BlockSafe TECHNOLOGIES™

Security Token Offering White Paper

Securing the Blockchain Ecosystem: Crypto Wallets, Exchanges & Permissioned Blockchains

Table of Contents

Overview

BlockSafe Technologies Inc., has developed products that secure the blockchain ecosystem (wallets, exchanges and private blockchains) from hackers. The company is launching an SEC-compliant STO and is targeting a raise of up to $27 million via a 506(c) and Reg S offering to accredited investors. The token will be called BSAFE™.

Why BlockSafe Technologies

Tackles a big problem	Patented Products	Large Market
Crypto currencies and the block chain are under attack by hackers. $1.1 Billion has been stolen in the first six months of 2018[3]. Our products offer a comprehensive solution to this problem using proven patented technologies.	The Company has developed two products for immediate sale – (CryptoDefender™ & ExchangeDefender™). A third product, BlockchainDefender™. is in development. Our products are covered by 10 patents (6 granted and 4 pending).	The products address a market of cypto users (24 million today growing to 200 million by 2025[1]) and enterprises deploying private blockchains. The blockchain security market is expected to reach $355 billion by 2022[2]

Experienced Team	17+ years of innovation	Reputable Advisers
The team comprises of seasoned veterans who have founded companies in the technology industry.	The products are licensed from StrikeForce Technologies which has a 17-year history of innovation in the Cyber Security industry.	The BlockSafe advisory board includes prominent industry experts such as the former CIO of Homeland Security and the founder of Security University.

SEC compliant token	Passive Income	Token liquidity
The BSAFE™ token is an ERC 20 security token that complies with SEC regulations.	BSAFE™ tokens provide passive income in the form of 10% of the revenue from the products.	The Company has an agreement to list the token on a SEC compliant exchange.

BSAFE™ Security Tokens Compared to Other ICO Tokens Offerings

The BSAFE™ Token holder will receive a passive income based on all sales. The typical ICO & Equity token does not pay passive incomes. Every time someone purchases BlockSafe Technologies software, the BSAFE™ token holder will receive 10% of the revenue participation.

"If you don't find a way to make money while you sleep, you will work until you die". - Warren Buffet

	BSAFE Revenue Participation Token	Typical "ICO" Token
Compliance	US SEC - Compliant Security Token	Non SEC Compliant tokens
Team	Successful Cyber Security Team serving millions of people for over 17 years	Newly Assembled Team
Product	CryptoDefender & ExchangeDefender are ready for sale, BlockchainDefender is in development and scheduled for Q3/19	Early-Stage, No Product
Use of Proceeds	Complete BlockchainDefender, expand reseller channel, corporate operations, Brand Marketing	Funding High-Risk ideas
Passive Income	10% of company's gross revenues to be shared with BSAFE token holders	No Passive Income
Value Drivers	Two Products are ready for sale Products are Patented $355 Billion Dollar Market Opportunity No competition, First Mover Advantage	Potential future utility usage

The Blockchain Ecosystem is under attack

$1.1 Billion stolen in first six months of 2018[3]

Wallets are getting hacked by malware using keyloggers to steal secret keys and clipboard capture to change destination addresses. The estimate for unreported user wallet losses are over $350 million[4]. If your wallet gets hacked, you can't get the money back nor can you sue anyone.

There have been numerous heists of cryptocurrency exchanges, many of which were later shut down. In the Mt. Gox hack, nearly 650,000 Bitcoins were stolen[5]. BitGrail was hacked for $170 million[6]. Coincheck was hacked for $530 million[7]. Digital marketplace, NiceHash was hacked for $64 million[8]. South Korean exchange Youbit was shut down after being hacked[9].

Blockchain platforms are also vulnerable. The DAO, an Ethereum project, was hacked. The hackers stole nearly $150 million.

Hackers are winning ….. Until Now

Our Solution

Every 4 seconds a new malware specimen is released. We contend that anti-virus software cannot keep up with this. Instead, our approach is to:

Assume malware exists in a system and stop its actions. i.e ->

Stop keylogging, clipboard capture, screen-scraping, clickjacking.

Authenticate every transaction.

Secure Wallet
CryptoDefender™

Secure Exchange
ExchangeDefender™

Secure Blockchain
BlockchainDefender™

We believe that we are the only company with a comprehensive solution!

Market Opportunity

Crypto wallet users to reach 200 million by 2025 (40% CAGR)[1]
Blockchain security market to reach $355 billion by 2022[2]

CryptoDefender™ for the desktop

CryptoDefender for the desktop has the following features –

Keystroke Encryption prevents malware from spying on what you type. The keystrokes are secured between the kernel and the wallet application using military grade encryption. Now, the password you enter to logon or decrypt your secret key is safe.

Clipboard copy protection prevents malware from monitoring the clipboard to spy on, copy and paste the contents of the clipboard. So the destination address to which a crypto transaction is sent to is not modified.

Anti-screen capture prevents screen-scraping malware from taking screenshots of information surreptitiously.

Anti-Clickjacking displays hidden frames or frames originating from a potentially malicious domain. This neutralizes one of the favorite tricks of the hackers to download malware onto your computer.

Available for Mac and PC

CryptoDefender™ for mobile devices

CryptoDefender™ for mobile devices has the following features -

Secure Keyboard prevents the OS and malware from logging your keystrokes. All keystrokes entered in the custom keyboard are encrypted. Now, the password you enter to logon or decrypt your secret key is safe.

Secure Browser is a custom, secure locked-down browser that prevents the storage of cookies and other malware artifacts. The secure browser is recreated for every session. Now, you can safely access your online wallet or exchange.

