Using Block Chain to Establish Distributed Trust for IOT

By Christopher Gorog, MBA, PMP, CISSP
Edited by Tony C. Rossi, Esq. Chief Legal Officer – BlockFrame, Inc.

ABSTRACT

This White Paper provides an overview of the common problems existing in the Cyber Security Industry and gives a first look at next generation Block-Chain-enabled-solutions which are being used to solve these problem by enabling a framework for securing the Internet of Things (IOT). The solutions offered address global issues experienced across all current applications in the cybersecurity industry. Readers who are looking for Investment opportunities, those who have interest in early adoption opportunities for integrating existing products into new cyber ecosystem frameworks, and simply those looking to understand or get involved with next generation unified cyber security eco-systems efforts should fine this explanation fascinating.

Introduction

BlockFrame, Inc. is a company dedicated to building a future where cyber-security is implemented from the ground up. BlockFrame's Frameworks are changing the behavior of people by enabling the accountability of trusted transactions. This system implements a unique interface structure between multiple industry segments. BlockFrame and its partners are developing frameworks for cybersecurity creating models which resemble the trust chain implementation used by Bitcoin. As is the case with Bitcoin, transactions and responsible parties' actions become traceable anywhere in the world anytime in the present or future. The applications we will discuss provide the ability to create accountability for each data exchange while at the same time protecting individual privacy.

Solving Entire Industry Problems

Throughout history new developments have rendered previous processes, technologies, business models, or even entire ways of life obsolete. In the technology age we have become accustom to change and for the most part have a comfort level with the "next thing." Many people even seek what will or could be the next disruptive or ground breaking technology. It is easy to identify disruption in retrospect, but identifying what will become game changing ahead of time is not so easily accomplished.

What can we use to identify a technological change which will be significantly disruptive in the future? A key factor is that the disruptive change presented a solution to an existing industry wide problem. Microsoft and Apple provided a solution to the industry problem when computers were not easily accessible to the general population. These companies created an interface that made computers user-friendly. Neither of these companies invented computers or software, but they did revolutionize the way people use them.

Seldom does an industry alignment present the opportunity for a disruptive and ground breaking change. The position to take advantage of such an opportunity is often even less feasible. Often such new technology is embodied within consumer products or a services, as in the examples of Microsoft and

Apple. Recently we have seen changes in the form of services which attempt to solve social problems such as facebook or Uber. However, some of the most valuable industry solutions fall in the Business-to-Business sector. In order to relay these solutions, the following historical example of such and industry solution is relevant.

Industrial Revolution Industry Solution

In the mid-1800s a new trend was occurring which greatly extended the growth of the industrial revolution. Oil, which had been known about by humans for centuries, was beginning to be adopted for use in both public and private applications. However, a large problem existed industry wide. Every place oil was pumped out of the ground it was a different grade and it contained different concentrations of burnable components. It was not until 1862 when a chemist named Samuel Andrews developed the process of Fractional Distillation that a solution for this industry wide problem was discovered.

At that time of Samuel Andrews's discovery, the United States was in the midst of Civil War so commercializing this process was shadowed by current events. It wasn't until 1870 that the Standard Oil Company was formed with Fractional Distillation as its core intellectual property technology. Standard Oil and its more famous contributor John D. Rockefeller did not begin by owning oil wells and distributing oil. Their contribution was much more valuable as it provided a solution to the problem that the entire industry was experiencing at the time. The process of Fractional Distillation had to be adopted by each company who sold oil because there was no other unifying solution to make each supplier's product usable across every combustion product that utilized oil. In fact Fractional Distillation, is the process we still use today in refinement operations which enables the commoditization of oil worldwide.

Solving the Cyber Security Industry Problem

The Cyber Security industry is currently in a similar place that the oil industry was prior to 1870. Each product, application, or service that provides security solutions today has very unique applications of how the underlying security is implemented. Though each implements the same very small set of primitive security operations, and each maintains keys to do these operations, they all do this extremely differently. The industry problem is that no two security applications can work together. This contributes to the even larger problem that no unified method exists to trust devices or information transmitted between devices on networks which are already connected worldwide.

As is the case of the oil industry during the industrial revolution, the technology to connect systems and transmit data has come into existence long before the interconnecting systems that exist today. However for Cyber Security field, solving the industry problem requires a twofold approach. First a process for providing an underlying trust on each computer system and secondly the founding of a neutral prevailing body to handle the logistics and governance of the execution of the process for provisioning the underlying trust.

