THE PROMETHEUS PROTOCOL

White Paper v1.0

Rachid Ajaja
Dr. Amber Ghaddar
Matthijs De Vries

Table of Contents

Founders' Vision

"Prometheus protocol aims to be an open protocol that can be used by all the various actors and create a global decentralized capital market with a global governance fully compliant with local and cross-border regulations."

Executive Summary

The Prometheus Protocol is a comprehensive and layered architecture to facilitate cross-border transactions in capital markets in a completely regulated and compliant manner. It provides the framework to digitize all forms of assets in seamless compliance with the regulations in effect. The Prometheus Protocol is comprised of the following three layers:

- **Data Governance Layer** - To ensure that in-architecture data management complies with data privacy laws and the quality of data does not deteriorate over time or over distance.

- **Cross Border Regulatory Compliance Layer (CBRCL)** - To ensure automated validation of transactions and their compliance with applicable regulations. Trusted Legal Entities add/amend transaction governing logic after consensus to ensure consonance with regulation

- **Securities' Issuance and Lifecycle Management Layer** - To enable an end to end regulated issuance and management of the lifecycle of the issued digitized security

The Prometheus Protocol build on top of Distributed Ledger Technologies (DLTs) to achieve:

- **Transparency** in Data Governance
- **Security** in Transactions
- **Compliance** to Regulations

at the institutional level and top-down adherence to compliance and regulatory requirements across jurisdictions via its CBRCL.

The Prometheus Protocol leverages the best of 'code is law' and 'Law is by the People' philosophies. It provides templatized smart contract driven logic to automate transaction validation and to ensure their adherence to regulation. It also provides for upgradeability of this logic to stay aligned to their real-world regulatory counterparts that are amended by legislatures from time to time.

The Prometheus Protocol heralds the age of **true 'Open Finance'** with robust **Data Governance** where, users won't be required to undergo KYC checks at every financial institution but have complete sovereignty over their data by enabling their storage in an encrypted manner. This prevents unauthorized usage and access while enabling the users to request its deletion at any time.

Banking consortia can create private channels to enable faster communication and management of operations across borders. They can also create **unified procedural internal regulations** compliant to the regulatory directives and regulations of the various jurisdictions of operations.

Entities looking to **unlock unbankable assets** or to simply **digitize assets** can:

1. Create new issue
2. Create custom rules for subscription
3. Zero Knowledge Proof verification of prospective investors' eligibility
4. File prospectuses, term-sheets, and cap tables etc in a paperless fashion
5. Maintain asset ownership records in a secure and tamper-resistant manner
6. Enable cross-border trades of digitized securities while still being compliant

Overall, the Prometheus Protocol is envisaged to be a **multi-touchpoint, multi-party, and multi-stakeholder driven system of layers** that are governed by logical smart contracts, **compliant with the regulatory requirements** and possessing the **ability to upgrade themselves on regulatory amendments** as directed by the amended law texts and actioned by the compliance-monitoring entities on the Prometheus Protocol.

Business in the Age of Globalization: Parts, Problems, & Potential

Globalization led to the development of a common set of mutually agreeable rules between countries/jurisdictions looking to leverage faster integration of businesses across geographies and jurisdictions while ensuring traceability and auditability to prevent criminal activities such as terror financing and money laundering.

Regulatory Compliance for Integrity and Trust

Take the case of the metric units of measurement (such as kilogram, metre, and seconds etc) as a parallel. A majority of the countries agreed on a common definition of measurement units so that one metre in Australia would be the same as one metre in Canada.

Figure 1: Components of Compliance (Source: E&Y)

The world of Business and Finance took these concepts and came up with their own protocols that facilitated faster, simpler, and non-redundant transactions according to the laws governing business and finance in various countries. These formed the building blocks of a global regulatory compliance protocol. Thus, when a protocol adheres to the requirements of the laws of the land, it is said to be regulatory compliant (see Figure 1).

Regulatory Authorities routinely come up with frameworks to enable legitimate businesses to comply easily with their laws. Laws change with time and therefore regulatory compliance requirements must change as well. For example, the arrival of credit cards led to the formation of a new standard – PCI DSS (Payment Card

Industry Data Security Standard) created by the *Payment Card Industry Security Standards Council* to help prevent credit card fraud and bolster information security.

