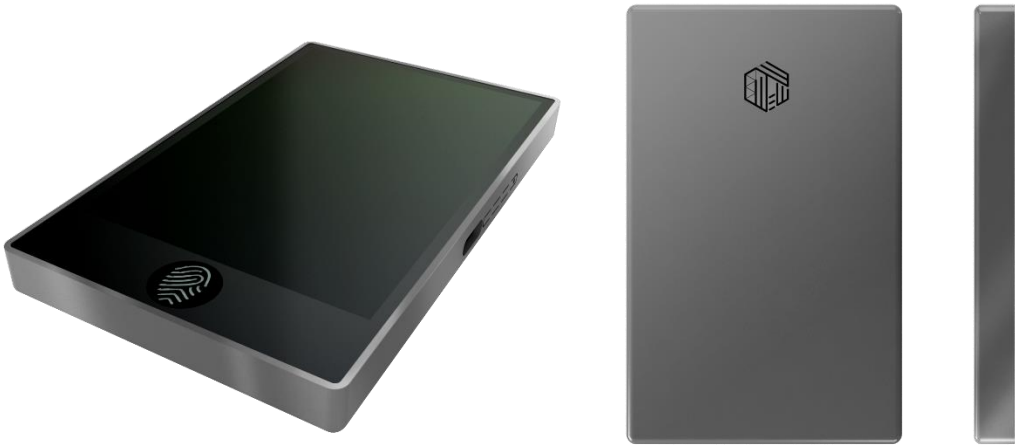
2) mitigating hardware tokens' exposure to targeted cyberattacks;

3) making sure hardware tokens are convenient to use and are compatible with both stationary and mobile types of devices;

4) guaranteeing user's anonymity when using the Internet.

Solution

To implement the aforementioned tasks our company has come up with three solutions that are available on a single device. Meet Diamond Guard: a secure and convenient hardware crypto wallet that can also provide a decentralized VPN connection.



Diamond Guard is a wireless device that allows owner to create trusted VPN networks. It caters to different needs and is compatible with both stationary and mobile devices.

Diamond Guard has several features to guarantee security of its owner's data. To begin with, Diamond Guard allows encrypting and storing user's private

keys as well as identification and private information. This is achieved through multifactor authentication system. Thus, the only way to access the data on the device involves passing both the fingerprint-identification system and the device's digital checks (login and password). Additional security control forces user to press a special button on the device to confirm vital transactions (including cryptocurrency transfers) or when accessing private keys.

All cryptographic operations on Diamond Guard take place in a protected environment that is isolated from input-output interface. That guarantees that the user is fully protected from untrusted environment that can be contaminated with malware. It also ensures that the functions of security and daily Internet activity are kept separate, thus limiting the possibility of a hacker launching a cyberattack.

In addition to having a USB type C interface, Diamond Guard supports wireless means for exchanging data, including Bluetooth, WiFi and LTE. That means that the device's encrypted storage can be accessed via any mobile device (albeit with the owner's endorsement). Moreover, Diamond Guard can serve as a VPN node and a firewall.

Diamond Guards makes it necessary for the owner to approve any transaction that requires his or her digital signature by pressing a physical button. That, in turn, makes it impossible to sign any digital document without the device's owner knowing about it. The system also guarantees that only a registered user can gain access to the owner's private keys. Furthermore, the option of secure

VPN connection will make sure the user is protected from the man-in-the-middle type of attacks.

Additionally, Diamond Guard also allows secure multiparty computation that requires trusted network via an open API connection. Using trusted isolated computer environment is necessary if the risk of any data breach during computation (e.g. injection of the wrong code) is effectively tackled.

These security features open possibilities for Diamond Guard's corporate users. For example, a bank can make ask us to install online banking software where access to users' account is only possible in a trusted environment isolated from input-output interface (as is the case with accessing owners' private keys on Diamond Guard). This, in turn, will guarantee that the accountant has transferred the funds to the correct recipient.