Neutral Governance and International Visibility

Cyber Security is responsible for the protecting and restricting access to the most sensitive components of each organization. Thus any prevailing body which has the ability to circumvent or gain global access to the private sensitive information of everyone in the eco-system needs to be neutral in its

allegiances and transparent in its governance operations. Such a governing body is paramount to the acceptance of any solution worldwide. Also, any industry solution for a network-connected-world must also implement a technology solution for transparency of its internal operation to external parties in order to maintain neutrality.

To maintain transparency and openness for governance, the solution we are introducing with this white paper relies on the international non-governing body, the National Cybersecurity Center, and also the power of a BlockChain distributed ledger technology platform. BlockChain technology which is well known from it largest use in the Cryptocurrency bitcoin, combines the power of immutability and distributed records of transactions. Block Chain provides a great tool with which to provide the visibility of operations and the trust of transactions which leads to accountability of all actors also leading to transparency of the governance process itself.

Fallacy in Current Approaches to Cyber Security

Over the last two decades the cyber security industry has moved in a direction which is not sustainable. As the world has moved from the networking of a few devices to the vast expansion of a worldwide internet, we only find that as people become more educated on technology, the problems with the deviant behavior of people that existed in the physical world transfers directly to the internet. This has become a problem of epic proportions.

We have also found that a new paradigm exists in the virtual world. Traditional boarders, boundaries, and physical limitations of interaction between people does not carry over to the internet. The Virtual world has no concept of distance and is borderless. However our designs and thought process for security in this virtual cyber space are based on our existing knowledge of the real physical world. Like our change into the virtual world of the internet, our thought process around protecting and enforcing virtual space (Cyber Security) must adapt to this new paradigm as well.

The internet, unfortunately, was not developed initially with security in mind. Widely used communication protocols do not first check conditions on the communicating parties before allowing electronic point-to-point connection. All communications are permissible and it is the responsibility of each party to monitor any and all communications at their own expense and/or accept the resulting risk should they not. The cyber security world has painted itself into a corner where the most widely used cyber security operations result in monitoring and collecting nearly all communications, storing all data, and analyzing these ever growing data sets from every source organizations interfaces with.

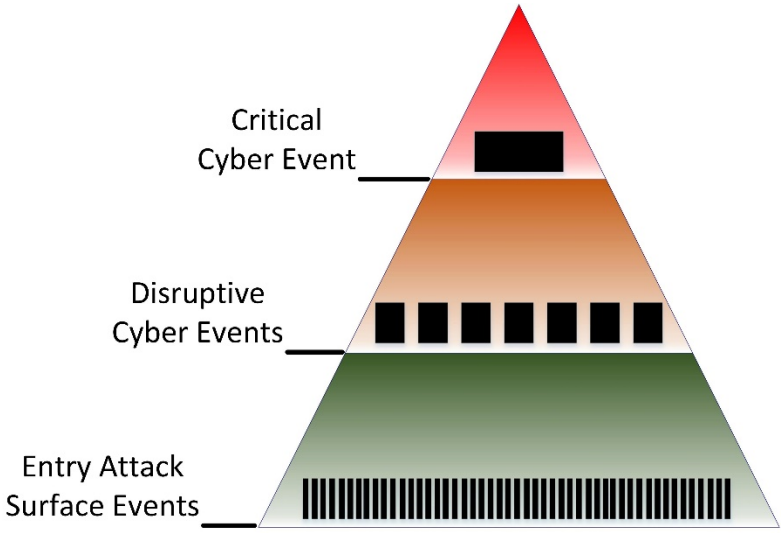
Data sets and communications are growing exponentially and the tools and/or human operators only have the ability to examine the collected traffic/data in a linear growth capability at best. Thus our attack surface grows at this same exponential rate as data, but our defense capability follows the linear ability for human absorption. Even to maintain the linear growth requires a continuous diligence of adding more tools, servers, and human resources on a continuous scale. Needless to say this trend is not sustainable on an indefinite basis, and many organizations have already reached a plateau in their ability to maintain this trend.

