Table of Contents

Motivation ................................................................................................................................. 3
SISHUB’s Vision ......................................................................................................................... 5
STEEL Ecosystem .................................................................................................................... 5
Anonymous STEEL Messenger .................................................................................................. 5
Free mode ................................................................................................................................. 6
Pro mode ................................................................................................................................. 6
Premium mode ......................................................................................................................... 6
Decentralized STEEL Network for secure data exchange ......................................................... 7
Cryptocurrency STEEL Wallet ............................................................................................... 7
SISHUB Blockchain Network ................................................................................................. 7
Decentralized Complex STEEL Antivirus Solution .................................................................. 7
STEEL Ecosystem’s Benefits .................................................................................................... 7
Complete Anonymity .............................................................................................................. 7
Ultimate Privacy ..................................................................................................................... 8
Superior Security .................................................................................................................. 8
High Usability ........................................................................................................................ 8
STEEL Token ........................................................................................................................... 9
Technical considerations ....................................................................................................... 9
Hybrid Peer-to-Peer Tor Network ........................................................................................... 9
PGP encryption ......................................................................................................................... 10
AES encryption ....................................................................................................................... 11
CBC encryption mode ............................................................................................................. 12
DSA Algorithm ....................................................................................................................... 12
HMAC .................................................................................................................................. 12
Building an Audience ............................................................................................................ 13
STEEL Roadmap .................................................................................................................... 13
STEEL Token Issuance .......................................................................................................... 13
Distribution of proceeds ........................................................................................................ 14
Distribution of tokens ............................................................................................................ 14
Token distribution event ........................................................................................................ 15
STEEL Team ............................................................................................................................ 16
Lead Advisors ........................................................................................................................ 22
Main Developers .................................................................................................................... 24

Email: info@sishub.network
Website: www.sishub.network
**MOTIVATION**

In just three recent years, the number of internet users increased by about 40% while 90% of the data on the internet has been created since 2016. Given even more data moving online with the Internet of Things, the amount of information on the Internet will expand exponentially.

Welcome to the era of knowing when we continue to digitize every aspect of our lives and finally realize that our privacy has critical value in a robust information society. We all have information we want to keep to ourselves, and since most of our communications take place online, we should take measures in order to protect it from prying eyes.

If you have been following the news, you’ve probably heard plenty of stories about privacy breaches, information leakage, cyber attacks and such. Last year was monumental for data breaches: in 2017, the number of data records compromised in publicly disclosed data breaches surpassed 2.5 billion, 88% up from 2016.

Anonymity, privacy, and security are central concepts in the online world, and if you don’t take them seriously, credit card numbers, confidential documents, personal photos are just a few of the things you can say goodbye to.

In fact, online safety needs different measures depending on your goals and activities. However, privacy, anonymity, and security have been reduced into a big mess of blurred lines and unclear definitions. So let’s first define these basic concepts so we can tell them apart:

**Privacy** is concerned with the collection and use of personal data. So when the internet giants gather your private information without your knowledge and sell it to advertisers at a mass-scale, they definitely compromise your privacy.

**Anonymity** is not just a poorly understood aspect of privacy. It is one of the amazing gifts of the internet that enables people to express their opinions and ideas without fear. Keeping their true identities under the safeguard of anonymity, people can confidently
discuss their bosses or spouses, challenge political authority, attack organized crime, and come forward with inconvenient facts and truth.

**Security** is a broad concept that encompasses different mechanisms, which guard our privacy and anonymity against unwanted intruders. Security can include network protection, authentication, and data encryption to name just a few.

International cyber wars, endless successful hacking attacks, and huge losses have become a modern threat. There is a constantly growing number of hacking of mobile devices, social media accounts, and private emails. According to the trend of the recent years, the number of attacks will increase by at least 50% in 2018 compared to 2017.

**Number of global data breaches pertaining to identity theft from 1st half 2013 to 2nd half 2017**

Since we become more reliant on online transactions concerning private information or money, these issues evolve into vital as we have much more to lose. Problems of privacy, anonymity, and security center on you having control over your private information and online activities.

On the one hand, it’s important for all of us to become more educated on these issues and to act on them while on the other hand, the challenge is to create anonymous, private, and highly secure solutions that can be easily adopted into everyday life.
We need to make privacy, anonymity, and security simple, ubiquitous, and understood by all. Only then will we be able to allow our innovative world to develop and prosper in safety and freedom.

**SISHUB’S VISION**

We believe that blockchain technology and blockchain-based solutions can become the answer to the challenges of privacy, anonymity, and security.

Unlike the traditional centralized platforms, which make for an extremely easy collection of private information, decentralized blockchain-based systems present the ideal solution to taking back control of your private data, because information passes through a variety of points, and it's much more difficult to track it across the network.

