Cybr – Cyber Security Ecosystem and Utility Token

White Paper — April 26, 2019

By: Shawn R. Key, Matthew Spaeth and David Donnenfeld

Cybrtoken.io

Cybr@Cybrtoken.io

Contents

Executive Summary	4
Enter CYBR	7
CYBR Real-World Application	13
CYBR Ecosystem Review	18
CYBR Architecture	20
The Company	23
The Team	28
Threat Intelligence Community (TIC)	30
Roadmap	31
Tokenomics	32

Executive Summary

Over $1B in financial losses occurred in the cryptocurrency space in 2018… and these were just the reported incidents. The primary cause was due to hackers who were able to circumvent the countermeasures and safeguards that exist in the crypto ecosystem. With an ever-increasing market cap, these financial losses will continue to mount until a "standard of care" is established and proper cybersecurity policy, procedures and controls are established.

Enter CYBR.

A Stolen Horse

Growing up in Virginia, I am often reminded of an expression Southerners use: "You don't lock up the stable after the horse has been stolen." When weighing the need for cybersecurity in the blockchain space, this old adage could not apply more nor be more appropriate.

An Abbreviated History

The parabolic rise and volatile nature of cryptocurrencies portends the enormity of its potential impact. There is widespread speculation. Some pundits predict a cashless society in less than a decade, and the more outspoken supporters of Bitcoin predict a price that shall eventually crest seven figures. The detractors, irrespective of authority and stature, utter a single word in dismissing the viability of widespread adoption, and that word is "scam". Not a pretty word. While it certainly speaks to the level of threat the old guard senses from the emergence of crypto and decentralized systems, it also smacks of a fundamental concern that these "monies" can be taken as easily as they can be created.

While swindlers and charlatans can be found in all businesses, if digital assets and virtual currencies cannot be secured, they can not be widely adopted. The irony of course is that crypto and blockchain technologies have garnered public support as a result of a collective distrust for our existing governments, monetary policies and fiat currencies on the whole. Certainly, there is compelling evidence that points to governing corruption across the globe. What can be said about crypto?

Consider the following:

In June 2016, Decentralized Autonomous Organization (DAO) had 50mm stolen. Running on the Ethereum network, written in the language of Solidity, a simple flaw was responsible.

In 2014, Mt. Gox filed for bankruptcy claiming it had lost 750,000 Bitcoin.

In January 2018, Coincheck, a Japanese cryptocurrency exchange, was hacked for approximately 534mm USD.

After being hacked in April 2017, South Korean Exchange Youbit stated it did its "best to improve the security, recruitment and system maintenance."

In December 2017, Youbit was hacked again, losing 17% of its total crypto holdings. Parent company Yapian filed for bankruptcy.

Bancor raised 153mm in June 2017 to develop a decentralized liquidity network, i.e. a decentralized exchange of the highest order. In July, it was hacked for 23.5mm.

On the same day as Bancor, a hack on a popular VPN compromised "My Ether Wallet (MEW)," a widely-used service to manage ethereum network cryptos.

The list could go on. Still, it would be remiss not to mention the astonishing number of individuals who have been hacked or scammed out of their crypto. The laundry list continues as high-profile ICOs have been victimized by phishing attacks, and there has been no shortage of exit scams in the space. Even simple human error can be costly as one unfortunate individual learned when he inadvertently spent 50 Bitcoin in transferring fees.[1]

1 50 BTC Mining Fees https://www.blockchain.com/btc/tx/d38bd67153d774a7dab80a055cb52571aa85f6cac8f35f936c4349ca308e6380

Hacking and Internet-based crimes are not unique nor confined to crypto. A 2017 Norton Report stated that $172 billion was hacked from nearly a billion consumers worldwide. More than half the adult population online can count themselves as victims of cybercrime and mainstream stories like the Equifax breach have grabbed headlines. However, the nascent asset class that is crypto and distributed ledger technologies ("DLT") is acutely vulnerable. Nothing can destroy a revolutionary overhauling of a monetary system faster than a plague of theft.

Stateside Measures

Security has become such a concern that congress introduced the "hack back" bill, allowing businesses to attack their attacker's computers or networks.

- Active Cyber Defense Certainty Act introduced this amendment to the Computer Fraud and Abuse Act anti-hacking law.

Two clichés come to mind when I see this — "sometimes the cure is worse than the disease," and "an ounce of prevention is worth a pound of cure."

- Identifying a hacker often takes time and analysis
- Hackers have become more savvy and readily circumvent detection
- Ordinary researchers are not capable of performing such analyses
- Hackers often leave clues in the code and spoof that evidence, e.g. leaving code from known hacking organizations in malware
- The amendment only applies within the United States
- Most attacks come from abroad; and
- Those that don't are often routed through servers that come from overseas.

Governing bodies have already enacted a number of stops on the "hack back" amendment:

- **Before taking action against attackers, the National Cyber Investigative Joint Task Force (NCIJTF) must be alerted.**
- **Prying into hacking networks may be an obstruction to ongoing investigations and non-permitted retaliation is potentially criminal.**

The NCIJTF is led by the FBI and the FBI defense review is worried that actions taken by private organizations could effectively trigger our government's international legal responsibility.

As DLT winds its way into the mainstream, the stakes are rapidly being raised. Quantifying prevention is not easy, but it is easy to overlook. When Equifax hackers made off with the private information of 143 million people, who is responsible for what is an en masse modern-day home invasion? Is it a victimless crime if insurance pays?

Reality is that the ultimately accountable Equifax is not held liable and as of now, no one is reimbursing lost crypto. If the last four digits of our social security numbers can be sold on the dark web, in what stead should we hold the security of digitized currency?

Digital assets are currently being used as mediums of exchange, as stores of value and more. They are the equivalent of money, bartering tools, precious metals as well as the lifeblood of emerging ecosystems. Make no mistake, horses have been stolen and many more thieves are coming.

We can no longer overlook the clear and present threat

to the technologies that are poised to reshape our world.

It is time to secure the blockchain.

Enter CYBR.

Good Cyber Threat Intelligence (TI) is continuously refined information that hones in on potential or current attacks that can threaten any system.

CYBR is an ever-expanding compendium of information combined with state-of-the-art software solutions that will be optimized for the blockchain. CYBR is a holistic security solution that will endeavor to secure wallets, smart contract transactions, and associated transactions and activities that take place in the blockchain space.

Unlike most token generating events ("TGEs"), where a theoretical idea is presented and implementation is to follow, much of the CYBR solution is already built and being utilized in enterprise environments.

To this point, it is safe to say there is a truly pressing need for top-flight cybersecurity in the realm of crypto. However, there are very few parties qualified to provide the needed level of security. With that in mind, let us momentarily stray from the traditional structure of a white paper. Thus far, the "why" has been addressed. Now, let us the broach the most critical component of such an undertaking — "the who."

The Vision and the Visionary

CYBR's founder, Shawn Key (detailed bio and related links under "Team" at CYBRtoken.io) is a cybersecurity veteran of some notoriety. He is attributed as the person first described as an "ethical hacker," based on an article in a governmental trade magazine.[2] The term presaged the popular "white hat hacker" by more than a decade after Shawn successfully found his way into numerous federal networks in 1999.

> "We invest in people, not ideas."
>
> – A maxim of venture capitalists

Shawn's facility and acumen in the field were widely noted and his early contributions to "information security," aka "information assurance," were seminal. A few years later, the industry would become known as "cybersecurity."

Some of his early work included one of the first patch management solutions, which was acquired by a company that eventually sold to IBM for some $500M USD. He quickly garnered a reputation as someone who could "see around the corner."

Over the last ten years, Mr. Key's cyber services company has maintained a flawless reputation, and is currently a subcontractor to Raytheon (see CYBRtoken.io under "Partners"). Raytheon has the distinction of earning the largest cybersecurity contract awarded in US history of 1.115B USD.