New Paradigm in Approaches to Implementing Cyber Security

As the sustainability of current approaches becomes less feasible, we see more and more attacks and breaches of data worldwide. Such attacks will continue to grow until there are dynamic changes to reverse this current trend. We can use the triangle in the Figure "Cyber Event Escalation" below to show how Cyber events are related.

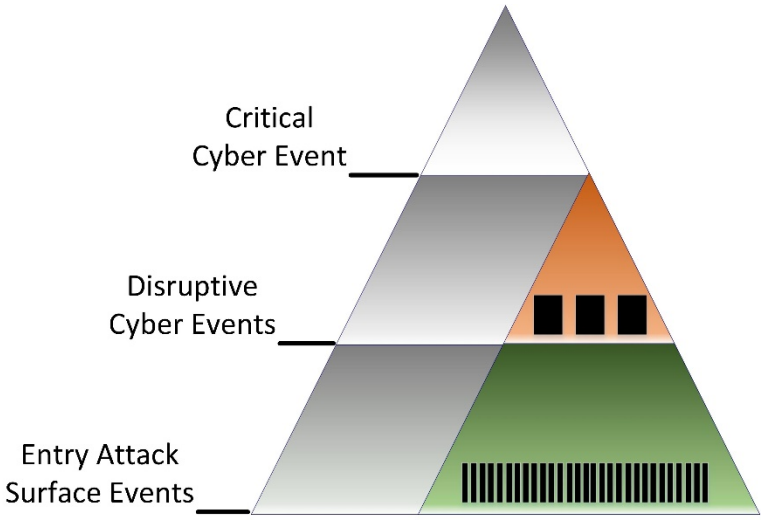
The Figure works from the bottom up. Many Entry Attack Surface Events occur frequently shown on the bottom row. Some of these bottom level events are cybersecurity threats and some are not however all events have to be assessed. The middle column represents events before they become critical. The top portion represents the critical cyber events that can cause the most damage.

Figure: Cyber Event Escalation



Making an impact on the reduction of Critical Cyber Events takes an approach of reducing the entry attack surface. The current approach to monitoring and policing traffic and data, which is growing at an exponential rate only exaggerates the problem. These current cyber security approaches will continue the current trend resulting in the growth of Critical Cyber Events. The only way to change the trend is through solutions which address the reduction of entry attack surface events which reduce the number of disruptive cyber events to a manageable scale which human actors would then have the capability to address. As you can see in the Figure "Reduction of Entry Attack Surface Events" reducing entry attack surface events must be done to a scale where disruptive cyber events are manageable and critical events are completely eliminated.

Figure: Reduction of Entry Attack Surface Events



This paradigm shift is realized by the nature of BlockFrame's Frameworks as they support the ability to create an eco-system of trusted computing devices. This eco-system approach to authorized vendors and products reduces the number of entry attack surface events to a manageable level.

Synergistic use of Blockchain and Cryptographic Trust Root

The solutions offered by BlockFrame Inc. use BlockChain technology in addition to a chain of trust hierarchy to create a strong synergy enabling the immutable identification of any device as well as the unification of underlying cryptographic keys used for communications.

A cryptographic key is a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa. This key remains private and ensures secure communication. The unified-communications-keying-approach offered by our solution establishes an underlying base security architecture which may then connect to any security product or application and provide whitelisting capability to all enabled devices. Whitelisting limits participants to those who have been verified. Blacklisting is an example of our internet today where anyone can participate in data transactions without verification.

Once each device has this capability, it is able to uniquely self-identify the trusted state of the system at the onset of communication. An ecosystem of self-identifying devices removes the ability of outside devices to impersonate or spoof communications as they cannot produce trusted communications without being a part of the ecosystem. The BlockFrame solution is used to establish such an ecosystem.

The technology outlined enables for the first time an industry wide approach to identity assurance of any Internet of Things (IOT) devices while also providing a governance support on an industry wide scale. BlockFrame Inc. solutions provide a Cryptographic Trust Center (CTC) in the form of a simple integrated circuit chip which is placed within each eco-system enabled IOT device. A cloud support service operated in partnership with the National Cybersecurity Center (NCC) neutral governance body then offers Trust as a Service (TaaS) functionality enabling the provisioning of trusted components in each

device. The process for provision is designed to ensure that no human has access to the provisioned components and thus cannot be circumvented without global awareness to any instance which would equate to a violation of privacy. The overall operation will enable an Eco-system to coordinate and set the base underlying security components on each IOT device. This will provide a unified support for linking any current or future security solution to a global governance process using a block chain distributed ledger for worldwide logistics.

