CAUTION

This white paper has been prepared in compliance with industry best practices and regulations as understood by the authors at this time. This white paper is not a prospectus or offer document of any sort, and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction.

Prospective contributors should carefully consider the matters set forth under the caption “Risk Factors” of this white paper. If you are in doubt about the contents of this white paper, you should consult your investment advisor, stockbroker, lawyer, banker, dealer or any other financial consultant.

Prepared by:

The Stealth Grid™ Team

NOTE: This white paper is a work in progress and defines the intent of the company to market current products, continually develop existing products, and develop additional proprietary capabilities for these products. The implementations of these technologies are built on new models for computer science and security, and it is expected that significant changes will be continually required to meet evolving requirements.
# TABLE OF CONTENTS

Stealth Grid™ Blockchain Technologies: Anonymous, Encrypted, Decentralized ........................................ 4
Summary .................................................................................................................................................. 5
Three Trends Driving StealthCrypto® Mesh Network .................................................................................. 7
The Next Major Opportunity .................................................................................................................... 8
Overview ................................................................................................................................................. 9
Stealth Grid .............................................................................................................................................. 11
Stealth Grid .............................................................................................................................................. 11
StealthCrypto®, StealthCrypto® Pay™, StealthCrypto® Wallet™ ................................................................. 11
StealthCrypto™ Smart City - Smart Nation .................................................................................................. 12
Priorities & Vision ................................................................................................................................... 12
StealthCrypto® Key Exchange .................................................................................................................... 12
Quantum Key Generation & Authentication ............................................................................................... 13
Quantum Key Distribution at the Application Layer .................................................................................. 13
StealthCrypto® Mesh Network Delivered Quantum Entropy ....................................................................... 13
StealthCrypto® Hypertree Specification ...................................................................................................... 14
Blocks -Block-times .................................................................................................................................. 15
Data at Rest & in Motion ............................................................................................................................ 16
Flexibility .................................................................................................................................................. 16
Benefits .................................................................................................................................................... 16
Mobile Communications/Blockchain ........................................................................................................... 16
Enterprise/Government Communications (email, VOIP, FTP, Collaboration). .......................................... 17
Security Software as a Service (SaaS) ........................................................................................................ 17
Internet of Things (Platform, Devices, Semiconductors) ............................................................................ 17
Verifiable Identity-Based Encryption .......................................................................................................... 17
Quantum Blockchain Security-Qubit BlockChain™ .................................................................................. 18
StealthCrypto® Quantum Mesh Network Insurance .................................................................................. 19
Stealth Grid™ Containerization .................................................................................................................. 19
Creating the StealthCrypto Phone™ .......................................................................................................... 19
Our StealthCrypto Cloud Apps are Addicted to the Backbone .................................................................. 21
StealthCrypto® Decentralized App-Store ..................................................................................................... 21
Stealth Grid’s™ Unique Proposition ........................................................................................................... 21
Value Creation ......................................................................................................................................... 22
Mesh Scalability ....................................................................................................................................... 22
Backhaul ................................................................................................................................................... 22
Flexible Bandwidth Support ....................................................................................................................... 22
Market Forces .......................................................................................................................................... 22
STEALTH GRID™ BLOCKCHAIN TECHNOLOGIES: ANONYMOUS, ENCRYPTED, DECENTRALIZED

Decentralized Infrastructures: Stealth Grid™ foresees “a radically decentralized, more highly interconnected world. A global society that will fundamentally change your costs, efficiency, and reach, opening up a wealth of new opportunities for those who prepare for it; the infrastructure for the next generational social and economic systems.” StealthCrypto’s® blockchain innovations will decentralize networks, communications, as well as servers, and will radicalize infrastructure. We’re no longer speaking about monolithic resources with prohibitive barriers to entry, the quintessential server farm controlled by a centralized actor. Stealth Grid™ is building a decentralized global meshed network – StealthCrypto® – that adopts the sharing economy model for network access, creating communications that provide an economic incentive that allows users to share their unused data storage, bandwidth, or mine for profit. Monetizing the free exchange of data storage and bandwidth, via a secondary market, allows for free market forces to drive network growth where it is most needed.

StealthCrypto® will also leverage their quantum mesh network technology to build a decentralized IoT and communication’s future. A quantum mesh network is a network topology in which each node is capable of relaying data for others and utilizing a proprietary end-to-end quantum security encryption algorithm and authentication that is dynamic. With a hyper-dimensional model, data is not only moving from blockchain nodes and servers, but is also creating a more complex Hilbert space with hyper dimensional models and overlay patterns. All mesh network nodes cooperate, and with each participating node, the reach, throughput and resilience of the network is strengthened. These applications will shift the balance of power away from centralized authorities in the field of communications, data storage, currency, business, and even politics and law.

QUANTUM CYBER SECURITY

Stealth Grid™’s platform is building the world’s largest fully decentralized, incentivized, self-sustainable, wireless mesh telecommunications and data storage network using blockchain technology. By marrying StealthCrypto Cloud™ and StealthCrypto® unified communication applications, StealthCrypto® Smartphone ™, storage and a StealthCrypto® quantum meshing network with a StealthCrypto® Utility Token Offering we are able to offer unequalled, private, unified encrypted communication, telecommunications, data storage, IoT meshed devices (M2M), and authentication to support wallet-oriented micropayment systems, secure contracts, and securely manage transactions. This provides resilience against attacks on the communication servers by replacing them with decentralized StealthCrypto® nodes which anyone can host, and thus receive StealthCrypto® coins as compensation.

The StealthCrypto® meshed network will enable universal access to high-speed broadband for all. To achieve this, we have an ambitious, yet realistic, vision of building the world’s largest decentralized, community distributed, data storage and telecommunications network based on blockchain technology. The secure, unified meshed communications network is therefore owned and operated by no single entity, rendering attacks on hosts ineffective.
Communication meta-data cannot be gathered at one central point, as it is dynamically scattered over thousands of hosts all over the world making it very hard to work out who is talking to whom, even when parts of the internet are under surveillance.

The Stealth Grid™ Platform thus utilizes the power of our existing data storage, telecommunications, and takes unified communications a step further, by fundamentally changing the architecture from a server-centric network to a decentralized network that is owned and run by its users, and financed with the StealthCrypto® coin. Genuine dynamic split encryptions key identification, dynamic data split encryption end-to-end and a dynamic GeoDistributed Stealth Grid™ will prevent any kind of manipulation, interceptions and “man-in-the-middle” (MITM) attacks on all communication levels.

THE STEALTHCRYPTO® ECOSYSTEM WILL:

✓ Create the network
✓ Expand the network
✓ Sell the network
✓ Own the network
✓ Share the network
✓ Build the network
✓ Be the network

SUMMARY

Civilization is on the cusp of a major disruption in information technology. One that has game-changing potential for just about everything we do: the way we do business, the way we communicate, even the way we meet our basic needs. What makes this disruption different is a decided shift toward the empowerment of the individual, and away from “providers.” A shift to where individual freedom and privacy will start to matter more than convenience and reliability. There will be 1.84 billion mobile devices in 2020 and 14.4 trillion IoT market by 2022. In the midst of this growth, we are positioned to be the quantum cyber security solution.

Throughout history, with every technological breakthrough there was resistance, even disbelief, that the tried and true systems could ever go by the wayside. There were visionary companies that positioned themselves to benefit and even drive these emerging technologies. We look at companies on the cutting edge of today’s technologies to predict what may come next and ask:

What are their behaviors today telling us about what they expect to happen tomorrow? Where are we headed?
The elimination of the gateway, replaced instead by the decentralized mesh network?
The connected world as we know it today is badly broken. Cyber intrusions are a daily occurrence, with increasingly dire consequences. Most cryptography in commercial use relies on factoring as a hard-to-invert problem for its underlying security. With the arrival of more powerful super and quantum computers this type of security will be antiquated.

Stealth Grid™ is launching products that are supported and purchased by the StealthCrypto® coin. Completely unified and encrypted communications products that are presently ready for market include StealthCrypto® Cloud™ decentralized data storage, file sharing, encrypted email, call, instant messaging, Video Call, and VoIP – all of which are united with our StealthCrypto® Cloud™ data Trust Center.
Our Team is in the final phases of building a secure phone that will be ready Q1 2018 and StealthCrypto® NAS Container, a hybrid of a NAS unit and Wi-Fi Router that will create a quantum meshed network for data storage, mining, IoT communication, authentication, and telecommunications.

The reality is that in a hyper-connected world, data and privacy are not safe. A rapid increase in connectivity via technologies such as the internet, social networking, IoT devices and smartphones has brought about a steep-change in our ability to communicate. At the same time, current data storage, telecommunications, video calling software and instant messaging are not completely secure and are prone to surveillance and exploitation by governments, corporations and malicious third parties, as well as being less efficient and cost-effective than might be expected.

Our civilization and economies are facing a technological revolution. In an interconnected world, cyber-security becomes crucial to individuals, governments, cities as well as enterprises. As of now, most individuals and companies are not prepared to provide sufficient security regarding their communication. Stealth Grid™ intends to change that.

To combat this impending security crisis, we need a robust decentralized, autonomous, quantum mesh network that works across the many different paradigms of device communication. Stealth Grid’s quantum cyber security solutions make decentralization, encryption and authentication faster, easier and stronger. Stealth Grid™ protects data from being compromised by using proprietary StealthCrypto® dynamic end-to-end split data encryption layered with Polymorphic Hashed Encryption™ (PHE) which is Dynamically Split GeoDistributed™, creating a meshed decentralized network for StealthCrypto® telecommunications, authentication, IoT, and data that uses proprietary AI Cyber Security™.

Stealth Grid™’s proprietary dynamic split encrypted authentication process integrates a polymorphic encryption algorithm and authentication for StealthCrypto® meshed Trust Centers which provide an impenetrable stealth wall of security and autonomy. StealthCrypto® generates unique new keys (using quantum generated random numbers), for every transaction. It is a quantum computer resistant scheme, designed for today’s and tomorrow’s connected world.

*Bill Buchanan Professor of Cryptography, Napier University, Edinburgh, Scotland:

“One day, and I think it might be soon, we will wake up and RSA will be cracked. Either it will be super computers cracking the prime numbers, or it will be quantum computers, but when it happens there will be no proper identity on the Web and all the tunnels will be broken.”