Diamond Guard's unique selling point is its multifunctionality. One compact device offers its users many advantages at once:

1. It does not require any drivers or special software to connect to computers, smartphones or tablets;

2. It uses the fingerprint authentication to enhance security;

3. It collects the user context data through GPS and GLONASS systems allowing the owner to disable Diamond Guard's functions if it has been accessed from an unauthorized location;

diamondguard.io
info@diamondguard.io

DIAMOND GUARD

4. It supports wireless connection and is highly convenient to use with other devices;

5. It provides VPN connection that allows user to establish a trusted wireless network;

6. It ensures safe storage of cryptocurrency;

7. It provides secure, encrypted storage of user's private keys, personally identifiable information and his or her private files (Documents, presentations etc);

8. It supports the proxy signature digital scheme whereby any transaction is visualized in an isolated environment;

9. It allows users to mint GRD coins;

10. It provides opportunity for trusted computing via the Trust Zone technology;

11. It can be used for One-Time Programmable (OTP) operations;

12. It has the high-throughput processor and is highly effective when working with large files;

13. It can be used as OTP token;

14. It supports the remote wipe feature that allows user to send a command to a computing device and delete data;

15. It deletes the data automatically if device's case is physically opened;

16. It has file parser;

17. It is compact and can fit into user's pocket.

Key Functions

Protecting confidentiality

Problem Threat of data theft and compromise of personal information.

Solution Data encryption and guaranteed destruction of data in case of imminent malware threat or if the device has been opened up.

Problem Exposure to unsecured networks and malware.

Solution Establishing secure and trusted computation environment through task parallelism (using a separate CPU for each thread on the same data). Diamond Guard also offers hardware solutions prohibiting unauthorized code execution.

Problem Targeted and mass hacking attacks.

Solution Protecting user from the man-in-the-middle type of attacks via using VPN.

Safeguarding privacy

Problem Risk of audio interception and online traffic interception.

Solution Set up protected VPN connection disguised as SSL/http traffic.

diamondguard.io
info@diamondguard.io

Problem Tracking user's location and network restrictions imposed by provider.

Solution Using anonymous network that randomly allocates the number of intermediate nodes, with Diamond Guard devices acting as those nodes.

Problems Danger of owner's device being blocked and threat of a denial-of-service type attack on servers.

Solution Using self-organizing and decentralized VPN.

Private keys protection

Problem Loss of private keys as a result of contracting malware.

Solution Multi-factor authentication system for protecting private keys that includes hardware, digital and biometric mechanisms. Making sure user's private keys can be stored exclusively on Diamond Guard. Equipping the hardware crypto wallet with its own private processor.

Problem Mobile devices require different methods of protection than stationary ones.

Solution Diamond Guard is compatible with both stationary and mobile devices. It also has its own screen to visualize key operations with data.

Problem Danger of faking signature queries via software driver.

diamondguard.io
info@diamondguard.io

Solution Diamond Guard has a verification system and requires the owner to physical confirm any transaction.

Cryptocurrency protection and mining

Problem Existing crypto wallets are vulnerable to malware.

Solution Storing cryptocurrencies in a hardware wallet.

Problem Using existing devices for working with cryptocurrency is fraught with risks. To initiate any operation requires user having a trusted system as well as a secure communication channel.

