Information Assurance Platform: Blockchain information assurance and artificial intelligence for decentralised security and attestation (IAP)

team@iap.network original publication date: March 2018

> **The IAP is a next generation distributed ledger technology information assurance, regtech and cybersecurity platform**. Applications built on the IAP solve problems surrounding the storing, processing and transmission of information for individuals, organisations including distributed autonomous organisations (DAOs) and non-government organisations (NGOs), companies and governments. The IAP team is comprised of cybersecurity white-hats, industry and academic advisors and governance, risk and compliance experts with centuries of combined professional experience.
>
> **Blockliance** is a distributed multi-chain ledger application that will utilise the IAP to solve governance, risk and compliance (GRC) security and business problems.

Abstract

Blockchain technology naturally lends itself to the assurance of information. Most real world examples of this emerging and evolving technology are focused on financial applications: currencies, transactions and the exchange of value. While these issues are certainly interesting, projects like Ethereum have shown that the real potential of blockchain reaches further into the future, and deeper into society, than originally envisaged. Whilst blockchain technology has not yet become universally applicable, the next generation of blockchain technology brings a maturity to the space that benefits both on and off chain technologies.

The Information Assurance Platform[1] (IAP) is a suite of protocols, next generation blockchain technology and cryptography for incentivised and verifiable management of the assurance of information between parties in a decentralised, flexible, scalable, secure, private, immutable and resource efficient manner.

The IAP framework is a governance and ethics system with artificial intelligence that allows individual applications to ensure that the possibilities of the use cases are set within defined criteria. IAP is for individuals, developers, organisations and civic bodies to reliably and securely contribute to and benefit from an environment within which arbitrary data points and processes can be attested to and verified in computationally efficient ways. The IAP is suitable for applications in a range of sectors, including critical infrastructure.

For businesses IAP enables data driven artificial intelligence solutions to customers and users, saving costs and increasing visibility into data in a secure and private way. For the assurance of information internally and externally, the IAP's initial application (Blockliance[2]) can be used to solve several pain points regarding attestations and assessments for governance, risk and compliance (GRC).

The IAP is constructed of a mixture of established technologies, tried and tested cryptography, distributed computing infrastructure, hierarchical network structures and distributed ledger technologies already deployed globally, combined with emerging technologies, cutting edge protocols and applications of existing cryptographic primitives in new ways.

The IAP is both local and global. Use cases already exist in the areas of information assurance for identity & privacy management, regulatory compliance and cybersecurity, know-your-customer (KYC), anti money laundering (AML), digital forensics, blockchain security, and transparency of process. Use of the IAP can assist in merging both traditional and blockchain based technologies, frameworks, protocols and design to the benefit of both sides.

The IAP is a platform that is dedicated to the assurance of information in a decentralised, trustless[3], reliable, efficient, accessible way.

The IAP has the ability to provide for the ethical and appropriate application of decentralisation of data, which can maintain the privacy of related data and processes; meaning that it has wide reaching implications in many different areas of business, society, culture, government and personal interaction.

With its next generation of distributed ledger technology, the IAP brings blockchain technology to a point where its value outside of financial instruments can be fully realised. Adoption is possible when businesses, end users, developers and society stand to benefit, and there is a low barrier to entry in doing so.

Designed to be fully compatible with all generations of blockchains, the IAP works alongside existing non blockchain systems, protocols, and legacy technology to provide a bridge to decentralised services and facilitation of the enhanced security, monitoring and control they can provide.

Index

1.0 The Problem

1.1 Background

A problem of trust and the assurance of information impacts all areas of life and society, and is central in any interaction between two or more parties, be they individuals, devices with computers inside them, organisations, DAOs, corporations or governments.

Society requires trusted third parties in order to mitigate the risks of trust and assurance. However, there are sometimes incentives for such parties to act in untrustworthy ways, and the incentive to do so often increases with the size of the party.

The problem manifests itself in many ways for individuals: higher prices for medical insurance[4], refusal or unequal costs for privileges such as financial support and the loss of career opportunities. Individuals spending or donating their money or time sometimes doubt the credibility or ethical standard of a producer or organisation involved in the supply chain of a product.

The problem presents itself persistently in the Internet of Things (IoT). Separate categories of devices used to exist, but the modern home or business landscape is made up of different kinds of computers labeled slightly differently, many of them not looking like computers in the traditional sense. Far from just entertainment or professional peripherals, computers run public transport including aeroplanes, lifesaving technology such as internal medical devices and almost everything else in between. Specific purpose computers are built for all imaginable uses from keeping our food cold to warming our homes. Whether these individual but slightly different computers remain, or they are replaced by a more general purpose computer, it is clear that our future socio-economic problems will involve computers and that more generally; computers will be running inside most things. A central problem therefore is the safety, monitoring and control of such devices, systems and networks. The IAP, with its IAP client and agent makes solving these issues feasible.