Stealth Grid® has developed, and continues to develop, certain proprietary technology relating to quantum cyber security technology. This technology provides StealthCrypto® nodes for a mesh decentralized network that uses dynamic end-to-end cryptographic splitting software and hardware.
Not long ago, the rise of the global mesh was a matter of conjecture, and lied in the realm of futurist predictions. Today, it is increasingly becoming a predictable result driven by the convergence of three trends:

1. Moore’s Law: Emerging technologies continue to shrink in size while becoming more powerful. Allowing for the wow factor of their initial rollout, they will also become less expensive. Moore’s Law, named after Intel co-founder Gordon Moore, states that processor density will double every 18 months. This principle has now held true ever since 1975. For example, look at your iPhone, whose processor density doubled in capacity and halved in size every 18 months. If we extrapolate Moore’s Law to new solid state storage, we can say that today, a typical mobile phone has a 32 GB capacity at a cost of a few hundred dollars, in 5 years a device the size of a ring will probably have 1 TB of capacity and will cost about $50. In 10 years, a device the size of a pencil dot will hold 10 TB and will cost about $10. And in 15 years, we will be able to hold all of the world’s information on a device the size of a phone.

2. The 30-Year Cycle: Every thirty years, new technology completely disrupts the marketplace. For example, the Pony Express was made obsolete by the telegraph, invented in 1845 by Samuel Morse. Exactly 30 years later, Alexander Graham Bell introduced the telephone. In 1905, Marconi pioneered the radio. David Sarnoff at RCA helped bring television to the masses in the 1930s. The 1960s brought cable television, and the biggest disrupter of all in communications and content delivery was ushered in during the 1990s: The Internet. We are now due for the next cycle. Ironically, disruptive technologies are rarely taken seriously when they are first introduced. The telephone was originally a rich man’s toy. When cable television first arrived, it was difficult to imagine a paid service usurping traditional broadcast television — until the advent of Ted Turner’s first “superstation” in 1976, followed by others that led cable television to become a staple in almost every American home. And now the Internet has replaced (or is in the process of replacing) what is left of every basic mode of communication and entertainment that came before it: Netflix and Hulu subscriptions instead of broadcast and cable television, satellite and streaming music instead of AM and FM radio, smartphones vastly outnumbering landlines, and yes, limited choices available on standard TV. On the other hand, mobile technologies such as smart phones and tablets rose out of consumer desire for convenience and reliability. These devices are easy to set up and use and they provide convenient access to massive amounts of information, news, and entertainment. However, consumers are starting to understand how these devices compromise their privacy by tracking their virtual and physical movements and sharing their information with corporations who seek to monetize it. This loss of privacy will drive consumers to make future technology choices that respect their privacy.

3. Convenience and Reliability Versus Trust and Freedom: The first two trends created new generations of centralized institutions, ranging from Bell Telephone to Microsoft. This trend, by comparison, is rapidly ushering in a new global era of decentralization. As new technologies emerge, adoption has historically been based on consumer tradeoff between Convenience and Reliability vs. Trust and Freedom. For example, in the beginning cable TV was not convenient or reliable. It required a service provider to run wires into and throughout the home and install and connect a separate box to each TV. But its success was driven by a drive for freedom from the limited choices available on standard TV. On the other hand, mobile technologies such as smart phones and tablets rose out of consumer desire for convenience and reliability. These devices are easy to set up and use and they provide convenient access to massive amounts of information, news, and entertainment. However, consumers are starting to understand how these devices compromise their privacy by tracking their virtual and physical movements and sharing their information with corporations who seek to monetize it. This loss of privacy will drive consumers to make future technology choices that respect their privacy.
We are now seeing trends toward more convenience AND more privacy, in a way that stands the old paradigm on its head. This leads us straight to the use of FireChat in Asia and using Uber instead of calling a taxi company. Soon, finding capital, labor, and other resources through the mesh network will be the new normal instead of relying on a big bank or large corporation. We are already seeing this with BitCoin and cryptocurrency. It is happening now. You can either watch it happen or make it happen.

**THE NEXT MAJOR OPPORTUNITY**

Every thirty years, there are technological advances, along with corresponding economic opportunity. From television in the 1930s, to the World Wide Web in the 1990s, to the growth of social media in the 21st century, these enabling technologies permanently changed the fabric of society — and brought with them a relatively narrow window of time to monetize and commercialize them. Here are a couple of examples:

With Google in the early 1990s, search engines became the enabling technology for using the Internet. Early search engines such as Lycos and AltaVista soon gained market share — the former selling to a Spanish company for over $12 billion. By the dawn of the 21st century, their success spawned literally dozens of competitors. All these competitors did more or less the same thing until a couple of garage entrepreneurs, Larry Page and Sergey Brin, completely upended the market for search. Google’s PageRank algorithm, which ranked pages by their popularity rather than their keywords, served as the foundation for a company that now dominates over 70% of the Internet search market while expanding to become a ubiquitous provider of cloud services. Parent company Alphabet now has a market value of nearly half a trillion dollars as of early 2016, eclipsing Apple to become America’s most valuable public company as of this writing.

Ironically, the Lycos search engine still exists today — and it sold in 2010 for $36 million, less than the annual revenues of an average auto dealership. In 2004 Harvard student Mark Zuckerberg — reportedly after getting dumped by someone he was dating — created “Facemash,” a Hot-or-Not-like site that randomly compared photos of other students that he reportedly collected by hacking a Harvard network site. After nearly risking expulsion from school, he and several classmates eventually expanded this into a linked network of Ivy League students, and later the world. This wasn’t Zuckerberg’s last brush with privacy issues, but by being an early adopter for linking people online, Facebook is now far and away the world’s most widely used social network with annual revenues of nearly US $20 billion per year. And, it is the world’s largest entertainment company — without creating any content of its own.

What is the commonality between Google and Facebook? Both began as a way to find out information about people and organizations. Neither was intended to be monetized in the traditional sense. But both leveraged being early adopters to become market leaders. We believe the next leverage opportunity is the move toward a quantum mesh of peer-to-peer communications, data storage and transactions — underpinned by the ability to quantify trust between individuals. If you know what signs to look for, you see that this major revolution in technology is already upon us, bringing with it a rare and short-term opportunity to profitably exploit this market segment.
Today, organizations are turning to blockchain, a system that acts as a digital record-keeper, utilizing multiple hardened data centers around the world to verify changes to data sets. Data centers have to adapt to new business strategies. StealthCrypto® is building the world’s largest fully decentralized, self-sustainable, wireless mesh telecommunications network, plus data storage using blockchain technology. Using this network, StealthCrypto® will compete with centralized legacy telecommunications distribution models to provide universal fast Internet access. Backed by a global team with deep expertise in wireless, data storage, unified communications and blockchain technologies, StealthCrypto® will combine wireless advances with the emerging technology of blockchain to create a new paradigm and eliminate the gap caused by traditional cable and telecom wireless systems that are unsecure and handled poorly.

Each StealthCrypto® unit (or node) – which consists of a core router capable of communicating across a mixed spectrum of wireless TCP/IP, Bluetooth, and IoT spectra – will be the first hybrid NAS units integrated with the StealthCrypto® router. Additionally, each unit has a built-in functional cloud server and data store that can host edge computing applications, mining, smart contracts, IoT devices, and backless server support. This turns a network of StealthCrypto® servers into a dedicated peer network that can connect to the Internet, making a mesh of Internet servers possible.

The global StealthCrypto® Network will be owned and operated by the owners of StealthCrypto®. NAS integrated wireless routers, offering users high-speed, low-cost internet access whenever they are within range of a StealthCrypto® router. Each StealthCrypto® mesh network node supports a firmware-based blockchain infrastructure, and will communicate with other StealthCrypto® nodes to maintain the integrity of that blockchain. With this capability, a StealthCrypto® Network can be used to support wallet-oriented micropayment systems, mining, secure contracts, and securely manage transactions. The broader the StealthCrypto® Network, the more robust these abilities.

Each StealthCrypto® node operates autonomously in the order-driven market, which determines packet transit pricing in real time based on local network conditions. Internet access, data storage, and communications is billed and paid for in the native cryptocurrency of the network, StealthCrypto®. Node owners earn StealthCrypto® tokens by providing wireless broadband connectivity or data storage to neighboring nodes or roaming mobile users. The interconnected StealthCrypto® NAS unit routers also negotiate with, and pay each other for, connectivity in StealthCrypto®.

StealthCrypto® NAS routers are autonomous, with only the NAS router owners setting certain key operational parameters. A high level of security is provided to routers, their owners and their StealthCrypto® wallets through a sophisticated digital identity layer, combined with the blockchain technology built into each router.

This public offer of the StealthCrypto® cryptocurrency will raise funding for the ongoing development of the StealthCrypto® network, manufacturing of the StealthCrypto® routers, and to support realistic deployment efforts for rapid global growth. StealthCrypto® Cloud™ has already created digital infrastructure for the next generation of cloud services, ensuring telecommunications with rapid, seamless, and secure transmission of data, voice, and video to an increasing number of users.
• Data is dynamically split encrypted and is stored and GeoDistributed through blockchain locations and different countries, but divided into smaller “pieces.” No single location stores the entire file, and no single company is responsible for it. This ensures data integrity while making it difficult for hackers to obtain a copy of the entire file.

• The ability to download data from several sources simultaneously increasing network speed.

• International users get better performance by accessing data from locations in different regions.

• The building of a decentralized mesh network of StealthCrypto® nodes and completely decentralizing the VPN node network by using StealthCrypto® technologies and overlay on existing VPN and proxy protocols, as well as other solutions.

• Development of the StealthCrypto® Cloud™ node network, as an open and distributed peer-to-peer platform embedded with sustainable protocols, while using continuously evolving censorship evasion mechanisms, developed by the community. Once developed and released, StealthCrypto® Cloud™ technology will enable anyone around the world to both provide and receive access to content and privacy, removing censorship imposed by third parties.

• Empowerment of users through privacy controlled products such as the StealthCrypto® Phone™ which utilizes the meshed decentralized communication network featuring hard kill switches.

• The world’s largest de-centralized, community-distributed, telecommunications network based on blockchain technology – a first of its kind in the telecommunications industry.

By providing genuine dynamic split encryptions key identification, dynamic data split encryption and a dynamic GeoDistributed Stealth Grid™, secure preventative measures can be established against any kind of manipulation, interceptions and “man-in-the-middle” (MITM) attacks on all communication levels. With the emergence of Bitcoin, the crypto community has been growing. Stealth Grid™ has developed an unbeatable security model, which is professionally designed to meet the highest standards of cryptography for securely exchanging and storing all kinds of data.

StealthCrypto® Cloud™ is the most secure encrypted, peer-to-peer communication hybrid platform for social and business communication based on blockchain. The core technology of Stealth Grid® provides a new generation of automated end-to-end dynamic split encryption, as well as dynamic geo-distributed models with disruptive authentication algorithms using quantum number generators of decentralized IBE – the key distribution through blockchain. Stealth Grid® is building a fully distributed cloud for blockchain-based Stealth Grid® distributed applications. Stealth Grid® aims to provide distributed applications running on the blockchain, scalable, secure and easy access to the services, the data-sets and the resources they need.
• Consumers want their personal information to be secure, for example their address, credit card, data, IoT security, communications.