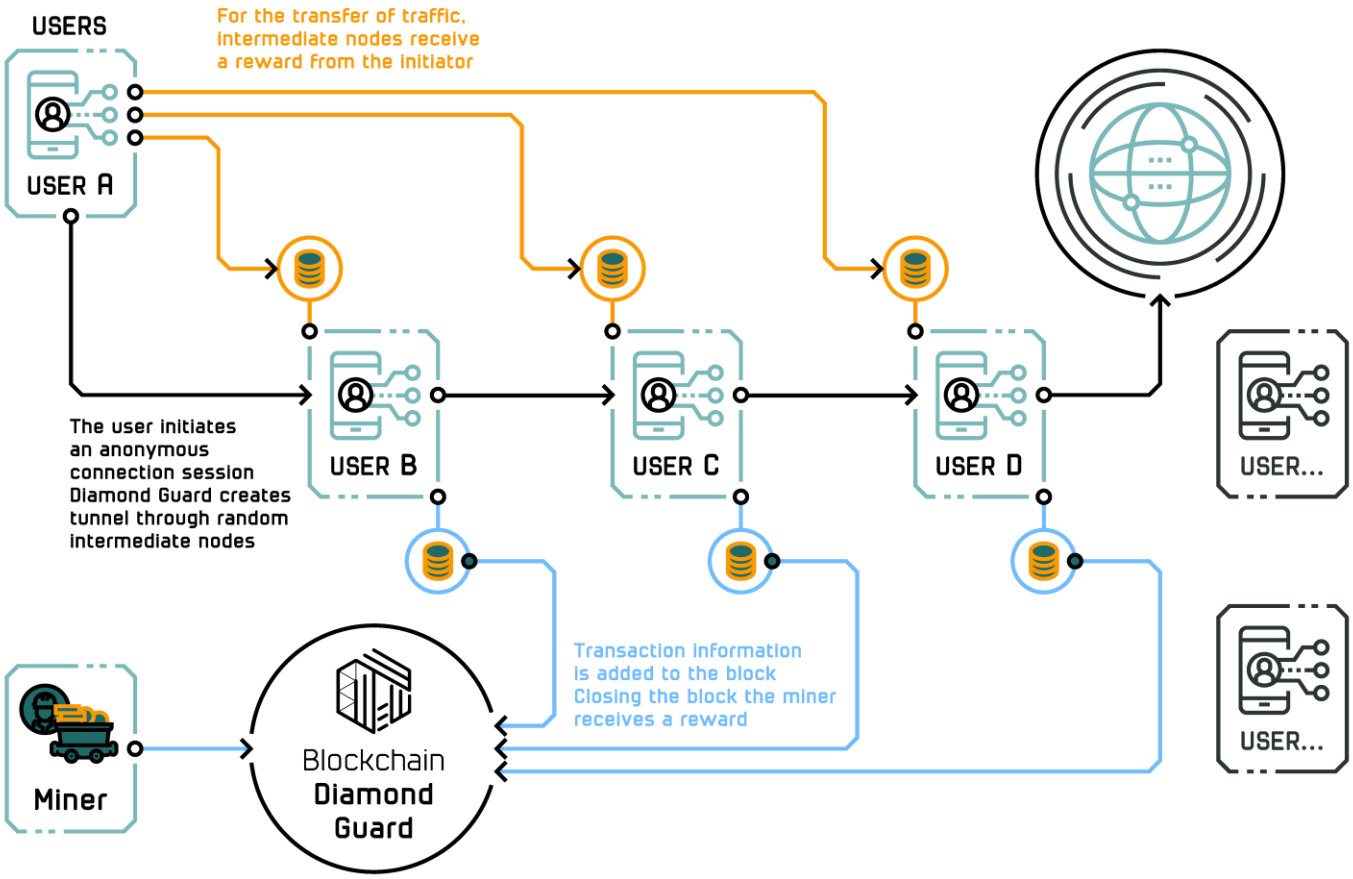
Solution Providing user with a safe computation environment and secured communication networks.

Problem Low return on investment in devices that provide for secure storage of cryptocurrency and operations with it.

Solution Opportunities for cryptocurrency minting and receiving payments for providing other users with VPN traffic through Diamond Guard device.