Decentralization provides us with the opportunity to control own identity and share private data without powerful mediators supervising information and money flows.

Security Intelligent Systems Ltd (SISHUB) is proud for bringing a new game changer solution -- a decentralized anonymous STEEL Ecosystem, which is designed to create a single solution for highly secured data sharing, messaging, and payment transactions.

The STEEL Ecosystem simultaneously offers the best guarantees of privacy, anonymity and security due the use of a decentralized block chart, blockchain technology, hybrid Tor network, and implementation of PGP encryption, which after 20 years has proven its superb capability of protecting that inherent right for privacy and freedom online.

This is what makes the STEEL Ecosystem a completely anonymous and safe environment. Our solution allows exchanging confidential information online with clients, colleagues, patients or friends in a completely secure manner.

The STEEL Ecosystem contains the anonymous STEEL Messenger, the decentralized STEEL Network for secure data exchange, cryptocurrency STEEL Wallet, own SISHUB blockchain network and decentralized complex blockchain-based STEEL Antivirus software for desktop and mobile devices.

**THE STEEL ECOSYSTEM**

Considering all your needs for confidentiality of business and personal correspondence and private data, the STEEL Ecosystem provides a decentralized peer-to-peer network controlled by no one and incentivized by the STEEL token.

**Anonymous STEEL Messenger**

Aiming to keep users’ one-to-one and group communication reliably private, we present the STEEL Messenger, which main appeal is the full anonymity it offers. The design parameters we’ve selected suggest a messaging system that ensures strong security properties.
These are the main features of the STEEL Messenger:
1. Enabling the node function.
2. Built-in wallet to store and exchange tokens and cryptocurrency.
3. Desktop synchronization.
5. Audio calls (encryption with the AES algorithm).

Since the STEEL Messenger uses PGP encryption system, it will provide privacy and security on a level unapproachable by any other existing messenger. The PGP encryption process, including the keys sharing, is automated while the users need only to set their own priorities for speed and security matters, choosing from the following options:

- **Free Mode**
  - Maximum speed
  - Centralized system
  - PGP encryption
  - Invisible texting
  - Saving messages for messages history
  - Creating private groups
  - Free-of-charge mode

The message is self-destructed by default in 7 days after it was delivered to a user or a private group (unless the user sets the automatic timer for the destruction at the set time).

To switch to the Pro or Premium Modes, the user will enter a PIN code, stored in a decentralized network.

- **Pro Mode**
  - Medium speed
  - Decentralized system (10-100 nodes)
  - PGP encryption
  - Invisible texting
  - Saving messages for messages history
  - Creating private groups
  - Messages are not editable
  - Paid mode
  - Echo optional feature: sending and receiving of random encrypted irrelevant messages for creating white noise

If the message recipient is online, the message is deleted by default in 24 hours after it was delivered to a user or a private group. In case the message recipient is offline, the message is deleted by default in 7 days with 24 hours prior notification.

- **Premium Mode**
  - Ultimate privacy, anonymity and security
  - Maximum decentralization engaging the whole peer-to-peer network
  - Double encryption of all messages
  - PGP encryption, low speed
  - Invisible texting with random keyboard adjustment

Email: info@sishub.network
Website: www.sishub.network
• Saving messages for messages history
• Creating private groups
• Messages are not editable
• Paid mode
• Echo optional feature: sending and receiving of random encrypted irrelevant messages for creating white noise

If the message recipient is online, the message is self-destroyed by default in 24 hours after it was delivered to a user or a private group. In case the message recipient is offline, the message is self-destroyed by default in 7 days with 24 hours prior notification.

The user can disable the PGP encryption, in consequence of which the user’s phone calls by using the STEEL Messenger will be centralized and encrypted with the AES algorithm.

When inactive, the STEEL Messenger window will automatically close itself after a specified period of time using the timer method.

Decentralized STEEL Network for Secure Data Exchange
The STEEL Ecosystem is based on a decentralized hybrid Tor network design through which the users’ correspondence and data exchange can be facilitated in a highly secured manner. Since the network and the data it contains are encrypted, you can share files without being afraid of hacking and data intercepting during transmission.

Cryptocurrency STEEL Wallet
Our built-in cryptocurrency wallet enables the users to exchange and transfer various tokens and currencies to other users of the STEEL Ecosystem.

SISHUB Blockchain Network
The STEEL cryptocurrency will be based on its own blockchain to avoid Ethereum network’s vulnerabilities and ensure a highly secured environment for our users.

Decentralized Complex STEEL Antivirus Solution
Our blockchain-based antivirus software is a flexible adaptive protection system, which will both detect viruses and invasions of private data as well as search and correct defective settings along with other flaws or weaknesses of the security system.