• The government institutions grid deals with all kinds of sensitive information daily, for instance, tax data.

STEALTH GRID™’S PRIVATE SOCIAL & CRYPTO COMMUNITY

A unified encrypted mesh network to provide high security and high quality services for social and crypto communications, such as instant messaging (chats), voice and video calls, photo/video and file sharing, offering an extensive set of local security functions.

STEALTH GRID™’S STEALTH CLOUD™

The base cryptographic secure technology, Stealth Grid™’s Stealth Cloud™ acts as a separate product designed to be integrated into the existing networks for dynamic split encrypted, dynamic geo distributed and dynamic split authentication, and secures data exchange and storage. This solution allows the easy integration of Stealth Grid™’s core cryptography and security model into any existing infrastructure regardless of complexity. It also provides all essential benefits without complicated technical upgrades or investment in expensive equipment.

Securely protect data in motion and at rest when utilizing StealthCrypto's® dynamic split encryption, which relies on dynamic geo distributed models within the meshed network. With disruptive authentication algorithms using quantum number generators of decentralized IBE – key distribution through blockchain – it can neither be predicted nor anticipated what the properties of the encryption system are, as it is constantly changing and moving. Data is dynamically split encrypted and stored in user selected distinctive data centers around the globe.

STEALTHCRYPTO®, STEALTHCRYPTO® PAY™, STEALTHCRYPTO® WALLET™

We are developing a cryptocurrency, StealthCrypto®, and token wallet. We will focus on the user experience – to make it as easy as possible to set up and use a wallet within our application containers and StealthCrypto® Cloud. To ensure highest-level confidentiality, Stealth Grid™ has issued a unique authentication crypto token StealthCrypto® Coin as a unified network currency to simplify and secure blockchain transactions. Another purpose of StealthCrypto® Coin usage is simple and anonymous money transfers between Stealth Grid™ users by using an integrated StealthCrypto® Pay funds transfer system.
STEALTHCRYPTO® COIN

Only 400,000,000 limited StealthCrypto® coins will be produced. The decentralization movement and technologies like blockchain will lead to a fundamental reversal of power, putting people in control of their digital lives. The proposed StealthCrypto® coin (QMN) will be built on a C# codebase using sources from the NBitcoin/ NStratis project and the Stratis Bitcoin Full Node implementation layered with our proprietary authentication technology. It will run under the .NET Core technologies, therefore making it developer-friendly and capable of running on various operating systems such as Windows, different versions of Linux, and more recently some Mac OS X versions.

STEALTHCRYPTO® SMART CITY - SMART NATION

We connect the dots to produce breakthrough solutions that are as unique as the cities and governments that we help. Integrated with Stealth Grid®’s cyber security solutions and the StealthCrypto® Trust Center’s cloud platform, we reach across sectors with the robust combination of sensors, real-time connectivity, data acquisition and management, ultimately driving collective awareness which leads to better decision-making. Stealth Grid® vertically integrates by utilizing the StealthCrypto® cryptographic platform that authenticates users according to client policies which govern the level of access for cities across the world. We also open key interfaces to enable our best in class partners to provide cities with new applications.

PRIORITIES & VISION

The main goal of the Stealth Grid® is to simplify the most secure, reliable, modern, advanced decentralized, autonomous cryptography and encryption technologies and make them available to everyone. Stealth Grid® is the first network to adopt blockchain for real-time communication networks and industrial usage. By joining the Stealth Grid® eco-network, you can do whatever you did before – have chats, calls, photo/video and document exchange, without having to worry about security and confidentiality issues in your virtual world, regardless of whether your communication is for personal or business purposes. That is why we call the company Stealth Grid® Living stealth in the digital grid!

STEALTHCRYPTO® KEY EXCHANGE

StealthCrypto® is developing an asymmetric split encryption and authentication scheme that provides absolute security and the simplicity to share the secret keys with anyone autonomously. True random number generator (TRNG) solves the fundamental problem of all cryptosystems – the need for true randomness – in order to ensure that encryption keys, tokens, PIN numbers, seeds for pseudo RNGs and digital signatures are unique and cannot be predicted. Benefits of a fresh, new, random split encrypted, asymmetric key generated for each transaction means securely authenticating and exchanging the symmetric keys of your choice. And because of the random element, StealthCrypto® is quantum computer resistant.

The blockchain is revolutionizing many businesses and markets. It has an enormous potential regarding cybersecurity. Stealth Grid® uses blockchain technology to develop bullet-proof solutions for B2C and B2B markets. By providing genuine dynamic split encryption key identification, Stealth Grid® can prevent any kind of manipulation, interceptions and “man-in-the-middle” (MITM) attacks on all communication levels.
Quantum Key Generation & Authentication

StealthCrypto®, Quantum Key Generation and autonomous Global digital Id and eliminating the set up and management challenges associated with certificate based solutions. Unlike PKI, StealthCrypto® is being designed to scale to the levels required for massive deployments characteristic of the Internet of Things and blockchain. With no certificates to manage, StealthCrypto® can protect billions of devices with ease.

Securely protect data in motion and at rest when utilizing StealthCrypto’s® dynamic split encryption, dynamic geo distributed models. With disruptive authentication algorithms using quantum number generators of decentralized IBE – key distribution through blockchain – it can neither be predicted nor anticipated what the properties of the encryption system is, as it is constantly changing and moving. Data is dynamically split encrypted and stored in user selected distinctive data centers around the globe.

Quantum Key Distribution at the Application Layer

The ultimate in quantum-safe security for long-term data protection; guaranteeing provably secure key exchange for encryption and other security devices on point-to-point backbone and storage networks. In an increasingly treacherous cyber-security landscape, StealthCrypto® authenticates the sender of a message, be it a person or thing. By authenticating or verifying the sender of every message, StealthCrypto® ensures that any and all messages received are from trusted sources.

StealthCrypto® Mesh Network Delivered Quantum Entropy

Cryptography with StealthCrypto® Quantum powered entropy engine that provide full quantum entropy (one bit of quantum entropy per output bit) at the rates necessary for data center, cloud, large-scale internet of things (IoT), and mobile applications. This will increase with the adoption of our decentralized Quantum mesh network that will create a quantum supercomputer.

With StealthCrypto® NAS and Smart Phone model StealthCrypto® distributes true entropy from a quantum source to properly seed random number generation across data centers and networked devices (a similar concept to network time protocol (NTP) for ensuring access to consistent date/time).

- Cryptography
- IBE Authentication
- Crypto-currency
- Tokenization

- Authentication
- Digital Identity
- Payments
- Communications

The StealthCrypto® Entropy Engine provides high-speed, true random numbers in a convenient PCIe card form factor in our NAS Units. Utilizing a quantum entropy source that exploits the laws of quantum mechanics to create true unpredictability. Capable of delivering 350Mbit/s, the Entropy Engine can satisfy the demands of even the highest-performance crypto-systems.

Tamper protection of their cryptographically sensitive parts with repeaters instead of trusted-nodes. These devices will relay quantum signals without measuring them, and will thus not require any specific cryptographic protection.

Although it is traditionally implemented over optical fiber links, QKD will work over the decentralized global mesh network a handheld device and a fixed terminal such as an ATM. Once loaded, key material is gradually consumed to secure communications.

One StealthCrypto® autonomous Global ID, on Blockchain and under your control by creating a single digital identity. Provide a Quantum Secure Digital Identity (QSDI) global ecosystem that is far superior than existing ID systems, which is global in nature, but yet secure, private and available on demand.
The following default parameters are to be adopted for a standard hypertree construction:
\[ j = 0 \ (j \in \{0 \leq x \leq 2\}), \ h = 12 \ (h \in \{1 \leq x \leq 14\} ), \] upper bound of signatures possible: 236, minimum signature size: 2.21kb, maximum signature size: 7.65kb.

i.e. A single XMSS tree, \( h = 12 \) with 4096 signatures available, which may be extended with further trees of up to \( h = 14 \) as required. For most user’s additional trees are unlikely to be required at all.

Example STEALTHCRYPTO signature

Assuming the most complicated hypertree construction where \( j = 2 \) and \( h = 14 \), a signature for transaction message, \( m \), where \( n \) is the OTS quantum generated keypair position for each XMSS tree, would require:

- Signature tree, \( j = 2 \): OTS signature of \( m, n \), merkle authentication proof, merkle root of signature tree
- Certification tree, \( j = 1 \): OTS signature of Merkle root from signature tree \( (j = 2) \), \( n \), Merkle authentication proof, Merkle root
- Original XMSS tree, \( j = 0 \): OTS signature of Merkle root \( (j = 1) \), \( n \), Merkle authentication proof, Merkle root

Verification involves generating the OTS quantum generated key from \( m \) and the signature, then confirming the supplied Merkle authentication proof generates the signature tree Merkle root. This becomes the message for the next OTS signature and from this the next OTS quantum number generated is generated, the supplied Merkle authentication proof used to recreate the certification tree Merkle root, which becomes the message for the next certification tree OTS signature, and so on. A signature is only valid if the merkle root of the highest tree, the original XMSS tree, \( (j = 0) \) is correctly generated.

Notice the OTS quantum generated keys are not required for verification of the XMSS tree signature. In fact, the merkle root for each tree can also be deduced and therefore omitted with hypertree signature verification if the sending ledger address is known (as this is a computed derivative of the merkle root for the highest XMSS certification tree \( (j = 0) \) within the STEALTHCRYPTO signature).

As the signature scheme is state full the wallet implementation must retain and update \( n \) for each XMSS tree generated in the hypertree for a given address.

Design and randomness

For every block each validating node which is staking the current epoch reveals the next consecutive previous hash in the chain to cryptographically prove participation and vote to be the winning block selector. Quantum number generated for a pseudorandom number sequence of 32 byte outputs from seed data taken from the blockchain (the genesis block initially, then added entropy taken from concatenated recent block header hashes for each subsequent epoch).
Bitcoin has a time between blocks of roughly 10 minutes, but with natural variance this can on occasion lead to fairly long periods before the next block is mined. Newer ledger designs such as ethereum have improved upon this and benefit from a much shorter block-times (15 seconds) without the loss of security or miner centralization from high rates of orphan/stale blocks. Ethereum uses a modified version of the Greedy Heaviest Observed Subtree protocol which allows stale/orphan blocks to be included in the blockchain and rewarded. As the STEALTHCRYPTO® plans to use a proof-of-stake algorithm from the outset we expect to safely use a block-time of between 15 and 30 seconds.