Our inability to trust the information we are given about the world presents unique but common problems in the assessment of risk and the estimation of costs to our time, energy and money. This gives us, and the systems we use and rely upon, an inaccurate picture of reality that is based on guesswork. The data that we can collect is typically stale by the time we seek to use it, resulting in our predictions being based on inductively forceful logic instead of real-time facts. We currently expect and assume this level of imprecision and accept the risks involved in making guesses about the actual state of reality. In many cases, the validity period of data points are shorter than their period of acquisition, making many facts true only ‘in the past tense’. We accept this as a normal state of affairs, but a true picture of reality would allow us to answer a variety of significant questions that can enhance decision making and reduce risk.

The problem of trust and assurance similarly affects private and public enterprise, leading to increases in the operational costs of doing business. Important decisions about humanitarian aid, military support, and the application of political policies are similarly impacted by the problem of information assurance. Charities, relief and aid organisations want to act in a transparent manner, but doing so can often be an expensive proposition, as can adequately enforcing ethical standards on those in their supply chains. The lack of recognisable and appropriate controls surrounding data and the lack of assurance available for information has serious implications in many areas of society. Businesses, organisations, governments and individuals need reliable information in order to reduce risk, whilst also endeavoring to maintain the privacy of many other kinds of information. This dilemma is well established and the traditional solution has been a compromise, with an inevitable sacrifice of either privacy or trust. Instead of being able to solve the problem directly, we have relied on mitigations such as the transference, avoidance, exploitation or acceptance of risk.

In addition, the centralisation of data creates problems globally. In the developing world and areas experiencing instability or unrest, traditional approaches to the assurance of information cannot be relied upon to provide the assurance required. When power changes hands at the top of society, the assurance of information is often conspicuously lacking. Similarly for those who hold the keys to important data and systems, having only part of the picture and being unable to fully rely on that part represents significant risk and cost. Governments find it difficult to track funding and reduce corruption.

In more stable parts of the globe, recent misadventures in economic policy, corporate responsibility and market disasters have highlighted the risks inherent in systems that rely solely on centralised authority and the true costs of constant compromises between privacy and transparency.

1.2 Decentralisation VS. Centralisation

This reliance on centralisation affects day to day life. Our performance, reputation, activities, achievements, qualifications, education, certifications, skills and things we cannot directly prove or attest to in any trustless way are expected to be arguable points; issues of perspective, interpretation and personal bias. Society places trust in centralised authorities outside of our control. Trust in these authorities is established over centuries, or enforced via laws, coercion or instilled by marketing, public relations and other techniques, all of which says nothing deductively for their future credibility or trustworthiness. In some cases, centralisation provides an appropriate model and is a strong alternative even when considering some forms of decentralised ledger technologies. In such cases, our concern for the privacy of activities, or certain data points related to them, and our inability to trust external parties (or ourselves) to manage this risk, leads to a choice being made between the siloing of information and associated risks, or the loss of privacy and associated risks.

Centralised silos of data represent both immense value and significant risk to their owners. Individuals are given little choice as to how their data is handled. In the majority of cases the data provided is not controlled by the source of that data. Long, complicated legal statements are required for the most basic of activities and services, the detailed implications of which are generally not widely understood. As such, society operates under an anticipation and assumption of loss; the loss of control, the loss of data and the loss of certain rights. The owners of these silos (government, corporations and institutions) operate within similarly risk-bound constraints. Failure to properly manage the confidentiality, integrity and availability of their data, or the data of their users, has become a common news story of the internet age[5,6]. Neither side accepts the risks; significant resources, in the form of public funds, business costs, and taxes on the electorate are spent in treating these risks.

Systems that are expected to assure safety, monitor and perhaps respond, and provide actionable data for the teams and systems that respond to incidents that impact business, or health or a community's interests in some particular way, are currently trusted because of faith placed in a trusted third party. Third parties provide an important societal function. Decentralisation replaces trust in single third parties with trust in axiomatic truths, such as mathematics or trust in distributed third parties with a probabilistically low chance of manipulation.