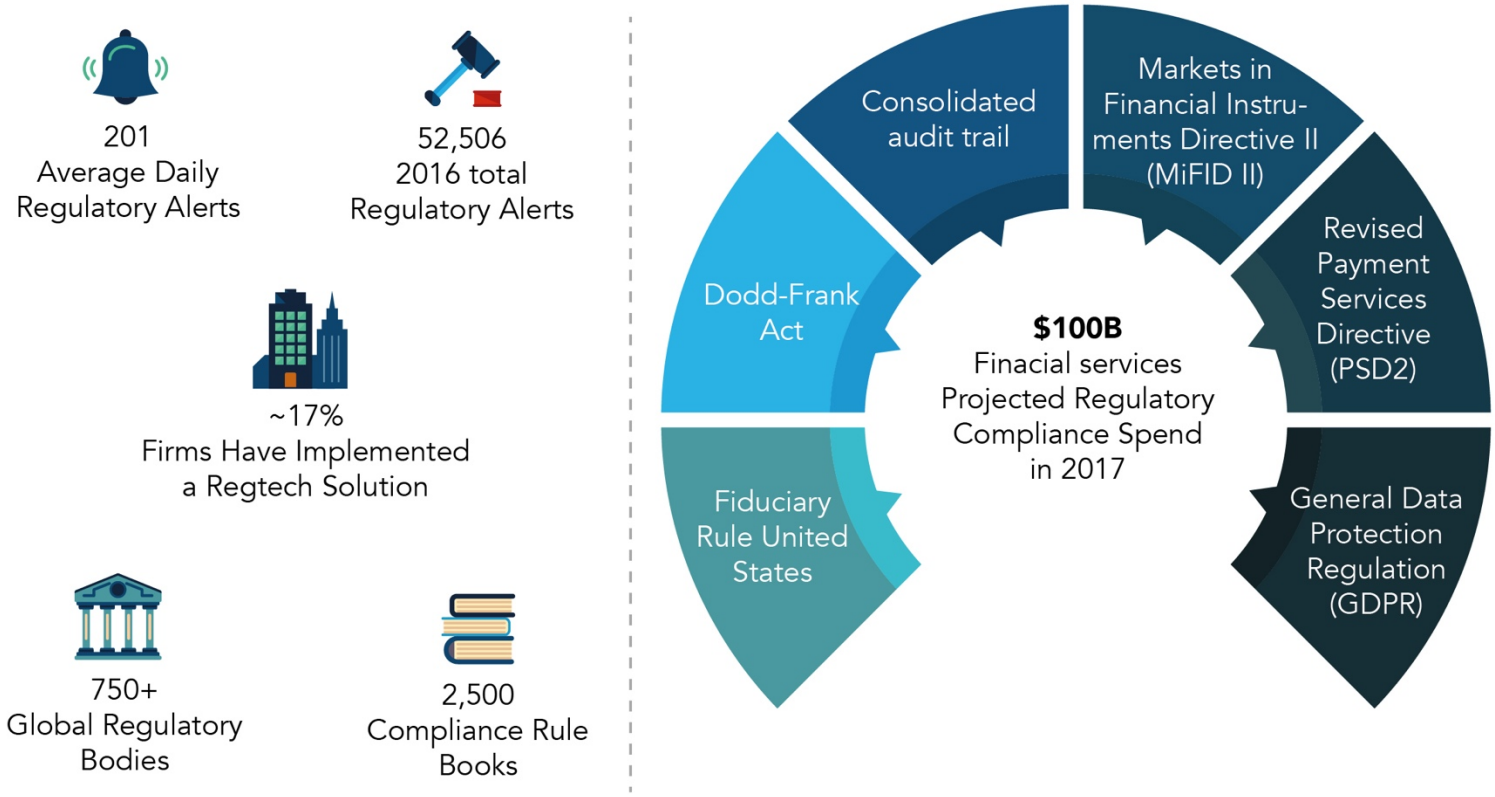

Figure 2: Concerns in Compliance (Source: CB Insights)

Similarly, the arrival of cryptocurrencies led jurisdictions across the world to rethink concentrating power in institutions. Post the initial fears, the banking institutions now view Blockchain technologies as a solution to their own woes regarding:

- Transparency;
- Regulatory compliance across diverse jurisdictions (See Figure 2) and;
- most importantly, better servicing their customers by enabling faster transactions, lower risks (counterparty, operation etc..) with overall much lower costs.

The technological front has been highly productive and has provided specialized Blockchains (*a subset of Distributed Ledger Technologies*) to address the problems faced by the modern banking and financial systems stressed under the rapidly increasing number of people availing banking services and the exponential growth in

securities. The rising tide of globalisation (peppered with state nationalisms) makes it harder to arrive at a consensus as to who gets to draw the line and where.

Ironically, breaking this impasse is exactly what the Blockchain promises to deliver – make collusion impossible and foster greater transparency across the board.

With transparency achieved, the next step in compliance with regulation is a suitable data governance structure. It shall ensure that the collection, processing, and storage of data is aligned to the best practices for privacy *and* to the relevant regulations in applicable jurisdictions.

Robust Data Governance for Privacy and Security

What is Data Governance?

Data Governance is the collecting, storage, processing, and the overall management of data of users, legal entities, transactions and everything in between. The key aim of data governance is to comply with consumer-protection regulations such as GDPR, MiFID II and others while also ensuring that high data quality and security persist throughout the entire data lifecycle.

Just as there are laws to govern what we, as a people, can and cannot do, data governance is used to create rules for how and by who can a particular piece of data be accessed, processed, and transmitted.