Modern cryptosystems rely on high quality randomness and can consume surprisingly high quantities of random numbers to generate keys and perform cryptographic operations. If these random numbers are less than truly random, key finding attacks become a realistic and undetectable threat creating an invisible back-door for attackers and eavesdroppers.

Poor random number generation becomes a single point of failure, an issue that is compounded by the fact that measuring the quality of random number generators is notoriously difficult. This means that proving keys are truly random and unpredictable and that any crypto systems that use them are as secure as expected is almost impossible. In the era of ubiquitous encryption, it starts to matter which random number generation systems are strong and which are weak.

HMAC-DRBG

In HMAC-DRBG, the state is composed of a key K, a value V and a counter c (to keep track of when a reseed is needed - it is not used for generation itself). The actual generation of random bits uses

V := HMAC(K, V)  
in a loop and concatenates these new values of V until enough output is generated.

After this, an update function is called, which changes both key and value by two HMAC calculations:

KnewVnew = HMAC(Kold, Vold || 0x00) = HMAC(Knew, Vold)  

Update can alternatively also incorporate additional data A provided by the application, using four such calls in total:

KtmpVtmpKnewVnew = HMAC(Kold, Vold || 0x00 || A) = HMAC(Ktmp, Vold) = HMAC(Ktmp, Vtmp || 0x01 || A) = HMAC(Knew, Vtmp)  

(If additional input is given to the generate-function, update will be called before and after generating more output.)

This will also be used for seeding and reseeding.

HMAC-DRBG's security depends on the key K staying secret (intermediate values of V are output directly as pseudorandom bits), i.e. on the key-retrieval-resistance of the HMAC.

Optimally, we want the HMAC output be a pseudorandom function of the input.

Initialization: The HMAC_DRBG_Instantiate_algorithm function sets K to 0 and V to 0x01010101...01, before calling first the Update function with the seed material as "additional data".
DATA AT REST & IN MOTION

StealthCrypto® keeps data dynamically secure by using dynamic split encryption, dynamic split geo distribution, and a dynamic split encrypted authentication process that authenticates users according to client policies which govern level of access. Data is highly vulnerable to outside threats, and not a day goes by when yet another supposedly protected system is hacked and valuable information is stolen. StealthCrypto® ensures that data is only available to authenticated parties, locking out cybercriminals and better protecting people, places and things.

FLEXIBILITY

StealthCrypto® can be used with embedded private keys on devices and end-points, and/or with no requirement for secure local storage, or on the StealthCrypto® Cloud™ NAS Server and mobile devices.

BENEFITS

StealthCrypto® Trust Centers™ (TC’s), or NAS systems, offer a true peer-to-peer communication and data storage that can be embedded on a chip and can be configured for cross-domain secure communication, between stand-alone Trust Centers or StealthCrypto® Cloud NAS servers. In this way, it’s social by design. Stealth Grid™ products and solutions are based on the underlying thought of creating an eco-system of safe interaction for consumers as well as business customers. Business opportunities today are diverse. Stealth Grid™ intends to be positioned as a pioneer, a global influencer, and a thought leader regarding blockchain usage for cyber-security purposes.

MOBILE COMMUNICATIONS/BLOCKCHAIN

Mobile and blockchain developers can deploy StealthCrypto® to secure authentication and key exchange requirements. Its certificate-less feature and peer-to-peer functionality make it a perfect security ingredient for e-banking solutions and so much more.
Security Software as a Service (SaaS)

The combination of StealthCrypto® protected apps that use a downloadable software secure element solves the SMB security challenge without the need and cost of deploying hardware secure elements.

Internet of Things (Platform, Devices, Semiconductors)

Commonly used devices rely on semiconductors as a part of their functionality and increasingly these products are able to communicate with each other through the internet. There are very few security standards within the IoT and yet millions of devices are being deployed daily with no embedded security. Dated security approaches such as PKI are overly complex to set up and manage, are not secure enough and cannot scale.

StealthCrypto®-protected devices, monitored through an IoT StealthCrypto® protected platform, scale easily and will provide you with global visibility of your assets.

Verifiable Identity-Based Encryption

Identity-Based Encryption (IBE) was proposed in 1984 by renowned cryptographer, Adi Shamir, and advanced in the 1990s as a “breakthrough approach to encryption key management.” Quantum resistant hash-based signatures rely upon the security of a one-way cryptographic hash function which takes a message, and outputs a hash digest of fixed length, i.e. SHA-256, SHA-512. Using a cryptographic hash function, it should be computationally infeasible to brute force m from h (pre-image resistance), or brute force h from h2, where h2 = hash (h) (second pre-image resistance), while it should be very hard to find two messages (m1 /= m2) that produce the same h (collision resistance). Grover’s quantum algorithm or a pre-image attack may be used to attempt to find a hash collision requiring O (2n/2) operations. Thus to maintain 128 bit security, a hash digest length of at least 256 bit must be selected — assuming a perfect cryptographic hash function.

Our connected world has changed a lot since then, however, in response to today’s cybersecurity challenges, StealthCrypto® is bringing to market next-generation IBE. StealthCrypto® dramatically improves on IBE by eliminating the need to protect the public parameters and adding authentication at the application layer. This is achieved by using dynamic split encryption, dynamic geo distributed models with disruptive authentication algorithms using quantum number generators of decentralized IBE – key distribution through blockchain.
By harnessing the unique properties of quantum mechanics, Stealth Grid has developed a portfolio of quantum-safe security solutions. Our Quantum Key Generation, Quantum Key Distribution (Quantum Cryptography) and Quantum-Safe Network Encryption solutions offer unparalleled protection for data with long-term sensitivity and value.

Our products are designed to help governments, financial service companies, healthcare organizations, cloud service providers and commercial enterprises worldwide protect mission-critical data into, and beyond, the era of large scale quantum computers.

The ultimate in quantum-safe security for long-term data protection; guaranteeing provably secure key exchange for encryption and other security devices on point-to-point backbone and storage networks. StealthCrypto® quantum secure solutions address these challenges through a proprietary process that is integrated in decentralized resolutions. Our authentication components are based on an quantum cryptography StealthCrypto® is a proprietary cryptographic algorithm that adds a critical authentication ingredient to our digital society, instantly rendering all connections impenetrable to outside threats. Lightweight and easily scalable, StealthCrypto® is will replace the blockchain infrastructure as we know it.

Further, StealthCrypto® Ecosystem is capable of disrupting all existing approaches to encryption, including anything that relies on RSA – which experts in the field predict is close to the end of its product life cycle. Randomness, quantitatively measured by entropy, is the measure of uncertainty or disorder within a set of data.

The higher the level of unpredictability, the more random the data is and the more valuable it becomes, particularly for cryptographic operations. Developing a random number that is generated by a process whose outcome is unpredictable, and which cannot be reliably reproduced, ensures optimum security. Random numbers are important for strength of cryptographic protocol only for quantum and stochastic cryptographic. Here random numbers are an essential part of data exchange between communicating parties but also for contemporary deterministic cryptography where maximal entropy of the random numbers maximizes overall cryptographic strength.

In the design of StealthCrypto® it is important that the cryptographic security of the signature scheme is secure against classical and quantum computing attack both in present day and also future decades. The global adoption of the StealthCrypto® mesh network will increase the strength of the Quantum resistance solution within the topology architecture.
Creating the Stealth Crypto Phone™

Stealth Grid™ is the developer of the StealthCrypto® Phone™, an ultra-secure mobile phone that is the first open source blockchain smartphone and NAS Units. The smartphone features hard kill switches, empowering its users to take back control of their privacy. All phones feature a built-in privacy control center giving users full access and function control on their phone.

Smartphones were never designed with security or privacy as a major factor, though these are essential to ensure the trust of the blockchain network. As technologies such as cryptocurrency mining, trading, and online payments become available for these devices, they turn into even more valuable targets for malicious actors.

Many apps that we download harvest data by asking for more permission types than are really needed (for example, flashlight apps that need access to your contacts) and so jeopardize our privacy. Nowadays, smartphones are just as vulnerable to hackers and malware as PCs, but are even harder to protect.

Another problem with modern smartphones is that they have so many capabilities. Thanks to a hypercompetitive marketplace, there is a constant race to add more and more features. This has two implications:

1) security often lags behind, and 2) the potential attack surface is enormous. It is relatively easy for a determined attacker to hack a device, access it and obtain data. There have been several attempts to tighten up smartphone security – like the introduction of end-to-end encryption on some widely-used messaging apps such as WhatsApp and WeChat. But unfortunately, this is not enough. While an app may be secure, this does not help if you have already been tricked into downloading a piece of malware that sends screen captures of your messages or records your calls.

To prevent such attacks, smartphones must be secured not only against external intrusions, but also at the hardware low-level of the phone itself. This can only be achieved by tightening the operating system, which means that a phone must be developed with security in its entirety, as the necessary level of protection cannot be achieved through app development alone. These considerations have forced manufacturers of secure mobile phones to develop phones which are both expensive to produce and provide limited usability in favor of security, therefore leaving no room for advanced features.
We plan to tackle and solve these security and privacy challenges while maintaining full, uncompromised usability. StealthCrypto® Phone™ gives our users enormous power over his or her privacy.

• Bank of switches allowing physical disconnection of the battery, Wi-Fi, Bluetooth and geolocation, the camera and the microphone, and more
• Resistant to Stingray or any other IMSI catcher device
• Developed in the United States, designed in Canada
• Coming in Q2 2018

The StealthCrypto® Phone™ contains a platform that will allow the user to physically disconnect the battery, Wi-Fi antennas, Bluetooth and geolocation, the camera and microphone, etc. It also will not allow the phone to connect to a Stingray or any other IMSI catcher device.

The StealthCrypto® Phone is creating a new paradigm for wireless networking: StealthCrypto®, an autonomous, decentralized mesh network. Mesh networks technology is helping to enable the 4th generation of wireless mobility by using basic radio frequency (RF) physics in a new way — overcoming inherent limitations to achieve unprecedented coverage, throughput, flexibility, and cost-efficiency. Mesh networking offers a new model of seamless mobility that's already transforming wireless data and voice communications for citizens, on the battlefield, in police work, at the scene of fires, and in other settings where instant, wireless information access can provide both economic, quality of life, and safety benefits.

From these military and first-responder applications, mesh networks are being quickly adopted in municipal wireless broadband networks, as well as in several vertical markets such as mining, manufacturing, transportation, and other enterprise settings. Mesh networks provide the required ease of deployment and high throughput in even the most difficult environments. Increasingly, you'll see mesh networking technology transforming commercial settings, public places, and even home networks.