An active decentralized application (DApp), running on the STEEL decentralized peer-to-peer network, will be dedicated to informing the users about all the recent viruses and security threats. The STEEL Antivirus software is available both for desktop and mobile devices.

STEEL ECOSYSTEM’S BENEFITS

Complete Anonymity
The STEEL Ecosystem provides high anonymity protection to its users, using a decentralized hybrid Tor network design. Due to its decentralized nature, the STEEL Network allows a total removal of the user identity while the user’s message and transactions history are decentralized within blockchain.
Ultimate Privacy
Within the STEEL Ecosystem you can safeguard your data from prying eyes with ease.

Unlike most of the messaging applications, the STEEL Messenger doesn’t collect the users’ personal information as well as information about geographic locations and other sensitive data.

Immediately after leaving your device, the information is encrypted and cannot be decrypted by intermediate nodes. Using the PGP end-to-end encryption, the STEEL Ecosystem provides the ultimate cryptographic privacy when senders use the public key to encrypt their messages, which can only be decrypted by someone who has access to the private key.

Superior Security
Any existing messenger has weak points, which cannot be neutralized as a matter of principle, because of centralized control, centralized architecture, and SMS authorization, based on the outdated phone routing system, which was designed back in 1975 and is unsurprisingly full of security flaws.

In case of the MTProto encryption protocol usage, the encryption of messages is enabled in secret chats only and is disabled by default. Furthermore, the MTProto was never audited by any independent party, which raises a big question among the industry experts regarding its security and preparedness against future cyber attacks.

We at SISHUB see no reason why use a less secure home-brewed encryption solution when well-studied, provably secure encryption schemes, such as PGP, exist.

The STEEL Ecosystem is based on PGP encryption, allowing users to communicate freely with each other, without jeopardizing one’s privacy.

Due to the decentralization principle, the users’ data is not stored in a single server. In centralized systems, an intruder can attack one of its servers and compromise the entire database. Such threats are irrelevant to decentralized environments.

The data within the STEEL Ecosystem is distributed among the Network’s nodes, and each node can contain a part of the Network’s database. Functioning as a distributed network, the STEEL Ecosystem has no single point of weakness susceptible to security breaches.

High Usability
The issues of privacy and security are something each one of us needs to take care sooner or later in this always connected world. Unfortunately, most of the Internet security and privacy software is too complicated to use.

In order to make security and privacy solutions approachable for a wide audience, including new and less-experienced users, the STEEL Ecosystem will become a user-friendly environment where any operation is intuitive and easy to handle.

For instance, the process of sharing encryption keys will be done automatically so that the users need only to set the security level of their choice.
The crypto wallet and an exchanger within the STEEL Ecosystem will make great choice even for first-time users. It will be as easy to send some cryptocurrency to a person from your contact list as it is to send them a message.

THE STEEL TOKEN

The STEEL Token is a utility token integrated across the STEEL Ecosystem as a native payment system. The main feature of STEEL cryptocurrency is the ability to support the data sharing and communications within overlay networks and decentralized applications.

The STEEL Token provides options required for the creation of a fully decentralized, fast, and feeless payment system, and will be used to simplify payments for various STEEL services, such as sending messages within the STEEL Messenger or using the STEEL Antivirus software.

STEEL will also be used to power a STEEL reward system -- a well-defined process that ensures fair reward distribution within the STEEL Ecosystem.

A user can become an active node within the network and receive rewards for supporting the network.

The revenues coming from the STEEL Ecosystem’s paid services, such as the STEEL Messenger or the STEEL Antivirus software, will be divided as follows:

- 75% will be distributed proportionally among all nodes in the network.
- 25% will be used for the operation of the STEEL Ecosystem.

TECHNICAL CONSIDERATIONS

The STEEL Ecosystem is based on hybrid peer-to-peer Tor network and uses PGP, AES, CBC, DSA, HMAC, SHA-256 algorithms as well as tunnels and complex identification instead of IP-addresses.

Hybrid Peer-to-Peer Tor Network

The STEEL Ecosystem will run on a blockchain supported hybrid peer-to-peer (P2P) Tor network, which offers truly anonymous internet access and transactions. This revolutionary decentralized network architecture is an overlay computing network based on its participants’ equality where each node (peer) serves both as a client and a host.

In a P2P decentralized architecture, each peer is of equal privileges and obligations, and none is superior to the other. There are neither any central authorities nor centralized servers or “supernodes” to control the communication between peers. Unlike the client-server architecture, the peer-to-peer network allows keeping the network efficiency with any number and any combination of accessible nodes: any peer can depart or join the network without significantly impacting its smooth functioning.
Since there is no central authority in charge, the information instead of going through one point passes through a variety of points. The STEEL Ecosystem disguises user’s identity by spreading the traffic across multiple nodes in the STEEL P2P network, and encrypting that traffic so that the information recipient can't trace the traffic back to the sender.