2 www.govexec.com/magazine/1999/04/information-insecurity/5989

In recent years, Shawn's focus has been on the underlying solutions that make up the CYBR Ecosystem:

CYBRSCAN — a real-time vulnerability analysis solution that can assess the security posture of ANY public facing IP address. The solution is highly scalable and its database of digital identifiers is crypto-centric, meaning it seeks out the vulnerabilities and potential exploitations that primarily are relative to the crypto and blockchain infrastructure.

BLINDSPOT — The endpoint solution that roots out malicious code using fuzzy logic, machine learning and artificial intelligence (AI). BlindSpot incorporates proprietary algorithms that identify exact AND partial matches of malicious code, preventing advanced persistent threats (APTs) from exploiting operating system, application and other code flaws that can lead to data and/or financial loss.

The software solution has gone through its share of iterations and pivots but the concepts of detecting malicious code and associated bad actor activity were consistent themes throughout his numerous grants and awards received for his work. These include, but are not limited to:

- Mach37 Cyber Accelerator: awarded $150,000 in grants via Mach37 and the Center for Innovative Technology (CIT).
- Dell Founders 50 Club: recognized Shawn's technology as one of the top 50 most disruptive technologies in the world.
- Tandem NSI, associated with the National Security Agency (NSA), awarded Mr. Key for one of the best technologies in the D.C. metro area.

MALWARE INFORMATION SHARING PLATFORM (MISP) — a centralized location for emerging threat data that can be turned into actionable intelligence. With the CYBR MISP, proliferation of threats can be minimized and financial losses significantly reduced.

THREAT INTELLIGENCE PORTAL (TIP) — If two minds are better than one, then thousands are better than two. The TIP accepts threat intelligence "tips" from the CYBR community, which in turn is rewarded in CYBR tokens for its contributions. Think of the TIP as a 365/24/7 bug bounty on steroids.

Origin of Solutions' Concepts

Mr. Key was intrigued by cryptocurrency and with each passing hack, this interest morphed into the central preoccupation in his life. He quickly found that many of the exploitations were similar to "traditional" attacks. What he dealt with in every day enterprise systems mirrored the methodologies used in the majority of reported hacks. He determined that BlindSpot was applicable to the blockchain and it became his mission to optimize it for cryptocurrencies in securing smart contracts and associated transactions. Although it poses some unique challenges and there are inherent differences, Mr. Key realized that his experience could improve the security posture of the world of crypto. The last year has been solely focused on what has evolved into CYBR.

Welcome to the CYBR Security Ecosystem and Utility Token.

Not Your Father's Antivirus

While antivirus ("AV") software hasn't sounded relevant for a long time, threat detection and eradication has remained at the fore for government and many private sector organizations. Sensitive data and the protection of these assets have grown in scope, commensurate with our advancements in technology. Unfortunately, the general public has not benefited from this growth and the displays of negligence in corporate America provide unimpeachable evidence to this point.

There have been numerous data breaches of sensitive information and despite the headlines they've captured, it has ceased to be a priority to those responsible for securing said data. Society pays the cost for the mishaps of Target, Equifax and similar while specialized agencies have continually evolved against growing threats.

As crypto takes hold and drives towards critical mass, the need for a gold standard of security and an attendant solution has never been greater.

Elegant, Robust

CYBR, like good TI itself, is a multi-fisted attack that provides real-time safeguards, countermeasures, threat intel and secure transactions via three distinct methods:

- **CYBRscan — proprietary software solution that identifies vulnerabilities on ANY IP-based device in ANY language.**
- **BlindSpot — A proprietary software that powers a potentially borderless landscape of threat identification.**
- **Portal (MISP/TIP) — CYBR utilizes a real-time, pedigreed data feed heretofore not available to the general public.**

Identifying a threat is one thing, removing it is another and it's still another to prevent its return. Standard issue solutions can tell you something is wrong, but can't necessarily eradicate the problem nor detect the evolution of threats. They are simply obsolesced by current malware.

Work-a-day antivirus software is nothing more than a compilation of known threats with basic search capabilities. Today's malware has adapted and can morph into a slightly different version of known viruses. The result is that malicious code is no longer identifiable by standard AV software. The permutations of known viruses that can continually plague networks are known as advanced persistent threats ("APTs") and standard software has no solution for it.

BlindSpot not only detects "bad actor," associated illicit file activities and APTs; soon they will be disrupted. The three primary tenets of risk management in relation to TI and ensuring data are as follows:

1. Confidentiality
2. Integrity
3. Availability

BlindSpot captures attack signatures by deploying a combination of fuzzy logic, machine learning in concert with artificial intelligence. Whence identified, this information is distributed to the protected community via the blockchain. As previously mentioned, to augment the supporting data that runs concurrently with BlindSpot, one of the CYBR's token initiatives is to reward community members for identifying suspicious activities via the TIP. This influx of data will also provide CYBR with TI that will differentiate it from other competitors and allow CYBR to have the largest repository of TI digital identifiers in the world.

Being Smarter

Smart contracts are a protocol that executes the terms of a contract. The potential efficiencies it offers are myriad and game-changing. It is a revolutionary time-saver that can considerably reduce expenses, sidestep legal entanglements and associated costs. The applications for smart contracts are growing by the day and they are the lifeblood of distributed ledgers. The company believes that the primary stumbling block for mass adoption of blockchain technology is security and aims to establish a "best practices" standard. Any executor of code is aware of the inherent issues, but unfortunately, even the most outspoken and vocal leaders of the blockchain neglect to properly acknowledge this growing risk.

We can ill afford to analyze vulnerabilities after an attack. While open source is inspired and shall pave the way for innovation, there must be a standard. Auditing can go a long way but ultimately, the safe harbor that CYBR can provide shall raise the bar and be the benchmark by which security on the blockchain shall be measured.

For example, smart contract programming in Ethereum is known to be error-prone and many of these common errors are known quantities. The DAO hack, for example, was the result of a recursive calling vulnerability. Essentially, hackers with an initial minimum balance were able to repeatedly withdraw that balance. There was no fallback function and thus, repeated withdrawals were made, as balances were not updated in real time. Such gaffs are imminently avoidable. This contract would not have met any security expert's minimum standards, yet some 50mm was heisted.

To summarize, CYBR is an advanced cybersecurity solution that deploys its proprietary software, BlindSpot and layers it with a comprehensive data feed to proactively identify hackers.

Mission Critical

There is a pressing need to dramatically reduce the average time of detection in identifying and contending threats. Without it, the adoption of DLT hangs in the balance. The implementation of a proactive defensive as well as preventive approach to cybersecurity is sorely lacking in the space. CYBR seeks to solve that problem.

CYBR's mission is to provide a seamless continuum of threat security and establish a gold standard of cybersecurity on the blockchain.

Governance, Risk Management and Compliance (GRC)

In traditional cybersecurity, the term GRC is abuzz. The acronym stands for Governance, Risk (Management) and Compliance. Currently, an enormous number of vendors are providing this service in integrated, point solutions or domain specific capacities.

Each of the core disciplines is comprised of four basic characteristics — processes, technology, strategy and people. Dependent upon an organization's risk tolerance, company policies and any external regulations are what determine the level of engagement. Once identified and assessed, operational rules or parameters that the GRC "quotient" supports are integrated or merged holistically across an organization.

As nebulous as it sounds, the field is rapidly growing and its efficacy remains unquestioned.

What this translates to for CYBR is the need to establish a robust community as their input creates the checks and balances for a decentralized world. GRC implemented into security is the voice of a unified whole that lacks central authority, but compensates with efficiency and consensus. Although the world of crypto is an ever-moving target, establishing best practices, attracting key opinion leaders ("KOLs") as well as supporters is paramount. The CYBR token itself shall derive much of its utility by the provision of token to active members who can successful identify and report threats.