Mesh networks are revolutionizing wireless mobility, and Stealth Grid™ is committed to leading the way by developing technology to be completely off-the-grid that operate independently of any network infrastructure. This means the StealthCrypto™ Phone™ will let you stay in touch with your friends and teammates no matter where you are.

StealthCrypto® Phone™'s meshed network dramatically increases the effective range beyond point-to-point range by relaying data through other devices. At Stealth Grid™, we aim to democratize mobile communication with technologies that enable smartphones to communicate without relying on centralized infrastructures. By providing a long-range mesh networking technology with partners and our StealthCrypto® Cloud™ NAS, that is secure, easy-to-use, and accessible to everyone, we can lay the foundation for creating a truly open, decentralized digital communication network, built for and powered by the people.
**OUR STEALTHCRYPTO® CLOUD™ APPS ARE ADDICTED TO THE BACKBONE:**

- Hardened android operating system with granular security management and streamlined, security-optimized components
- Permission enforcement module controls access to network, data and sensors, keeping you in control of your security policies
- Baseband firewall protects against over-the-air attacks with constant monitoring of baseband processor activity, baseband attack detection, and automated initiation of countermeasures
- Two-layer storage dynamic split encryption system protects data at rest against unauthorized access
- Biometric technology security enabled by fingerprint recognition and iris scan
- Secure encrypted messaging through Private StealthCrypto®
- Documents, photos and videos transferred securely over Private StealthCrypto®
- Secure, encrypted voice and video calling
- StealthCrypto® wallet, safe and secure

---

**STEALTHCRYPTO® DECENTRALIZED APP-STORE**

Most users retrieve the apps they use through an app store, managed by the OS vendor of their device. These stores provide users with little value, mostly in the form of auditing and reviewing apps ensuring better protection of the users from malware, at a high cost: stores charge roughly 30% of the developer’s proceeds, including most forms of in-app payments, out of developers’ pockets. Most estimates put the combined revenues of Apple and Google app stores in recent years at between $50-$100 billion annually.

But the damage to users is even higher. The operators of the app stores use their monopolistic power to impose censorship on the app offering: from barring apps that contain unapproved content (such as gambling or adult content apps), to bolder limitations on apps that pose a risk to the operator’s business (for example, Apple blocked all blockchain wallets for the lion’s part of 2014).

The Stealth Grid™ D-App Store is a decentralized and tested app store for any type of app on the StealthCrypto® platform, in which users pay developers 100% of their subscription fees directly. Auditing services providing security protection, parental control, etc. may be provided by trusted 3rd parties and sold directly to the subscriber.

---

**STEALTH GRID’S™ UNIQUE PROPOSITION**

Decentralized networks introduce tremendous challenges starting with network scalability, payment speed, security and privacy. Based on Stealth Grid™’s legacy in developing and launching the StealthCrypto® smartphone, we have planned a new distributed Quantum mesh network economy which is based on the StealthCrypto® smartphone and NAS connected devices, to address these upcoming challenges.
Mesh networks have many advantages, with a lack of scalability so far being a limiting factor in applicability. With the increase of the number of nodes with the growth of a mesh network, functionality of the network is often compromised. This drag occurs because of both protocol overhead and the inability to offload packet congestion. In some circumstances protocol overhead disproportionately grows relative to the overhead of carrying the data itself. Collisions, timeouts and a full halt to all packet routing can occur.

These scaling problems are almost impossible to overcome in a standard mesh network because there are no alternate pathways or protocols to relieve the congestion. In particular, a regular stand-alone mesh network operating with a single protocol over a single spot on the radio spectrum will simply not scale well.

On the contrary, the StealthCrypto® mesh network was conceived as a robust global network without these traditional mesh technology limitations. In this respect, StealthCrypto® Network displays the following features:

**MULTIPATH**

StealthCrypto® operates simultaneously across multiple protocols and frequency bands of the radio spectrum. It supports path as well as link diversity. Multiple paths can potentially be resource pooled to route and forward packets. It can also be used either simultaneously or in a backup configuration, for increased reliability, end-to-end throughput, network efficiency and fault tolerance.

**BACKHAUL**

StealthCrypto® is designed to reduce the required number of hops to as low a number as possible. This is best achieved by providing a direct high-speed route to the backbone from as many points in the network as possible, which would represent the network’s backhaul. The network’s backhaul would predominantly be supported by its users connecting, or bridging, their StealthCrypto® NAS routers to existing home and SoHo broadband routers.

Alternatively, in the case of larger StealthCrypto® networks, through interconnecting, or peering, to exchange points. It is also envisioned that several StealthCrypto® networks would be peering with each other directly, thus localizing network traffic.

**FLEXIBLE BANDWIDTH SUPPORT**

StealthCrypto® will pioneer the notion of flexible bandwidth in cases where StealthCrypto® users, by means of additional StealthCrypto® token micropayments, would acquire higher bandwidth for a specific period of time, when required.

**MARKET FORCES**

The StealthCrypto® bandwidth market would solve congestion problems by means of the automated setting of higher prices resulting from high demand. High prices in a particular zone would attract node operators seeking higher returns. Analytics will be provided to indicate where infrastructure can be added, as well as the type of infrastructure likely to earn the most traffic. As a result, market forces attracting infrastructure deployments where needed would then realize the exponential scaling of the network.
SUSTAINABLE USAGE MODEL AND INCENTIVES

Bandwidth market exchange

The StealthCrypto® bandwidth marketplace is designed as an open and autonomous exchange for trading Internet connectivity using StealthCrypto® as an intra network micropayment medium of exchange. StealthCrypto®’s Ecosystem and products deliver the opportunity to execute a widespread, trusted and cyber protected, peer-to-peer resource sharing, from one consumer electronic device to others. This ecosystem gives the community of blockchain developers the opportunity to create a diverse domain of trusted and secured resource sharing applications and services, per micro payment, for example:

• Resources - data connectivity, energy, computational power

• Data - local weather, traffic status

The sky is the limit!

MINING REVENUE

Each StealthCrypto® wireless node is a fully operational node in the StealthCrypto® (blockchain) network. Nodes are authorized to participate in blockchain consensus processes via their PoET/PoV semiconductors. Occasionally, nodes are identified as block leaders and are rewarded in StealthCrypto™, which are funded by a portion of market transaction fees.

GOVERNANCE

The Stealth Grid™ Corp is tasked with the governance aspects of the StealthCrypto® Network. This covers a relatively broad range of particularities and can be defined by the ensuring of a fair and open involvement by participants, infrastructure owners, and users in a secure and sustainable marketplace economy. Stealth Grid™ will decide, through consultation with all stakeholders and experts in the field, on the rules set and delegation of tasks, in alignment with the stated goal of growing the world’s largest and most inclusive wireless mesh and data storage network.

STEALTH GRID™ PROVISIONAL PATENTS & TRADEMARKS

• Provisional Patent Number 62/536,810
SYSTEMS AND METHODS AUTONOMOUS BLOCKCHAIN AUTHENTICATION SPLIT ENCRYPTION SCHEME USING IDENTITY-BASED STEALTHCRYPTO ENCRYPTION, AUTHENTICATED USER/PEER AND IOT TAC, DYNAMIC STEALTHCRYPTO® BLOCKCHAIN TRUST CENTER, QUANTUM RANDOM NUMBER KEY GENERATION, CRYPTOCURRENCY, POLYMORPHIC HASHED DECENTRALIZED DATA PROTECTION AT REST AND IN MOTION WITH DYNAMIC SPLIT ENCRYPTION AND DYNAMIC GEODISTRIBUTION.

• Provisional Patent Number 62/510,662
SYSTEMS AND METHODS DYNAMIC SPLIT ENCRYPTION AND MULTILAYERED POLYMORPHIC HASHED ENCRYPTION (PHE) AND DYNAMIC SPLIT GEODISTRIBUTION, FOR DATA AT REST AND IN MOTION AND DYNAMIC POLYMORPHIC CERTIFICATE-LESS AUTHENTICATION

• Provisional Patent Number 62/475,438
SYSTEMS AND METHODS CRYPTOGRAPHIC POLYMORPHIC ENCRYPTED ALGORITHM DESIGNED FOR MULTILAYER DYNAMIC SPLITTING DATA AT REST AND IN MOTION AND DYNAMIC POLYMORPHIC AUTHENTICATION
The following roadmap describes a timeline that is based on our token sale. If we do not raise this amount then the roadmap will not change, but timing will be much more reliant on further traditional investment. This roadmap comprises technical development product launch, together with business development and strategic partnerships, as we intend to keep on growing our distribution and channel partnerships while we continue to develop our technology and platform.

The StealthCrypto® Token is essential to the function of the StealthCrypto® ecosystem. StealthCrypto® is a functional Token that will be used on the platform to access various features, products and fees. Furthermore, as StealthCrypto® services and products become more liquid and valuable over time, we anticipate it could be used to rebalance individual portfolios. In other words, liquidity generated by StealthCrypto® can enable users to shift allocations between various currencies quickly and easily.

In short, StealthCrypto® Token transactions will consist of:

• Offered and purchased services & products
• Participation in the Quantum mesh network
• Portions of subsequent payments paid to providers by users
• StealthCrypto® smartphone and monthly services
• Mining transaction fees paid to the infrastructure owners.

StealthCrypto® is building a strong network of international corporate and organizational partnerships to ensure it is able to deliver and roll out network coverage, user and community development, and support as broad of a geography as possible.

StealthCrypto® will have in-house sales and a marketing team along with outsourcing the distribution and support functions of the StealthCrypto™ Network technology to specific market channels. These will include direct to market, as well as value-added vendor channels.

Early implementations of the StealthCrypto® Network will require a customized project approach, or may be conducted in association with existing community mesh networking projects. In either case, subcontractors to the StealthCrypto® will ensure that network design principles are applied to ensure optimized coverage for the end users of the StealthCrypto® Network. Local licensing and community participation are essential to the success of the quantum mesh network, and experts in the process of implementation will be deployed as subcontractors.
Launching unified blockchain peer to peer communication products that include, IM, cloud storage and file sharing, email, voice, and video conferencing that use Dynamic Split Encryption, Dynamic GeoDistribution, authentication, and our proprietary Quantum cyber security technology. Additionally launching our Stealthcrypto® phone.

