

# CryptoSecure™

**Providing Hackproof Platform Solutions  
that are Secure, Private, and Trusted**

**Secure Private Keys  
Secure Accounts  
Secure Transactions  
Secure Cryptocurrency Exchange  
Secure Communication**

*“Financial markets organizations, restricted by stringent regulations, are investing in blockchain solutions across business areas to cut down on existing business frictions, rather than to grow.*

*Our research highlights why you need to quickly get on board, or lose out on not just the benefits, but miss out on setting the standards and defining how the ecosystem will operate.” IBM Institute for Business Value*

**11 March 2018**

# CryptoSecure™

## INDEX

<b>INTRODUCTION</b>	<b>3</b>
CryptoSecure Mission	3
Security is the Threat	3
Major Issues to Security and Privacy - The Challenge	5
The CryptoSecure Solution	5
<b>HOW CRYPTOSECURE WORKS</b>	<b>6</b>
Objective	8
Resolving Identity and Transactional Issues	9
Issues Overview	9
Technology	9
Security Factors	10
Products	11
Patent Protection	13
<b>BLOCKCHAIN</b>	<b>13</b>
<b>CRYPTOCURRENCIES</b>	<b>14</b>
Trust – Security – Confidence	14
<b>CRYPTOSECURE TECHNOLOGY RECOGNITION AND PEDIGREE</b>	<b>15</b>
<b>CRYPTOSECURE ESTABLISHMENT</b>	<b>16</b>
<b>SERVICE OPERATOR/ADMINISTRATOR</b>	<b>16</b>
<b>CRYPTOSECURE BETA TEST &amp; LAUNCH OFFER</b>	<b>16</b>
CryptoSecure ICO	17
CryptoSecure Coins (SECURE)	17
<b>OPERATIONS ROADMAP</b>	<b>18</b>
<b>FINANCES</b>	<b>19</b>
Use of ICO Proceeds	19
Marketing and Business Development	19
Target Market	19
CryptoSecure ‘SafeWindow’ Use Detail	20
Operational Revenue and Costs	20
<b>LEGAL CONSIDERATIONS</b>	<b>21</b>
Legal Landscape for CryptoSecure SECURE Coins and Related Rights	21
CryptoSecure Participation Rights	22
Legal Costs	22
CryptoSecure Product Development	22
Accuracy of Information	23
Consents	23
<b>SUMMARY &amp; INQUIRIES</b>	<b>23</b>

# CryptoSecure™

## INTRODUCTION

By using CryptoSecure today, your trading, cryptocurrencies, private keys and other transactions can avoid hackers and be totally PRIVATE and SECURE!

The CryptoSecure Platform will ultimately comprise of further enhancements and products that assure military-grade security, privacy, and trust across the entire cryptocurrency chain. The major marketplace product launch milestones being:

1. CryptoSecure 'Safe Window'	March 2018	Secures private keys
2. 'SafeWindow' Premium	Q2, 2018	Secures private keys
3. CryptoSecure Wallet	Q2, 2018	Further security
4. CryptoSecure Exchange	Q1, 2019	Secure trading assets
5. Trusted Solaris OS/OTP Platform	Q1, 2019	Optimal security

## CryptoSecure Mission

1. To provide a cryptocurrency use and transactions platform with unprecedented security, privacy, and asset protection.
2. To become the premier cryptocurrencies and blockchain security solutions provider.

## Security is the Threat

Over the past 12-18 months, despite some major corrections, cryptocurrency markets have grown exponentially. Being a digital market, the hacking of private keys, accounts and exchanges resulting in major losses and theft of cryptocurrencies, is equally exponential and continues unabated.

**Security is the major threat to cryptocurrency market growth, as without it there is no trust.**

**Q. How do you know if your private key has been hacked?**

**A. *Your cryptocurrencies have been stolen.***

**Q. How do you know if your PC, laptop and/or smart device has been hacked?**

**A. *You DON'T.***

**Q. How can I secure my cryptocurrency trading, private key, and wallet?**

**A. *Simple – CryptoSecure.***

**As is very evident, cryptocurrency exchanges, private keys, identities, transactions, and wallets are currently NOT safe, secure, or private.**

# CryptoSecure™

**CryptoSecure is out to change this landscape as it launches breakthrough security solutions.**

Despite blockchain itself being secure and immutable, investor wallets and cryptocurrency accounts increasingly continue to be subject to theft, exploitation, hacks, phishing, and fraud. Associated reported cryptocurrency theft over the past 12 months was well over \$1 billion, with incidents of unreported theft from user wallets estimated at **an additional \$350 million**. Examples of recent significant incidents include:

- In February 2018, BitGrail was hacked for \$170 million
- In January 2018, \$530 million was hacked from Coincheck
- Digital marketplace, NiceHash was hacked for \$64 million in December 2017
- South Korean exchange Youbit shut down after being hacked blaming North Koreans
- In November 2017, Tether was hacked for \$31 million
- In 15 minutes in October 2017, 39 parties had their EtherParty token purchases stolen
- The Enigma ICO in September 2017 saw around \$500,000 being stolen through phishing
- \$50,000 was phished during the KICK ICO in August 2017
- The Bithumb exchange incident in Korea where over 31,000 accounts were compromised
- A phishing exercise for Ethers in July 2017 netted the perpetrators \$600,000
- Veritaseum lost \$8.4 million in July 2017
- Coindash was hit for over \$7 million in July 2017
- The \$32 million Parity hack affected Edgeless Casino, Aeternity and Swarm City ICOs
- Bitcurex exchange shut down after 2,300 Bitcoins were stolen from client accounts
- Bitfinex accounts were hit for 119,756 Bitcoins in August 2016