BlockFrame Framework Market Adoption

The research project which the BlockFrame application is founded on has already gone through years of R&D and patent filings to identify the base components required for an underlying expandable distributed trust solution. Though no solution will ever encompass all possibilities, the product in development includes several design iterations executed to identify and empower as many current and future use cases as possible while providing the flexibility to augment for future needs.

Research and Development Phase

As can be seen in the Figure "Market Adoption Pyramid" this ecosystem encompasses the entire cyber security market and can be best described as a rising tide which is lifting all ships. All segments of the Cyber Security Market can benefit and partners from each segment will have the opportunity to participate or adopt the ecosystem at various stages. Research and Development partners are already engaging as these types of visionary organizations see value in not only adoption of the ecosystem but in its support and development.

Early Adoption Partners

Early adopters from each industry segment can partner for first of a kind security status in their particular segment. Visionary companies and products are aligning for temporary advantage of exclusive status within their industry as they integrate products and software with eco-system enabled solutions. Partnering for early stage adoption enables the ability to align with other segment companies which are also self-identify as forward thinking cyber security industry leaders.

Strong Product Use Case for Early Adoption

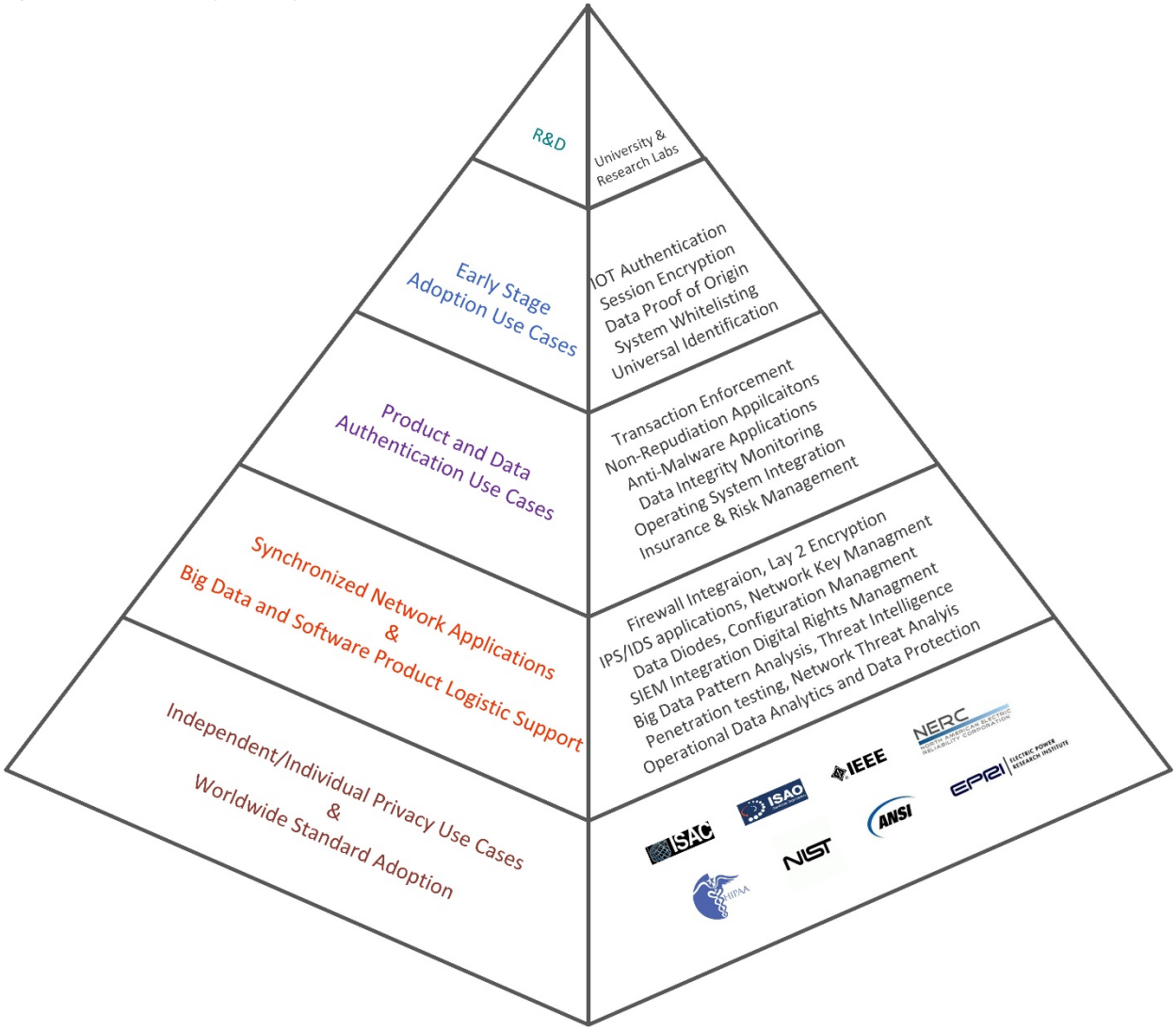
Initially the strongest solutions for adoption will be in the IoT segment with an especially high value to those operations requiring high levels of distributed trust. Much of the work to date has been in the area of energy system to enable distributed energy production and clean energy applications such as personal electrical vehicles.