From a business standpoint, this "open-sourcing" of security creates an enviable dataset and encyclopedia of intelligence.

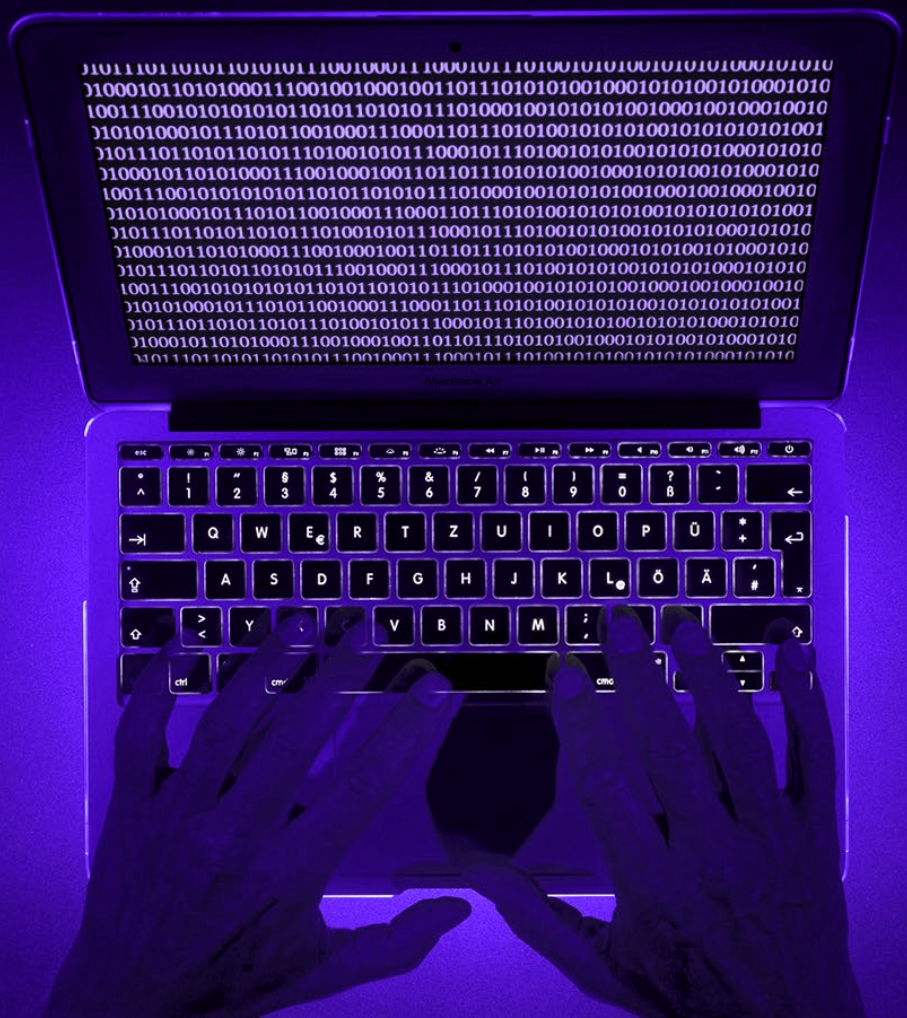
All this leads CYBR to lay claim to an overused buzzword. Although the word "ecosystem" is bandied about in tech circles, let us remember what the definition actually states:

> ***Ecosystem:*** *a biological community of interacting organisms and their physical environment. (In general use) a complex network or interconnected system.*

And this is precisely what CYBR's governance is.

- CYBR offers incentives to subscribers whom:
  - — Successfully identify threats
  - — Offer needed fixes
  - — Provide actionable intelligence
  - — Detect and report threat-related activities
- Intel is then verified
  - — If criteria are met, data is analyzed and ranked
- Ranking is based on risk factor as determined by programmed AI algorithms
- Done in real-time with signature lists updated automatically
- Once processed and identified, the information is disseminated to subscribers
  CYBRscan — Cyber Security Scanning and Monitoring Solution

CYBR
Real-World Application



CYBRscan is a revolutionary new cloud-based, vulnerability and continuous monitoring solution designed for EVERYONE, but equipped with specialized capabilities for the crypto community and blockchain ecosystem.

Historically, we have relied on anti-virus (AV) and malware scanners to determine if our systems are at risk. These solutions previously required a client to be installed on the device which was being assessed. The problem is that these solutions rely on digital fingerprints that must be IDENTICAL to the malicious code found on a device. If a piece of malicious code deviates from that exact match, the safeguard tool will not identify it. CYBRscan incorporates fuzzy logic, which allows our solution to look for exact AND partial matches of malicious code. This means polymorphic and pleomorphic malware (advanced persistent threats) can be identified and remediated BEFORE an exploit occurs. Simply stated, CYBRscan identifies the threats that seek to circumvent existing safeguards and countermeasures.

When applied to a device storing a crypto wallet, a URL where transactions take place or even an exchange where crypto is traded, CYBRscan will assess vulnerabilities pertaining to version control, patch management, man-in-the-middle (MITM) attacks, distributed denial of service (DDoS) attacks, and much, much more. In fact, CYBRscan currently assesses for over 40,000 existing and relevant vulnerabilities that can allow for cyber threats to exploit the system and cause financial loss. In 2018 alone, nearly $1B USD in crypto losses due to hacks occurred. (Source: www.coindesk.com/nearly-1-billion-stolen-in-crypto-hacks-so-far-this-year-research)

So what are the capabilities of CYBRscan?

ONLINE VULNERABILITY SCANNING

State-of-the-art vulnerability testing suite, which integrates scanning, reporting and managing threats into one easy to use Admin Control Panel.

CYBRscan makes network vulnerability assessment seamless across your cloud, on-premises, and/or hybrid environments. If your device has a public IP address and an Internet connection, CYBRscan is the solution of choice for you.

UPTIME MONITORING

24/7 monitoring of your assets to check whether they are responding. You get an alert when an asset goes offline. Generate automatic reports, which shows the trend, timelines and many more.

WEBSITE MALWARE SCANNING

24/7 monitoring of your assets for malwares and blacklisting. You get an alert when an asset is infected and also when it gets blacklisted. You will be able to generate reports, which provides the test results, trends and more details on blacklisting and infected malware.

ON-DEMAND PENETRATION TESTING

Additionally, CYBR offers penetration testing, which provides a customized, comprehensive and periodic security assessment of various kinds of applications such as internally developed, and commercial enterprise web applications. CYBR analysts can conduct expert validation for specialized environments and critical systems that may have vulnerabilities that are not easily identifiable via automated means.

How Does CYBRscan Work?

1

Set up your CYBRscan private cloud space

- Consolidated dashboard
- Individual product dashboard
- Reports
- User administration

AND MUCH MORE

2

Add your personal/ organization's assets

- Manage those assets
- Monitor an individual or group

AND MUCH MORE

3

Assign security tests to assets

THE SUITE ENABLES MULTIPLE TESTS, INCLUDING:

- Vulnerability scanning
- Penetration testing
- Uptime monitoring
- Malware monitoring
- Thematic security testing

4

Run/schedule test

Run your tests depending on the security tool you assigned to assets. Tests can be run on demand or scheduled at your convenience. There are various scan profiles including PCI and HIPAA.

5

Generate report

You can download test results at any time. Depending on the tool selected, your report contains detailed information and advice on how to fix any identified issues.

6

Mitigation

You can assign findings requiring action to users. They can prioritize and track mitigation on any finding or any asset at any time.

Summary

Simply stated, nothing like CYBRscan exists for the average crypto user. Historically, solutions like these cost thousands of dollars and required dedicated security analysts with advanced training to operate the scans. Continuous monitoring has just not been an option, as the cost to the average user is astronomical. Not any more. In closing, CYBRscan provides everyone the power of an advanced, enterprise, cyber security solution. Finally, the hackers of the world have a worthy adversary, which plans to create a significant dent in the mounting financial losses to the crypto ecosystem.