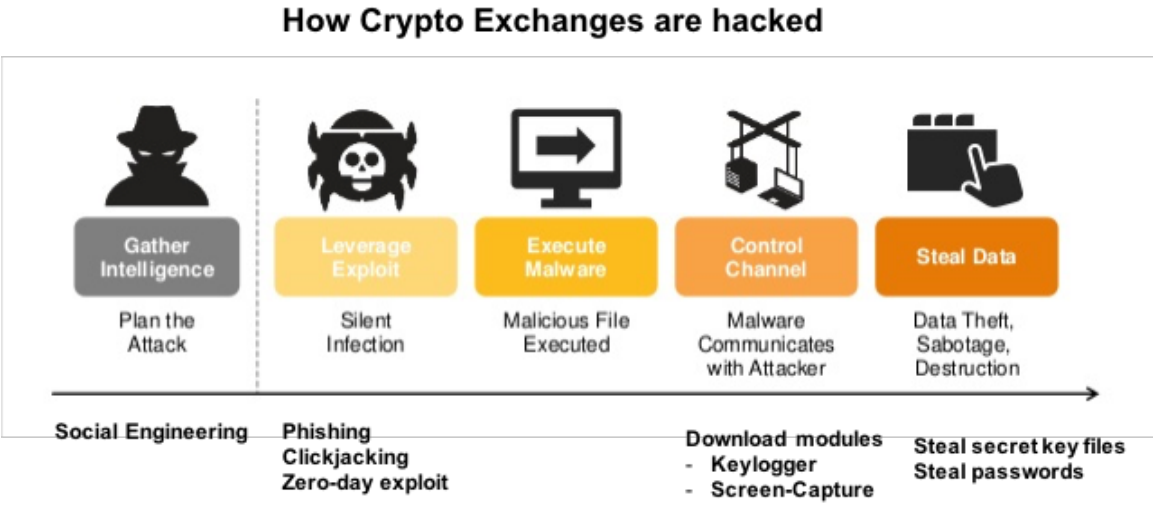
Password/Data Vault enables the AES-256 encrypted storage of passwords, keys and data. Access to the vault can be secured via fingerprint. The Secure Browser can be launched from within the vault.

Strong Password Generator This creates strong passwords based on user-defined preferences, and then stores them in the Password Vault for future usage.

Available for Android and iOS

ExchangeDefender™

Crypto exchanges have hot wallets and cold wallets. The wallets store user secret keys as well as the exchange's secret keys. Most of the keys are stored offline in vaults (cold wallet). A portion of the keys are stored on servers connected to the internet (hot wallet) to facilitate transactions. These servers are susceptible to a data breach just like any other hacker attack.



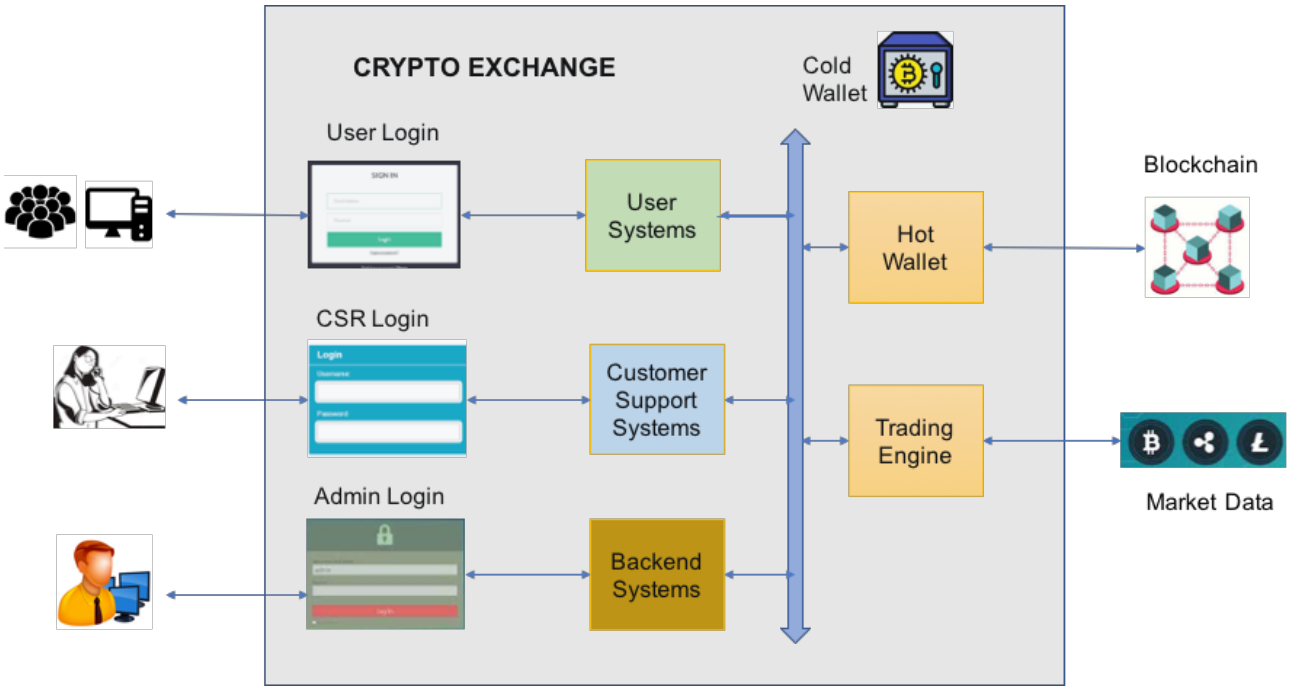
Exchange Defender comprises two products to protect the internal systems of the crypto exchange. These are – CryptoDefender™ (described earlier) and ProtectID®. CryptoDefender™ protects the exchange's computers and mobile devices from keylogging, screen capture and clickjack attacks. ProtectID® secures access to the internal systems via two factor out-of-band authentication. The ProtectID® system is shown below –