As data moves from physical books to digital books, data governance policies protect data from:

- Unauthorized Access
- Misuse and Identity Theft
- Manipulation and Subversion

In a real-world scenario, a financial institution onboards a new client after a strict and lengthy due diligence that can be done in-house but most of the time is outsourced to a third party (KYC provider). The KYC provider receives and processes a form for verification and sends back the result to the financial institution. Transaction history and record-keeping is managed by yet another provider.

Seamless communication between the above is maintained by a fourth technology provider that serves as the conduit. This technology provider may also outsource certain functions to lighten their workload. Hence, data is received, processed, and stored by multiple agencies in multiple jurisdictions.

Any leaks in this process can lead to severe data breaches and expose personal information of thousands, if not millions, of unsuspecting users. The recent Experian data breach[1] is just one such example.

Regulators and governments in various jurisdictions understood the need for and came up with robust data governance policies, regulations, and directives to protect their citizens from identity fraud. At the national levels, countries such as Singapore came up with PDPA laws[2] to prevent the data of their citizens from being carried out of their jurisdictions.

Where Does Current Data Governance Falter?

Today, businesses have administrative offices in one jurisdiction and branches in several others (example: Banks), data localisation laws came up short and transnational regulations such as GDPR gained traction.

However, such a system still fails (See Figure 3) to provide full autonomy to the users with respect to their data. The Open Banking initiatives seen in the European and certain Southeast Asian jurisdictions which enable users' financial and other data to be shared with third party developers or other financial institutions, in order to be used to the benefit of these users is a step in the right direction. However, they are limited in scope.

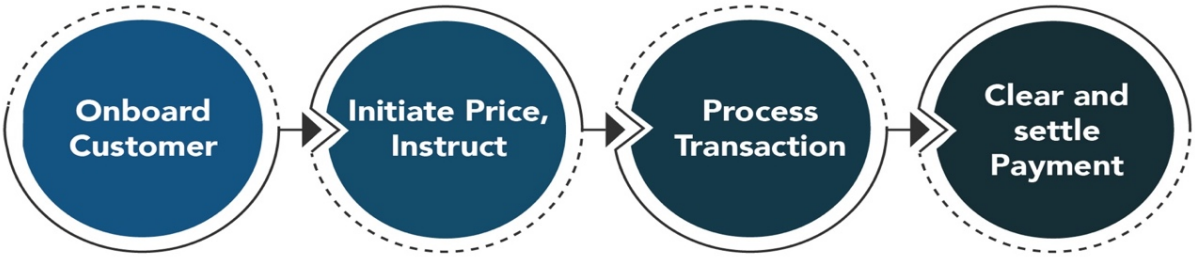

Figure 3: Traditional Investment Process (Source: MuleSoft)

While PSD2[3] mandates opening up data to third parties' APIs, the Open Banking initiatives enables a standardized mechanism for sharing it. A key concern is the fact that PSD2 does not specify any standards for APIs which will most likely result in banks creating their own versions of APIs. This will cause third parties to create different channels for accessing different APIs and that's a security flaw.[4]

Potential of Robust Data Governance

[1] https://www.bankinfosecurity.com/interviews/experian-breach-lessons-learned-i-2936

[2] https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview

[3] https://eur-lex.europa.eu/eli/dir/2015/2366/oj

[4] https://www.globalbankingandfinance.com/psd2-the-challenges-facing-the-banks-when-it-comes-to-third-party-application-data-access/

To provide greater autonomy to users with respect to their data and increase their trust in the system (See Figure 4), the institutions need to move from open banking to open finance (cross-border sharing of data in a regulated and compliant manner). Where even open banking is non-existent, open finance can seem unattainable.