"Any File Type, Any Language, Anywhere"

BlindSpot can see through the polymorphic camouflage used by the world's most advanced hackers. Utilizing digital file fingerprints and leveraging an adaptive 'brain,' BlindSpot locates partial matches within the files on endpoints including systems, servers, laptops, desktops, USB drives, and even mobile devices. BlindSpot is also designed to monitor traffic flowing through the network (available in subsequent release).

Most attacks happen weeks or even months after initial penetration. Even the simplest attacks tend to have a fuse that is typically several days. To map out a system, probe for information, and obtain or forge credentials takes time. However, the moment malicious tools land on a network, BlindSpot sees them — even if the files are not copied to your systems. BlindSpot is preventive as it identifies and alerts of merely potential illicit activities before Zero Day.

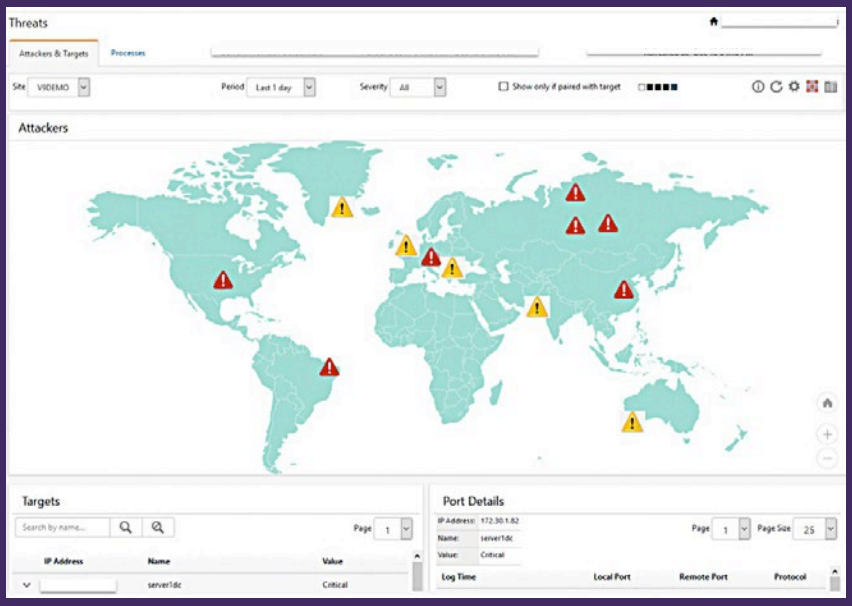
BlindSpot reveals concealed hacking tools, even fragments of more complete sets.

The software continuously monitors file activities from an endpoint searching for digital fingerprints. Whenever it finds partial matches of any file type in any language, it is reported back and kept in perpetuity on a temporal repository. The constantly updated database of known malicious files and hacking tools locates and alerts subscribers to any indication of hacking, malicious files, or illicit activity.

Just like with humans, once a fingerprint has been taken, you no longer need the person to identify them. Even a partial print is enough, and sometimes a smudge will do. Once BlindSpot has taken a digital fingerprint of a file, the file is no longer needed to identify it. And they are tiny — even a multi-gigabyte file has a digital fingerprint that is no larger than 10k bytes.

BlindSpot can identify matching files even when the digital fingerprint is only partially there. With advanced processing capabilities, file fragments, recovered data from a hard drive, partially downloaded documents, damaged files (both intentional and accidental) and other incomplete file structures can be properly fingerprinted in a way that still allows matches to be found.

BLINDSPOT



System Compliance

All government systems go through certification and accreditation. BlindSpot offers malicious code protection for both security considerations and required compliance. Guidelines found in NIST 800-53 Revisions 3+ Security Requirements for System Integrity, SI-3 Malicious Code Protection, state that malicious code protection mechanisms must be employed at information system entry and exit points, including workstations, notebook computers, and mobile devices, to detect and eradicate malicious code. BlindSpot's continuous monitoring and updating of its known malicious file repository provides the required real-time and monthly re-scans of files. It also alerts appropriate staff when malicious code is found, provides reports on potential malicious files, illicit activity, and offers follow-up with brief false positive reports (less than 0.01%). BlindSpot helps organizations meet the mandated security requirements while ensuring continued compliance.

Intellectual Property Protection

Track sensitive information as it changes and moves around the enterprise.

Government entities and corporations are addressing the issue of monitoring documents. Files that contain sensitive information or intellectual property can no longer be safely stored on a secure server with the only requirement for access being the perfunctory credentials. People, either unwittingly or with malicious intent, copy and paste parts of documents, move files to USB drives, transfer files onto a laptop, share them with co-workers, or exfiltrate confidential information to outside networks and systems. BlindSpot carefully guards networks, and can even track USB drives. BlindSpot can send alerts regarding questionable activity with specified documents/files or with specific computers or even individual activity.

It is a sensitive information watchdog that catches both unintentional and malicious exposure to non-secure systems. BlindSpot will create a set of digital file fingerprints that can track across networks and systems, ensuring the proprietary and sensitive information for organizations, 365/7/24.


CYBR Ecosystem Overview

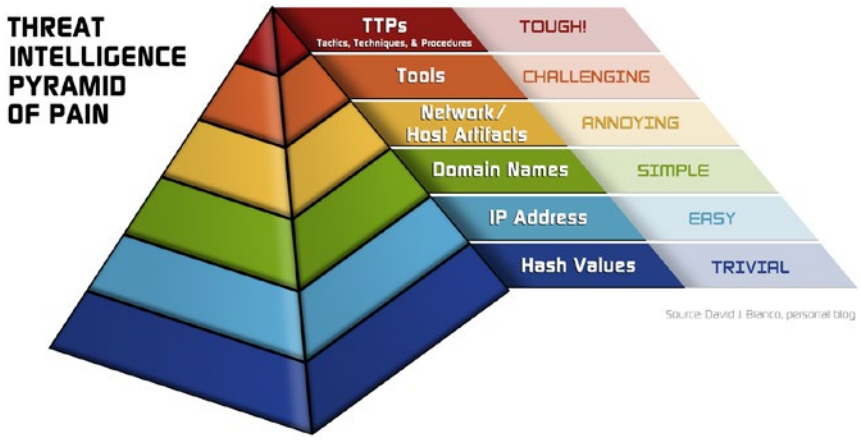
Information technology systems face danger every day as do smart contract transactions and any blockchain project in existence. Hackers work around the clock in an effort to infiltrate systems, steal tokens, take control of systems and the litany of nefarious motives the mind can conjure. Most importantly perhaps, they seek to steal investments from wallets and exchanges.

The CYBR Ecosystem is holistic; arithmetic from part to whole. Via a portal that provides real-time scanning (CYBRscan), safeguards, countermeasures and threat intelligence (MISP/TIP), and an endpoint solution coupled (Blindspot), virtually anything can be detected and stopped that seeks to affect the confidentiality, integrity and availability of crypto smart contract transactions.

CYBR Ecosystem Overview:

- Identifies and disrupts evolving threats to blockchain-based transactions
- Detects advanced and polymorphic threats that seek to circumvent detection by existing safeguards and countermeasures
- Ensures safe transactions by vetting token addresses
- Near synchronous feed of information — emerging threats, new attacks, phishing sites, bad actors and more
- Two years of development with current product sales
- Automated/scalable

In the world of cybersecurity, associated threats and necessary solutions are typically described in what is commonly referred to as the "threat intelligence pyramid of pain" as pictorially represented below:



The keys to a viable cyber security solution includes four core components:

1. Holistic- infrastructure protection in totality
2. Countermeasures and safeguards provide pro-active security
3. Timely threat identification
4. Immediate transition from data to actionable intelligence

CYBR's holistic, cybersecurity solutions provide the technological capability to meet these requirements.