diamondguard.io
info@diamondguard.io

DIAMOND GUARD



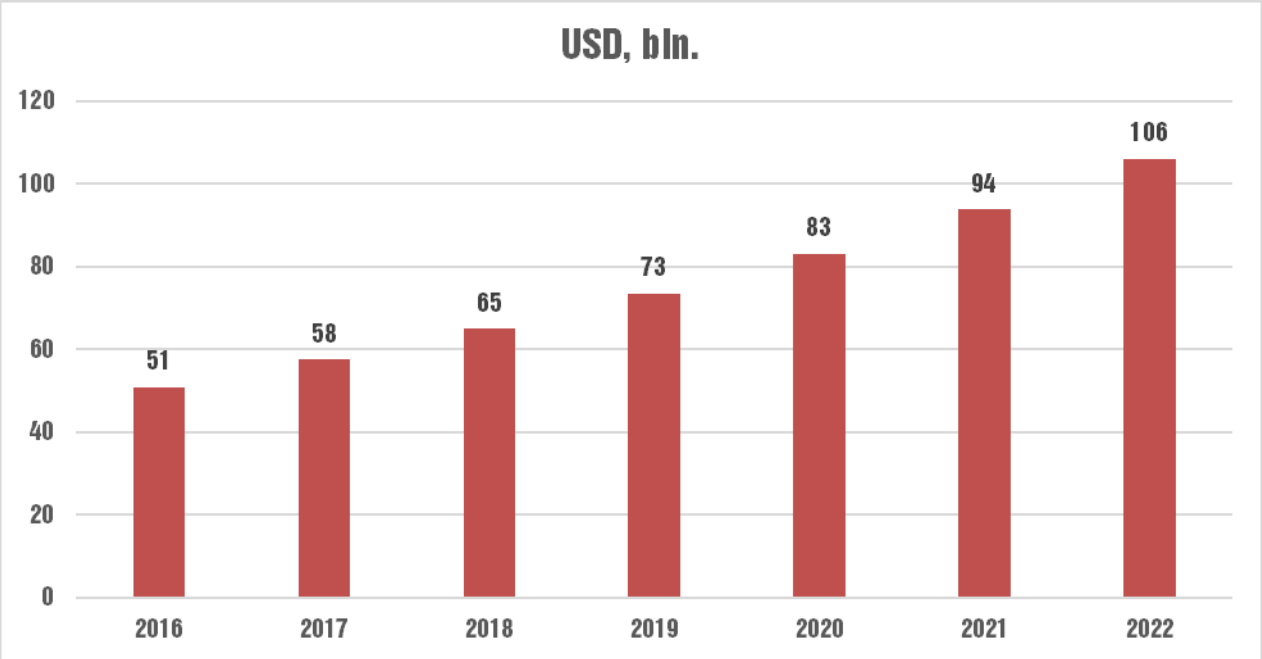
diamondguard.io
info@diamondguard.io

DIAMOND GUARD

Market

Countries: United States, Europe, Russia, China, Latin America, Asia.

Global VPN services market is projected to reach $106 billion dollars by 2022 with compound annual growth rate of 13% (Market research future).



The total market capitalization of cryptocurrencies market continues to grow by 150% in annual terms and reached $170 billion in September 2017. According to the Cambridge University study, between 5.8 million and 11.5 million crypto wallets are estimated to be currently active. That figure has increased substantially from 2013. Then the total number of active wallets was estimated at between 0.26 million and 2.6 million. Taking into account the industry's rapid growth, one thing

becomes clear: tens of billions users remain highly exposed to security risks during manipulations with cryptocurrency.

Global hardware token market is also growing. It is expected to reach $2.1 billion by 2018.

We look forward to offering our product on the international market. Our goal is for Diamond Guard annual sales volumes to reach $10-18 million two years after launching the project.

Business model

Monetization

There are two sources of monetization:

1) Device sales
2) Commission received from minting GRD tokens

Expenses

At first, the main expenses will comprise the costs incurred when developing the product. This includes salaries for the programs, the engineers, the designers and the testers.

After a Minimum Viable Product is built, there will be a need for additional expenses pertaining to marketing and the costs of maintaining infrastructure.

Subsequently, about a third of all expenses will be consumed by marketing needs. The rest will be spent on Research and Development, maintaining infrastructure and operating costs.

DIAMOND GUARD

Team

Our team has worked together since 2009. Our main expertise lies in the areas of cybersecurity and mobile app development. We have also worked with individual orders, designing custom hardware and software solutions for specific needs of various clients.

At the moment we are registered in Singapore as “QUASAR SYSTEMS SG PTE. LTD.”, 16 Raffles Quay, #33-02, Hong Leong Building, Singapore 048581. In future we are planning to organize a spin-off in the same jurisdiction.

MARIA ATAMANOVA

CEO, FOUNDER

In charge of overall management and operations

Maria has more than 6 years of experience as manager of managing large IT companies. She has worked as adviser to startups in Russia and abroad. Maria is a founder and CEO of Cleverbits, a company that provides a platform for mobile app development.