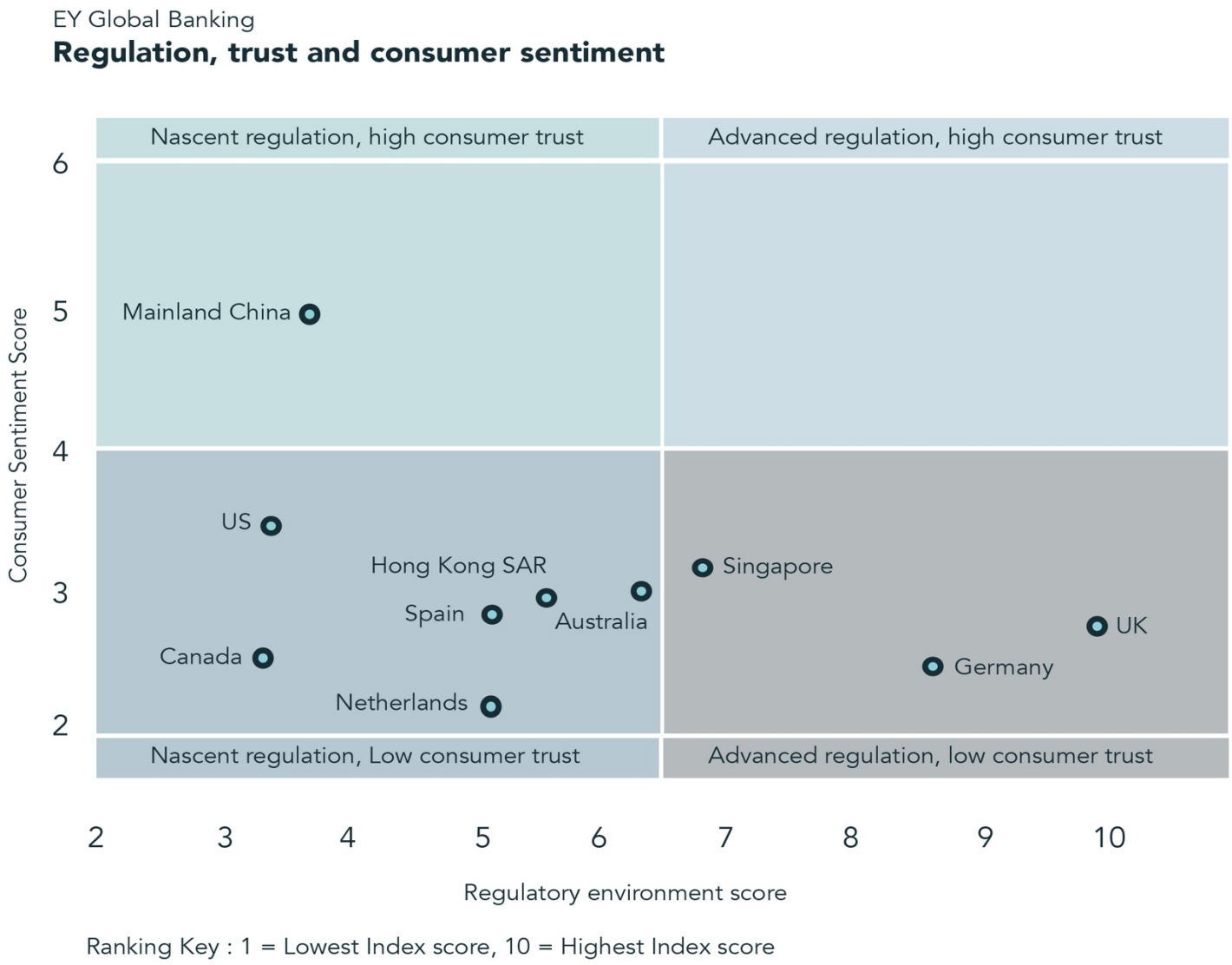

Figure 4: Regulation, Trust, and Sentiment (Source E&Y)

This is where distributed ledger technologies can step in and forge mechanisms that can provide seamless and regulated data governance at a fraction of the cost. Open finance with distributed ledger technologies can provide:

- Operational Transparency
- Blockchain Role Based Access Control to prevent misuse
- Tamper-Proof Automatic Bookkeeping via Blockchain Ledger
- Consensus Building Among Regulators

Thus, robust data governance requires not centralized and siloed pockets of data storage cells but:

- Decentralized data storage
- Role-Based access to qualified entities (like financial institutions)
- Tamper-resistance
- Retention of data quality

Financial Institutions that require absolute control over their data for their customers' privacy concerns can also leverage Blockchain/DLTs. They can create a permissioned access yet transparent flows within their private environments to enable better security with greater in-house accessibility.

Decentralizing Data Governance

Recent breaches, combined with a growing number of real and alleged misdeeds by several large technology and data companies—including tax evasion, manipulating users, monopolistic behaviour and market abuse, cooperation with legally questionable government surveillance, fostering abusive work cultures, and facilitating crimes such as election tampering and human trafficking—have raised high levels of concern.[5]

On decentralization, one banking executive described its promise thus: "Every bank, exchange and clearing house, we all have our own sets of the same data, which get out of sync and have to be updated and reconciled. The distributed ledger is the first technology that could implement a shared golden copy of that data." [6]

The key benefits of decentralized data governance lie in:

[5] EY-securing-the-financial-future-with-data-governance
[6] EY-securing-the-financial-future-with-data-governance

- Access Accurate Data from Multiple Locations - The ‘Global State’ of the Blockchain as the one true copy brings trust in the data without the need for a trusted intermediary.

- Transaction Automation - Instead of intermediaries, lines of code (smart contracts) become the executors of action items such as transfer of funds. There is no longer the need for human interference in the validation or processing of the personal information of either the sender, the recipient or the transaction.

- Security, Reliability, and Immutability - Fudging and data manipulation become practically impossible as the Blockchain resists any change to its ‘Global State’ unless agreed by consensus.

Decentralized data governance removes the threats of hacks on centralized sources by eliminating centralized sources altogether. It is also compatible with Data Privacy laws such as GDPR due to its ability to anonymize all personally identifiable information (PIIs) transmitted across devices, jurisdictions, or channels, while segregating data ownership.