2.0 The IAP

2.1 Vision

IAP Vision: *"The Information Assurance Platform aspires to conquer the issue of trust and assurance, enabling risk free information assurance for devices, individuals, organisations, companies and governments globally."*

2.2 Components

The IAP is a next generation blockchain comprised of the following high level components. For a detailed explanation, please refer to our technical whitepaper:

Core: The Core will launch using Ethereum[7], but will ultimately include multiple public chains including its own main chain to process security data, leveraging the distributed redundancy that enables. Ethereum and other public blockchains provide the ability for deployment of smart contracts that support protocols used by the IAP. IAP stores a very small amount of data on the initial system Core. Core provides an ultimate source of integrity as to the security of components in the IAP, in a transparent and auditable way. Ethereum is the same blockchain being considered for use by R3 and IBM and already in use by Microsoft[8]. Core contains an oracle layer and other gateway modules to interface existing technologies with the other components of the platform, bridging the blockchain ecosystem and the world, providing easy access to the power of blockchains for information assurance.

Client: The IAP client is designed to be a multi-party multi-tenant open source Information Assurance Application node (IAA node). The nodes form the basis of the decentralised network. Nodes facilitate the polycentric governance system and other applications of the IAP tokens. The client can be customised to be light weight in a granular way, from monitoring and attesting to its host device internal state to providing a full API, or only performing the duties of a network node. Applications can thereby use the IAP client as a universal "device daemon"[9]. The client allows the IAP to track the state of arbitrary configurations and computational outputs from any device that is able to gain even intermittent network connectivity. In doing so, the IAP enables the option to maintain the control of the privacy and confidentiality of the host device and data.

Chains: Multiple multi-party computational chains that branch from Core. Using IAP on-chain agents, Chains does the heavy lifting of the various applications of the IAP. Chains enables artificial intelligence and machine learning services for compatibility and visibility into core service and components. In the case of one of the initial applications, Blockliance, Chains will provide distributed computing channels for the proof of process and verification requirements of the application. Chains bind and deliver CyberTraces (see 2.6).

IAP Standard: The IAP includes the IAP open standard that will facilitate the creation and interaction of applications that utilise the platform and its components and component features such as Universal Daemonisation and CyberTraces to solve a variety of problems related to the assurance of information. The IAP team will continue to develop and support this standard with contributions from participants in the network.

2.3 Participants

The Information Assurance Platform involves multiple parties ('participants') exchanging messages between endpoints, using a mixture of cryptographic tools and computational verification to achieve information assurance goals. Central to the application security, scalability, performance and use are IAP tokens. As computational consensus drivers for the network, the IAP tokens provide glue for the different subsystems of the platform; in particular its combination of protocols.

- **Network Verifiers** receive fees for running the Information Assurance Application nodes (IAA nodes). Each application of the IAP can use these nodes in different ways. Verifiers can use their single IAA node to support multiple applications of the IAP. Anyone can be a verifier and run an IAA node. Minimal computational resources will be contributed.

- **Devices** perform functions and attest and commit to their host device's state in a way that is publicly verifiable and does not compromise the privacy or confidentiality of the host device.

- **Validators** can use tokens to receive verification of information assurance attestations from proving entities.

- **Provers** can use tokens in order to assure validators of their attestations to the same data points, computational output or information assurance attestations.

- **Data providers**: Parties and devices engaged in applications utilising the IAP that provision data for the consumption of the AI.

- **IAP token holders**: Tokens are used in the security mechanisms for reaching decentralised consensus and accurate verification mechanisms. For applications built on the IAP, the tokens are a valuable and key component of the system. Token holders can contribute to the security, scalability and decentralisation of the platform and can benefit from the utility of their tokens. Since they are integral to the network they also enable use of the network.

- **Code contributors** receive tokens as an incentive for contributing code commits to compatible projects which use the Information Assurance protocol. Code can be accepted into projects via the IAP governance mechanism. Example: Secure code scanning for smart contracts

- **Ethical hackers**: Can get paid in tokens for responsibly reporting and disclosing vulnerabilities in applications in a trustless, verifiable and decentralised way.

2.4 Polycentric Governance, Ethics, and Distributed Autonomous Organisations

The IAP's stated vision is to conquer the issue of trust and provide risk free information assurance globally. A key part of this vision is the system of polycentric governance and ethics that is central to the IAP. The governance of digital trust is an increasingly significant question as society and industry converge on the problem of trust and assurance. The IAP is central to solving this problem by providing a reliable, decentralised, immutable, secure platform via which digital trust and risk can be effectively and ethically managed for devices among the Internet of Things (IoT), individual personal interactions, organisations, companies and governments.

The IAP enables application developers to ensure that their application is used within a defined set of constraints and that data is handled in a manner that they intend from the outset, in a transparent and auditable way.