With alarming regularity, the headline stories highlight the major threats to private key security, and the security deficiency of cryptocurrency wallets and exchanges. **What is NOT reported are the 1,000s of personal account thefts. Just this year cryptocurrency theft is running at around \$9 million per day.** Some recent industry publication includes:

- <http://www.independent.co.uk/news/business/analysis-and-features/cryptocurrencies-hackers-fraudsters-digital-financial-transactions-bitcoin-virtual-currency-failures-a7982396.html>
- <https://www.wired.com/story/why-its-so-easy-to-hack-cryptocurrency-startup-fundraisers/>
- <https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html>
- <https://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers/#340c161738ba>
- <https://www.cryptocoinsnews.com/stealing-bitcoin-with-a-name-and-a-phone-number/>
- <http://fortune.com/2017/08/22/bitcoin-coinbase-hack/>
- <https://teiss.co.uk/threats/cryptocurrency-hacks-hacking-unhackable-blockchain-secured-accounts/>
- <https://thehackernews.com/2017/07/bitcoin-ethereum-cryptocurrency-exchange.html>

# CryptoSecure™

## Major Issues to Security and Privacy – The Challenge

Tackling cryptocurrency private key security, wallet and account transactions, asset security, and privacy, involves major technological innovation able to resolve multiple threats including:

- Key-loggers
- Spyware
- Man-in-the-Browser
- Man-in-the-Middle
- Ransomware, Viruses, and Trojans

- BIOS/Firmware hacks
- WebGL Shader processes hiding in the GPU
- Elements of social engineering
- Passwords, private keys, other data
- Public Wi-Fi networks

If cryptocurrencies are to be more efficient, secure, and private, five major security issues need to be addressed and resolved:

- Private key security
- Identity security and privacy
- Wallet, account, and transactional security
- Exchange security
- Methods of securely communicating and transacting in a massively wireless world

**If not resolved, the hacking problems that exist today will continue to escalate dramatically.**

For the cryptocurrency market to continue its growth and to become a serious alternative for fiat currencies, total security is essential. If not provided, then global mass market trust, confidence, and adoption will not be realized.

## THE CRYPTOSECURE SOLUTION

In its simplest and most basic explanation:

**No one can hack into anything that DOES NOT EXIST and/or CANNOT BE SEEN.**

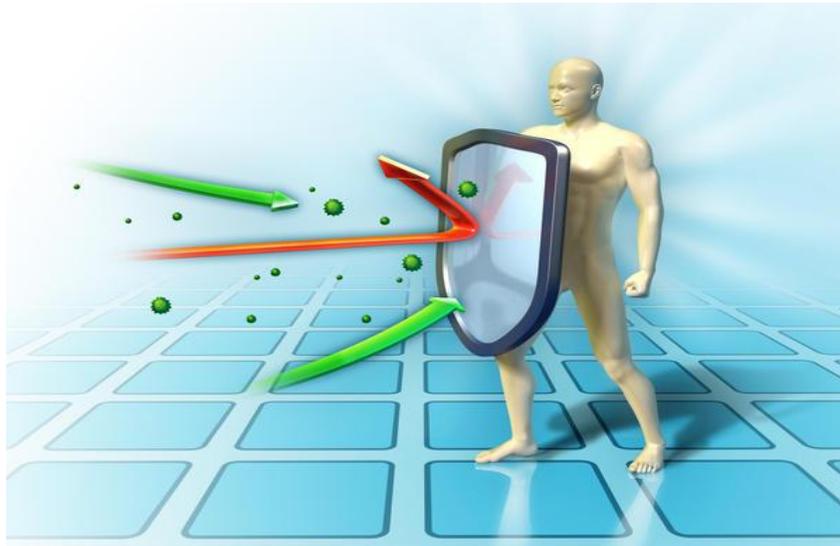
The CryptoSecure Platform solution for cryptocurrency security of private keys, transactions, and wallets ensures your assets always remain safe and are never exposed. With CryptoSecure:

- A new **invisible** virtual computer (VM/Identity) is created for every online session
- Transactions are conducted through instantly created **invisible** virtual devices
- On completion of each transaction, the virtual computer and device disappear

Basically – a new cloud-based CryptoSecure ‘machine’ is created for each new session. It’s like acquiring a new computer for each trading session and disposing of it when the session finishes.

# CryptoSecure™

Coupling this level of security with a CryptoSecure peer-to-peer Cryptocurrency Exchange within a hybrid military-grade blockchain/TrustedSolaris OS/One-Time-Pad Platform framework will provide the most comprehensive security and trust within the industry.



## HOW CRYPTOSECURE PLATFORM WORKS

**The CryptoSecure Platform sidesteps every known attack vector assuring the entire technology stack integrity.** No other known technology can ensure the integrity of all possible combinations of software modules, user authentications, tracking, applications, browsers, plug-ins, and live internet connections on a device.

The four major components of the CryptoSecure Platform security solution will comprise:

- A CryptoSecure digital identity (virtual computer) that changes with each session
- Military-grade technologies and products that prevent private key compromise and account takeovers
- First product 'SafeWindow' providing 'invisibility' of transactions and communications
- A CryptoSecure Platform wallet incorporating additional security
- An authentication process for each transaction replacing and/or supplementing the two-factor authentication commonly used on mobile devices and most PCs

By using CryptoSecure 'SafeWindow', private keys, and wallets will not be able to be compromised, nor will a user's identity or transactions. Each transaction will be conducted by an 'invisible' trusted avatar using an 'invisible' private key within the user's CryptoSecure 'invisible' wallet or account. In each case the avatar, private key, wallet, or communication disappears after each session.