DIAMOND GUARD

ALEXANDER MAMAEV

CVO, CO-FOUNDER

In charge of long-term corporate strategy and market positioning

Alexander holds a PhD in computer science and has more than 9 years' experience in working in the IT and cybersecurity industries. He is a former chair of Cybersecurity and Discrete mathematics at National Research Nuclear University MEPhI, a Russian university. Alexander also acts as technical adviser to several startups and is a CEO of the Digital Forensics Laboratory.

EVGENY MEDVEDEV

PR DIRECTOR

In charge of brand promotion and media contacts

Evgeny has many years of journalistic experience behind him, having published over 1.000 articles on various topics, including foreign affairs and

Russian politics. Evgeny worked for the leading publications in Russia, including RBC business daily and Forbes magazine. He had previously taken part in various PR campaigns and special projects.

In our team we have five more people which are responsible for developing, testing, marketing and selling the company's products.

Advisers

Information on advisers supporting our project is published on the website www.diamondguard.io in the appropriate section.

DIAMOND GUARD

Development Roadmap

NOVEMBER 2015

Diamond Key's first version – a hardware wallet for storing user's private keys – was created

MARCH 2016

Diamond Key found initial popularity among customers in energy and financial markets.

SEPTEMBER 2016

Relying on internal investments, developers managed to create the Diamond Key prototype that could perform several key functions at once. VPN decentralized technology in the works.

FEBRUARY 2017

Diamond Guard project launched. Identifying and refining the target market.

MAY 2017

DIAMOND GUARD

Development of Diamond Guard's product line started.

JUNE 2017

ICO fundraising preparations began.

DECEMBER 2017

ICO launch. The company aims to raise $30 million. Preparing Diamond Guard.

APRIL 2018

Launch of the Diamond Guard prototype that can support the key functions. Start of BETA device testing and audit.

JUNE 2018

Launching Diamond Guard mass production. Developing the blockchain for minting the GRD token.

AUGUST 2018

First batch of Diamond Guard devices is shipped to customers.

GRD Token Creation Details

On the Crowdsale stage we will use “GRDe” tokens created using Ethereum platform via smart contract. On the next stage we will launch Diamond Guard blockchain with “GRD” token, based on the Graphene technology.

“GRDe” will later migrate to “GRD” in 1:1 proportion.

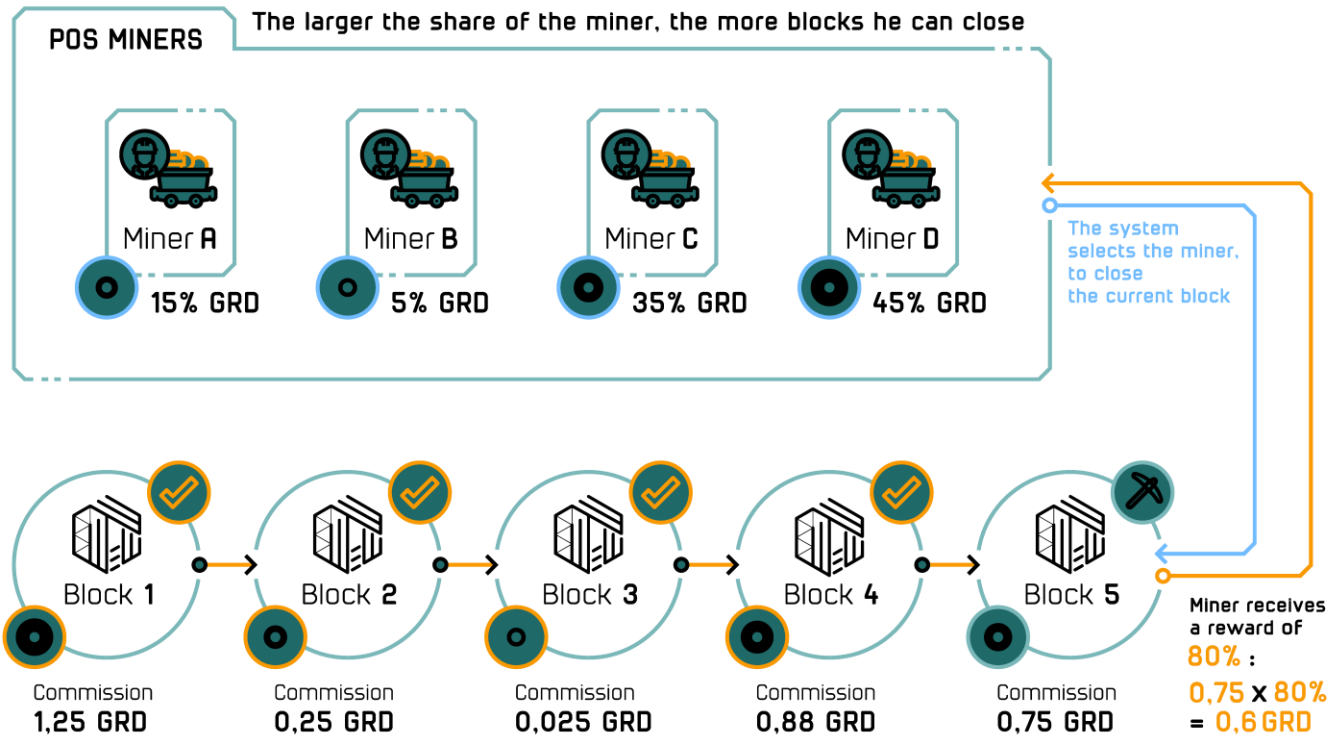
The «GRD» token is a digital asset compatible with the Diamond Guard-type products.