Such applications require trusted communications along with proof of origin on data for the safety of electrical-mechanical operation, and to enable non-reputable transactions from communications received from distributed renewable energy devices which are out of the control of utility networks.

Other initial adoption uses are those which require mission critical communications, and the ability to renew and refresh security posture often. Highly sensitive operations for Homeland Security or Distributed mission critical networks require trust of devices as their primary mission. Those may include

IOT devices used to monitor bio-rhythms of mission critical personal, or any other applications with large sensor networks reading sensitive data from critical networks.

Figure: Market Adoption Pyramid



Industry Support Cloud Services

As cloud services for industry support come online, opportunities for partnerships in the implementation of governance will be available and will require many jurisdictions to be involved for this adoption. In this area we also welcome and look forward to the integration of partners worldwide which will align under the industry support offered by the initial support body the National Cybersecurity Center. Much like lawyers' Bar Association, or the World Health Organization, this support will be replicated by local governing organizations on a world wide scale.

Industry and Logistics Support

An exceptional strength of this solution revolves around the industry neutral partnerships with the National Cybersecurity Center (NCC), the Cyber Resilience Institute (CRI), and other partners committed to creating a neutral industry presence. Many challenges to cybersecurity solution exist in a large part due to the nature of the scope of ownership and control of the governing organization. This aligns with the DHS efforts and the Presidential Directive PPD-21 to produce public-private-partnerships for supporting the development of cyber security and protection of critical infrastructure.

The NCC has an international status as a non-governing body which permits them to take ownership of the governance independent of any industry player or governmental control. The industry registrar which is being designed under this program is intended to be turned over to these neutral organizations for operational oversight. These neutral bodies will need to organize and design features to be overseen by committees which will maintain their neutrality. Initial features which have been identified as needed will be initially outlined as part of this effort and then later transferred to the governance of the NCC and CRI. They include the following identified items as well as more as the governance committees mature:

1) Operational network requirements for security posture renewing
2) Attributes of trust components within distributed device
3) Versions control and updating of components
4) Vetting of brokering agents and ecosystem trusted organization
5) Aligning risk factors and levels to industry models
6) Operational procedures and dispute resolution
7) Determining data visibility, public, private, sealed etc.
8) Due process for governance and legal proceedings

Current Status of the Ecosystem

Industry governance growth has begun through existing partners and industry relationships. These organizations support policy, or political neutrality required to further the industry adoption for this solution. Governance organizations act as international non-governing bodies to maintain the industry governance aspects or as subject matter experts in domains required for global adoption.

Research Laboratories function to support in the integration of technology and align as a government technology transfer partner for public private partnerships. Overall the industry growth capabilities for this application are exceptional as the technology and social organization needed to support growth in this industry are already aligned for engagement during market adoption. The support of such partners, provides an underlying support to adopt this technology which will connect every security application currently in the market place.

We encourage engagement form public, private, and education sectors where organizational missions align to the initiatives outlined in this white paper. Whether you are looking for early adoption integration of products, have interest to support in the R&D phase, or are just looking to be involved with

cyber industry driving efforts, we welcome you to reach out to BlockFrame Inc. or the National Cybersecurity Center to engage with us on areas for possible alignment to support this project.