# CryptoSecure™

## Is CryptoSecure Hackproof?

Technically, as many IT specialist will advise, nothing is hackproof. In stating that CryptoSecure products such as 'SafeWindow' are hackproof, they are as close to hackproof as you can get. It is near impossible for hackers to get a user's private key or to access their wallets, as it is close to impossible to find the user's 'invisible' isolated session. As soon as the user closes the trading session, everything disappears never to be seen again. This does not mean that a user's cryptocurrency cannot be hacked through their exchange, other interactive points, or by not following use directions.

Ultimately as CryptoSecure completes the build-out of the entire cryptocurrency environment operational platform, using technology developed for military and government use, as well as its licensed and other proprietary technologies, the closed-loop will be hackproof. This will enable all market participants, such as exchanges, wallet providers, etc., as well as token holders to participate within this closed, trusted CryptoSecure Platform.



The CryptoSecure 'SafeWindow' product is progressively being adapted for specific cryptocurrency use and, ultimately, will be substantially further enhanced within the Platform.

The CryptoSecure Platform and 'Remote Isolation' technologies ensure the endpoint device being used is secure, anonymous, and untraceable from hackers – **the optimal invisibility**.

## Resolving Identity and Transactional Issues

Digital Identity is a core value in all digital transactions and interaction, and identity theft is rampant across all online activities. User Name and Password authentication (2FA) is no longer sufficient protection and, as blockchain and cryptocurrencies integrate into commerce, transactional, value and communication enterprises, identity protection and security become critical.

Ultimately, CryptoSecure will maintain a distributed ledger of validated identities within a blockchain enhanced Trusted Computing environment. When users are communicating or transacting, they will be issued random CryptoSecure avatars that bypass any malware or endpoint hack on a local PC, laptop or smart device. CryptoSecure provides a secure isolated environment from which to conduct online transactions or communications. It does this by creating invisible endpoints that sidestep malware laid down by hackers and provides immunity from malware/ransomware by isolating the execution to a remote machine.

# CryptoSecure™

Using the recently release first CryptoSecure ‘SafeWindow’ App creates a user avatar on the user’s PC. It then launches a remote machine (computer) that appears on screen as a CryptoSecure ‘SafeWindow’ where cryptocurrency transactions can be securely, and anonymously processed.

The CryptoSecure solution is predominantly cloud based and is delivered as Software-as-a-Service (SaaS). The user’s remote virtual computer is locked to a specific physical device ensuring their session cannot be hijacked. It effectively delivers secure endpoints via the cloud which bypass all known attack vectors including BIOS Basic Input/Output System) firmware hacks.

**Using CryptoSecure security solutions is equivalent to buying a brand-new computer for every transaction and then discarding it after use. It is a factory-reset where the system architecture upgrades on each login to the latest supported version of every software component.**

To ensure the local keyboard and operating system are not susceptible to any local key-logger attack or other compromise, additional solutions are incorporated. These include a virtual keyboard generated and delivered as an image interfacing with the CryptoSecure ‘SafeWindow’. This App is available as a free download at Google Play and the Apple Store .



This “Invisible Keyboard,” is patent protected and runs from a separate device, such as a cell phone or tablet, bypassing the local PC completely. The keyboard displayed on the cell phone or tablet screen is, in effect, a secret handshake exchanged with the remote machine. An encrypted connection is established so that only the remote machine with which it is paired can interpret a user’s actions on the phone or tablet. **No character ever exists in the mobile device and there is no feedback mechanism, other than a vibration, making it invisible to the operating system.** When a user enters characters into a password field, the characters appear as asterisks on the local PC. The user can also connect multiple devices in parallel to further scramble input, so the complete sequence does not need to be entered through one device.

## Issues Overview

- Most cyber-attacks target access through a PC, tablet, or Smartphone end points, as these are the weakest link in any network or online presence. ‘Dirty’ browsers and devices should not be used when security is paramount (as in transactions involving cryptocurrencies).
- Most connected devices regularly using the Internet, especially when connected wirelessly, are already breached (dirty) and at risk of exposure to identity and financial theft.

# CryptoSecure™

CryptoSecure can deliver the entire technology stack within which transactions are conducted ensuring the integrity and security of the total system. CryptoSecure technologies will provide users with pristine new endpoint virtual computers built almost instantly at randomized Internet addresses. These invisible devices are then used for all online transactions.

- **For CryptoSecure wallet users, the user and the endpoint are both secure, anonymous, and untraceable.**
- **CryptoSecure Platform security solutions bypass all known hack attack vectors including BIOS hacks, key loggers, man-in-the-middle, man-in-the-browser, ransomware, etc.**

## Technology

- Client options for deployment include USB boot image for PC hardware and SaaS for existing operating systems and users. Remote data centers host the backend service.
- 3 Factor Authentication (FA) guarantees it is a specific user logging in from a specific machine. Username/password, CryptoSecure software and hardware signature of the device ensure the user session cannot be hijacked.
- Optional 4FA or 5FA options, such as biometrics or location, can further improve security.
- A virtual user (avatar) is instantaneously created through a blockchain enhanced Trusted Computing environment to conduct transactions.
- A hardened Linux Internet virtual machine (VM) is instantly randomly created forming a pair-coupled connection with the physical device. Thin client architecture displays a virtual user and a virtual desktop over an encrypted connection.
- The architecture is self-evolving creating future-proof infrastructure on-the-fly. Thousands of new virtual machines every few minutes, if needed.