CYBR Architecture

The CYBR architecture primarily consists of three key components:

1. **Web Portal (MISP/TIP)**
2. **CYBRscan**
3. **BlindSpot**

Web Portal

The CYBR Web Portal serves as the CYBR Community User Interface (UI) for the Ecosystem solution. It offers a holistic solution that ensures the cybersecurity of smart contract associated transactions and its threat intelligence can be used to contribute to the security of the blockchain. There are numerous features and capabilities associated with the CYBR Web Portal.

At a high level, they include:

1. **Threat Intelligence**
2. **Verification**
3. **Token Sending/Receiving Capability**
4. **Downloads**
5. **Support Page**

These are currently broken down into subset capabilities, which include:

1. Threats
   a. New Threat Advisories
   b. Search Threat Intelligence Database
   c. Threat Intelligence Feeds
      i. CYBR
      ii. Partner Feeds
2. Verification
3. Verify Token Address
4. Verify Website
5. Send/Receive
   a. CYBR Wallet Details
   b. Send Tokens
6. Download BlindSpot
   a. Windows
   b. OSX
   c. LINUX
   d. IOS
   e. Android
7. Support
   a. FAQ
   b. Knowledge Base
   c. Contact Us

CYBRscan

Robust scanner that scales to allow thousands of simultaneous users to conduct vulnerability scans against laptops, smart phones, websites and other IP-based infrastructure.

BlindSpot

Hackers share and use a variety of tools and techniques to gain and maintain access to crypto and similar associated systems. The most noteworthy and effective techniques are advanced persistent threats.

As mentioned earlier, APT's exploit vulnerabilities in systems that traditional cybersecurity technologies are ill-equipped to deal with. Hackers can now actively camouflage their tools by changing known malware signatures into new files. Without known signatures, this polymorphic malware exploits a gap in most current file detection systems; leaving enterprises open to exploitation.

Traditional signature-based systems simply can not compete and estimated to be roughly 25% effective in contending with APTs.

BlindSpot, even as the files morph and change, sees through it all. It is an adaptive security solution and the heart of the CYBR Ecosystem that can see through the polymorphic camouflage used by the world<s most advanced hackers.

Note: A deeper dive into the technical specifications can be found in the CYBR "Yellow Paper".

TI Portal (MISP/TIP)

Aggregates cybersecurity-related data globally and turns it into actionable intelligence via alerts, analysis and reporting. The TI Portal will contain the largest repository of known vulnerabilities and threats on the planet, and will be easily searchable so that information can be accessed BEFORE an exploitation or hack occurs.

Planned Capabilities

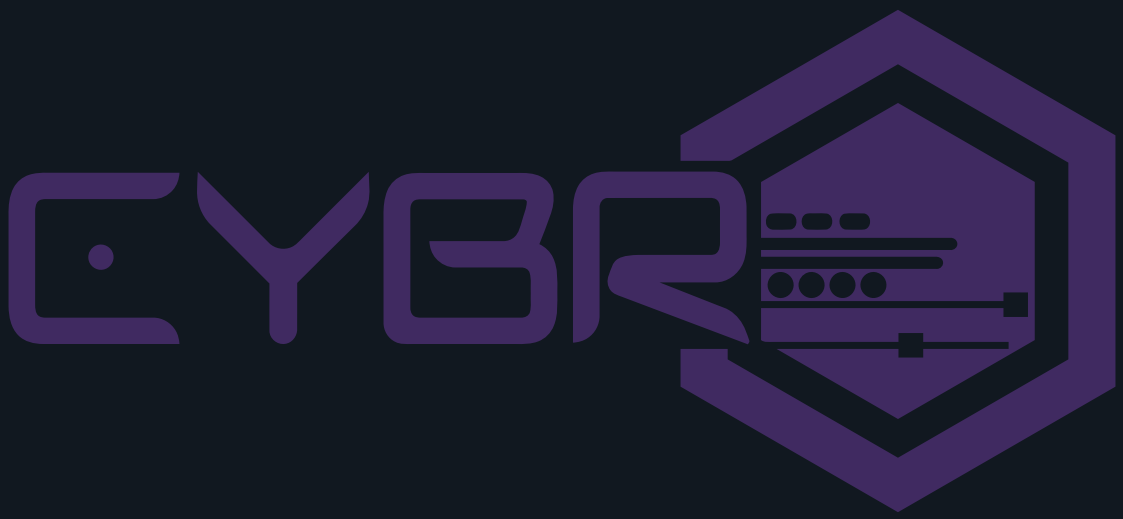
CYBR WALLET

The CYBR Portal shall offer a proprietary CYBR wallet, which incorporates a Token Name Service ("TNS"). The unique TNS feature resolves and reduces public addresses to common names. This provides users the ability to send tokens to known, vetted persons and entities without the concern of sending to incorrect or bogus addresses.

The wallet also includes a facial recognition and biometric (fingerprint) capability, which allows smart contract transactions (send/receive) to occur without the need to enter the private key or the incorporation of a mask (e.g. Metamask). Private keys are NEVER compromised when executed in this fashion.

This capability is exclusive to the CYBR Ecosystem.

The Company



It is imperative that a company, crypto or otherwise, ensures the profitability of the company to ensure return on investment (RoI) for its investors and stakeholders. Stated bluntly: revenue counts.

Too many "companies" in the crypto space today will fail because they will not be able to establish a profitable business model.

CYBR Past Performance

CYBR has existing, world-class partnerships in cybersecurity and blockchain. The company currently holds over $6M in task orders for the Department of Homeland Security (DHS) DOMino program, a $1.115B Indefinite Delivery Indefinite Quantity (IDIQ) contract as a subcontract to Raytheon Corporation.

CYBR holds the following General Service Agency (GSA) contract vehicles and related specializations:

- GSA Multiple Award Schedule (MAS) 070 47QTCA18D00KW
- HACS SIN 132-45A (Penetration Testing)
- HACS SIN 132-45B (Cyber Hunt)
- HACS SIN 132-45C (Incident Response)
- HACS SIN 132-45D Risk and Vulnerability Assessment

CYBR also holds the following National Security Agency ARC:

- NSA ARC Number: 15908

CYBR's past and current clients/partners include, but are not limited to:

PARTNERS

Raytheon
IBM
General Dynamics Information Technology (GDIT)
Lockheed Martin Federal Systems (LMFS)
Dell
Hewlett Packard Enterprise (HPE)
ManTech
Science Applications International Corporation (SAIC)
UNICOM (formerly GTSI)
DEI
EdgeSource
American Systems
21CT
Paragon
Channel Systems
Trigent Solutions
Stratford University
Eastern Michigan University
Western Kentucky University
MKM Global
Cognizant
Campbell and Company (Abu Dhabi)

CUSTOMERS

Department of Homeland Security (DHS)
Department of Defense (DoD)
Department of Transportation (DoT)
Department of Energy (DoE)
Department of Interior (DoI)
Federal Bureau of Investigation (FBI)
Joint Terrorism Task Force (JTTF)
Internal Revenue Service (IRS)
U.S. Mint
Office of the Comptroller of the Currency (OCC)
Federal Reserve Board (FRB)
Federal Reserve Bank
Health Resources and Services Administration (HRSA)
Accenture
DMR
bioMérieux
CareFirst Blue Cross and Blue Shield
Stratford University

Resultant to these relationships, CYBR is able to submit for grants and funding which are not insubstantial, often into the millions. Such funding would allow CYBR to create and update a word-class cybersecurity solution that can transcend the blockchain and potentially disrupt the entire cybersecurity industry.