Distributed Autonomous Organisations (DAOs) can benefit from the IAP in several ways. DAOs can utilise the IAP to lend legitimacy and visibility to their structure and operations by enabling a route to meeting the spirit and letter of existing regulations and requirements. In doing so they can mitigate the risks associated with the technology being ahead of the regulators. We explore some of these in this whitepaper, via example in the case of Blockliance, wherein DAOs can explore risk ratings and security posture profiles that draw comparisons to industry standards and best practices.

According to reports, ‘artificial intelligence and machine learning capabilities are growing at an unprecedented rate’[10] but the dual-use (i.e. the ability of both attackers and defenders to use) possibilities of AI are currently not receiving enough consideration. The IAP’s system of polycentric governance and ethics is a viable foundation for the considered, controlled and monitored application of AI to ecosystems such as the Internet of Things (IoT) and critical infrastructure. The IAP governance and ethics team aims to encourage (i) an expansion in the stakeholders engaged in the security considerations of AI, (ii) research by technical and policy specialists such as our team and government advisors into artificial intelligence governance and control, (iii) an awareness among engineers and developers as to the risks of AI, and (iv) develop and define best practices based on information security and cybersecurity models.

2.5 Universal Daemons & CyberStates

The IAP’s Universal Daemon[11] (UD) is a version of the IAP Client that can be deployed to compatible devices that are able to gain intermittent network connections. The UD’s primary function is to report on its host device’s internal state; a tool called CyberState. State is represented by a stream, a file or collection of files. In it’s simplest form, a UD reports the CyberTrace of a flat file, providing a distributed file integrity monitoring capability that is also authenticated, decentralised, reliable, and accessible globally. In more advanced scenarios, device state may include real-time streams of audio visual data or packet capture of network traffic, enabling intrusion detection and protection systems and artificial intelligence for networks.

2.6 CyberTraces (Assurance Proofs) & CyberShields (Computational Verifications)

The IAP enables users to create assurance proofs known as CyberTraces. CyberTraces are independently verifiable, cryptographically assured evidence events. CyberTraces can be associated together in evidence chains, privately or publically, and are publically verifiable in auditable ways without sacrificing the privacy or confidentiality of data.

CyberTraces rely on a variety of mechanisms including cryptographic scalable computational integrity and privacy proofs, encryption, hashing and certificates. Users can deploy private CyberChains via the Client that enable organisations to provide future proofs for data verification, information assurance and transparency purposes. In this way, CyberTraces provide business with the ability to manage their future risks in a way that has hitherto not been feasible.

The computational integrity of the functionality of the tools within the IAP is assured by a computational tool called a CyberShield. CyberShields use a variety of zero knowledge proofs to provide the ability for independent verification of tool output while maintaining privacy and confidentiality of the work. CyberShields are also available for off-chain computations and as such are a useful tool in their own right. For more information on CyberShields, please see the IAP Technical Whitepaper.

2.7 CyberChains (Evidence Chains)

The IAA node (see IAP components) facilitates the creation of evidence chains known as CyberChains. CyberChains tie together CyberTraces in a way that maintains Chain of Custody (CoC) for verifying parties such as auditors, assessors, central authorities, supply chains or other interested parties. CyberChains constantly report their internal state to IAP Core, enabling global verification of their validity and integrity without sacrificing the privacy or confidentiality of their data.

2.8 Global Reality State Transition System

The IAP's UD combined with the network of IAA nodes enables the collection of a stream of digital and analog information about the world, via the Internet of Things (IoT).

The IAP enables a global reality state transition system (RSTS) that is able to reflect the internal state of any device connected to it. Facilitating this is the IAP client, a customisable multifunctional client that enables device based daemonisation for any device that is capable of acquiring some type of network connection, and smart contracts. This system enables the collection of data that provides accurate and current information on the state of reality for applications and other devices to use in many different ways. Participating devices have the option to become data providers and opt in to securely reporting the data collected by their internal processes (available memory, bandwidth, connection speed, etc) and external sensors (light, temperature, velocity, height, depth, energy, etc.).

The result is a more accurate picture of the state of reality that combined with machine learning will enable the next generation of smart devices and inter-machine operations that significantly reduce risk, enhance decision making and improve our experience of everyday life.