## Security Factors – Including Planned Future Enhancements

- CryptoSecure ‘SafeWindow’ replaces the visible user with an invisible virtual machine that disappears without trace after each use.
- CryptoSecure ‘SafeWindow’ replaces ‘dirty’ (infected) PCs, tablets or smartphones with pristine new endpoints which evaporate without trace after use.
- Every component within the entire CryptoSecure technology stack is controlled so secure use of private keys, wallets and accounts can be assured.
- The fundamental principles of CryptoSecure technology are simple. The visible user is replaced with an untraceable virtual machine sidestepping the endpoint device and any inherent issues completely. **It is analogous to an anonymous wallet holder using a completely new computer for every critical online transaction or communication session.**

# CryptoSecure™

- CryptoSecure sessions are locked to specific devices ensuring they cannot be hijacked.
- Virtual machines (VM's) are built in less than two seconds and evaporate without trace when transactions are completed along with all local history. **Each login initiates a completely fresh rebuild with no past history.**
- The VM's hardened Linux image is designed to minimize the attack surface and the self-evolving architecture ensures latest version updates of all software modules.
- Drive-by-Download vulnerabilities which exist in any browser or plug-in are handled by an instantaneous rebuild feature which is like a factory reset. This also guarantees the latest versions of all software modules.
- Existing security measures, like 2FA, are augmented - not replaced.
- Potential compromises in wireless keyboards, BIOS/firmware or using Key-loggers, screen snapshots or other malware are sidestepped.
- CryptoSecure security solutions provide a temporary, disposable, 'SafeWindow' online presence immune to malware, as well as being invisible to hackers.

## Products and Indicative Timeline

The ultimate CryptoSecure product range will incorporate the following:

### CryptoSecure 'SafeWindow' – Available March 2018



- An exclusively licensed (cryptocurrencies and blockchain use) software App that is progressively being modified for specific cryptocurrency applications. It is downloadable on any PC or smart device. Whilst it cannot control the local Operating System it foils key-loggers or screen-snapshot malware by using an “invisible” and safe keyboard.
- The “Invisible Keyboard” creates the illusion of a keyboard on smart devices and an encrypted connection ensures only the remote VM it pairs with can interpret a user's actions on the smart device. As no character ever exists on the smart device itself and it is invisible to the device operating system.

# CryptoSecure™

## **CryptoSecure ‘SafeWindow’ Premium - Available Q2, 2018**

- For ultimate security, CryptoSecure will provide a hardware device (USB key) and a downloadable version providing complete control over the entire system and technology stack. All attack vectors known are sidestepped including malware, viruses, as well as BIOS hacks.
- The premium product is fully developed and exclusively licensed for CryptoSecure use and incorporation in cryptocurrency and blockchain applications.

## **CryptoSecure Wallet ‘Lite’ - Available Q3, 2018**

A dedicated CryptoSecure cryptocurrency wallet. The wallets will be multi-currency allowing easy implementation of several different cryptocurrencies. All cryptocurrency funds can be automatically secured via 2FA or 3FA cold storage allowing you to keep your crypto funds locked up and preventing all external access.

## **CryptoSecure Wallet - Available Q3, 2018**

Before release by CryptoSecure, it will be modified as a cryptocurrency wallet optimized to address specific additional cryptocurrency security and functionality requirements.

## **CryptoSecure Exchange – Available by Q1, 2019**

- The CryptoSecure enabled exchange will provide for a level of seamless end-to-end security unmatched within the cryptocurrency markets.
- The exchange plans to not maintain any records of closed transactions, thereby preserving privacy rights, and confidentiality.
- The CryptoSecure Exchange will operate on a fee basis.

## **‘CyberAvatar’ – Incorporated as a free upgrade Q3, 2019**

- A CryptoSecure user avatar incorporating Trusted Computing user identity security will be incorporated, pending successful completion of development, as a free upgrade.

## **‘CyberTrack’ – Incorporated as free upgrade Q4, 2019**

- A proposed highly sophisticated transactional tracking layer that provides instant alerts regarding any data changes and/or intrusions whatsoever. Subject to successful completion of development, this feature will be integrated as a free upgrade.

# CryptoSecure™

## Patent Protection

The CryptoSecure security solutions for cryptocurrency private key security, transactions, and wallets are proven robust technologies supported by four Patents held by GoPC Pty Ltd, a CryptoSecure products Licensor. Further Patents, in planning and in process, together with proprietary intellectual property, will remain confidential to CryptoSecure, and to GoPC and Key Capital Corporation, the CryptoSecure product Licensors.

CryptoSecure security solutions use a combination of technologies developed and in development specifically for CryptoSecure, as well as technologies exclusively licensed and/or partnered.

## BLOCKCHAIN

Over the past 20 years the Internet has changed our lives, the way we communicate, transact, pay bills, and receive and share information, etc. Many companies have leveraged the Internet with some becoming among the largest and most valuable companies in the world.

Blockchain is similarly disruptive and will re-write most everything, especially in communications, transactional, security and financial markets – **the cornerstones of all commerce.**

Blockchain technology provides an ingenious way to securely store data and verify its integrity through a decentralized and distributed network. Blockchain inherently protects all transactions by adding each transaction to the distributed blockchain ledger so that they cannot be changed.