Authentication methods include:

- Out-of-Band – #, PIN, OTP, Voice
- OTP Delivery to Phone via SMS, Voice, Email, and/or Push
- Out-of-Band Push – Accept/Deny, PIN, and/or Fingerprint
- Hard Tokens – Key Fob, USB Key, and/or Wallet Cards
- Mobile Tokens – iOS, Android,
- Desktop Tokens – PC/Mac/Linux

ExchangeDefender™ Use Case

A typical crypto exchange architecture is shown below –

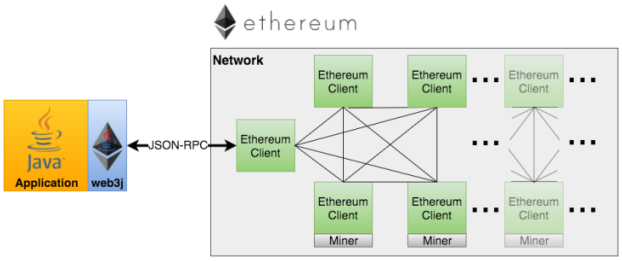


ExchangeDefender can secure the following vulnerability points –

Vulnerability	Endpoint Protection	Login Authentication	Transaction Authentication
User Login	X	X	
CSR Login	X	X	
Admin Login	X	X	
Hot Wallet			X

BlockchainDefender™

Currently, blockchains can be accessed directly by applications. The following figure depicts this (source – web3j.io).



Blockchain Defender acts as a gateway between the application and a private blockchain. It examines every message, checks if it is allowed as per enterprise rules & policy, scans the contents of data fields for malware and authenticates transactions via the ProtectID® system. Features include –

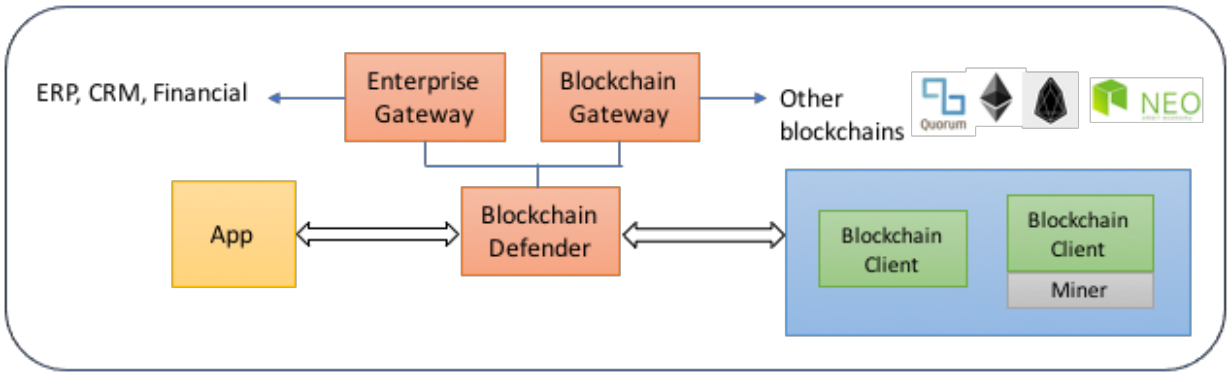
Authentication of blockchain transactions

Content Scanner to stop malware before it enters the blockchain

Rules & Policy Engine to define how messages are processed

Load Balancer & DDoS Mitigator balances traffic and shields the blockchain

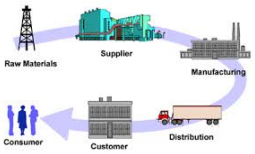
It can also pass the blockchain messages to enterprise systems or other blockchains via appropriate gateways.



BlockchainDefender™ Use Cases

Healthcare

- 56 % plan to implement private blockchains by 2020
- Shared blockchain ledger expected to cut costs, improve decision making and reduce fraud
- Compliance & Security requirements will require access to the blockchain to be audited and controlled



Supply Chain

- Most companies, we believe, will use blockchains in the supply chain by 2027
- Lower costs, increased transparency, better product tracking, faster shipping and reduced fraud
- Compliance & Security requirements will require access to the blockchain to be audited and controlled