3.0 Blockliance

3.1 Blockliance Mission

Blockliance Mission: ***"Through automation and assurance, we improve GRC outcomes, by enabling implicit trust and safety between parties, in order to save time and money while enhancing corporate partnerships and safety for consumers and end users."***

3.2 The Problem & Background

Current efforts to reach regulatory compliance are costly, unreliable and difficult to scale for most organisations. Engaging in these mandated projects frequently requires expertise in the particular framework in question, often with very different methodologies and levels of proscription and assessment. This has led to the compliance consulting industry being worth an estimated $65 billion annually[12] by 2025. The highest cost for these consultancies is that of quality assurance; the necessity to perform on site visits, detailed technical and legal checks of controls and paperwork, and the assurance and quality control of the findings. The risks are clear; failing to properly QA this work can lead to suspension or loss of licenses required to perform the audits that drive the business. As such, companies providing compliance as a service (CaaS) or simply providing the opportunity to be assessed, typically have very low profit margins and unnecessarily high costs thanks to having to protect themselves from human errors that can lead to punitive actions on behalf of the governing bodies they represent to assess.

Regulators in the United States and Europe have imposed over $342 billion of regulatory fines in the last decade on banks alone[13]. This figure does not include organisations, charities or corporations other than banks or governments. Regulation from governments and other centralised authorities is an expensive and mandated part of doing business in many globally competitive industries. The London-based HSBC Bank spent $2.2 billion on regulation and compliance in the first nine months of 2015, up 33% year on year[14]. It is rare for even small organisations to be able to completely avoid some form of compliance, regulatory and legal requirements set upon it by outside authorities. In Canada alone, the cost to small and medium sized enterprises was almost $5 billion in 2011[15]. In many cases, the requirements cause the organisation to create entirely new departments in order to cover the additional work. In addition to this high financial cost, risk, compliance and security departments in organisations across the world find a significant amount of their time taken complying with these regulations; often from multiple authorities with multiple compliance frameworks simultaneously. The result is that security departments frequently report reduction in security as an unintended consequence of attempting to reach compliance status while maintaining their additional responsibilities[16].

The regulations, frameworks and legal requirements that are imposed by authorities on entities engaged in business, charitable work, religious endeavours, humanitarian aid and similar organised work are typically intended to provide feasible and efficiently verifiable methods by which to enforce certain controls and standards on unknown and arbitrary types of organisations. In practice, the breadth and depth of scenarios in which these standards are applied vary wildly. The result is a high risk of deviance from the intended outcome, a low level of trust or verification, and a centralisation of power in the hands of validating entities who have mixed levels of professionalism and quality control[17].

The constant updating of compliance requirements to meet the ever shifting threat landscapes and business and legal goals prompts the continuous review and redesign of models used to facilitate the understanding, application, scoping, verification and assurance of the companies under regulation. The cost of this process continues to grow, in real financial terms and in terms of opportunity costs to regulators, governments and corporations. 69% of companies expected regulators to update their frameworks within 2017, and over one third of all companies expect their budgets for compliance to increase within 2018[18]. Setting up regulatory functions is difficult as specialists can be hard to find and reliable consultant firms are often costly.

The creation of a decentralised, immutable, trustless, adaptive, upgradeable global computational attestation and verification machine will solve the principle pain points of the GRC problem, and do so in a time and resource efficient manner. The IAP lends itself ideally to this kind of problem, and these types of applications.

The sum global GRC footprint represents a disparate collection of arbitrary requirements and testing procedures, written in multiple languages, combined with mandates from vastly differing legal systems and industries. These are observed to have varying levels of quality, assurance and control. The system is broken and bloated, and many participants ask how it can be taken into the future in a way that affords a higher level of quality control and trust, proper governance on behalf of the authorities involved and assurance between proving and verifying parties that is low cost and reliable.

3.3 The System

The Blockliance system uses a governance, risk and compliance (GRC) application of the Information Assurance Platform (IAP), with its unique assurance license token model. In doing so, it solves governance, risk and compliance security and business problems by providing a standardised, decentralised, immutable, trustless and cost-effective system for individuals and organisations to provide information assurance verifying parties of arbitrary types the ability to validate the attestations of assessed entities in a flexible, adaptive and efficient way, while reducing complexity and risk.

3.4 The System Parts

- An automated and upgradeable GRC aware dataset validation module with artificial intelligence.
- An automated and standardised assurance system that enables both sides of any assurance relationship to engage in trustless and integrated assessment and validation of information over agreed time periods. This utilises the downloadable, dedicated, private IAA nodes with IAP Core.
- A security metrics and risk rating system that enables valuable insights and actionable data for enhanced decision making, third party assurance, justification of budgets and expenditure, cybersecurity return on investment (ROI) and the ability to contribute to and benefit from further big data analytics and features.
- The Blockliance console dashboard that enables the visualisation and operation of the features of the system.