Within the next decade, blockchain technology applications are expected to become just as important as the Internet itself and equally as valuable.

***“Our research highlights why you need to quickly get on board, or lose out on not just the benefits, but miss out on setting the standards and defining how the ecosystem will operate.”*** IBM on blockchain

***“We think blockchain is going to potentially transform every industry.”*** Microsoft Azure

## CRYPTOCURRENCIES

The concept of decentralized, digital, ‘private currencies’ is nothing less than revolutionary, as is evidenced by the rapid growth in the cryptocurrency market. However, the single most significant cryptocurrency concern is the hacking of private keys, as this leads to immediate economic loss.

For all the forecasts, predictions, and the promise of cryptocurrencies to be realized, the rampant hacking needs to be eliminated. Private key, transactional, wallet, and communication security is paramount. Without total security, there will be no trust or confidence in cryptocurrencies, and there will be no mass market.

# CryptoSecure™

**CryptoSecure is committed to becoming a significant catalyst, and major market player through provision of ground-breaking hackproof security solutions.**

## **Trust – Security – Confidence**

Globally, there is clearly a declining confidence in banks, governments, and authorities (including regulators) as highlighted by numerous events globally.

Despite financial markets being highly regulated their failings are a matter of record evidenced by multi-billion-dollar fraud/failure by 'trusted' and 'regulated' parties like Lehman Brothers, WaMu, IndyMac, Netbank, American Savings and Loan, Bank of New England, Sachsen, the Icelandic banks, LTCB of Japan, New Frontier Bank, Madoff, Enron, Tyco, Parmalot, Adelpia, Bre-X and many others. In the penny stocks, venture and OTC markets, there is little that regulation and oversight can do to protect investors, as the record constantly demonstrates.

The unfortunate reality is that despite our sophisticated systems and complex laws, **consumer, user, and investor protection leave a lot to be desired. Trust and confidence is severely damaged for the average person.** In current flawed regulated markets, denying free-choice alternatives or early investment opportunities in equities or in cryptocurrencies is also not a true and fair solution.

It is imperative that security, trust, and confidence in cryptocurrencies are integral pillars of this fast-moving change across industries. This in turn provides **major opportunity for the ground-breaking CryptoSecure Platform security solutions.**

**Combining blockchain transparency, security, and immutability with CryptoSecure protection for use in protecting cryptocurrency private keys, wallet, and other account transactions will introduce ultimate trust, and a unique security value to blockchain and cryptocurrency markets.**

A 2016 World Economic Forum paper predicts blockchain will be **the 'beating heart' of the global financial system**, identifying it among 10 emerging technologies forecast to disrupt global industry. Clearly, **early movers are presented a generational opportunity for ground-floor participation.**

# CryptoSecure™

## CRYPTOSECURE TECHNOLOGY RECOGNITION AND PEDIGREE

CryptoSecure security technologies, including those licensed, partnered, and under development, have solid pedigrees and global recognition.



**World Cup Tech Challenge  
Winner Silicon Valley 2016**



GoPC Pty Ltd (BankVault), a major CryptoSecure partner and licensor, is a globally-recognized and awarded cyber security innovator



Cyber economy researcher and publisher, Cyber Security Ventures, has included BankVault in the prestigious current Cybersecurity 500, the industry's definitive list of the hottest and most innovative companies in the cybersecurity industry.



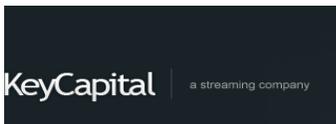
Trusted access technology being incorporated into CryptoSecure solutions is partially based on Trusted Systems authentication and security systems developed at the Lockheed Martin Trusted Laboratories business unit – which was subsequently sold by Lockheed Martin.



CryptoSecure plans to incorporate advanced surveillance monitoring and reporting for detecting unauthorized data changes. The core technology originated at US defense contractor Aerospace Corporation to provide real-time alerts to any unauthorized data change.



Authorities planned to be incorporated into the CryptoSecure solutions are based on an originating 1995 OTP (One Time Pad) patent subsequently incorporated in security solutions using Sun Microsystems Trusted Solaris by parties now appointed as CryptoSecure consultants.



Select Key Capital personnel have extensive experience and expertise in development of high security Trusted Systems application of OTP, and Trusted System integration.

# CryptoSecure™

## CRYPTOSECURE ESTABLISHMENT

The CryptoSecure SECURE cryptocurrency has been established as a decentralized nationless enterprise currency with its economy to be managed by its Service Operator, Crypto Investor, Inc., a Belize corporation governed under English Common Law, augmented by local legislation. Crypto Investor is a Blockchain focused consulting group, project developer and project incubator working on a small pipeline of select innovative industry opportunities.

CryptoSecure Platform security solutions have emerged through Crypto Investor initiating a cryptocurrency and blockchain security opportunity and engaging parties that, within the past two decades, have developed digital security innovations including through relationships/projects with the Aerospace Corporation, Electronic Data Systems, Sun Microsystems and, most recently, with GoPC Pty Ltd and Key Capital through exclusive license agreements.

## SERVICE OPERATOR/ADMINISTRATOR

Crypto Investor, Inc., management, and core consultants have diverse commercial and technical experience and expertise. Crypto Investor will serve as the appointed CryptoSecure Service Operator/Administrator and will manage and/or oversee all aspects of product development, deployment, and operational coordination. Crypto Investor will also manage the CryptoSecure cryptocurrency economy.