Finance

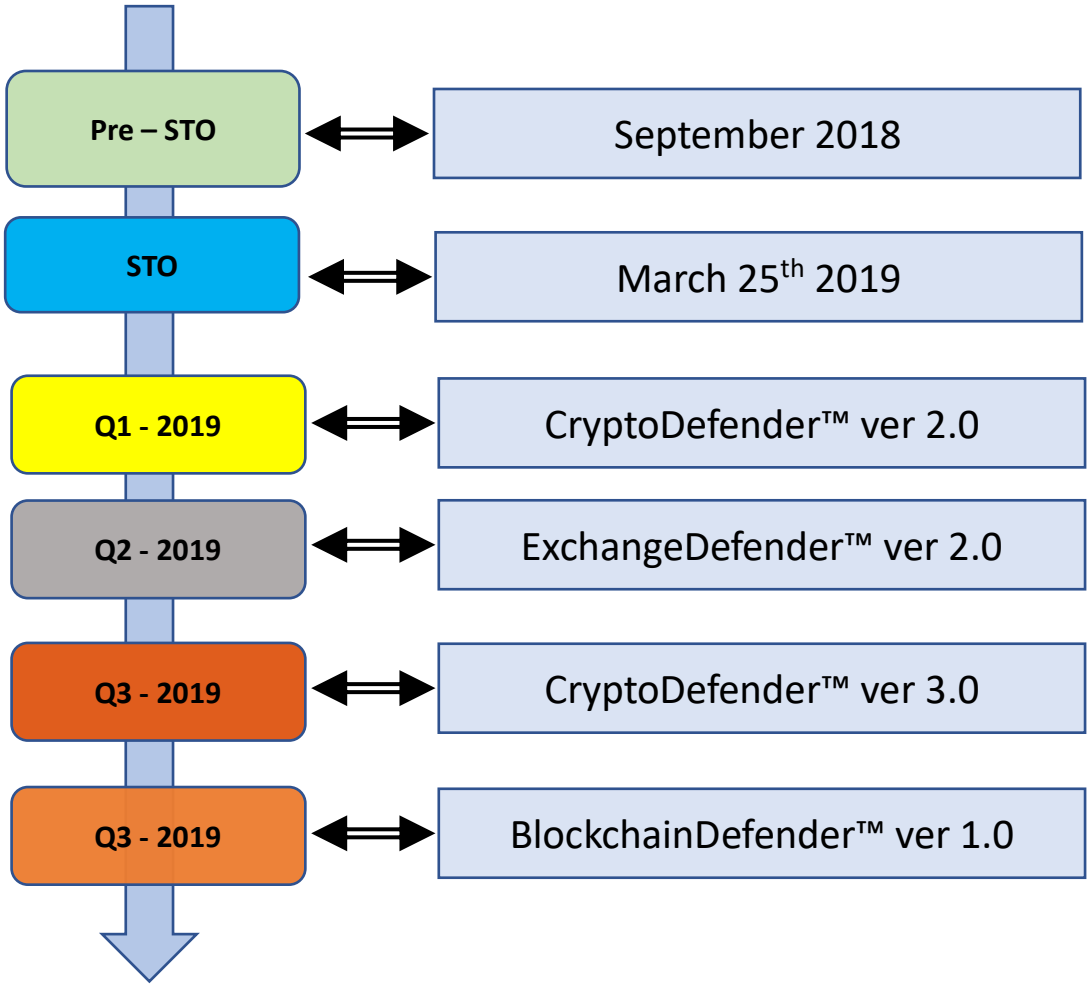
- Large industry consortia formed to facilitate use of blockchains in the financial industry
- Lower back office costs, faster settlement, greater transparency and easier cross-border payments
- Compliance & Security requirements will require access to the blockchain to be audited and controlled

Government

- Federal and state governments worldwide studying uses cases and conducting pilot programs
- Use cases include moving land records, business registration, health registries, etc. to the blockchain
- Compliance & Security requirements will require access to the blockchain to be audited and controlled

BlockchainDefender enables Compliance and Security requirements to be met

Roadmap



(The timeline represents estimates only and is subject to modification)

What we have accomplished so far –

- CryptoDefender™ Version 1.0 developed and released in app stores
- ExchangeDefender™ Version 1.0 developed and available for sale
- BlockchainDefender™ proof-of-concept developed, Version 1.0 under development
- Signed agreements with three resellers to distribute the products
- In discussions with six wallet companies to distribute the products
- In discussions with several exchanges to list the BSAFE™ token

Business Model – Projected Sales

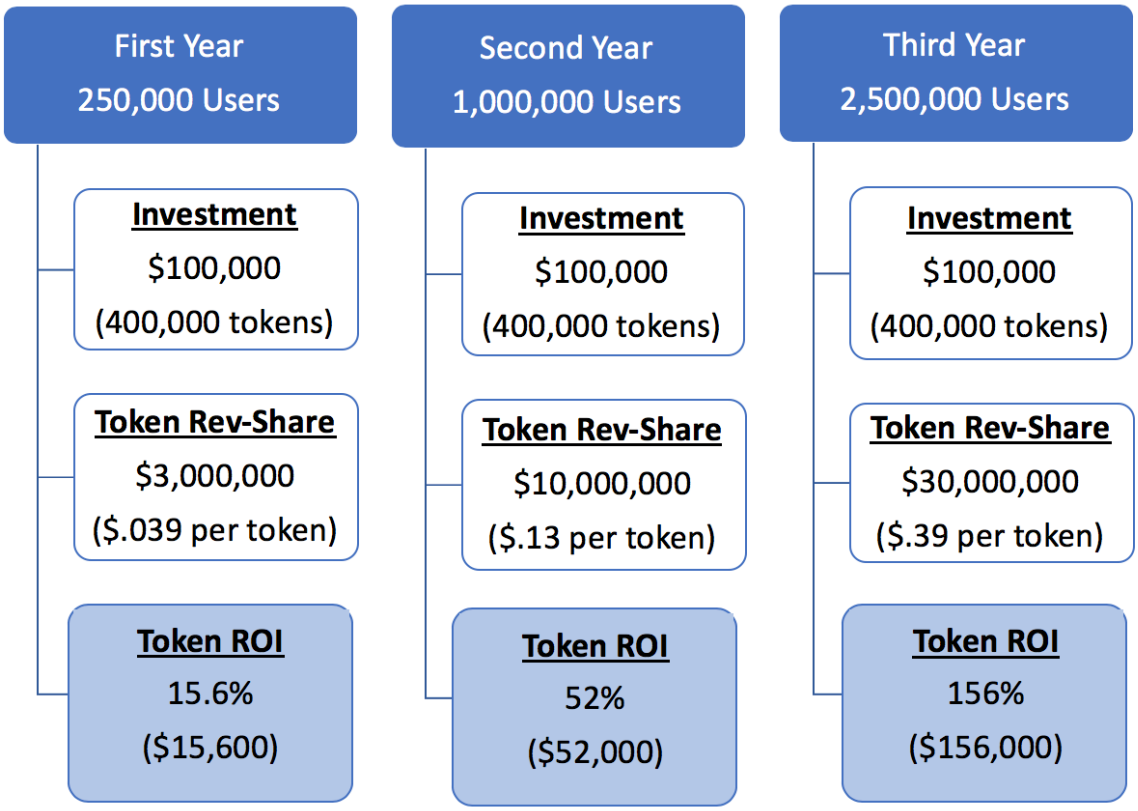
CryptoDefender – Will be distributed through Crypto Wallets, Crypto Exchanges & Crypto Influencers via an affiliate program.