1. Stealth Cloud™ Trust Center is a “zero knowledge” process that allows the client to hold their keys, and control their data. No outside company can access or control your files, unlike traditional cloud storage providers. Highly redundant - Stealth Cloud™ stores tiny pieces of your files on dozens of dynamically split encrypted nodes across the globe with their dynamic GeoDistributed™ platform. This eliminates any single point of failure and ensures highest possible uptime.
2. Stealth Cloud™ Dynamic Split Encrypt and dynamic GeoDistributed™ application
3. Stealth Cloud™ Voice Secure Cloud Base Encrypted hybrid P2P calling
4. Stealth Cloud™ Video Chat, Video Conferencing, Video Collaboration, and Video Calling; all encrypted
5. Stealth Cloud™ email encrypted end-to-end
6. Stealth Cloud™ Instant Messaging
7. A digital wallet will be implemented within the StealthCrypto® Network.
8. Transparency dashboard: all parties involved in the StealthCrypto® Network can see the development of the main KPI’s affecting the performance of the business and the Stealth Grid™ StealthCrypto® cryptocurrency.
9. Creator and distributor dashboard for content ingestion, distribution and configuration of the smart contracts.

StealthCrypto® has signed an agreement with Earth Bank which will run on our ecosystem to create the world’s first quantum-secure network. StealthCrypto® is a massive, totally decentralized, self-sustainable mesh network built on the blockchain. With no central servers, Earth Bank’s network is fundamentally designed to be hacker-proof. We will provide the simple tools to help institutions, banks, governments and organizations to interface with our system.

The StealthCrypto® Token provides a license to activate the existing suite of unified encrypted communication products, quantum mesh network products & services, StealthCrypto® ecosystem and data storage, with various license levels:

- Personal
- SMB
- Corporate
- Fortune 500
- Fortune 100
- Distributor
- Customized
STEALTHCRYPTO® TRANSACTIONS WILL CONSIST OF:

- Offered and purchased services & products
- Participation in the quantum mesh network
- Portions of subsequent payments paid to providers by users
- StealthCrypto® smartphone and monthly services
- Transaction fees paid to the infrastructure owners

PHASE TWO 02 2018

STEALTHCRYPTO® DISTRIBUTED NETWORK – QUANTUM MESHER NETWORK (PROJECTED)

A StealthCrypto® meshed peer-to-peer cloud storage network would implement end-to-end dynamic split encryption and dynamic geo distributed models with disruptive authentication algorithms using quantum number generators of decentralized IBE – key distribution through blockchain. This would allow users to transfer and share data without reliance on a third-party data provider. The removal of central controls would eliminate the possibility of traditional data failures and outages, as well as significantly increase security and privacy. The proposed solution to these additional problems is to use a hash challenge algorithm. Redundant copies are uniquely encrypted, and the hosting node must hash the data and a given seed to return a unique hash. These unique hashes not only serve as proof that the file is being stored, but also that it remains unmodified. Furthermore, failure of these challenges will initiate a process to restore the desired redundancy. In this way, a single, honest node can verify the integrity and availability of the file. Malicious nodes will not be able to complete challenges and are thus dropped from the network.

The StealthCrypto® Cloud™ NAS System is fully decentralized, with files distributed and stored all over the world, on different containers. This allows the network to be robust to attacks, with no central point of weakness. The StealthCrypto® Cloud™NAS has an embedded Wi-Fi router container that connects to peer-to-peer cloud storage, telecommunications, communications, IoT connections, and mining, and is powered by a decentralized meshed network. Important files deserve a great storage and backup strategy to protect against unexpected hardware failure, natural disasters, accidental deletion or cyberattacks.

StealthCrypto® Cloud™OS is the StealthCrypto® Cloud™modified version of Rockstor (CentOS), with modifications on the kernel and block devices. The filesystem StealthCrypto® Cloud™OS uses Btrfs.

Btrfs is intended to address the lack of pooling, snapshots, checksums, and integral multi-device spanning in Linux file systems, these features being crucial as the use of Linux scales upward into larger storage configurations. Btrfs is designed to be a multipurpose filesystem, scaling well on very large block devices.
StealthCrypto® Cloud™ is a super powerful NAS (network attached storage) computer. Instead of storing files in the public cloud, the StealthCrypto® Cloud™ acts as your personal cloud. StealthCrypto® Cloud™ is a combination of reliable hardware and a super intuitive StealthCrypto® Cloud OS. It is based on Linux and allows easy storage management, configuration of peer-to-peer backups, and a native wallet.

**UNIFIED ENCRYPTED COMMUNICATIONS**

StealthCrypto® Cloud™ NAS is secure, easy-to-use, and accessible to everyone. With StealthCrypto® Cloud™ NAS we can lay the foundation for creating a truly open, decentralized digital communication network, built for and powered by the community (no more Telco’s). StealthCrypto® Cloud™ creates a secure communication meshed platform (fixed or mobile). This quantum resistant service can replace TLS/SSL and SSH and facilitate secure email, VoIP, and authentication.

**CRYPTOFORTRESS™ BANK**

StealthCrypto® Cloud™ will also act as a small bank. Earn Bitcoin or StealthCrypto® Coin by renting unused space as well as “cold storage”. Cryptocurrencies are the currencies of the future. The user can earn coins without any prior technical experience. StealthCrypto® Cloud™ will make that process very simple. Just plug it in and connect it to the internet. Everything else is done by the device.

StealthCrypto® Cloud™ is a Peer-To-Peer (P2P) cloud computing network that allows users from all over the globe to cooperate in the creation of a decentralized internet. Users can sell the resources of their machines to those looking to host their data in a more private, secure and efficient way. The StealthCrypto® Cloud™ platform will not only offer a better alternative to traditional cloud services in terms of technology, but it will also strive to be competitive in terms of price. Besides that, we also strive to make our technology intuitive and as user friendly as already existing top-tier services. We want to make sure this new internet is accessible to everyone, regardless of their knowledge, thus we want to focus on providing a seamless transition from traditional services to StealthCrypto® Cloud™ without compromising on features.

**P2P BACKUP**

The StealthCrypto® Cloud™ will be a micro datacenter. It connects to a peer-to-peer network underpinned by blockchain. You store data locally and enjoy backups in the decentralized cloud. It eliminates single point of failure, because data is backed up in multiple regions that you choose.

You can access StealthCrypto® Cloud™ from anywhere around the world. You can access files on the go and you can run different services on top of StealthCrypto® Cloud™, like StealthCrypto® Cloud™ Unified Communications or media servers. Dynamic end-to-end split encrypting the data and Dynamically Split GeoDistributed™ data that is protected before the initial upload and sent and while data at rest. No one else can view or change. The distributed nature of the Stealth Cloud network provides your data with physical security, meaning that no third party can access or delete it, as can happen with existing centralized solutions.

Solving the problem of universal Internet access requires a multitude of solutions. StealthCrypto® intends to be a major player in this space with the ambitious goal of building the world’s largest decentralized, community-distributed, telecommunications network based on blockchain technology —
a first of its kind in the telecommunications industry. The unique selling points of StealthCrypto® bringing together multiband meshing capabilities with novel blockchain technologies to solve the economic sustainability challenge will ensure StealthCrypto® is well positioned to be a major player in the game of universal service provisioning.

On the StealthCrypto® Network, participants, the owners of StealthCrypto® mesh NAS routers, as well as users, would use digital identities which they themselves create and exercise full control over, in order to gain access to network resources or interact with digital identities of others. This decentralized schema would provide extensive opportunities to lock down most of the vulnerabilities that we face online.

As a result, the ability to access and set parameters of any StealthCrypto® mesh NAS router will only be under the control of its owner. Without access to the private key used by its owner, it would be impossible to compromise or hack a specific router. Private keys are also intrinsic to the inclusion of particular devices that participate in the global consensus model of the StealthCrypto® blockchain.

### TEAM

#### CEO, LARRY CASTRO

- leads overall company strategy and is a recognized leader in cybersecurity with more than 30 years of experience. His expertise includes the multiple sectors of technology, cloud broadcasting, cybersecurity, and digital media. He has also built a golf portfolio as an international golf professional, golf fitness visionary, sports marketing strategist and, more recently, executive roles as lead developer, owner, manager and designer of some of the world’s most renowned golf resorts, sports and entertainment facilities. He recently served as an executive for a cross platform technology that was brought to the public market through his strategies and execution. He serves as an active advisor to several technology and sports entertainment companies and has served as the Director and founding Chief Executive Officer at multiple companies.

Mr. Eilers is a highly motivated and energetic team member that provides support for Stealth Grid’s direct and indirect commercial go-to market functions, including negotiations, drafting of master agreements and transaction documents for acquisition of the full breadth of our products and services. He assists in integration and operational infrastructure initiatives, as well as support to the marketing channels and alliances team. He also develops advancements for our business operations and processes, which are in accordance with legal and compliance requirements for ICO’s. He specializes in publicly traded securities, and is well versed in traditional IPOs, reverse mergers, and upholding compliance.

### DEVELOPMENT TEAM

#### PROJECT LEADER / SOFTWARE ARCHITECT, JORGE ANDRÉS RAMOS EGUNOA

Mr. Egunoa has a master degree in systems engineering with 10 years of experience in various software development projects, with strong experience in web and mobile technologies, C# and .NET Framework. He enjoys researching new technologies, methodologies, etc. to exploit creativity. He prefers working in organized environments with clear measurable objectives and greatly values teamwork.

#### SECURITY ARCHITECT, JAMES SCOTT

James Scott (Large Data Architect, Splunk Architect) holds top secret and Q security clearances. After completing Oracle University courses in Oracle 10gR2 Grid Control, Oracle 10gR2 Administrator II,
Oracle 10gR2 Administrator I, Oracle 8 Database Administrator I, Oracle SQL Plus and Entity Relationship Modeling. James has an expert’s understanding of big data, engineering and security. He is also an HTML, XML, CSS, JavaScript, Ruby, BASH, Sed, Awk and Perl expert.

SECURITY ARCHITECT, RANDY Hест

Sr. Manager, Program/Project Management, Hewlett Packard Enterprise Cyber Security Hewlett Packard Enterprise. Heist leads a Cyber Security Program & Project Management team for one of the largest and most diverse IT environments supporting more than 350,000 workers world-wide. He is a Systems Engineering Principal, SAIC IT Services and has managed multiple enterprise IT projects/programs for legacy and vendor SW development, infrastructure, network, ERP, and enterprise application retirement. He led a large-scale enterprise-wide systems integration, and cyber security initiatives for hardware, software, infrastructure, networking, enterprise computing, and databases. Hest is an IT leader, successfully deploying service-oriented architecture (SOA) for corporate ITS, including enterprise ERP, SAP, Deltek Costpoint/T&E, SOA, EDI, and DW. Technologies he has managed and integrated include: Deltek Costpoint, Deltek T&E, Deltek MRP, SAP R/3, Oracle CRM-OD, Documentum, Lotus Notes, McAfee ePO, McAfee Enterprise Security Suite, ISO 27001, PeopleSoft, Symantec, Gentran EDI, Hyperion, Cognos Reports, Sharepoint, and Altiris.