Using the decentralized peer-to-peer network is ideal for protecting users’ privacy and anonymity during data exchange between peers.

As all functions and tasks are distributed across the network, there is no single point of failures. The STEEL Ecosystem is self-organizing with strong immunity to technical failures, censorship, and hacking attacks.

**PGP Encryption**

Pretty Good Privacy, or PGP, is one of the most secure end-to-end encryption tools, which provides cryptographic privacy and authentication for data communication. In recent years, PGP has become increasingly popular among journalists, dissidents, whistleblowers, and human rights activists.

There are no publicly known methods or cases of breaking PGP encryption by cryptographic or computational means. None of the algorithms it uses contains cryptanalytic weaknesses, which is essential to the overall cryptographic security of PGP encryption.

“PGP empowers people to take their privacy into their own hands. There’s a growing social need for it. That’s why I wrote it.” – Phil Zimmermann
With the rise of the blockchain technology, this well-proven method is widely used to protect private information involved with financial transactions, and to prevent cryptocurrency theft.

PGP is based on the public-key method where a pair of keys is responsible for encrypting and decrypting data. Users create a public key and a private key: the former is used for encryption and checking digital signature while the latter is in charge of decryption and creation of digital signature. When generating the keys, their owner’s name and e-mail address is set, as well as key type, key length and duration.

In case of sharing encrypted messages in a decentralized network when each user stores parts of the encrypted messages of all users, a public PGP key will act as an encryption key.

The per-session key is generated with the help of cryptographically secure pseudo-random number generator and is encrypted with a public key of the recipient with the help of RSA or Elgamal algorithms (depending on the type of recipient’s key). Each public key is bound to a username or an e-mail address.

PGP supports three key types: RSA v4, RSA legacy (v3), and Diffie-Hellman/DSS (Elgamal according to GnuPG terminology). The RSA legacy key length must be between 1024 and 2048 bits, the Diffie-Hellman/DSS and RSA key length can be anything from 1024 to 4096 bits. The RSA legacy keys contain one key pair, while the Diffie-Hellman/DSS and RSA keys can contain one main key and additional keys for encryption. In this case, digital signature key in the Diffie-Hellman/DSS keys always consists of 1024 bits. The duration period for each key type can be defined as unlimited or limited up to a certain date. A secret phrase is used to protect a key container.

PGP supports message authentication and integrity checking of digital signatures. It’s used by default together with encryption but can also be applied to a plain text. A sender uses PGP to create the RSA or DSA signatures (the RSA or DSA algorithms are used depending on the key type): a hash for plain text is created (also known as a digest), then a digital signature of the hash is created with the help of the sender’s private key. For hash creation, the MD5, SHA-1, RIPEMD-160, SHA-256, SHA-384, SHA-512 algorithms can be used. New versions of PGP support MD5 to keep compatibility to the previous versions.

PGP compresses data before encryption to reduce the volume of shared messages and files and to make it more difficult to perform cryptanalysis. Compression is performed according to one of the following algorithms: ZIP, ZLIB, BZIP2. The compression is not performed for already compressed and short files.

**AES Encryption**

The Advanced Encryption Standard, or AES, is one of the most largely used ciphers for the encryption of data and US government standard for protection of classified data.

The AES algorithm transforms one 128-bit block into another by using a secret key required for such transformation. For decryption of this 128-bit block, another transformation with the same secret key is performed.
For encryption of a text, the AES algorithm uses the so-called key schedule received from the key instead of a password or its hash.

All the system notifications within the STEEL Ecosystem will be AES encrypted. In case the PGP encryption is disabled by the STEEL user, her or his phone calls within the STEEL Messenger will be centralized and encrypted with the AES algorithm as well.

**CBC Encryption Mode**

Cipher Block Chaining, or CBC, is one of the encryption modes for symmetric block code with the use of feedback mechanism.

Each block of plain text (except for the first one) is XORed with the previous ciphered block before being encrypted. This way, each ciphertext block depends on all plain text blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.

**DSA Algorithm**

Digital Signature Algorithm, or DSA, is a cryptographic algorithm using a public key to generate a digital signature, which is created secretly but it can be publically checked. The DSA algorithm is based on the computational complexity of logarithms in finite fields and is a US Federal Information Processing Standard for digital signatures.

DSA combines two algorithms, both of which compute hash messages with the help of cryptographic hash function. Algorithm S uses a hash and a secret key to create the signature; algorithm V uses hash messages, signature and public key to check the signature.

The system operation requires a conformity base between author’s (a person or a company) actual data and public keys, as well as all required parameters for the digital signature scheme (hash function, plain numbers). For example, certification centre can serve as a conformity base.