- Opportunity – 24 Million Wallets & Growing Daily (200M by 2025)
- Monthly Subscription 5.99 (two devices) $9.99 (five devices)

CryptoDefender Projected Sales (monthly subscribers):

- 250,000 subscribers 1st year - $2.5M monthly ($30 Million Year)
- 1,000,000 subscribers 2nd year - $10M monthly ($120 Million Year)
- 2,500,000 subscribers 3rd year- $25M monthly ($300 Million Year)

Token Passive Income



In addition to the above token ROI, you still own the tokens!

For the above per-token ROI calculation, we used the following formula:
(10% of annual gross sales ÷ 75% (76,500,000) of the token allocation = per token passive income).

Go-to-Market Strategy

- Crypto Wallets – We will partner with Crypto Wallets and offer them a monthly revenue share for each of their users that subscribe to our CryptoDefender monthly subscription service.

- Crypto Exchanges – We will offer Crypto Exchanges our ExchangeDefender Solution to protect their internal networks from hackers. Additionally, Crypto Exchanges can receive a monthly revenue share for each of their users that subscribes to CryptoDefender subscription service.

- Blockchain Integrators – We will partner with Blockchain Integrators to sell our Blockchain Defender and CryptoDefender solutions.

- Blockchain Platforms – We will work with all the leading Blockchain Platform providers to insure BlockchainDefender platform compatibility.

- Affiliate Ambassador Program - We are finishing up a multi-tiered ambassador affiliate portal for the leading crypto influencers & enthusiasts to offer to their followers.

- FusionPR – We have contracted one of the industry's leading Blockchain PR firms to create awareness thru Industry Analysts, Blockchain editorials & Crypto Influencers.

- We contracted the Blockchain company that built the Dragon Coin token community (raised over $430M) to build our off-shore token investment community.

Token Offering

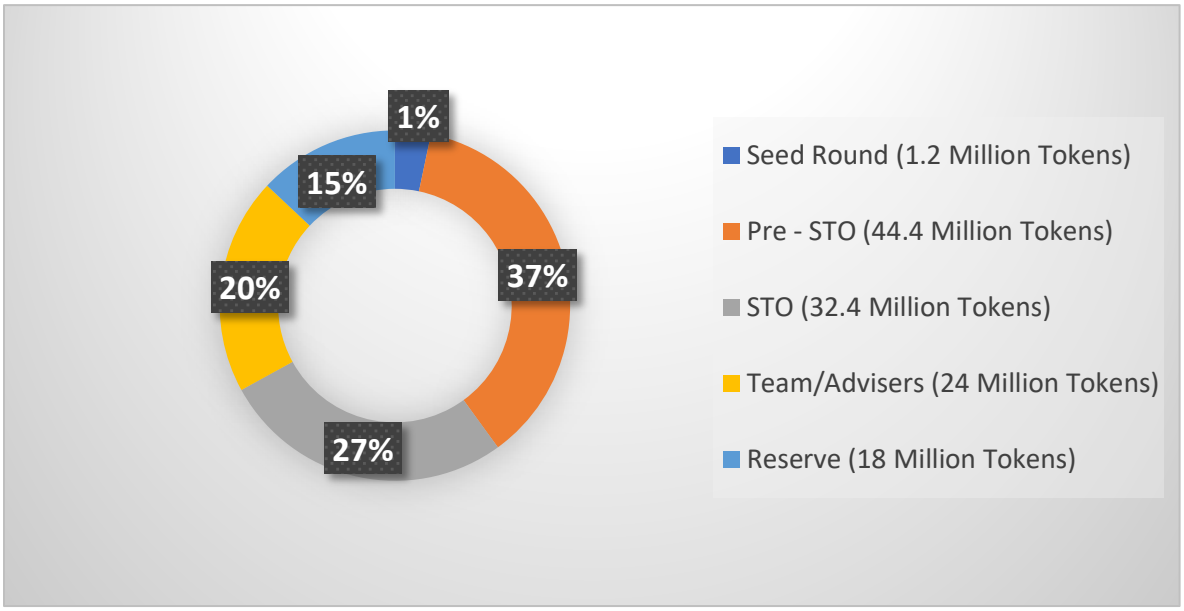
Symbol	Platform	Token Supply	Hard Cap
BSAFE™	ERC-20	120 million	$27 million