The Service Operator will provide the means to effectively manage and materialize any actions required to continue the development and commercialization of the CryptoSecure economy products, as well as the optimization of the CryptoSecure cryptocurrency economy in general. This provides for ready interaction wherever required with any other entities, private, corporate, or governmental. Should Crypto Investor at any time cease to provide this service, be incapable of providing this service or resign from any aspect of its contracted service operation, Crypto Investor shall immediately appoint an alternative party to act for CryptoSecure and/or the interests of the CryptoSecure cryptocurrency economy.

Should, for any reason, any formal licensing or similar be required in any global jurisdiction in which CryptoSecure security products are offered and/or sold, Crypto Investor will seek such licensing and/or approvals as required.

Crypto Investor does not and will not claim or register any kind of property, trademark or other rights pertaining to any of the CryptoSecure security solutions in its own right. All intellectual property rights, patents trademarks, branding and other rights will remain exclusively held for the benefit of the CryptoSecure economy and, where applicable, of its partners, and/or licensors.

# CryptoSecure™

## CRYPTOSECURE 'SAFECWINDOW' ICO LAUNCH OFFER

Following successful CryptoSecure Beta Testing of the licensed CryptoSecure 'SafeWindow' product as it is being adapted for the cryptocurrency and blockchain market, the 'SafeWindow' security product will be **available at almost half price** during the ICO period and through to 30 June 2018.

As security of private keys and cryptocurrency wallets is paramount and critical to all cryptocurrency dealings, and wallets, it is expected that there will be significant interest in and demand for the CryptoSecure 'SafeWindow' product. Especially as **there is no other known product offering an equivalent level of protection for private keys and cryptocurrency transactions.**

### CryptoSecure 'SafeWindow'

#### Launch Offer (available to 30 June) Regular Pricing

Monthly: US\$25.00

Monthly: US\$45.00

Annual: US\$250.00

Annual: US\$450.00

### CryptoSecure 'SafeWindow' Premium

CryptoSecure 'SafeWindow Premium' is a unique operating system (OS) that runs remotely and separate and independent from the installed OS. After each use, simply restart your computer to resume the factory installed OS.

#### Available Soon (to 31 December) Regular Pricing

Monthly: US\$65.00

Monthly: US\$120.00

Annual: US\$650.00

Annual: US\$1,200.00

A 'Store' link for the purchase of the promotional CryptoSecure 'SafeWindow' product is available at **CryptoSecure.com**.

## CryptoSecure ICO

The CryptoSecure ICO is scheduled to close on 26 April 2018. Participation in the CryptoSecure SECURE coins is through exchange with Ether (ETH). For the duration of the ICO, CryptoSecure is using a fixed price of US\$975 per ETH, which is a substantial premium to current market. The CryptoSecure ICO may be closed any time at the exclusive election of the Service Operator

ICO Round 1 – To March 21	9750 SECURE Coins per ETH
ICO Round 2 - To April 4	6500 SECURE Coins per ETH
ICO Round 3 - To April 18	4875 SECURE Coins per ETH
ICO Round 4 - To April 26	3900 SECURE Coins per ETH

# CryptoSecure™

## CryptoSecure Coins (SECURE)

A CryptoSecure Coin (SECURE) is a secure blockchain Ethereum ERC20 standard software accounting unit (smart contract) that has utility as a cryptocurrency able to be traded on exchanges and used to purchase goods and services. SECURE coins are also required to purchase monthly or annual CryptoSecure security software licenses, and in future other CryptoSecure services, including transactional fees for using the planned CryptoSecure peer-to-peer exchange.

SECURE coins provide the utility for all CryptoSecure partners and users to purchase, license, and/or otherwise use the range of CryptoSecure security and related products and/or services.

SECURE coins are not to be considered legal tender, securities, or commodities. They are specifically a utility cryptocurrency for use within the CryptoSecure economy, and able to be traded on the cryptocurrency market. SECURE coins are not redeemable for cash through CryptoSecure. Although SECURE coins may be traded on cryptocurrency exchanges, CryptoSecure disclaims all responsibility for their negotiability.

SECURE coins are a digital cryptocurrency asset, bearing value by themselves based on their underlying utility use and properties only. SECURE coins, like fiat currencies, convey no voting rights, no equity interest, or any other interest or entitlement in CryptoSecure, other than being the utility cryptocurrency of the CryptoSecure economy.

Crypto Investor, Inc., acting for the SECURE economy, reserves the right in its absolute discretion to deny any application to acquire the initial CryptoSecure 'SafeWindow' products and/or SECURE coins. Although CryptoSecure is a decentralized nationless enterprise, the CryptoSecure economy principles are aligned with Anti Money Laundering (AML), Counter Terrorism Financing (CTF) and, where applicable, Know Your Client (KYC) best practice and any regulations that may apply at any time or considered to be in the interests of the CryptoSecure economy in any geographic location.

At the time of ICO emission 2,000,000,000 minted SECURE coins will be automatically distributed across the CryptoSecure Service Operator, the CryptoSecure Licensors and project development partners, and well as to CrypDonate.org a social enterprise, as per details below.

These coins will be subject to strict escrow conditions regarding any sale into the market as follows:

- Year 1.           Zero sales permitted
- Year 2.           Any sales limited to 5% of respective holdings over 12-month period
- Year 3.           Any sales limited to 5% of respective holdings over 12-month period

Further, over the 3-year escrow period the coins cannot be lent out or borrowed against.