The Blockliance system relies on a distributed multi-chain ledger involving multiple, separate participant to mitigate security issues, to enhance the performance of the network by lending computing resources and for token holders to enhance the network by participating in the selected consensus model protocols. Each participant, whether entities engaged in information assurance activities on the proving, verification or other perspectives, uses tokens to benefit from the network services. With the use of partner settlement layers, this can be done in an invisible, hassle-free and convenient way with traditional or modern methods of payment.

3.5 Blockliance Participants

- **Blockliance Verifying Parties**: Assessors of some standard or framework of requirements or recommendations. Qualified and licensed assessors from any kind of compliance framework can use Blockliance to reduce their overheads, streamline their compliance engagement activities and outsource parts of their verification and quality assurance procedures to the blockchain. Examples include: Qualified Security Assessors, consultants and consultant organisations assisting companies with their compliance goals, internal auditors who need to maintain organisational independence, external auditors engaged in costly “trust but verify” engagements, and many other types of assessor including the public or the attesting party themselves.

- **Blockliance Regulated entities**: Individuals, organisations, corporations, companies and any other group that is required by law or other regulations, recommendations or internal policies to perform and attest to certain facts and processes about themselves or certain divisions or departments internally, in order to reach compliance goals, attain certain licenses, or successfully complete applications for competency or certain types of activities.

3.6 Distributed Autonomous Organisations (DAOs)

Blockliance facilitates not only the compliance of traditional organisations but also DAOs, regardless of where they are running. The governance and compliance of these types of organisations can be solved efficiently and transparently thanks to the components of the IAP via the application of Blockliance.

The future includes DAOs in many industries and the true potential of these types of organisation is yet to be fully realised. Blockliance, with the help of the IAP, will support the DAO ecosystem with the data and convenience required to enable DAOs to define for themselves how best to approach the matter of regulation in a way that is efficient, open source, decentralised and secure. This will empower existing DAOs with the confidence of acting in good faith and where possible, meeting regulatory requirements or best practices in a demonstrable way, and where appropriate to create their own best practices and define their own recommendations.

For those seeking to create a DAO, the transition can involve significant risk in a legal and regulatory environment that has not yet caught up to the technology. Blockliance is the first application that will provide this layer of assurance between parties in a way that is understandable to those seeking to regulate and those seeking to reduce their risks.

3.7 Risk Ratings, Security Postures & Insurance Premiums

Blockliance will manage sufficient data for cybersecurity industries to be embraced by the insurance industry. In order to position the industry in an insurable way, and help the industry define the manner in which this will happen, Blockliance will provide the platform that enables all actors to engage with their security and risk postures in a secure, reliable, efficient and affordable way.

The future of cybersecurity is inevitably a heavily insured one. It is a normal and expected precaution that all nurses, doctors and medical staff are fully qualified and that their qualifications have not expired or been in doubt at all times when they are practicing or employed. With advances in medical equipment, the speed with which medical devices are connected to networks, and the alarming rate of medical device hacking[19] already happening, cybersecurity is set to be of central importance to the medical industry and public health policy now and in the future. Those who maintain these devices, secure the networks they connect to, assure the security of information and data that runs through and across them, and configure and test the controls that protect them (heart monitors, insulin pumps, etc[20]) will also soon be required to maintain qualifications and licenses that are key components in the insurance of the industry. This will likely extend beyond medical care and into other areas of cybersecurity, such as critical infrastructure and telecommunications.

There are typically four main items that need to be addressed before an industry is ready for the level of insurance that the medical industry already experiences, namely: (i) significant risk, (ii) adequate funds for insurance premiums, (iii) enumerable insurance events and (iv) sufficient actuarial data. The cybersecurity landscape already provides three out of these four basic requirements, and Blockliance will enhance the third while providing the fourth; sufficient actuarial data. Blockliance does this in a way that improves the risk profile of companies, helping to drive lower insurance premium costs, and assure third parties as to the safety of their supply chains, vendors and partners, at a time when supply chain risk management is becoming increasingly important; the federal National Institute of Standards and Technology (NIST) has updated its Cybersecurity Framework to specifically include additional considerations for controlling supply chain risk management (SCRM)[21]. The risk ratings made possible by Blockliance and the IAP will drive this future of regulatory technology[22] by helping providers and regulators work together to make more focused, quantifiable risk based decisions. The savings will be passed onto the industry with those involved in Blockliance benefitting early.

4.0 Roadmap

IAP Vision: ***“The Information Assurance Platform aspires to conquer the issue of trust and assurance, enabling risk free information assurance for devices, individuals, organisations, companies and governments globally.”***

Blockliance Mission: “Through automation and assurance, we improve GRC outcomes by enabling implicit trust and safety between parties in order to save time and money while enhancing corporate partnerships and safety for consumers and end users.”