Standard: ERC20. Additional emission will not be provided. Legacy token type - utility token: the GRD token is a digital asset that can be used to buy Diamond Guard devices or pay for VPN traffic.

GRD tokens use the Proof-of-Stake (PoS) algorithm to manage transactions. Each validator owns some stake in the blockchain in the form of GRD tokens and is rewarded for ownership of currency. The more of these tokens the validator has, the more blocks he or she has the right to process. Validators receive 80% from each transaction fee paid in GRD tokens.

Becoming validator is simple. It requires user to use Diamond Guard or download the «Diamond Guard Wallet» application from the official website and log in using individual login and password.

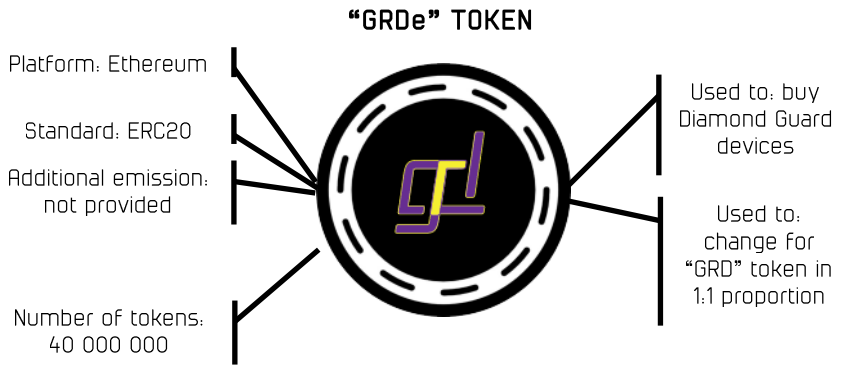
The total supply of GRD tokens is fixed at 40 000 000.

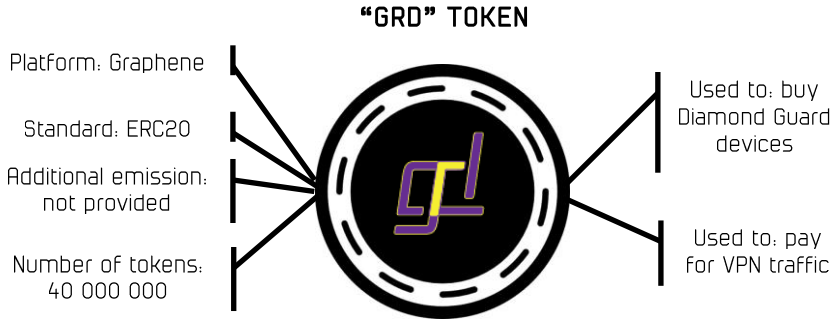


The GRD token does not provide its holder with the right to take part in managing the company. Neither can GRD be used as a security. At the same time GRD token holders will get a vote on any changes pertaining to Diamond Guard blockchain. Each holder's vote share will be proportional to the number of tokens he or she has.

diamondguard.io
info@diamondguard.io

DIAMOND GUARD





diamondguard.io
info@diamondguard.io

ICO Terms

Token sale will occur in two phases: pre-ICO and ICO.