Empowering Assets with Tokenization

Securities' ownership, since its origin, has been pieces of paper that were legally enforceable. The standardized security documents were easy to understand for the courts of law. With regulations in place, it was easy to resolve disputes. Technological advances, and mainly the exponential increase in securities volume, drove the *dematerialization* of these documents. These now "paperless" book-entry securities are not only exchanged, held but also issued electronically through an accounting entry in the issue account held by the *Central Security Depository.*

This enabled faster trading as the sale/purchase of securities did not require an actual transfer of the security documents but just needed a new entry into the book under the new legal holder account.

Tokenization of assets emerged as a viable alternative, at least among certain sections of technologists. They envisaged tokenized assets to be the unshackling of the siloed nature of asset ownership. On the compliance front though, tokenized securities falter, on paper and in practice.

There are these unanswered questions such as:

- If regulations change tomorrow, how to incorporate them into a tokenized security?
- How to comply with regulatory authorities in terms of KYC, DD and AML?
- How to enable dispute resolution mechanisms?
- How to enforce a transaction or reverse it

There are two ways by which existing players have attempted to answer them:

- **Bake regulation into the token** - which veers into 'code is law' territory and implies that to amend the regulatory code within the token, a new token will have to be issued.

- **Immutable regulations into the smart contracts** - which injects unchangeable smart contract logic between regulators and legal owners of tokenized securities, defeating the purpose of decentralization and being a step back instead of forward.

This brings us to *digitized securities* - a Prometheus Protocol innovation that marries the best features of traditional securities and tokenized securities.

A digitized security is a token representing a traditional security that sits in the issuer account of a traditional CSD, the token is the tradable component and features all the

benefits of a tokenized security while streamlining most processes of a traditional security lifecycle. Digitized securities are the next step in the dematerialisation of not only the security, but the various processes linked to its issuance, trading, custody, clearing and settlement. Only when Digital CSDs become a commonly acceptable (and authorized) solution, can we start implementing tokenized securities. The Prometheus Protocol is fully adaptable to both cases.