2017	**Relevant Milestones**
2017 Q1-Q3	• Proof of process mechanism research • Universal Daemonisation (UD) research • Dataset template designs for BIT, HIPPA, HITRUST • Reducible dataset validation research to ISO27k1 • Research into verification mechanisms • SCIP research and testing
2017 Q4	• Research of Chains anti-fraud system • Design of verification system
2018	
2018 Q1	• Blockliance.io registered • Partnership with Kaizen SG Cybersecurity • Design PoC of ISO 27k1 dataset • Whitepaper distributed • Partnership with Movaci Cybersecurity • Appoint key additional staff • HCE/ASM research • Virtualisation tests for IAA node
2018 Q2	• Acquired seed investment
2018 Q4	• Complete MVP for Information Assurance Toolbelt AP/EC • GRC oracles for PCI • Partnership with additional CaaS company • Documentation for Zero Knowledge Proofs • Design of off-chain AI systems
2019 Q1	• Partnership with top tier consultancy • Complete MVP for Information Assurance Toolbelt UD • Design of on-chain AI systems • Academic review of the system governance proposals • Independent, external secure code scanning of all repos (continual) • Token Economics & Utility Model Design
2019 Q2	• AI module interface for Blockliance • Complete MVP Blockliance PCI Interface

	• Auditor / assessor review of system • Security Metrics Prototype
2019 Q3	• IAP Governance & Ethics Milestone • MVP for Information Assurance Toolbelt
2019 Q4	• MVP for Blockliance • Start of crowdfunding round

5.0 Distributed Ledger Technology (DLT) vs. Blockchain

For the purposes of this whitepaper, blockchain technology has a class relationship to distributed ledger technology (DLT). Blockchain is an instance of the class of DLT. Where blockchain usually differs is that the data is repeated across nodes rather than distributed in a sometimes dissimilar way. There are other differences, and much is down to implementation.

6.0 Other Applications

There are a growing number of potential use cases for IAP. Research into feasibility has been conducted for the following:

Cybersecurity

- Continuous Identity and Authentication
- Supply Chain Security
- Internet of Things (IOT) device monitoring and control
- Digital identity, authentication and signing of video/audio (AAA to combat deepfake etc)
- Secure code scanning
- Vulnerability management
- Intrusion detection and analysis machine learning and AI
- Malware analysis with machine learning
- Disaster Recovery and Data Redundancy
- Digital forensics
- GRC (Risk Management)
- Change management & auditing, FIM

Development Operations & Security

- Dependency management
- Smart contract security
- Secure continuous delivery assurance
- Asset discovery and scanning

Society, Charity, Humanitarian

- Transparency in donations and funding

- Peer to Peer Safety
- Soft skills marketplace
- Assurance of expenditures
- Asset tracking
- Ethical assurance

Identity management & Privacy

- Personal career management
- Account takeovers mitigation
- Personal document assurance
- Qualifications and education assurance
- Licensing assurance
- Reputation assurance via Universal Daemons (UD)

Medical & Health

- Medical record integrity and trust
- Lower insurance premiums
- Realistic, quantifiable, political health policies
- Assurance of compliance and best practices

Business

- Lower costs for reaching compliance
- Business functions as algorithms
- KYC, AML, anti-fraud
- Streamlined licensing
- Risk profiles and insurance premiums
- Reputation assurance

Government

- Polling of electorate (referendums, elections)
- Direct politics
- Transparency of spending and allocation
- Proof of process
- Trustless enforcement of contracts
- Tax
- Duty tax rebate

Law enforcement

- Transparency of process
- Equality of application of law
- Verification of data with privacy
- Chain of Custody
- Integrity of evidence
- Forensic Science

The Team

Founders

- William Vacher, Cybersecurity
- Tony Woodhouse, Engineering

Founding Team Members

- Steve Franks, Frm Group CTO, Telenor
- Philipp Wiendl, DevSecOps, Infrastructure
- John Cattral, Blockchain Architect
- Christopher Mosby, Cybersecurity, GRC
- Robin Ankele, Cryptography
- Angela Robinson, PhD, Cryptography
- Dr. Angel-Carlos Roman, PhD, Artificial Intelligence
- Wisaroot Panti, Cybersecurity Engineer
- Amit Kannaujiya, Information Security, GRC
- Marc Merius, Blockchain Developer
- Nemanja Djordjevic, Design, UX
- Tanazith Kowsurat Esq, Legal Counsel