# CryptoSecure™

The Smart contract should provide for the following transfers at emission:

Wallet Interest	% of total Issue	Number of coins
Crypto Investor	12.5%	500,000,000
Crypto Investor on a/c team members & consultants	7.5%	300,000,000
GoPC Pty Ltd (Licensor & dev partner)	15%	600,000,000
Key Capital Corporation (Licensor & dev partner)	10%	400,000,000
CrypDonate.org (Social Enterprise)	5%	200,000,000
<b>Total</b>		<b>2,000,000,000</b>

A further total 2,000,000,000 minted SECURE coins will be held through CryptoSecure economy Treasury. They will be available for exchange during the ICO. Following the ICO all Treasury coins not exchanged shall remain in the CryptoSecure Treasury wallet and be subject to potential sale or exchange at future dates, be available for beneficial JV/partnerships/relationships, possible strategic acquisitions, or continue to be held in Treasury.

## OPERATIONS ROADMAP SUMMARY

### Platform, Infrastructure, and ICO

Current & January 2018	Feb/March 2018	July/Dec 2018	Jan/Sept 2019
Smart Integration Product optimization starts Risk Management integration	1 <sup>st</sup> Enhancement <b>'SafeWindow' Launch</b> <b>ICO launch</b>	CryptoSecure Wallet	Trusted Solaris OS & OTP CyberTrack incorporated Exchange launch

## FINANCES

CryptoSecure seeks exchange SECURE coins for at least 2 million Ether and an ambitious target in excess of 12 million Ether through its ICO. Net use proceeds, after launch costs, will be proportioned pro-rata between the 2 million and 12 million or more Ethers generate through the ICO in accordance with the indicative schedule as follows:

### ICO Breakdown: Use of net ICO proceeds in Ether

ICO Value	2,000 ETH	6,000 ETH	12,000 ETH
Continued development and/or acquisitions	80%	89%	90%
Consultants	6%	3%	3%
Legal/Accounting	6%	1.5%	1.5%
Marketing	8%	6.5%	5.5%

# CryptoSecure™

Any balance of SECURE coins held in treasury (up to a total 2 billion) following the ICO may be progressively offered at future dates dependent upon circumstances. They may also be used for strategic acquisitions or joint ventures and other value add relationships.

## Marketing and Business Development

It is expected that CryptoSecure will benefit substantially from both traditional and social media exposure as the security products offered are regarded as break-through for private key, identity, and transactional protection in the digital cryptocurrency and blockchain environment, especially with regard to the security of cryptocurrency private keys, wallets, and transactions.

Marketing will be supported through traditional and social media exposure and, further, through blockchain and cryptocurrency communities, trade shows and conferences.

A major CryptoSecure marketing advantage is that its initial 'SafeWindow' security product will have launched into the market at highly attractive pricing, in tandem with all public relations and promotional activity coordinated through the CryptoSecure Service Operator. Importantly, revenues from sales of the CryptoSecure 'SafeWindow' product are expected as from March 2018.

## Target Market

The CryptoSecure target market comprises all parties that:

- Trade cryptocurrencies
- Participate in ICOs
- Hold cryptocurrency wallets
- Issue cryptocurrency wallets
- Transact cryptocurrencies
- Issue cryptocurrencies, especially ICOs
- Hold cryptocurrency accounts

## CryptoSecure 'SafeWindow' Use Detail

By using the 'SafeWindow' product, users never need to enter their cryptocurrency private key into any physical computer, laptop, or smart device ever again – it is all done invisibly through an invisible keyboard protected by military grade encryption and technologies.

All CryptoSecure 'SafeWindow' product purchasers will be entitled to respective automatic free upgrades as the CryptoSecure products continue to be enhanced. Operationally, the CryptoSecure Platform product(s) will predominantly be provided as a Software as a Service (SaaS).

# CryptoSecure™

**If CryptoSecure captures just 5% to 10% of the cryptocurrency user market over the next three to five years, revenues to the CryptoSecure economy will grow rapidly and significantly.**

Additionally, on the CryptoSecure exchange launch in early 2019, the total end-to-end security will then provide opportunity for substantial revenue increase.

## Operational Revenue and Costs

Revenue and operational costs attributed to management of the CryptoSecure economy will be accounted for periodically on CryptoSecure.com. The costs will predominantly be incurred through the provision of services managed through the appointed Service Operator. The costs will include management fees, operational costs, cost of goods, costs of development and infrastructure and payable royalties and/or licensing fees.

## LEGAL CONSIDERATIONS

**Legal Landscape for CryptoSecure SECURE Coins and Related Rights:** As discussed herein, cryptocurrencies and blockchain developments are an area of interest for many regulators around the globe, including those in South Korea, Japan, Singapore, Hong Kong, European Union, China, the United States, and other jurisdictions where continued regulatory commentary actively originates. CryptoSecure SECURE coins are a pure cryptocurrency and are not considered legal currency tender or securities. Like Bitcoin and many other decentralized and nationless initiatives, the CryptoSecure SECURE coins hold great promise. However, the CryptoSecure economy intends to conduct its operations in accordance with the laws of any relevant jurisdictions, where and if applicable to it, and/or as required. As such, CryptoSecure SECURE coins and potentially a number of related rights may not be available in certain jurisdictions. In some jurisdictions there may be a requirement to first obtain licenses or other permitting as may be deemed to be required by regulatory and/or financial law before CryptoSecure SECURE coin holders in those jurisdictions may activate operational accounts.