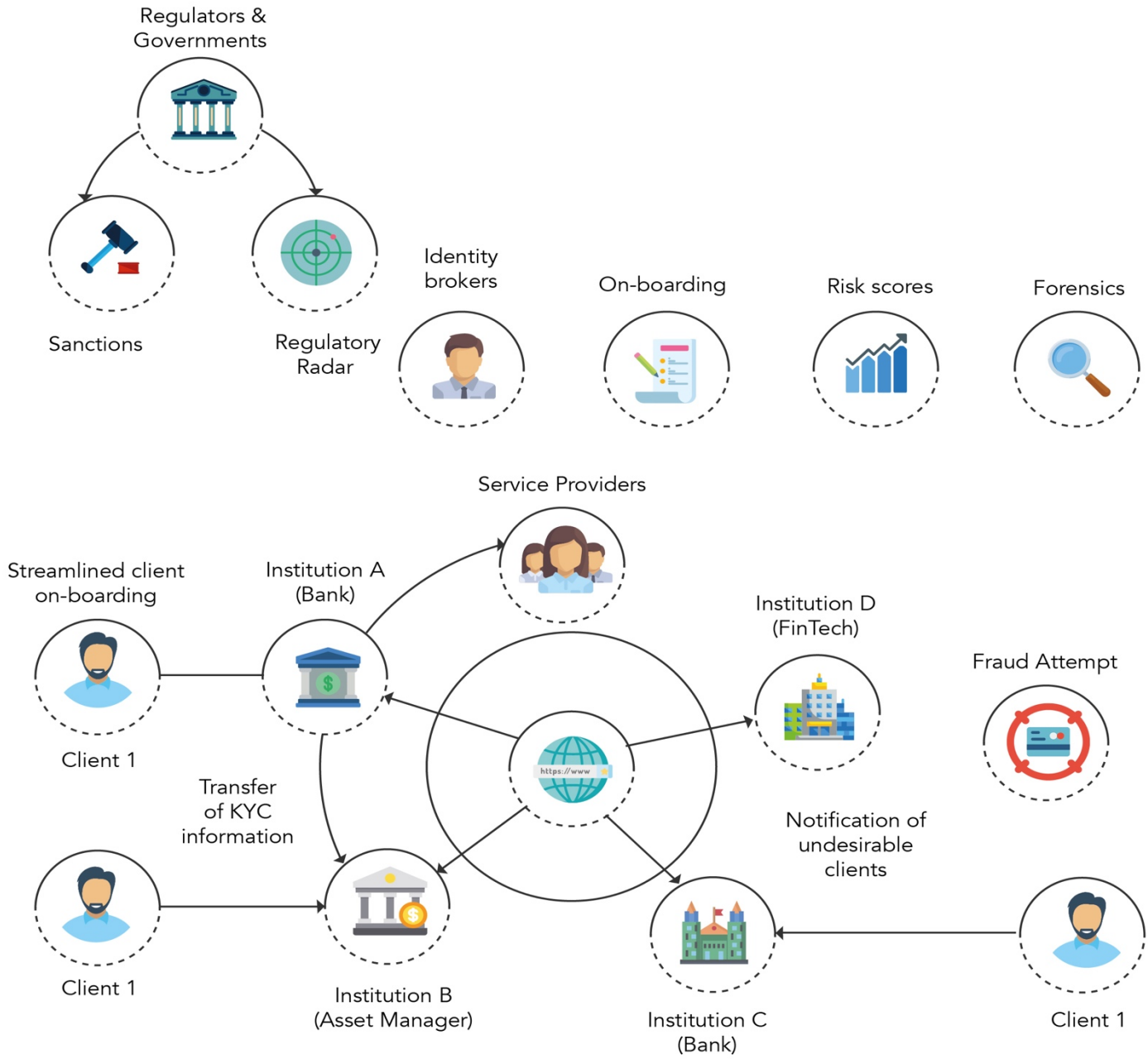

Figure 5: A Collaborative Compliant Ecosystem (Source E&Y)

It is pertinent to note that FINMA (the Capital Markets regulator in Switzerland) still does not allow digital CSDs while other countries such as Canada do. This is a good example to showcase the flexibility of Prometheus Protocol's digitized securities as they can be held in both, traditional depositories, as well as, digital depositories. Thus, on the Prometheus Protocol, investing, trading and managing tokenized securities is not dependent on the presence of digital CSDs in a jurisdiction. Cross-Border compliance is achieved not by reinventing the wheel but by enhancing and strengthening collaboration between actors. (See Figure 5)

On the question of regulatory compliance, Prometheus Protocol's digitized securities are built upon a layer of upgradeable smart contracts which provide the facility of being amendable and continuously stay in sync with regulatory updates.

This architecture of digitized securities also answers a key question plaguing essentially all cryptocurrencies -- Can you reverse invalid transactions? In the event of court rulings etc, securities might be required to change hands without the willing concurrence of one party. Digitized securities, with complete compliance and oversight by depositories, digital depositories, digital custodians, and regulators are architecturally capable of giving effect to legal and regulatory rulings -- a key component of compliance.

Pain Points Not Yet Addressed

Following the Great Financial Crisis of 2008 which wiped off tens of trillions of dollars from the market within months, the interest in decentralization assumed greater acceptance. However, the notion that globally trusted institutions (such as banks) could be replaced by truly trustless systems, is inherently flawed in its assumption.

The financial institutions that were created and maneuvered with governmental support and oversight have become paragons of credit creation and wealth management. Strict controls and adherence to compliance frameworks makes them some of the most secure entities in the world of finance. These need to be involved in upcoming frameworks as the most experienced players instead of removing them from the process. Decentralized ledger technologies that fill the gaps and clear the opacities that crept into the financial systems come with their own set of challenges.

Prometheus Protocol addresses the following problems faced by actors on both sides of the coin by bringing them together as the connecting link that bridges the best of both worlds:

In Traditional Legal-Financial Structures

Regulatory Authorities – Local Jurisdiction in a Global Market

Turf wars aside, the regulatory bodies are finding it increasingly difficult to implement their mandate as the world grows smaller. Take the example of the Bitcoin for example. If I send you a Bitcoin today, it is completely off the records of the regulators.

So, what happens in the event of a monetary dispute regarding this bitcoin? The regulatory authorities will be unable to enforce their mandate and judgements simply because bitcoin infrastructure does not fall under the explicit mandate of these regulatory authorities.

Similarly, there is no KYC performed on either you or me before we transacted that bitcoin. Even on most centralized exchanges (outside the US), KYC is as rudimentary as asking people to take a selfie while holding a government document. This is not really KYC. That is in direct contravention to FATF[7] guidelines on preventing money laundering and terror financing. Also, the island-isation of data makes it near impossible for regulatory authorities to access/source data from other jurisdictions.

Even within the same jurisdiction, something as small as device or format incompatibility renders cooperation difficult.

[7] https://en.wikipedia.org/wiki/Financial_Action_Task_Force_on_Money_Laundering

Financial Institutions – Damned if you Do, Damned if you Don't

Caught in the middle of the crossfire, banking institutions, throughout history, have been judged too harshly due to the simple fact – they're in the business of Money. The observed increase in the cost of the compliance function (See Figure 6) over the last 10 years is no longer sustainable, especially at a time when most organizations are trying to streamline their cost base to protect profits and growth.

The costs of compliance are manifold.

Banks need to:

- Verify and validate user data and transaction history
- Store the data and history in a secure environment to prevent unauthorized access
- Enable robust data governance to allow data access to entities which need it

The cost for each of these activities adds up to over millions of dollars *annually*[8]*.* Even after incurring these costs, the institutions grapple with security issues and vulnerabilities due to the absence of industry-wide standards for validation, storage, and retrieval.

With security vulnerabilities come liabilities and according to a Thomson Reuters Culture and Conduct Risk 2018 survey, 70% of compliance senior practitioners believe that this liability is only going to rise in the years to come. This will necessitate an increase in budgetary allocation and 61% of the surveyed practitioners believe so too.