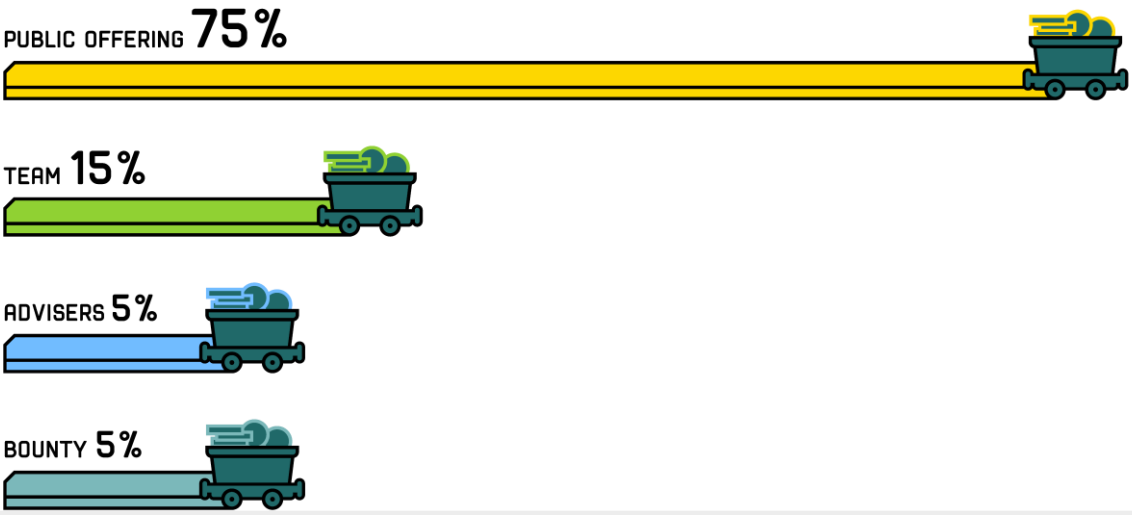
Applicants who want to buy GRD token will need to undergo the KYC procedure.

The amount of coins received by potential buyers will be proportional to the sum they paid during pre-ICO and ICO.

Token's price during pre-ICO will be set at 0.001 ETH per token unit or its BTC equivalent.

GRD Token's price during ICO will be announced earlier than a month before the ICO start. The token's ICO price will not amount to less than three times its pre-ICO value.

Post-ICO bounty pool allocation:



Bonuses:

• Day 1: +25% bonus tokens;

• Day 2-7: +20% bonus tokens;

• Week 2: +15% bonus tokens;

• Week 3: +10% bonus tokens;

• Week 4: +5% bonus tokens;

• Week 5: 0% bonus tokens.

Bounty campaign:

• Facebook campaign: 10% of total reward;

• Twitter campaign: 10% of total reward;

• Bitcointalk signature campaign: 15% of total reward;

• Diamond Guard network discussion – 10% of total reward;

• Translation services pertaining to Bitcointalk campaign: 15% of total reward;

• Reward for special support: 40% of total reward.

The membership in bounty campaign is rewarded with blockchain tokens during an ICO. After the ICO is finished, 75% of the tokens will be sold go to open

diamondguard.io
info@diamondguard.io

sale. The remaining 25% will be allocated among founders, consultants and bounty campaign members in accordance with the aforesaid scheme.

Information disclosure

To ensure the transparency of our team's activities after carrying out the crowdsale and increasing the confidence of the buyers of the tokens "GRDe", the principle of publishing quarterly reports revealing information about work on the product will be implemented. The auditor will be selected after the end of the crowdsale by voting among the holders of the tokens "GRDe".