PRE – STO	Target Date Sept. 2018	Tokens for Sale 44.4 million	Token Price $0.25
STO	Target Date March 2019	Tokens for Sale 32.4 million	Token Price $0.50

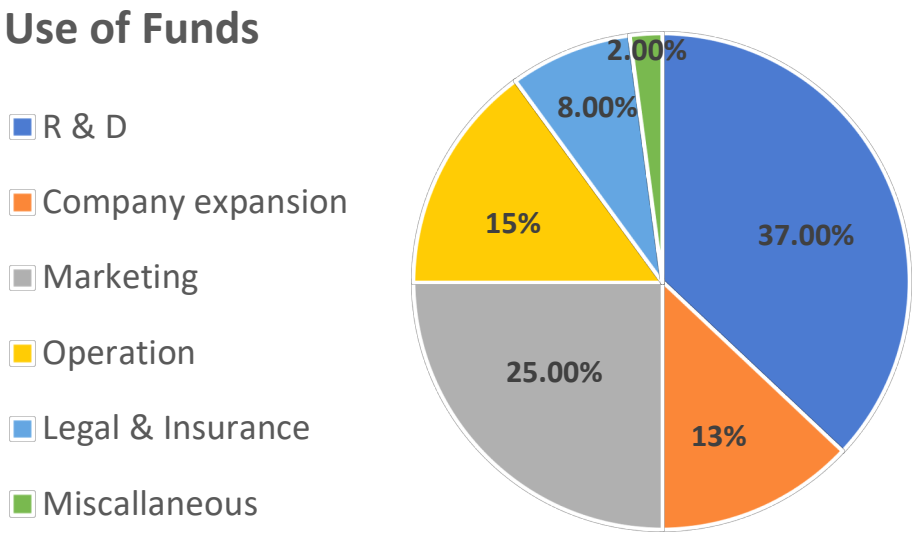
Equity is available for investments greater than $1,000,000.

Accepted Currencies
Bitcoin, BitCoin Cash, ETH, Litecoin, Ripple, & USD

Token allocation and Use of funds



The Use of Funds is subject to adjustment as determined, in their sole discretion, by Company management.



Team

George Waller
CEO

George serves as the CEO of BlockSafe Technologies. George is a co-founder of StrikeForce Technologies, Inc., and is an entrepreneur and technologist with over 30 years in the computer industry. George played a pivotal role in introducing two of the leading cyber security technologies i.e., out-of-band authentication and keystroke encryption to the marketplace. Today, these technologies are widely used in Banking, Healthcare, Education, manufacturing and government sectors.

Prior to founding StrikeForce, George served as Executive Vice President and Chief Strategist at: Connexus Corporation, RxRemedy, TeachMeIT, Incubation Systems, and HealthSCOUT.

George studied aerospace engineering at the Academy of Aeronautics.

Mark Kay
President

Mark joined StrikeForce Technologies in May 2003. Previously, he was an established leader, CIO and managing director at JPMorgan Chase for 26 years. During his employment at JPMC he led strategic and corporate business groups with global teams up to a thousand people. His tenure also included responsibilities as chief operating officer and global technology auditor. Mark's business concentrations included Securities (Fixed Income and Equities), Proprietary Trading & Treasury, Global Custody Services, Audit, Cash Management (including Money Transfer and Demand Deposit), Corporate Business Services and Web Services.

Prior to JPMC, Mark was a Systems Engineer at Electronic Data Services (EDS) for over five years, where he developed his technical and people skills. He holds a BA in mathematics from CUNY

Scott Whitman
COO

Scott is an entrepreneurial sales leader who focuses on top-line sales while building strong customer relationships. An executive strategist and business development leader with cross-functional expertise in business, sales and product development, Scott has 34 years' experience in B2B and consumer retail. Scott holds a BS in accounting and finance from Babson College.

Ram Pemmaraju
CTO

Ram is one of the founders of StrikeForce Technologies and the inventor of the company's ProtectID® product.
Ram has several years' experience in security systems and telecommunications. His prior job was at Coreon, where he developed OSS systems for DSL carriers. Ram was the founder and chief engineer of Digitech Telecommunications, a network security systems company that manufactured data encryptors (certified by NSA), callback systems, and access control and voice scramblers. He was employed at Computer Sciences Corporation, Synergy Systems, Bellcore and Bell Labs amongst other technology companies, typically as a chief architect or systems engineer. Ram has an MSEE from Rutgers University and a BE in electrical engineering from Stevens Tech. He holds several patents in computer security.

Steve Ferman
VP Business Dev

With over 35 years in technology, Steve was among the first online data backup distributors in 2004 with Asigra, where he started a successful channel reseller program. Since 2007 he has helped businesses navigate and migrate from brick and mortar offices and data centers to the cloud.

Dave Mamane
CMO

As CMO of Blocksafe, Dave brings 20+ years of expertise in marketing, and track record as a CEO and VP of successful global retail operations. Proven ability to develop successful marketing strategies and cultivate key relationships with editors, publishers, bloggers and influencers in order to build brands, and inspire long-term customer loyalty. Brings both an innate and acquired aesthetic sense; a keen eye for what will draw traffic, sell product, and inspire emotional connection.

Board of Advisors

Steve Cooper - As the first CIO of the US Department of Homeland Security, Steve led the development of the IT Strategy for Homeland Security, guided the implementation of the unclassified and classified networks of the new department, oversaw the creation of the department's enterprise architecture, and provided the vision for the use of IT across the department.