It is noted that in the USA the SEC, in May 2017, advised any party involved in any ICO needs to be aware that although not regulated, companies and their promoters need to recognize their fiduciary duty to investors and protection of investors should be forefront. More recently, the SEC on 25 July 2017 advised: *“U.S. federal securities law **may apply** to various activities, including distributed ledger technology, **depending on the particular facts and circumstances**, without regard to the form of the organization or technology used to effectuate a particular offer or sale.*

The **European Central Bank (ECB)** has stated it did not regard or want to see virtual digital currencies labeled as money or currencies. More recently, in July 2017, the ECB advised the European Parliament it continues to monitor virtual currencies and, although of the opinion that virtual currencies have little impact on the ‘real’ economy, if associated risks are seen to increase then regulatory response would be more effective if coordinated at international level.

# CryptoSecure™

China has recently placed a ban on cryptocurrency ICOs, although this is believed to be under review as China seeks a way to control and/or monitor its citizens' activities in this regard. South Korea has banned ICOs totally.

CryptoSecure SECURE coins are cryptocurrency utility coins and not securities. CryptoSecure SECURE coins once issued and/or exchanged are non-refundable or reversible. CryptoSecure SECURE coins are not purposed for speculation or investment. No promises of future performance or value are made with respect to CryptoSecure SECURE coins, including no promise of inherent value and no guarantee that CryptoSecure SECURE coins will hold any particular value. Further, as CryptoSecure SECURE coins are a decentralized and nationless cryptocurrency they are not regulated by any country or authority.

Participation in all cases is up to the individual and it is incumbent upon any participant to ensure that they comply with the laws of their own respective jurisdiction.

**CryptoSecure Participation Rights:** CryptoSecure SECURE coin participation rights are limited to their utility and use rights and the SECURE coins hold no voting, direct equity, or other rights in the CryptoSecure economy that supports the SECURE coin cryptocurrency. With regard to the planned CryptoSecure SECURE coin ICO, CryptoSecure SECURE coin rights are limited to their use for exchange with multiple cryptocurrencies during the ICO or subsequent offer(s) as functional utility coins and as a cryptocurrency. During the ICO and any subsequent offer CryptoSecure SECURE coins are therefore first exchanged as a functional good in exchange for other cryptocurrencies. All such received coins or tokens may be used freely by the CryptoSecure economy to secure its planned operations as detailed in the indicative Use of ICO Proceeds section herein, absent any conditions.

CryptoSecure SECURE coins are intended for participants knowledgeable in dealing with cryptographic coins and/or tokens and blockchain-based software systems.

**Legal Costs:** Legal requirements include but are not limited to all final required or desired structuring, especially prior to the CryptoSecure SECURE coin ICO release. Ongoing resources may also be required for possible contingent legal work as a number of global authorities and/or governments ultimately may form views on cryptocurrencies and their offerings that may have an impact on CryptoSecure and/or the CryptoSecure SECURE coin ICO. Although CryptoSecure SECURE coins are not considered legal tender or securities, a contingency legal fund will be reserved for any potential future issues should they arise.

**CryptoSecure Product Development:** While each of the CryptoSecure security components is well developed, the overall software integration is still under development and will continue to be so as key operational aspects from its CryptoSecure 'SafeWindow' base moves to full development and commercialization. Although there exists every confidence for the CryptoSecure continued security product enhancement, there can be no assurance that planned product enhancements as described within this Whitepaper will be successfully integrated with the base BankVault 'SafeWindow' security product within the targeted timeframes, if at all.

# CryptoSecure™

**Accuracy of information:** The CryptoSecure Whitepaper and website include projections and information obtained and prepared internally through market research, publicly available information and industry publications. Such market research, publicly available information, and industry publications often state that the information they contain has been obtained from sources believed to be accurate and reliable. Consequently, CryptoSecure provides no assurance as to the accuracy or completeness of such included information.

**Consents:** Save for CryptoSecure and Crypto Investor Inc and their officers, no person has approved the content of this Whitepaper or the CryptoSecure website, or provided consent to the inclusion of his, her, or their name within this Whitepaper or the CryptoSecure website.

## COPYRIGHT AND TRADEMARKS

Except for any material in the public domain, this CryptoSecure whitepaper, its design, text, content, files, graphics, translations, and all trademarks, logos, service marks, symbols, trade dress and all materials provided in or through this whitepaper are protected by all applicable copyright and trademark laws and/or applicable international conventions and treaties. All such material including copyright and trademarks are the exclusive and proprietary property of Crypto Investor, Inc. on behalf of the CryptoSecure economy, and/or its third-party licensors, and/or service providers. ALL RIGHTS RESERVED.

## SUMMARY

**The CryptoSecure Platform introduces its breakthrough security products to the market as well as its cryptocurrency opportunity.** This provides for CryptoSecure SECURE coin holders the opportunity to capitalize on the potential rise of the rapid adoption of the CryptoSecure breakthrough blockchain and cryptocurrency security technologies, across all markets, through the CryptoSecure product and Cryptocurrency participation. The more users of CryptoSecure products and services, the more CryptoSecure can grow.

Following listing on cryptocurrency exchanges, CryptoSecure expects its SECURE coins to be highly liquid. CryptoSecure security products represent a major breakthrough in enabling the security of cryptocurrency private keys for accounts and wallets – **thus broadening CryptoSecure SECURE coin application, utility use, exposure and appeal.**

The **primary CryptoSecure objective** is to **establish CryptoSecure as a leader in the provision of blockchain and cryptocurrency security solutions and products.**

## INQUIRIES

For all inquiries and/or further information visit [CryptoSecure.com](https://CryptoSecure.com) or email [info@CryptoSecure.com](mailto:info@CryptoSecure.com)