Industry Advisors

- Paul Ashburn, Co-Managing Partner, BDO
- Jeff Hall, PCI Guru
- Daniel Miessler, Cybersecurity Director & Author
- David Langer, Business Development
- Chris Doerfler, Blockchain & Governance
- Benjamin Martin, Public Sector Advisor
- Dr. Stephen Boulter, Phd, Professor of Ethics, Oxford Brookes
- Thomas Fisher, Education Frm Scotland Yard SCD 9
- Simon Gibbons, COO ICR 360, Digital Forensics
- Tahmeed Rab, Kaizen Cybersecurity
- William Bautista, Frm. Cisco Senior Security Engineer
- Patrick Dougherty, Mathematics
- Terry Blackburn, CEO, Ensign Media Ltd.
- Paul Warren, Data Science

Partners

- BDO
- Movaci Cybersecurity
- GoPomelo
- Kaizen Solutions Group
- Aperio Forensics
- Ensign Media

References

[1] IAP Team Members. IAP. “The IAP Official Guide.” https://iap.network

[2] Blockliance, built using the IAP. https://blockliance.io

[3] Trust is distributed across the network globally, rather than in one third party or central authority. e.g. Ethereum. “Ethereum Whitepaper”. https://github.com/ethereum/wiki/wiki/White-Paper

[4] Tom Baker. “Health Insurance, Risk, and Responsibility after the Patient Protection and Affordable Care Act”. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1759366

[5] New York Times. “Cyberattack May Have Affected 143 Million in the U.S.” https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

[6] Wired. “Biggest hacks of 2017”. https://www.wired.com/story/2017-biggest-hacks-so-far/

[7] Ethereum. Ethereum. https://ethereum.org

[8] Mark Russinovich CTO, Microsoft Azure. “Announcing the Coco Framework for enterprise blockchain networks.” https://azure.microsoft.com/en-us/blog/announcing-microsoft-s-coco-framework-forenterprise-blockchain-networks/

[9] Daniel Miessler. “The Real Internet of Things.” https://www.amazon.com/Real-Internet-ThingsDaniel-Miessler-ebook/

[10] Maliciousaireport.com. “The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation”. https://maliciousaireport.com/

[11] CIO Whitepapers Review. “What is a Daemon.” https://whatis.ciowhitepapersreview.com/definition/daemon/

[12] Grand View Research. “Enterprise Governance, Risk & Compliance Market Worth $64.6 Billion By 2025”. https://www.grandviewresearch.com/press-release/global-enterprise-governance-riskcompliance-egrc-market

[13] Thomson Reuters. “U.S., EU fines on banks' misconduct to top $ 400 billion by 2020: report.” https://www.reuters.com/article/us-banks-regulator-fines/u-s-eu-fines-on-banks-misconduct-to-top400-billion-by-2020-report-idUSKCN1C210B

[14] Gomedici.com. “Strategic Analysis of RegTech: A Hundred Billion-dollar Opportunity.” https://gomedici.com/how-can-regtechs-help-financial-services-industry-overcome-the-burden-ofcompliance/

[15] Daniel Seens. “SME Regulatory Compliance Cost Report.” http://www.reducingpaperburden.gc.ca/eic/site/pbri-iafp.nsf/vwapj/09-2013_eng.pdf/$file/09-2013_eng.pdf

[16] Neil Roiter. “Smaller public companies bear significantly higher pain in terms of revenue and costs per employee complying with Sarbanes-Oxley.” http://searchsecurity.techtarget.com/magazineContent/SOX-compliance-burdens-midmarket-securityteams

[17] Jonathan Stempel. “Target, security auditor Trustwave are sued over data breach.” https://www.reuters.com/article/us-target-trustwave-lawsuit/target-security-auditor-trustwave-aresued-over-data-breach-idUSBREA2P0B020140326

[18] Thomson Reuters. “Fintech, Regtech, and the role of compliance 2018”. https://risk.thomsonreuters.com/en/resources/infographic/fintech-regtech-and-the-role-ofcompliance-infographic.html

[19] Jessica Twentyman. “Hacking medical devices is the next big security concern”. https://www.ft.com/content/75912040-98ad-11e7-8c5c-c8d8fa6961bb

[20] Peter Sayer. “Implantable medical devices can be hacked to harm patients”. https://www.csoonline.com/article/3146604/security/implantable-medical-devices-can-be-hacked-toharm-patients.html

[21] NIST. Cybersecurity Framework updated to version 1.1. https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_withmarkup.pdf

[22] Kabir Kumar. “The real promise of regulatory technology”. https://techcrunch.com/2017/05/09/the-real-promise-of-regulatory-technology/

[23] IAP Network. "Information Assurance Platform: A Technical Overview". https://github.com/iapnetwork/docs/blob/develop/whitepapers/technical-whitepaper.md/