Ultimately though, CYBR believes it can help the individual, especially in the blockchain space. Crypto wallets are at risk, mobile devices running crypto apps are fraught with peril as evidenced by a recent 224mm USD lawsuit against AT&T regarding the alleged theft of some 24mm via a mobile device.[3] Even two-factor authentication does little to mitigate these risks. The company believes that by establishing itself in the B2B market will pave the way for consumer adoption.

Additionally, the company is involved with numerous global consortiums and recognizes the importance of proof of concept. CYBR will endeavor to provide protection for crypto organizations and enterprises through current solutions and emerging technologies, provided by an Internal Research and Development (IR&D) and Center of Excellence (CoE).

Core Competencies

There are almost as many potential types of hacks as there are hackers. Among the better known are simple web defacement, flooding, brute force attacks, SQL injection attacks and OS command. The need for intrusion detection is commensurate with the traffic and diversity of the network itself. Irrespective of size, scope, breadth and depth, BlindSpot's proprietary capabilities coupled with a real-time data feed and bolstered by communal support (the open source factor), the company believes there is no job beyond its scope.

CYBR shall endeavor to be known as the "guardians of the blockchain" and below is a highlight level list of existing capabilities.

AERIAL

- CYBR threat intelligence protects subscribers from malicious attacks.
  - Guards against Zero Day attacks and advanced persistent threats.
- CYBR can incorporate with existing networking, be it customized or out of the box, with limited configuration changes.
- CYBR's threat landscape meets regulatory and compliance standards.
- CYBR's B2B partners provide proof of concept to individual users.
- CYBR is poised to deliver a B2C solution to "normies" entering the space.

3 www.cnbc.com/2018/08/15/cryptocurrency-investor-sues-att-for-224-million-over-loss-of-digita.html

COMMUNITY AND TOKEN:

- CYBR's community is global watchdogs for the network.
- CYBR'S community provides a key utility for the CYBR token.
- Contributors can earn CYBR tokens for identifying verified, evaluated risks.
- Allocations are contingent upon "degree of difficulty," and level of threat.

HOLISTIC

- CYBR's BlindSpot, data feed and community shall prevent, detect and respond to qualified threats.
- CYBR's compendium of threat intel shall be continuously updated and deployed to subscribers.
- CYBR's solution — a seamless continuum of threat detection that integrates with existing networks, irrespective of customization.

CYBR'S HEARTBEAT

A fuzzy logic engine that will also incorporate the latest in AI and machine learning technologies to maximize pattern matching and heuristics capabilities currently powers CYBR's BlindSpot software.

- Fuzzy logic guards against APTs and identifies threats using proprietary weighted algorithms (much like a drone were it properly used).
- Support vectors/predictive modeling
  — Vectors of attack continuously change

While understanding yesterday's attack can be helpful, it does not guard us against tomorrow's. Thus the need for technologies that can "time travel."

PLATFORMS

Blindspot will be available for the following Operating Systems (OSs):

- Windows (10 and up)
- OSX
- Linux
- IoS
- Android

Note: BlindSpot is also available as a Software as a Solution (SaaS) and Client/Server solution.
Customized development is available upon request.

APPLICATION PLUG-IN (API) AND INDICTOR OF COMPROMISE (IOC) FUNNEL

BlindSpot can also be customized for existing platforms and frameworks.
The data feeds can leverage existing delivery mechanisms (i.e. AV) and function as:

- API
- IOC Funnel

Not So Neural Intuitive Networks

Artificial neural networks are comprised mostly of simple processing nodes that provide a feed-forward, which transmits data in a single direction. A unilateral process is quite limited actually. Although the name sounds compelling, BlindSpot's fluid exchange is much more dynamic and ultimately effective. Additionally, the network is continuously being entrained to all new verified information and is more representative of a developing system.

BlindSpot acts as the cell body, signaling the data feed and community, which serve as "dendrites," delivering and receiving information to and from BlindSpot via a synaptic highway. BlindSpot would also signal the "axon," to deliver validated information to subscribers.

Demonstrating Efficacy

CYBR's intelligence portal shall receive high volume data that relies on an ability to quickly detect and assess threat agents. This information is sent to subscribers in order to prevent systems from being compromised.

A "best-of-breed" threat intelligence engine is mission critical. CYBR's existing relationships in the field can assure subscribers that their data feed will be nonpareil.

Assessment

Much like a truth verification algorithm in oracles, threat intelligence data must be received from multiple sources and interpreted. Machine learning, AI and experience are great tools in converting information into actionable intelligence. For many security concerns though, it is also the proverbial bane of their existence.

Assessment and understanding still belongs in the realm of human thinking and nothing can take the place of experienced personnel. Parsing through information and high-traffic data feeds from virtual security checkpoints in an effort to identify and determine intrusions, can be likened to attempting to find a rabbit in a snowstorm. Optimizing systems for threat identification, continually compiling and archiving data are best practices, but lesser practitioners and solutions will overlook vital information.

The company's experience in managing threat intelligence platforms and their unrivaled access to robust data feeds, normally reserved primarily for government agencies and Fortune level companies, offers a leg up on its competition.

The Team

CYBR's team of executives, staff and advisors bring combined 125 years of cybersecurity, blockchain and information technology experience. Complete bios and profile information can be found on the main website (CYBRtoken.io). CYBR's founder is the primary key personnel member.

A brief bio of Mr. Key includes:

SHAWN R. KEY – CYBR Founder

- 20 Years as a Corporate Executive
- Published Author
- Accredited Professor
- Cybersecurity Subject Matter Expert (SME)
- CISSP Professor, Microsoft Certified Trainer (MCT)
- Program/Project Manager
- Chief Scientist — Product Development

NOTABLES

- TandemNSI Winner (Best of CyberSecurity) 2016
- Mach37 Cyber Accelerator Inaugural Cohort Member 2013
- Dell Founders 50 Club Cohort Member (2014)
- CIT CRCF Award Winner ($50k): 2015
- CRCF Matching Funds Awardee ($100k): 2015
- NVTC Destination Innovation award (Most Disruptive Technology, Security Category: 2014)
- AOL Fishbowl selection (2015)
- DC-iCorps selection: 2014
- Georgetown Hoyas Startup Finalist: 2015
- Tandem NSI Award for most disruptive technology
- Letter of Commendation, Joint Terrorism Task Force (2014)
- Army Civilian Medal of Honor Nominee (1999)
- Army Reserve Deputy CIO Nominee (2000)

Threat Intelligence Community (TIC)

Individual users and companies interested in earning CYBR tokens are welcome to join the CYBR Threat Intelligence Community (TIC).

CYBR tokens are required to access the CYBR portal, which offers the official download for BlindSpot — CYBR's proprietary intrusion and malicious actor detection software.

CYBR community members that have captured verified, evaluated risks or threat, information deemed valuable at the Company's discretion, and have shared said data with CYBR, these contributors may earn a reward.

Although no risk scoring metrics are currently in place, the company feels it is capable of assessing the information accurately. Thus, rewards shall be contingent upon "degree of difficulty," determined by the level and uniqueness of threat and/or intrusion.

CYBR tokens can also be earned by key opinion leaders, community leaders or shared for promotional purposes. Others who may submit suspicious network information may also qualify.