UI AND DESIGN TEAM

PROJECT LEADER / CREATIVE DIRECTOR, DANIEL SAAVEDRA

Daniel has more than 13 years of experience in different fields of design, product development, branding and advertising with a bachelor of arts degree in audio visual communications from Pacific University, where he later served as an adjunct professor for visual perception studies. He has worked with a variety of companies which have greatly expanded his design skills and business knowledge. He is able to jump from being a decision maker to a designer. This adaptability can also be seen in his design work where he is able to handle any task given, be it digital, branding or print.

GRAPHIC DESIGNER, CARLOS COSTANTINI

Mr. Constantini has over 10 years of experience with user interface (UI), user experience (UXD) and as a digital products and services (web and mobile applications) design expert. At 20 years old he began working in print design. Within the industry, he has worked in many fields such as branding, packaging and all kinds of graphics for printing and internet environments. In the last 10 years, he started a closer relationship with the systems area, and is focused almost exclusively on front-end design. His goal as a designer is to create functional and engaging experiences for users.
**LEAD TESTING & CUSTOMER SERVICE, FRANCO LADINO**

Mr. Ladino has a master degree in business administration with mention in strategic management. Requirements Analyst, Scrum Master, Sales and Quality Manage. He is an assistant project leader with over 8 years of experience in project management and software marketing.

**STEALTHCRYPTO® COIN™**

Stealth Grid™ is creating StealthCrypto® Token™s for a limited time. A fixed number will be created during the presale, and no more will be created thereafter. The StealthCrypto® Token™ provides a license to activate the existing suite of unified encrypted communication products, quantum mesh network products & services, the StealthCrypto® Ecosystem and data storage.

**VARIOUS LICENSE LEVELS:**

- Personal
- SMB
- Corporate
- Fortune 500
- Fortune 100
- Distributor
- Customized

**STEALTHCRYPTO® TRANSACTIONS WILL CONSIST OF:**

- Offered and purchased services and products
- Participation in the Quantum mesh network
- Qubit Blockchain
- Insurance
- Portions of subsequent payments paid to providers by users
- StealthCrypto® smartphone and monthly services
- Transaction fees paid to the infrastructure owners

StealthCrypto® holders will acquire a license through the coins smart contract to activate and use Stealth Grid™s suite of tools without having to pay additional licensing fees (transaction fees charged by third party card issuers and payment system providers remain applicable). StealthCrypto® coin (QMN) will be built on a C# codebase using sources from the NBitcoin/ NStratis project and the Stratis Bitcoin Full Node implementation layered with our proprietary authentication technology. It will run under the .NET Core technologies, therefore making it developer-friendly and capable of running on various operating systems such as Windows, different versions of Linux, and more recently some Mac OS X versions.
1. Introduction

1.1. These terms & conditions ("Terms") govern the use of the (i) StealthCrypto® website (www.StealthCrypto.io), "the website"), the only official and authorized website for StealthCrypto® tokens, (ii) the sale of StealthCrypto® tokens ("StealthCrypto®") through its token sale, and (iii) holding and use of StealthCrypto®.

1.2 Acknowledging these Terms creates a contract between the purchaser of StealthCrypto® tokens and Stealth Grid Ltd. World Trade Center 6 Bayside Road 1st Floor – Unit 1.02 Gibraltar GX11 1AA the the Stealth Grid™ ecosystem ("company"). StealthGrid™ is not a financial institution and does not provide financial advice or any other licensed services.

1.3. Stealth Grid™ provides technical and marketing effort to create and support the StealthCrypto® ecosystem as described in the White Paper. The technical and organizational structures of Stealth Grid™ are currently bringing a suite of products to market and various development stages. Stealth Grid™ has several products built and ready for market Q1 2018. Token acquisitions will pay for use of the suite of Unified Encryption products, data storage and services that are used, as well as maintenance, plus development of Stealth Grid™s family of products and services that will be supported by the users of the services obtained by the StealthCrypto® token sale.

1.4. Participants cannot contribute to the token sale if there are applicable legal restrictions in their country of residence. It is the responsibility of each participant to know and abide by these laws regarding the purchase of StealthCrypto® tokens.
2. STEALTHCRYPTO® SYSTEM

2.1 The StealthCrypto® token will be an ERC20 token on the Ethereum blockchain with the Symbol “QMN” The preliminary outline of the StealthCrypto® functions is given in The White Paper. The contents of the white paper are non-binding and are subject to change by Stealth Grid™ at its sole discretion.

2.2 The StealthCrypto® token will be the native cryptocurrency of the StealthCrypto® system. Funds collected through the token sale will be used to develop and use of the StealthCrypto Cloud™ products and products in the StealthCrypto® ecosystem. The values of StealthCrypto™ tokens are fully dependent upon the developments of Stealth Grid™ and market demand.

a. The StealthCrypto® Token is essential to the function of the StealthCrypto® Ecosystem. StealthCrypto® is a functional Token that will be used on the platform to access various features, products and fees. Furthermore, as StealthCrypto® services and products become more liquid and valuable over time, we anticipate it could be used to rebalance individual portfolios. In other words, liquidity generated by StealthCrypto® can enable users to shift allocations between various currencies quickly and easily.

In short StealthCrypto® Utility Tokens will:

• Be the payment mechanism for accessing and using services and products on the StealthCrypto® Ecosystem
• StealthCrypto® Phone
• NAS Units
• Insurance
• Portions of subsequent payments paid to providers by users
• Mining transaction fees paid to the infrastructure owners
• Pay for transaction fees.

2.3 The StealthCrypto® token does not represent or confer any ownership right or stake, share or security or equivalent rights, voting right or any right to receive future revenue shares, intellectual property rights or any other form of participation in or relating to the StealthCrypto® system, and/or Stealth Grid™ and its corporate affiliates, other than rights relating to the use of the platform.

2.4 Our token is a unit of payment inside a single system. According to law, the StealthCrypto® token is not a security. Stealth Grid™ makes no representation that the StealthCrypto® token is, or is not, a security.

3. TOKEN SALE “QMN”

3.1 Total token supply: 400,000,000
200,000,000 tokens for Stage 1 Token Crowdsale

Pre Tokens Sale to start on January 28, 2018. The initial token price (ICO) will be set at a minimum of $0.50, or present market value above $0.50, when ICO launches August 18, 2018

200,000,000 tokens will be reserved for Stage 2 Token Crowdsale (50% of total).
Stage 2 will happen no sooner than 2020, and all tokens will be sold at market price, not at a fixed $0.50 USD value (important note: all percentage below will be adjusted in accordance with actual amount raised, e.g. if we sell 70M of 100M tokens, the following numbers will be multiplied by 0.007).

• **STEALTHCRYPTO® FUND – 100,000,000 STEALTHCRYPTO®**

The StealthCrypto® Fund™ operates as part of our business model, ensuring a stable token with a bright future. It is in our best interests to ensure that the STEALTHCRYPTO® purchasing power grows over time and market manipulation is avoided.

A total of 400 million tokens will be issued. This is how it breaks down in dollars during planning - the actual price is subject to change:

### STEALTHCRYPTO ALLOCATION

![Stealth Crypto Allocation Chart](image)

3.2 HERE ARE DETAILS OF THE ABOVE CHART:

The *presale* will take place on January 28, 2018. There will be blocks of tokens sold at a discount. After each block is sold, the valuation will increase and upon activation of the ICO will determine the market price (to a minimum of $0.50 per token).

The *token sale* will offer 200,000,000 tokens to the public. They will be sold using a smart contract until all 200 million have been sold (according to a predetermined block), whichever comes first.

All unsold tokens from both the presale and the sale - If there are any StealthCrypto® coins left at the token sale closing date of September 30, 2018 they may be distributed into a bonus pool. It has been common in token sales to destroy any remaining coins. We have decided that there is no 100% guarantee that these coins are “burned” or destroyed and so we have decided it would be in the interest of the ecosystem that the remaining coins are used in a controlled manner to increase participation, which will increase the value of StealthCrypto® for selected token holders.
The target is $100 million at the sale-time price.

The projected cap will be 200 million tokens.

The marketing effort will receive 8 million tokens, or 4 percent. This is to pay all the people and companies who have worked so hard to create and manage the token sale. 2 percent of these tokens will be tradable immediately — they are bounty and contest rewards. The other two percent will be locked up for 9 months after the sale ends.

We reserve the right to use some or all of the 20 percent of tokens reserved for later funding as follows:

- To provide liquidity on one or more exchanges. Tokens not being used for liquidity will be “off the market.”
- For future offerings. Assuming a strong initial sale, we don’t plan another offering for at least three years. If we reach our cap, we will freeze all these tokens for three years.
- We may burn tokens if we feel that it contributes positively to the ecosystem.

3.1 The eighteen percent of tokens reserved for Stealth Grid™ will be dedicated to doing internal projects that will be built on top of the StealthCrypto® system. They will be an asset of the corporation. When the total sale reaches the cap of 100 million, all tokens will be issued from the smart contract.

3.2 Liquidity STEALTHCRIPTO® will be listed on several exchanges initially, and more as time progresses. The objective is to make STEALTHCRIPTO® available as widely and conveniently as possible to anyone who wishes to participate on the StealthCrypto® network.

3.3 Addressing Scalability with 18 decimal places, the STEALTHCRIPTO® in circulation is highly divisible to support very high transaction volumes. If this proves insufficient, the splitting mechanism can increase the STEALTHCRIPTO® in circulation.

3.4 Splitting STEALTHCRIPTO® is designed to accommodate extensive scaling of the StealthCrypto® network, with the commensurate growth in participants, users and micropayment transactions. The STEALTHCRIPTO® token can be divided into 18 decimal places, and therefore it is not envisioned that more STEALTHCRIPTO® tokens will be required anywhere in the foreseeable future.

However, should there be a need for more STEALTHCRIPTO® tokens in future to meet the volume requirements of the network; the facility to split tokens is in the design of the tokens. The Stealth Grid™ is responsible for the governance of such an event. Should a split be decided on, all STEALTHCRIPTO® tokens can be split into a minimum of two tokens. This would effectively mean that any STEALTHCRIPTO® residing at any address (for example in a user’s StealthCrypto® Wallet) would double. Such splits would occur at the same time globally.

A token split is not intended to raise the overall value of STEALTHCRIPTO® holdings, but simply as a mechanism to increase the available number of STEALTHCRIPTO® tokens in circulation.
3.5 Tokens will be divisible to 18 decimal places.