[8] https://legal.thomsonreuters.com/content/dam/ewp-m/documents/legal/en/pdf/reports/cost-of-compliance-special-report-2018.pdf

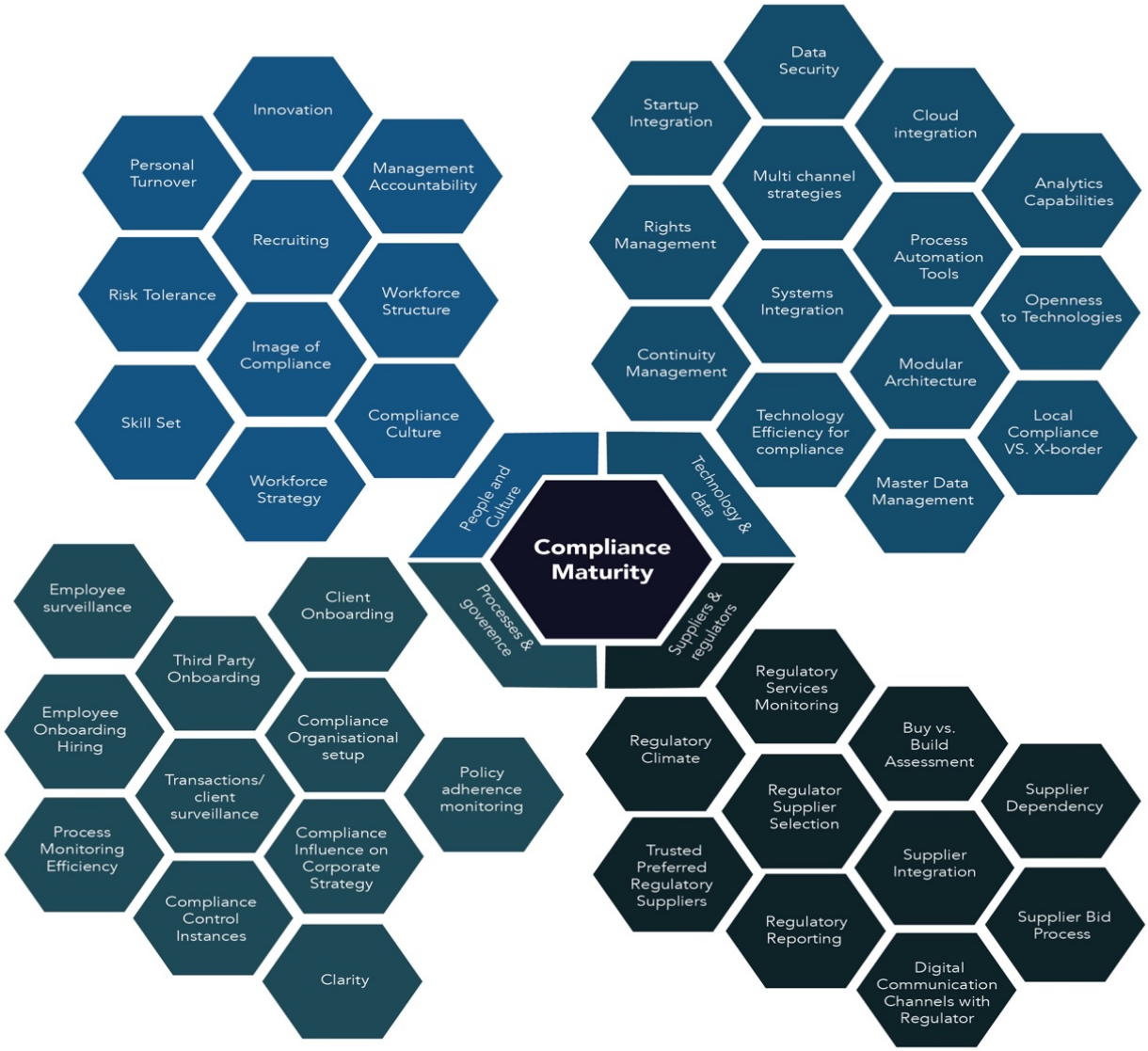

Figure 6: Compliance Maturity Assessment (Source: E&Y)

Securities Trading Markets – Resisting Globalization

Following dematerialization (also called Demat), the paper-form securities were replaced by book-entry securities. This makes the book-keeper responsible for maintaining correct records of trades. It presents two problems, namely:

- Bookkeepers are tied to one jurisdiction and limit the tradability of the securities
- Bookkeepers become the single points of failure in the trade cycle

Under the existing system, the depository in jurisdiction A is a separate virtual container from the depository in jurisdiction B. Thus, if I want to sell you securities, unless we both use the same depository, the process can take a long time, with a higher risk of failure.