**HMAC Mechanism**

Hash-based Message Authentication Code, or HMAC, is a message authentication code, using a cryptographic key in conjunction with a hash function. The HMAC mechanism is a specific type of message authentication code (MAC) described in RFC 2104, which is standardized by such organizations as ANSI, IETF, ISO, and NIST.

Two parties using HMAC share a secret key to validate information transmitted between the sender and receiver. As a data integrity check, the HMAC also ensures that the data stored or shared in an unsecured environment was not transformed by a third party.

Security of any MAC function on the basis of built-in hash functions depends on encryption strength of a basic hash function. The attractiveness of HMAC consists in the fact that its creators managed to prove the exact relation between the cryptographic security of the built-in hash functions and the strength of HMAC.
BUILDING AN AUDIENCE

Protecting your online privacy is no easy feat. We live in a world where cookie-based advertising, cyber attacks, and government spying have become the reality. 80% of social network users are concerned about advertisers accessing their information and 70% are concerned about the government watching their private data.

The STEEL Ecosystem closes the backdoor for any third party access, which is the norm in centralized forms of internet communication, such as email, online file hosts or portals.

Given that the STEEL Ecosystem provides means to exchange data that literally no one but the two parties can access and decrypt, its various features will be advantageous for privacy-concerned users.

We enable doctors and lawyers and other professionals bound to professional discretion to maintain the ultimate privacy of doctor/patient or attorney/client communication as well as startups and companies to ensure that their business data is secure.

Implementing the STEEL solutions can help anyone who simply can't afford to risk data breaches, to hold onto their data and money. Privacy, anonymity, and security solutions are applicable to anyone who uses a computer or mobile device on a regular basis — from a private user to a mega-corporation.

As more people realize the ugly consequences of privacy violations and data breaches, more and more users will join the STEEL Ecosystem to efficiently resolve their privacy, anonymity and security issues.

THE STEEL ROADMAP

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEC. 2017</td>
<td>Starting SISHUB Platform Development</td>
</tr>
<tr>
<td>APR. 2018</td>
<td>Developing an anonymous messenger</td>
</tr>
<tr>
<td>JUN. 1, 2019</td>
<td>Beta Release of STEEL Messenger</td>
</tr>
<tr>
<td>JUL. 2019</td>
<td>Development of SISHUB Blockchain Network</td>
</tr>
<tr>
<td>DEC. 1, 2019</td>
<td>Development of multicurrency STEEL Wallet</td>
</tr>
<tr>
<td>MAY. 2020</td>
<td>Development of STEEL Antivirus</td>
</tr>
<tr>
<td>MAR. 2018</td>
<td>Developing an encryption system</td>
</tr>
<tr>
<td>DEC. 16, 2018</td>
<td>Alpha Release of STEEL Messenger</td>
</tr>
<tr>
<td>JUL. 1, 2019</td>
<td>Development of decentralized STEEL Network for secure data exchange</td>
</tr>
<tr>
<td>NOV. 1, 2019</td>
<td>STEEL Messenger Release</td>
</tr>
<tr>
<td>FEB. 2020</td>
<td>Development of safe Cloud Storage</td>
</tr>
<tr>
<td>JAN. 2023</td>
<td>Integration of all services</td>
</tr>
</tbody>
</table>

STEEL TOKEN ISSUANCE

The amount of STEEL tokens to be issued: 35,000,000,000 STEEL

Email: info@sishub.network
Website: www.sishub.network
**Soft Cap:** 5,000 ETH  
**Hard Cap:** 50,000 ETH

All unsold tokens will be burnt, which increases the value of the sold tokens.

A lower limit of the STEEL budget enables developing the core features of STEEL Token and supporting the STEEL infrastructure while exceeding amount of funds will speed up the development and will result in a greater number of new users.

**Distribution of Proceeds**

- Platform Development – 35%
- Marketing – 25%
- Investments in Infrastructure – 22%
- Overhead Expenses – 10%
- Legal Expenses – 8%

**Distribution of Tokens**

- Bounty + Airdrop Programs – 2%
- Partners and Advisors – 5%
- Platform Development – 8%
- Project’s Team – 8%
- Tokens Sale – 77%
Token Distribution Event

Pre-ICO (Public Pre-Sale)

Start: 09.05.2018
Finish: 30.07.2018
Soft Cap: 300 ETH.
Hard Cap: 1000 ETH.
Minimum Transaction Amount: 1 ETH.
500,000 STEEL for 1 ETH.
100+ ETH = 500,000 STEEL + 10% Discount.
500+ ETH = 500,000 STEEL + 20% Discount.

Tokens can be bought via open registration.