Roadmap

Q2 2016 – Q2 2018

- East Coast office opened (Virginia)
- BlindSpot Enterprise Solution is developed and rigorously tested
- Larger pilots are deployed
- Enterprise sales generate revenue

2018

Q2

- The detailed design description for the CYBR Ecosystem is completed
- Over 30 million unique, digital identifiers are added to the BlindSpot database
- The Software as a Service (SAAS) model is repurposed for the blockchain and the CYBR Ecosystem Testnet begins development

Q3

- CYBR utility tokens are generated

2019

Q1

- CYBR Private Sale Opens
- IoS and Android client development begins
- Web App, API and IoC funnels development completed
- CYBRscan v1.0 Released

Q2

- Malware Information Sharing Platform (MISP) v1.0 Released
- Initial Coin Offering (ICO)
- CYBR will be listed on top exchange(s) for global trading

Q3

- Integration of numerous data intelligence feed providers (some partnerships already in place)
- Integration of AI and Machine Learning platforms and frameworks into CYBR Ecosystem (some partnerships already in place)

Q4

- BlindSpot v1.1 Release
- CYBR will market globally to disrupt and dominate anti-virus and malicious code vertical marketplaces

Q1 2020 AND BEYOND

- Assess technology posture/market conditions; drive CYBR into as many global market verticals as possible

DISCLAIMER

CYBR IS NOT A SECURITY. THIS DOES NOT CONSTITUTE AN OFFER TO SELL OR A SOLICITATION OF AN OFFER TO BUY CYBR TOKENS. THE INFORMATION CONTAINED HEREIN IS PROVIDED FOR EDUCATIONAL PURPOSES ONLY.

CYBR is a utility token that is the exclusive form of payment that will be accepted to purchase services and subscriptions that CYBR offers.

Tokenomics

CYBR's Token Generating Event consists of a pre-sale and subsequent public event. The stated dates are estimates and subject to change — subject to extensions and early termination. The soft cap shall be $2,000,000 (2M USD) and the hard cap shall be $15,000,000 (15M USD), although CYBR reserves to seek additional funding.

1 CYBR Token = $.10*

Founders' tokens will be locked for one year and large investors' tokens are locked for a minimum of six months. We changed the original token allocation to be more in line with the public tokens generated during the TGE. We moved large portions that were allocated to the team and others to the Economic Reserve to ensure that the initial supply, at launch, will be small enough so that token price appreciation will not inhibit CYBR platform use. If we priced our tokens too expensive at launch, then the steep price would discourage the use of the CYBR platform and any token price appreciation would just exacerbate this. That is why we decided to keep the circulating supply, and original price low: to leave room for the imminent growth we see coming. We plan to keep the majority of tokens in the Reserves locked up for five years while the platform matures, increases user base, and the initial price discount that early adopters have enjoyed is closed by the free market.

The Token Generating event was used to determine the appropriate level of CYBR tokens to release to the public. The tokens themselves will act as an access pass to the CYBR portal; the more you hold the more features will be available to you. We priced the tokens to give our early adopters a very big discount to say thank you for believing in us. The tokens allow you access with no need to renew subscriptions. As we grow and provide better and better service to the community, the world will begin to take notice and see the value that holding our token provides. As more and more people use CYBR tokens, the initial discount gap between our competitors and us should close. If anything, we would hope that the token value would appreciate to the point where a subscription to our service is now at a premium to our competitors because we will be offering a top-of-the-line service. In the very near future, we will be releasing our proprietary Cyber Wallet, which will come with some features that, if you choose to use them, will require a small amount of CYBR to be burned to further drive scarcity of the tokens proportionate with use. This will add further utility to the token and increase demand and scarcity.

Some potential clients might not want to go through the "hassle" of getting an Ethereum wallet and purchasing CYBR tokens. In fact, a lot of our potential clients are in the government space, and tend to be slow to move out of their comfort zone. We don't want this to hinder their use of our services, but doing cash deals would not benefit the CYBR token ecosystem, so any cash deal can easily be converted to CYBR token subscription by simply sending the number of

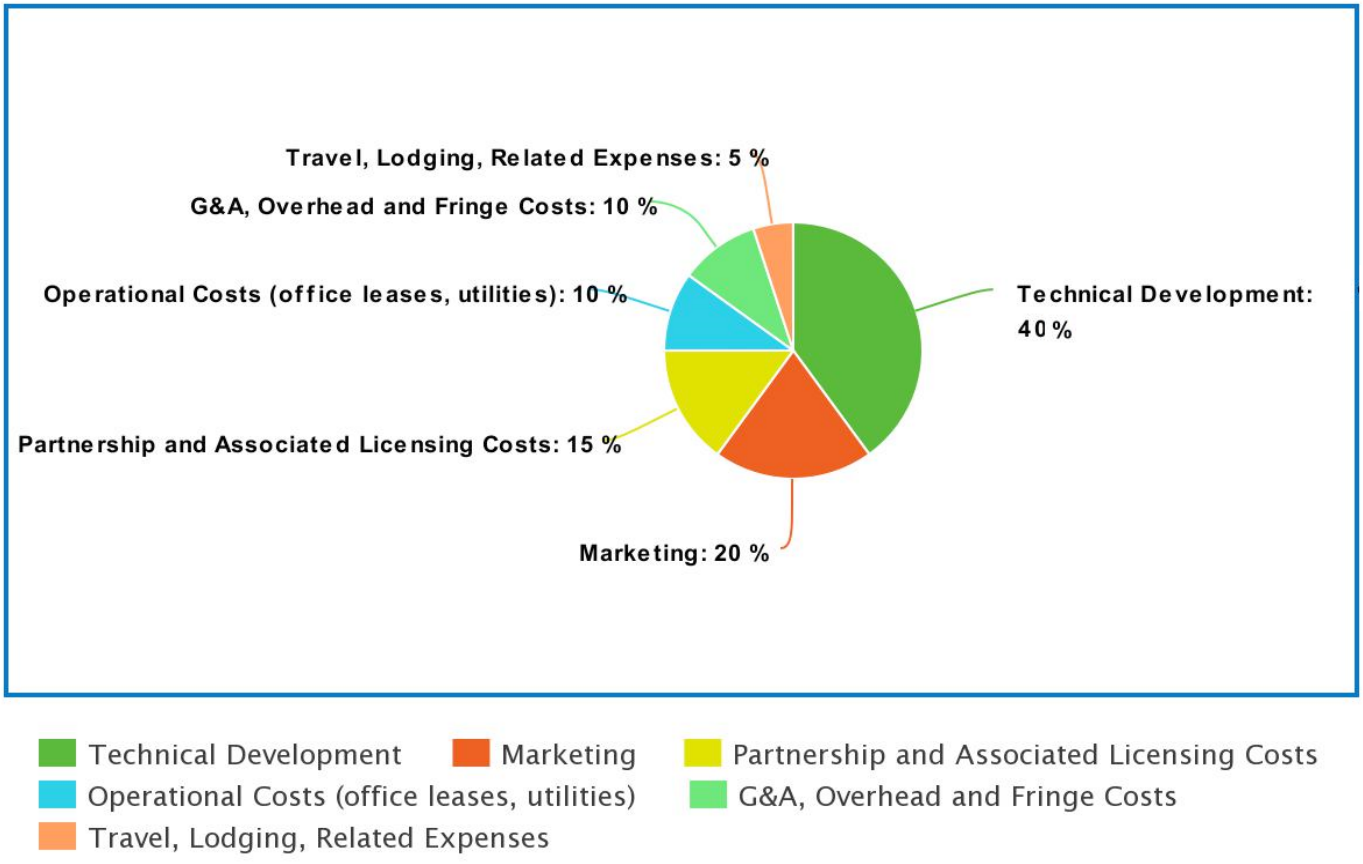
tokens needed for an unlimited subscription to a public burn address and use the remaining cash for CYBR operational needs.

The number of tokens required will vary depending on individual needs. Access to live monitoring would require approximately 5,500 tokens*. This service would cost upwards of $4,000 annually from one of our competitors. We need the tokens value to properly reflect the value of holding a subscription to our service, and we are relying on the free market to do this for us. The circulating supply of CYBR tokens is exceptionally small, with approximately 55,000,000 CYBR currently. That quantity would only allow for 1,000 clients holding 5,500 tokens, not even counting the casual user who holds just a few hundreds CYBR* just to gain access to M.I.S.P., or the big client with 500,000* for unlimited access. As more people join the CYBR ecosystem, it will be harder to find people willing to part with their CYBR.