Prior to joining Commerce, Cooper served as the Federal Aviation Administration's (FAA) Acting Assistant Administrator for Information Services and CIO. Previously, Cooper was the Deputy CIO, as well as IT Director and CIO of the FAA's Air Traffic Organization, where he oversaw a team of 400 professionals working to ensure the operational excellence of mission support and business systems and the underlying technology infrastructure. In February 2003, Cooper was appointed by President George W. Bush to serve as the first CIO of the Department of Homeland Security (DHS) where, among other accomplishments, he developed the Department's first IT Strategic Plan.

Sondra Schneider - A 20-year information security industry veteran, Sondra is the CEO of Security University, a Tactical Hands-on Cyber Security Warrior training company providing both SU and Industry's Information Security & Assurance Certifications. For the past 20 years Sondra has been traveling around the world training network professionals to be network and security professionals as a full time professor/CEO. In 2005 Ms. Schneider was awarded "Entrepreneur of the year" for the First Annual Woman of Innovation Awards from the CT Technology Council.

Howard Medow - serves in a key relationship role with a significant number of our clients, and is the Executive Sponsor for some of our most important national accounts, including American International Group, Bank of America, Credit Suisse, AWS, JPMorganChase, Nationwide Insurance, and T-Mobile, and Charles Schwab. Howard was the Top National Sales producer for over 10 years at CGA Computer Associates, a predecessor company of Sogeti and CapGemini America, where he eventually earned the role of Regional Vice President. In addition to his role at Modis, Howard sits on the Board of Directors of the Ivan G. Seidenberg School of Computer Science and Information Systems at Pace University in New York City, is an avid cyclist and enjoys auto racing. Howard holds a B.S. in Science from the Lehman College of The City University of New York and is married with two children and three grandsons.

Scott N. Schober - is the President and CEO of Berkeley Varitronics Systems (BVS), a 45 year old New Jersey-based privately held company and leading provider of advanced, world-class wireless test and security solutions. Scott has developed cellular test instruments used primarily for cellular buildout throughout the U.S. with a recent focus on security solutions for cell phone detection tools, Wi-Fi, Bluetooth and IoT used to enforce a 'no wireless' security policy enforced in government, corporate, military, educational, correctional and law enforcement facilities around the world.

Legal & Compliance

Safe Harbor Statement

Certain statements contained in this white paper, including, without limitation, statements containing the words “potential,” “estimated,” “believes,” “plans,” “expects,” “anticipates,” "hopes," "targets," "goals," and words of similar import, constitute “forward-looking statements” within the meaning of the Private Securities Litigation Reform Act of 1995. Such forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause the actual results, performance or achievements of BlockSafe Technologies, Inc. (“BlockSafe” or the “Company”) to be materially different from any future results, performance or achievements expressed or implied by such forward-looking statements. Such factors include, among others, the following: general economic and business conditions in those areas in which the Company operates; demographic changes; competition; fluctuations in market interest rates; changes in credit quality; and the Company’s ability to successfully market its products. Given these uncertainties, undue reliance should not be placed on such forward-looking statements. The Company disclaims any obligation to update any such factors or to announce publicly the results of any revisions to any of the forward-looking statements contained herein to reflect future events or developments except as required by law.

The white paper does not carry any right of publication or disclosure to any other party. No person may treat this white paper as constituting either an offer to sell, or a solicitation of an offer to buy, any interest in the investment. Any offering of securities may be made only pursuant to written offering documents, in compliance with federal and applicable state securities laws. The investment is available only to qualified individuals or entities, and potential investors should perform their own due diligence regarding the investments and tax treatment of such investments. This white paper may not contain all the details and information necessary for you to decide or evaluate. The Company does not take responsibility for the accuracy or the completeness of the information contained herein or makes any assurances for such information. This white paper is not and does not purport to be an appraisal of the assets, stock or business referenced herein. Neither this white paper nor any of its contents may be used for any other purpose without the prior written consent of BlockSafe.

Investment in the BSAFE™ tokens discussed herein involves a high degree of risk and any Investor may lose part or all their investment. Accordingly, prospective investors should consider carefully the following risk factors, which represent only a limited number of selected risk factors in addition to the other information concerning the Company and its business contained in this White Paper, there are other risk factors associated with BSAFE™ tokens. The Company undertakes no obligation to update the information provided herein.

Regulatory uncertainty

Blockchain technologies are subject to supervision and control by various regulatory bodies around the world. BlockSafe securities may fall under one or more requests or actions on their part, including but not limited to restrictions imposed on the use or possession of digital tokens, which may slow or limit the functionality or repurchase of tokens in the future. Blockchain technology, including but not limited to the issue of BSAFE tokens, may be a new concept in some jurisdictions, which may then apply existing laws or introduce new regulations regarding Blockchain technology-based applications, and such regulations may conflict with the current BSAFE™ token concept. This may result in the need to make substantial modifications to the BSAFE™ token, including but not limited to its termination, the loss of BSAFE™ tokens, and the suspension or termination of all BSAFE™ token functions. As of the date of this White Paper, the Securities and Exchange Commission has not determined that any token based regulatory filings (specifically, registration statements on Form A-1 and Form S-1) is effective and has not approved any token only exchange for the purchase and sale of tokens, although derivative exchanges which incorporate tokens have been approved as Alternative Markets.

Taxes

BSAFE™ token holders may be required to pay taxes associated with the transactions contemplated herein, whether in the United States or in their home countries. It will be a sole responsibility of BSAFE™ token holders to comply with the tax laws of the United States and other jurisdictions applicable to them and pay all relevant taxes.