The STEEL ICO

Start: 20.06.2019
Finish: 20.08.2019
Soft Cap: 5,000 ETH
Hard Cap: 50,000 ETH
Minimum Transaction Amount: 0.1 ETH

Tokens can be bought via open registration.

For further information and announcements regarding the token distribution event, please provide your email address at www.sishub.network. For larger purchases, the pre-registration may require proof of identity and residence.
THE STEEL TEAM

Artur Andonis
CEO & Co-founder
A seasoned marketing and sales professional with 14 years’ experience in large-scale project and business management. For many years, Artur took various managerial and corporate positions in Israeli companies, such as Hot Communication and the Tel Aviv Sourasky Medical Center (Ichilov).

Semion Tsitkilov
CFO & Co-founder
As an experienced entrepreneur, Semion manages an Israeli venture fund which invests in pre-seed startups and grows them to mature stages. He holds a BA degree in Mathematics, Informatics, and Economics from Moscow University and has been serving as the CEO of a private financial company for the last three years. Chairman of the board of directors at Veert, assets manager at Galili Ltd.

Vladimir Groshev
COO
A serial entrepreneur with 15 years’ experience in business development and project management. Vladimir was the co-founder and/or CEO of a number of successful technology businesses, such as PSK Consulting, the Russian Trader, and the VIST company.
Michael Lyabin  
CTO & Blockchain Developer  
Michael has fifteen years in IT-development (including encryption and infosec-related projects, as well as blockchain networks). He created applications and projects for safetyjabber.com, GoInteractive, UseNetDownloader, Maks Hosting. He is highly skilled in blockchain-based software development and databases creation.

Pavel Krivenko  
Strategic Planning  
During his 15 years professional career, Pavel has held key positions in a number of tech startups and established businesses. He was a creator of Q-BASE.CLUB Platform, CEO at the OOO LIRAiKO, CEO at the ZAO ZM-Grafik.

Gennady Vasilkovets  
.Net Developer  
Gennady has over seven years’ experience in .Net development, including the creation of Big custom centralized client-server applications for advertising campaigns in the USA, Europe and Ukraine as well as team leading projects in custom software developments for automatic and semi-automatic processes. Head of Advertising Department in YHTBA CORP (USA); experience in writing spyware Trojans for corporative needs.
Boris Balinskyi  
Front-end Developer  
Boris has an extensive experience in creation and implementation of web interfaces and applications for large-scale projects in USA, Europe, Russia, and Ukraine. He operates a wide range of technologies for developing and optimizing the work of highly loaded applications and has two years’ experience in UMI.CMS technical support.

Andrey Shakula  
Front-end Developer  
Andrey has several years experience in front-end and software development, website coding, including the creation of mailing forms for promotional campaigns

Andrey Shvydkyy  
.Net Developer  
Andrey is experienced in .Net development and accomplished software developer with the knowledge of programming languages, including C#, .NET Framework, Windows Forms (WinForms), Windows Presentation Foundation (WPF), etc.
Valerii Roman
.Net Developer
Valerii is an experienced .Net developer who has worked in the fields of information and networks security, automation, and program engineering.

Vitalii Lozovitskii
.Net Developer
Vitalii is an experienced .Net developer with extra knowledge of networking and software support and the creation of UI systems in Xamarin applications.

Ivan Pavlov
Antivirus Developer
Ivan has an extensive experience in networks and software security audit.
Vasiliy Holovchenko
Designer
A highly talented and extremely professional designer with proven experience in web and graphic design, including branding, prototyping, desktop and mobile interfaces, corporate styles, logos, web banner ads, and more.

Irina Belyaeva
Public Relations
Irina has worked with Chinese companies for more than ten years. She is an experienced PR specialist and a highly qualified trilingual translator (English, Chinese, and Russian). Irina is a graduate of the Beijing Foreign Studies University.

Roza Dolgieva
Marketing Communications
Roza is a qualified marketing communications manager and translator, experienced in international blockchain-based projects.
Evgenii Serikov  
Relationship Manager  
Evgenii is a blockchain enthusiast, cryptoinvestor, and trader

Natalia Vasilashko  
QA Engineer  
Natalia is a qualified QA engineer with great attention to details. She has a special expertise in IT field, and in international tax agreements and cooperations. At the present time, she is also a linguistics student at the National University of Shipbuilding (NUOS).

Yulia Stratonova  
Sales Manager  
Yulia is a forward-thinking dedicated sales manager with special expertise in financial products, negotiations with governmental facilities, and public tendering. She has achieved outstanding results working as a sales manager at RusOkna, AOMZ Glavneftesnab, and OOO Vaineimenen.
LEAD ADVISORS

Daniel Mester
Advisor
IT Wiz & entrepreneur, co-founder of a number of companies in the fields of social gaming, online trading, e-gaming, and e-commerce. More than 10 years experience in startup management in Israel and USA.