We don't want speculators holding our token, we are proud of our product. We want people to use our CYBRscan portal, and love it. Once we have proved our value and all CYBR holders are CYBR platform users, CYBR will be able to use the economic reserve to pay for day-to-day operations so that we can continue to deliver the best in class service to all our CYBR holders.

*Structured bonuses and subscription tier price structure are to be determined and announced.

Projected Use of Proceeds



Smart Contract Address

The CYBR Smart Contract is: 0xf51494955A43c23E34d83C1C5F1305B652fE0bCa.

Token Delivery

CYBR Tokens shall be distributed via a smart contract to the Ethereum address that was used to participate in the TGE. Upon completion of the event, the CYBR Tokens shall remain locked to avoid any secondary market trading activities.

Ongoing Development

The continued development of the CYBR ecosystem is a considerable allocation of resources. Adapting BlindSpot and the key components of support may be assigned to the core CYBR team and remuneration shall be necessary. Temporary and full-time staff will likely be comprised of cybersecurity, engineers, developers — both blockchain and software, infrastructure architects, AI engineers, data specialists, customer service, support, marketing strategist et alia.

Testing and Maintenance

Additional resources will be expended on the upkeep and testing of the CYBR platform. Given the nature of cybersecurity, testing is extremely thorough and often ongoing. Maintaining the integrity of our product offering is paramount and nothing will be released without taking needed precautions and assurances. There is also a relatively constant need to hone as well as maintain, and even upgrade, both software and hardware. These shall be part of operational costs.

Business Growth and Development

CYBR anticipates transitioning its focus from the B2B to the B2C sector. Certainly, the marketing and promotions of products and services is a notable consideration. The company believes that the eventual adoption of crypto for individuals portends a market that shall be underserved. Any sales and marketing is designed to support the manageable growth of the CYBR solution. CYBR feels poised to offer a cost effective, accessible platform that will appeal to the masses. Our focus on SMEs, blockchain projects and public sector work will expand to include individual users. It is our goal to secure long term security contracts with these potential customers CYBR is wholly confident in its ability to deliver a superior product to the end-users that will also provide a reduction in costs. Again, all transactions and subscriptions shall be made using CYBR Tokens.

Legal Considerations

Token Generating Event (TGE) is subject to Terms of Sale provision and will be published separately. Please refer to CYBRtoken.io for further information. Website implements special features restricting access to TGE until all terms, conditions and rules are explicitly and clearly accepted.

PLEASE READ THIS DISCLAIMER SECTION CAREFULLY. IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL, FINANCIAL, TAX, OR OTHER PROFESSIONAL ADVISOR(S). The information set forth below may not be exhaustive and does not imply any elements of a contractual relationship. While we make every effort to ensure that any material in this white paper is accurate and up to date, such material in no way constitutes the provision of professional advice. CYBR token does not guarantee, and accepts no legal liability whatsoever arising from, or connected to, the accuracy, reliability, currency, or completeness of any material contained in this white paper. Investors and potential CYBR token holders should seek appropriate independent professional advice prior to relying on, or entering into any commitment or transaction based on material published in this white paper, which material is purely published for reference purposes alone. CYBR tokens will not be intended to constitute securities in any jurisdiction. This white paper does not constitute 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. CYBR does not provide any opinion on any advice to purchase, sell, or otherwise transact with CYBR tokens, and the fact of presentation of this white paper shall not form the basis of, or be relied upon, in connection with any contract or investment decision. No person is bound to enter into any contract or binding legal commitment in relation to the sale and purchase of CYBR tokens, and no cryptocurrency or other form of payment is to be accepted on the basis of this white paper. No person is bound to enter into any contract or binding legal commitment in relation to the sale and purchase of CYBR tokens, and no cryptocurrency or other form of payment is to be accepted on the basis of this white paper.

This CYBR White Paper is for information purposes only. We do not guarantee the accuracy of, or the conclusions reached in this white paper, and this white paper is provided "as is." This white paper does not make, and expressly disclaims all representations and warranties, expressed, implied, statutory or otherwise, whatsoever, including, but not limited to: (i) warranties of merchantability, fitness for a particular purpose, suitability, usage, title or non-infringement; (ii) that the contents of this white paper are free from error; and (iii) that such contents will not infringe third-party rights, and its affiliates shall have no liability for damages of any kind arising out of the use, reference to, or reliance on this white paper or any of the content contained herein, even if advised of the possibility of such damages. In no event will Team CYBR or its affiliates be liable to any person or entity for any damages, losses, liabilities, costs or expenses of any kind, whether direct or indirect, consequential, compensatory, incidental, actual, exemplary, punitive or special for the use of, reference to, or reliance on this white paper or any of the content contained herein, including, without limitation, any loss of business, revenues, profits, data, use, goodwill or other intangible losses. CYBR makes no representations or warranties (whether expressed or implied), and disclaims all liability arising from any information stated in the white paper. In particular, the "Roadmap" as set out in the text of the white paper is subject to change, which means that CYBR is not bound by any representations to the future performance and the returns of CYBR. The actual results and the performance of CYBR may differ materially from those set out in the CYBR White Paper. Please note that contents of CYBR White Paper may be altered or updated at any time in future by the project's management team. The white paper has been prepared solely in respect of Initial Coin Offering of CYBR tokens. No shares or other securities of the Company are being offered in any jurisdiction pursuant to the white paper. The white paper does not constitute an offer or invitation to any person to subscribe for or purchase shares, rights or any other securities in the Company. The shares of the Company are not being presently offered to be registered under a Securities Act of any country, or under any securities laws of any state. The tokens referred to in this white paper have not been registered, approved, or disapproved by the US Securities and Exchange Commission, any state securities commission in the United States or any other regulatory authority, nor any of the foregoing authorities examined or approved the characteristics or the economic realities of this token sale, or the accuracy, or the adequacy of the information contained in this white paper under the US Securities Act of 1933 as amended, or under the securities laws of any state of the United States of America.

For any other jurisdiction, purchasers of the tokens referred to in this white paper should be aware that they bear any risks involved in acquisition of CYBR Tokens, if any, for an indefinite period of time. Some of the statements in the white paper include forward-looking statements which reflect Team CYBR's current views with respect to product development, execution roadmap, financial performance, business strategy and future plans, both with respect to the Company and the sectors and industries in which the Company operates. Statements which include the words "expects," "intends," "plans," "believes," "projects," "anticipates," "will," "targets," "aims," "may," "would," "could," "continue," and similar statements are of a future or forward-looking nature. All forward-looking statements address matters that involve risks and uncertainties. Accordingly, there are or will be important factors that could cause the group's actual results to differ materially from those indicated in these statements. These factors include, but are not limited to, those described in the part of the white paper entitled "Risk Factors," which should be read in conjunction with the other cautionary statements that are included in the white paper. Any forward-looking statements in the white paper reflect the group's current views with respect to future events and are subject to these and other risks, uncertainties and assumptions relating to the group's operations, results of operations and growth strategy. These forward-looking statements speak only as of the date of the white paper. Subject to industry acceptable disclosure and transparency rules and common practices, the company undertakes no obligation publicly to update or review any forward-looking statement, whether as a result of new information, future developments or otherwise. All subsequent written and oral forward-looking statements attributable to the Project CYBR or individuals acting on behalf of CYBR are expressly qualified in their entirety by this paragraph. No statement in the white paper is intended as a profit forecast and no statement in the white paper should be interpreted to mean that the earnings of Project CYBR for the current or future years would be as may be implied in this white paper. By agreeing to acquire CYBR token, I hereby acknowledge that I have read and understand the notices and disclaimers set out above.

No regulatory authority has examined or approved of any of the information set out in this white paper, thus no action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this white paper does not imply that the applicable laws, regulatory requirements or rules have been complied with. Please refer to our website for terms and conditions of participating in CYBR Initial Coin Offering.