3.6 All sales will be final.

3.7 All buyers are strongly encouraged to sign up for the Stealth Grid™ email list, which will be provided on the StealthCrypto® website. Stealth Grid™ will set up a treasury committee to manage funds.

3.9 Stealth Grid™ will maintain a blockchain-explorer page on the website, so all tokens can be seen publicly.

3.10 Stealth Grid™ will work to get StealthCrypto® tokens listed on several exchanges. We cannot guarantee they will be listed, accepted to specific exchanges or, in the case where they are listed on an exchange, remain on that exchange.

4. LIMITATION OF LIABILITY

4.1 In no event shall Stealth Grid™, members of Stealth Grid™ staff, contractors, or volunteers be liable for:

- Any lost profits, lost savings or incidental, indirect, special or consequential damages, arising out of your use or inability to use the services or products offered by Stealth Grid™ or the breach of any of these Terms by any third party;

- Any security risk such as hacker attacks, loss of password, loss of private key, or similar.

- Mistakes or errors in code, text, or images involved in the sale.

- Any losses resulting from the volatility in pricing of StealthCrypto®s in any countries and cryptocurrency exchanges.

4.2 This website and the StealthCrypto® tokens are provided on an “as is” basis and without any warranties of any kind, either expressed or implied. You assume all responsibility and risk with respect to your use of the website and purchasing of any amount of the StealthCrypto® tokens and their use. In any case, the total amount of our aggregate liability hereunder may not exceed US$500. If applicable law does not allow all or any part of the above limitation of liability to apply to you, the limitations will apply to you only to the extent permitted by applicable law.

4.3 By acquiring StealthCrypto's® and to the extent permitted by applicable law, the buyer agrees not to hold Stealth Grid™ or any employee or contractor of Stealth Grid™ liable for any losses or damages arising out of or in any way connected to the buyer's failure to properly secure the private key to the wallet containing their StealthCrypto's®: hacker's attacks, stolen devices, loss of passwords, etc.

4.4 We do not buy back tokens. We are not market makers. If you want to sell your token, please go to one of the exchanges that list the StealthCrypto® token, provided it'll be listed.

5. RISK FACTORS

5.1 The purchase and any other acquisition of StealthCrypto® tokens carries with it significant risk. Prior to participation, carefully consider the potential risks and, to the extent necessary, consult a lawyer, accountant, and/or tax professional to evaluate the risk entailed. Do not overcommit.
6.1 By acquiring StealthCrypto® tokens, whether directly or from another stakeholder, you represent and warrant that you:

- Have a basic level of understanding of the usage and intricacies of cryptographic tokens, such as Ethereum ERC20 tokens, and other blockchain-based software.
  - are at least 18 years old;

- waive your right to participate in a class action lawsuit or a class-wide arbitration against any officer, employee, volunteer, or representative of Stealth Grid™;

- are not exchanging or using StealthCrypto’s® for any illegal purpose;

- understand that there is no warranty, guarantee, or liability for defect with regards to StealthCrypto® tokens, express or implied, to the extent permitted by law;

- further agree to accept that you participate and/or use (in) the StealthCrypto® system at your own risk;

- Are in compliance with your local, state, and national laws.

5.2 We make no promises of possible gains or returns. You can potentially lose all your money if the market price drops to zero.

5.3 StealthCrypto® tokens are ERC20 tokens on the Ethereum blockchain. You must access and use them using an ERC20-compliant wallet. It is your responsibility to not lose your tokens.

5.4 This is early-stage project finance. The team is unproven. The market is unpredictable. It is possible that even if the sale threshold is met, funds won't be sufficient to feasibly develop the StealthCrypto® system or there could be enough execution error to cause the project to fail. By holding StealthCrypto®s, the acquirer acknowledges that he/she understands that while every effort will be made to execute Stealth Grid’s™ vision for the StealthCrypto® system, it is possible that it will never be realized.

5.5 Cryptocurrencies and project financing through cryptocurrencies have been the subject of regulatory scrutiny by various regulatory bodies around the world. Stealth Grid™ and the StealthCrypto® project may need to change their operations to comply with applicable regulation, and they may become subject to licensing requirements. StealthCrypto® tokens could be impacted by one or more regulatory actions or regulatory enforcement, which could impede or limit the ability to continue to develop the StealthCrypto® system. This uncertainty significantly adds up to risks connected with the acquisition and use of StealthCrypto’s®. Stealth Grid™ will make every effort to adopt its practices to accommodate regulatory needs and changes as they occur.

5.6 The field of digital cryptography is very new and for this reason there is a risk of unforeseen attacks on several or all parts of the StealthCrypto® system.

5.7 Forking: It’s possible that a group of people will take our software and modify it to accept a different set of tokens, or no tokens. This could devalue StealthCrypto® tokens.
6.2 If purchasing Tokens, you must comply with all applicable tax laws, including, but not limited to, the reporting and payment of income tax or similar arising in connection with the appreciation and depreciation of StealthCrypto’s. You bear the sole responsibility to determine such implications and act in accordance with the law that applies to you.

6.3 If you are purchasing StealthCrypto tokens on behalf of any entity, you are authorized to accept these terms on such entity’s behalf and that such entity will be responsible for any damage arising out of a breach of these terms by you or any other employee or agent of such entity (references to “you” in these Terms refer to you and such entity, jointly).

6.4 To the extent permitted pursuant to applicable law, you shall indemnify, defend, and hold Stealth Grid™ and/or its respective past, present and future employees, officers, directors, contractors, consultants, volunteers, equity holders, suppliers, vendors, service providers, parent companies, subsidiaries, affiliates, agents and representatives harmless from and against any and all claims, damages, losses, suits, actions, demands, proceedings, expenses, and/or liabilities (including but not limited to reasonable attorneys’ fees incurred and/or those necessary to successfully establish the right to indemnification) filed/incurred by any third party against Stealth Grid™ in connection with the StealthCrypto system arising out of a breach of any warranty, representation, or obligation hereunder.

7. PRIVACY POLICY

7.1. By purchasing StealthCrypto® Tokens, you agree to your personal data, i.e. e-mail address and/or name, being processed by Stealth Grid™ for its business purposes or the purposes of building, promoting, and communicating (about) the StealthCrypto® system and the StealthCrypto® Tokens.

7.2 Stealth Grid™ agrees to keep your email address and other personal data private and not share it with the public, e.g. by including it on any external lists or selling to any third parties.

8. FINAL PROVISIONS

8.1 Stealth Grid™ will cooperate with all law enforcement inquiries, subpoenas, or requests provided they are in congruence with International law.

8.2 Stealth Grid™ reserves the right to change, modify, add, or remove portions of these terms at any time during the sale and afterward by posting the amended terms on the StealthCrypto® project website (StealthCrypto.io, subsequently referred to as „the website”), as well as making a public announcement. The revised version will be effective at the time Stealth Grid™ posts it on the website unless indicated otherwise. Nonetheless, Stealth Grid™ will provide 10 working days’ notice of any substantial changes.

8.3 These terms shall be governed by and construed in accordance with the laws of USA in exclusion of the conflict of laws and all international conventions applicable.

8.4 Any dispute arising under these terms in or without the connection with the use or sale of StealthCrypto® Tokens shall be subject to the exclusive jurisdiction of the courts competent for

8.5 If any term, clause or provision of these Terms is held unlawful, void or unenforceable, then that term, clause or provision will be severable from these Terms and will not affect the validity or enforceability of any remaining part of that term, clause or provision, or any other term, clause or provision of these Terms.
8.6 The company may, at its sole discretion, assign its rights and/or delegate its duties under this contract. You may not assign your rights or delegate your duties, and any assignment or delegation without the written consent of the company, which the company may withhold at its sole discretion.

8.7 By acquiring StealthCrypto® tokens, you confirm that, to the extent permitted by law, you are authorized to acquire the tokens and accept to be bound by these terms in your relevant jurisdiction.

8.8 If you have any questions, please contact Stealth Grid™ by e-mail at info@stealthgrid.com
REFERENCES

A) Megatrends and market drivers 2025, Z punkt – The Foresight Company 2014


D) Definition of “blockchain” found at: https://en.oxforddictionaries.com/definition/blockchain

The Stealth Grid™ project plans to attract investments via the Initial Coin Offering (ICO) method, by issuing its own tokens with a limited emission, corresponding to a widely accepted standard, ERC20. After the ICO, no coins will be issued, so any inflation is ruled out. The token will use a smart contract written in the Solidity language. The principle of open and transparent funds distribution will be observed. All transactions will be shown in the smart contract.

The ICO’s start is scheduled for January 28, 2018 and is going to last for 35 weeks. Maximum target figures for attracted funds during the ICO is an amount equivalent to USD $200 million.

The tokens can be purchased with Bitcoin (BTC), BitcoinCash (BCC), Litecoin (LTC), Ethereum (ETH). If $200million is attracted (given that all the tokens will be sold out during the first two days), 400,000,000 tokens will be issued.

Investors will get the tokens within 7 days after the sale is closed.

If USD $200 million is attracted (given that all the tokens will be sold out during the first two days):

Stealth Crypto Value

$0.50 USD = 1 QMN

Total Token Sale

400M = $200M

QMN = QUANTUM MESH NETWORK (QMN)
**PROJECTED ROADMAP**

**QUANTUM CYBER SECURITY SOLUTIONS**
*Projected Q3 2019*

Launching unified blockchain peer to peer communication products that include, IM, cloud storage and file sharing, email, voice, and video conferencing that use Dynamic Split Encryption, Dynamic GeoDistribution, authentication, and our proprietary Quantum cyber security technology.

**QUBIT BLOCKCHAIN DEVELOPMENT AND TESTING**
*Projected Q4 2019*

Develop and Test Qubit Blockchain for implementation in our Quantum Mesh Network

Make technology acquisitions and submit patents for Qubit Blockchain as well develop channel partners and agnostic Stealthcrypto software and hardware.

QUBIT Exchange ATM

**QUBIT EXCHANGE LAUNCHING**
*Projected Q2 2019*

Launch Qubit Exchange and develop a Alt coin for the exchange.

**STEALTHCRYPTO® DISTRIBUTED NETWORK – QUANTUM MESSED NETWORK**
*Projected Q3 2019*

A StealthCrypto® meshed peer to peer cloud storage network would implement end-to-end dynamic split encryption and dynamic geo distributed models with disruptive authentication algorithms using quantum number generators of decentralized IBE – key distribution through blockchain.

Additionally launching our Stealthcrypto® phone.

**QUBIT BLOCKCHAIN LAUNCHING**
*Projected Q1 2020*

Launch Qubit Blockchain to be used within the Stealth Grid Technologies, StealthCrypto ecosystem and its Quantum Mesh Network.