Sasha Taback
Advisor
Member of Israel Blockchain Association Expert Board, CEO and founder at FIT Group, CEO and founder at Cluster - Disruptive Technologies HUB, CEO and founder at CoLab. Founder of IoT Israel and Robotics Israel Meetup.

Dmitry Pshenin
Advisor
Founder at ICOboard, managing partner at TokenUP Agency, head of partnership at IPOboard, cryptocurrency investor, ICO marketing expert, social media strategist, and networker.
Richard Trummer
Advisor
A cryptocurrency enthusiast and internet marketing expert. An experienced ICO advisor, involved as such in about 20 ICOs, such as COINEXIS, Bitozz, Redcab, Hydrocoin, Bdaq, Solomon.money, Zufly, Pimacoin, Sancoj, and others.

Giovanni Casagrande
Advisor
An experienced ICO advisor with special expertise in online marketing, blockchain tech, ICO regulation and compliance. A writer and public speaker, who brings two decades of traditional business experience coupled with the new decentralized frontier.

Egor Buravtsov
Advisor
Entrepreneur, Investor
Founder of ICO Summit Moscow, co-founder and CEO of PROMMASH LLC, special expertise and extensive experience in financial and banking sector (ABN AMRO Bank, The Royal Bank of Scotland, Raiffeisenbank, Gazprombank, Transkreditbank).
Ira Dolgin
Advisor
Member of Israel Blockchain Association Expert Board, CEO and co-founder at PickMoment, more than 15 years experience in marketing communications, content development, and digital marketing. Collaborations with Kin by Kik, Props by YouNow, CLOUDance, SecurityForest, Fixico, vEYE, CryptoSec, anyService, and others.

Main Developers:
@EsemevGlover, @Steel_Bill, @matrixa2011, @dwjenka, @dropdeaddd, @ccc, @pashadwwa, @cerez, @fegami, @rebordman, @segudha7, @weahha.

Blockchain Developers:
https://t.me/mikeether https://t.me/alex_ether

The Team consists of professionals with proven work experience and accomplished advisors in development, project management, marketing. The team guarantees successful launching of the Project and its development according to the Roadmap.

CONCLUSION

International cyber wars, endless successful hacking attacks on the corporate sector and huge losses by the most up-to-date and protected companies in the world have become a modern threat. There is a constantly growing number of hacking of mobile devices, social media accounts, and private emails. According to the trend of the recent years, the number of attacks will increase by at least 50% in 2018 compared to 2017. Hackers use specialized malware for cyber attacks less now, while zero-days exploits are becoming more widespread.

In this context, confidentiality of personal and business correspondence and private data has become a real issue recently. The thing is that this problem cannot be solved conceptually by using modern security architecture. The core functionality of networks, mobile devices, antivirus software allows full control over personal data of users and owners by spy agencies at any given time. No one can feel safe.

**We're developing a solution to meet these challenges to cybersecurity: STEEL Ecosystem.** This software complex includes the Anonymous STEEL Messenger, Decentralized STEEL Network for secure data exchange, Cryptocurrency STEEL Wallet, own SISHUB Blockchain Network and Decentralized Complex Blockchain-based STEEL Antivirus.
Software for desktop and mobile devices. Project’s unique advantages are the result of using a decentralized block-chart, implementation of PGP encryption and blockchain technology. This is what makes STEEL Ecosystem’s services completely anonymous and safe.

The Project has currently no existing analogues. The unique development, diversity of products within the developing environment of the STEEL Ecosystem together with its high potential demand allows us to forecast that its target audience consists of almost all categories of the internet and mobile devices users. The upcoming services will be able to solve the modern tasks of cyber security threats for private individuals, corporate sector, and government agencies and facilities. Potential buyers can count upon putting their money to get benefits from the Project since the idea itself and its realization will make the STEEL Ecosystem successful, widely recognized and implemented into mainstream usage.

Our STEEL ICO is not only for fund raising based on an abstract idea, we already have a real team and are working hard on developing the Product. The Project’s Roadmap is based on a workable timeline to allow us systematically and timely prepare a quality product. Moreover, first signals and feedback received from our potential buyers and website visitors indicate that our products are a promising and much-needed solution arousing great interest from all the people familiar with the Project.

STEEL by SISHUB is a reliable project targeted at successful future. All interested are welcome to participate in creating a brand new and promising STEEL Ecosystem at https://sishub.network.

DISCLAIMER

The information provided in this document is provided “as is” without warranty of any kind. Security Intelligent Systems Ltd disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose.