Value of BSAFE™ token

Once purchased, the value of BSAFE™ token may significantly fluctuate due to various reasons. BlockSafe does not guarantee any specific value of the BSAFE™ token over any specific period. BlockSafe shall not be held responsible for any change in the value of BSAFE™ token.

BSAFE™ tokens are not an investment

BSAFE™ tokens are not official or legally binding investments of any kind. In case of unforeseen circumstances, the objectives stated in this document may be changed. Despite the fact that we intend to reach all goals described in this document, all persons and parties involved in the purchase of BSAFE™ tokens do so at their own risk.

Number of new BSAFE™ tokens available for exchange

The number of new BSAFE™ tokens available for exchange may vary due to multiple factors such as the amount of funds received by BlockSafe through the sale of its BSAFE™ tokens, the total number of BSAFE™ tokens sold, market conditions, legal regulations, and other risks. BlockSafe does not guarantee any specific number of new BSAFE™ tokens available for exchange for a BSAFE™ token at any given time.

Quantum computers

Technical innovations, like the development of quantum computers, may pose a danger to cryptocurrencies, including BSAFE™ tokens.

Risks of using new technologies

BSAFE™ tokens are a new and relatively untested technology. In addition to the risks mentioned in this document, there are certain additional risks that the team of the BSAFE™ platform cannot foresee. These risks may manifest themselves in other forms of risk than those specified herein.

Force Majeure

BlockSafe's performance may be interrupted, suspended or delayed due to force majeure circumstances. For the purposes of this White Paper, force majeure shall mean extraordinary events and circumstances which could not be prevented by BlockSafe and shall include: acts of nature, wars, armed conflicts, mass civil disorders, industrial actions, epidemics, lockouts, slowdowns, prolonged shortage or other failures of energy supplies or communication service, acts of municipal, state or federal governmental agencies, other circumstances beyond BlockSafe's control, which were not in existence at the time of White Paper release.

Disclosure of information

Personal information received from BSAFE™ token holders, the information about the number of tokens owned, the wallet addresses used, and any other relevant information may be disclosed to law enforcement, government officials, and other third parties when BlockSafe is required to disclose such information by law, subpoena, or court order. BlockSafe shall at no time be held responsible for such information disclosure.

Integration

All information contained within this Whitepaper is provided for general information purposes only and is intended to present a guide to the decentralized services which may be provided by BlockSafe in the future. Nothing published in this document is intended to be (i) legal, financial, professional, tax or other advice; (ii) a recommendation to undertake (or to cease undertaking) any action whatsoever; (iii) an advertisement, solicitation or legal offer; (iv) an offer or a call to buy or sell stocks or securities, or that of any other related or associated company, (v) a promise of any voting or ownership rights of BlockSafe (vi) or a promise of receiving any passive income, any return on investment or any profit; and should not be construed as any of the foregoing.

Assumptions with respect to the foregoing involve, among other things, judgments about the future economic, competitive and market conditions and business decisions, most of which are beyond the control of the BlockSafe team and therefore difficult or impossible to accurately predict. Although the BlockSafe team believes that its assumptions underlying its forward-looking statements are reasonable, any of these may prove to be inaccurate. As a result, the BlockSafe team can offer no assurances that the forward-looking statements contained in this White Paper will prove to be accurate. In light of the significant uncertainties inherent in the forward-looking statements contained herein, the inclusion of such information may not be interpreted as a warranty on the part of BlockSafe or any other entity that the objectives and plans of the BlockSafe project will be successfully achieved. BlockSafe undertakes no obligation to update this White Paper. Please note that the BlockSafe project may be subject to other risks not foreseen by its team at this time.

BlockSafe strongly recommends that all contributors seek their own legal advice as compliance may vary, depending on their own status, nationality, the country they are resident/tax resident in, etc.

References

1. https://blockchain.info/charts/my-wallet-n-users

2. https://www.bloomberg.com/news/articles/2018-01-18/hackers-have-walked-off-with-about-14-of-big-digital-currencies?utm_source=Autonomous+NEXT&utm_campaign=bd3512d299-EMAIL_CAMPAIGN_2016_11_04&utm_medium=email&utm_term=0_c8cf357092-bd3512d299-95567749

3. https://www.bankinfosecurity.com/cryptocurrency-theft-11-billion-stolen-in-last-6-months-a-11073?rf=2018-06-13_ENEWS_SUB_BIS_Slot1&mkt_tok=eyJpIjoiWkRkaE16UXpPREUwTXpFMiIsInQiOiJCYWRxRmt1NkdsMllNXC9LaklNWUo2S3h1cFRcL21TQk52dTd4S2p5cSt1c2t1cU1mK2pJMnVRR1dBNDB1UVBBVTdHaTM4ZlByY3hjOVdRUlFlZGNcL2U2dnBQTnNtWjFsc0VHK0JlS09BKzlYODBTbW9kMWVzZnZjQmxSY2l4UzVWeCJ9

4. https://cryptosecure.com/media/CryptoSecure%20Whitepaper.pdf

5. https://coinjournal.net/uk-company-linked-to-the-theft-of-650000-bitcoins-from-mt-gox/

6. http://bitcoinist.com/bitgrail-cryptocurrency-exchange-hacked-170-million-nano-allegedly-stolen/

7. http://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html

8. https://www.reuters.com/article/us-cyber-nicehash/digital-currency-exchange-nicehash-says-bitcoin-worth-nearly-64-million-hacked-idUSKBN1E10AQ

9. http://bitcoinist.com/youbit-bankruptcy-hackers-assets/