DOCUMENT LIFETIME

Security Intelligent Systems Ltd shall occasionally update online documentation between releases of the related software. Consequently, if this document was not downloaded recently, it may not contain the most up-to-date information. Please refer to https://sishub.network for the most current information. From the Website, you can also download and refresh this document if it has been updated by the related date.

PRODUCT INFORMATION

For documentation, release notes, software updates, or for information about Security Intelligent Systems Ltd products and services, go to the company website: https://sishub.network.

TECHNICAL SUPPORT

For technical support, go to https://sishub.network and/or send us directly an e-mail to info@sishub.network.
FEEDBACK

Your suggestions and comments will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send your opinion of this document to info@sishub.network.

You can also join our community and receive the most updated information by subscribing to our Telegram groups:
Russian speaking news channel: https://t.me/sishub
English speaking news channel: https://t.me/sishubeng
Chinese speaking news channel: https://t.me/sishubchina
English speaking community: https://t.me/SISHUBEng
Russian speaking community: https://t.me/SISHUBrus
Chinese speaking community: https://t.me/SISHUBchi
Bounty Program community: https://t.me/BountySISHUB

Links to the Project Resources

Website: https://sishub.network/
Facebook: https://www.facebook.com/profile.php?id=100025145026502
Twitter: https://twitter.com/steel_sishub
Telegram: https://t.me/SISHUBrus
Reddit: https://www.reddit.com/user/Irina_sishub
Bitcointalk: https://bitcointalk.org/index.php?topic=3398122.0
Medium: https://medium.com/@sishub_irina
YouTube: https://www.youtube.com/channel/UCoJA2NZyUuEREhmgzjDYfKw

NOTICES

This document is provided for initial informational purposes only. It represents Security Intelligent Systems Ltd current product offerings and practices as of the date of issue of this document, which is subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of Security Intelligent Systems Ltd products or services, each of which is provided “as is” without warranty of any kind, whether express or implied.

This document does not create any warranties, representations, contractual commitments, conditions or assurances from Security Intelligent Systems Ltd, its affiliates, suppliers or licensors. The responsibilities and liabilities of Security Intelligent Systems Ltd to its customers are controlled by Security Intelligent Systems Ltd agreements, and this document is not part of, nor does it modify, any agreement between Security Intelligent Systems Ltd and its customers.
Additional documentation will be provided in later phases of the implementation and provide the necessary technical information.

RISKS

Buying STEEL Tokens involves risks, and buyers should be able to bear the loss of their entire purchase. All buyers of the tokens should make their own determination of whether or not to make any purchase, based on their own independent evaluation and analysis. Do not buy STEEL Tokens if you are not an expert in dealing with cryptographic tokens and blockchain-based software systems. Prior to buying STEEL Tokens, you should to the extent necessary consult an appropriate lawyer, accountant, or tax professional. If any terms are unacceptable to you, you should not buy STEEL Tokens.

DOCUMENT HISTORY

Paper copies are valid only on the day they are printed. Contact the Security Intelligent Systems Ltd Team if you are in any doubt about the accuracy of this document.

REVISION HISTORY

This document has been revised by:

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Revision Date</th>
<th>Summary of Changes</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>February 2017</td>
<td>Releasing Whitepaper</td>
<td>SISHUB Team</td>
</tr>
<tr>
<td>V2.0</td>
<td>May 23, 2018</td>
<td>Updating and Releasing Whitepaper</td>
<td>SISHUB Team</td>
</tr>
<tr>
<td>V3.0</td>
<td>May 26, 2018</td>
<td>Updating and Releasing Whitepaper</td>
<td>SISHUB Team</td>
</tr>
<tr>
<td>V4.0</td>
<td>June 18, 2018</td>
<td>Updating and Releasing Whitepaper</td>
<td>SISHUB Team</td>
</tr>
<tr>
<td>V5.0</td>
<td>June 20, 2018</td>
<td>Updating and Releasing Whitepaper</td>
<td>SISHUB Team</td>
</tr>
<tr>
<td>V6.0</td>
<td>June 25, 2018</td>
<td>Updating and Releasing Whitepaper</td>
<td>SISHUB Team</td>
</tr>
<tr>
<td>V6.1</td>
<td>July 1, 2018</td>
<td>Updating and Releasing Whitepaper</td>
<td>SISHUB Team</td>
</tr>
<tr>
<td>V7.0</td>
<td>July 7, 2018</td>
<td>Updating and Releasing Whitepaper</td>
<td>SISHUB Team</td>
</tr>
<tr>
<td>V7.1</td>
<td>July 11, 2018</td>
<td>Updating and Releasing Whitepaper</td>
<td>SISHUB Team</td>
</tr>
<tr>
<td>V8.0</td>
<td>July 28, 2018</td>
<td>Updating and Releasing Whitepaper</td>
<td>SISHUB Team</td>
</tr>
</tbody>
</table>