In Decentralized Ecosystems

Absence of Regulations – The Virtual Wild West

To put it simply, the absence of regulatory controls pretty much implies the absence of redressal mechanisms. The players tried workarounds such as performing '*their versions of KYC*' but that doesn't offer even a shred of what actual KYC provides. Here, the identity check is as rudimentary as asking users to click a selfie while holding up a government-issued document. This is validated manually and is not acceptable to most compliant institutions.

Additionally, the storage of questionably collected personal data in questionable jurisdictions and with questionable security infrastructure, raises legitimate concerns. Cryptocurrency exchanges getting hacked and getting their funds pilfered and user data stolen is no longer a novelty. Simply put: What can be built can be hacked. Thus, regulatory oversight is important from the perspective of legal recourse.

The absence of regulatory oversight also enabled the installation of several crowdfunding campaigns (better known as ICO[9]) that ended up either getting cease and desist notices from authorities after raising hundreds of millions or had the Founders dropping off the radar with whatever sums they raised.

Cons in the Name of Consensus – Not Tolerating Faults

When a law changes (also called regulatory change), the smart contracts, codebase, and/or tokens that were hard coded with the old set of laws (instructions) must either be modified or be completely replaced with the upgrade. This is inherently challenging in decentralized ecosystems since not all actors might be available at the same time to fully participate in the voting process, either for or against.

This is extremely important in architectures that 'claim to be 100% compliant' since that claim is underpinned on the belief that the code/instructions fed into their systems are also set in stone on the law books. History has never been kind to such rigidities.

Human Errors and PEBKAC[10] – Reversibility is not Entertained

In a non-decentralized world, human errors are rarely punishable, unlike in a decentralized world. If I send money to the wrong address, it's lost. Forever. Will this foster adoption? No.

[9] ICO = Initial Coin Offering

[10] *PEBKAC stands for Problem Exists Between Keyboard and Chair meaning problem is due to user's error.*

There is a need for enabling reversal of transactions performed unintentionally but this faces stiff denial from the radical proponents of decentralization.

Even in the centralized solutions that do feature legal recourse (such as centralized crypto exchanges, there is no mechanism to reverse faulty transactions once the funds are transferred from the centralized exchanges' ecosystems to something like a cold wallet.

Securities trading, on the other hand, have mechanisms to reverse and therefore nullify transactions baked into their system. These solutions, however important, are currently not available in the nascent tokenisation space.

What is needed is a compliance layer that houses legal and compliance entities that:

- Perform their mandates transparently
- Adhere to the legal compliance requirements of jurisdictions
- Process customer issues instantly, with minimal costs

Practically, transactions should be enforceable and should be reversible, at least, under legal direction without the presence of a trusted intermediary. This is a classic catch 22 situation. If you do not have a trusted intermediary, you cannot reverse transactions. If you have an intermediary, you should not have to trust it.

The emergence of zero-knowledge proof systems (especially zk STARK[11]) promises both these counter-positioned features. However, these systems are still in their early stages of implementation with nil to no acceptability within the larger banking and investment sectors.

Total Addressable Market - Potential and Opportunities

The Prometheus Protocol is comprised of three layers that collectively enable the following functions:

1. Data Governance
2. Cross-Border Regulatory Compliance
3. Regulated end-to-end Issuance & Securities Lifecycle

Thus, for better comprehension, the market potential is also divided into these three heads.

Market Potential of Data Governance

[11] https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/zk-starks/

Figure 7: Market Growth (2019-2024) (Source: Market Intelligence)

The data governance market is expected to register a CAGR of over 21.44%, during the forecast period, 2019 - 2024, and it is expected to reach a value of USD 4.35 billion by 2024[12]. According to EOL IT Services, the biggest challenges in Data Governance is employee compliance, i.e., ensuring that employees comply with overall data strategy, something often borne out by a lack of understanding rather than a lack of desire. Thus, as data creation continues to grow at over 40% per year[13], the need for customer data privacy is only expected to continue growing.

The region of Asia-Pacific is projected to be the fastest-growing region for the data governance market (See Figure 7), owing to the growing technology expenditures in economies, such as China, India, Singapore, and Australia. The demand for cost-effective data management and governance solutions and services among banking institutions and small- and medium-sized enterprises (SMEs) are further driving the demand for the data governance market in the region.

The European and the North American markets continue to be the flag bearer to rapid technology adoption and see the highest potential in terms of the absolute value of data governance technologies across all continents.

Market Potential of Cross-Border Regulatory Compliance

There are three broad categories of cross border regulation:

[12] https://www.mordorintelligence.com/industry-reports/data-governance-market
[13] https://www.forbes.com/sites/rkulkarni/2019/02/07/big-data-goes-big/#5a6949e820d7

1. **Passporting** - Common rules for member jurisdictions
2. **National Treatment** - Signatories treated as local market players
3. **Recognition** - Harmonious laws created by members

The issue of regulatory divergence on examination by the OECD and the International Federation of Accountants (IFAC) shows that the cost of regulatory divergence was significant or very significant to the financial performance of 75% of the institutions surveyed[14].

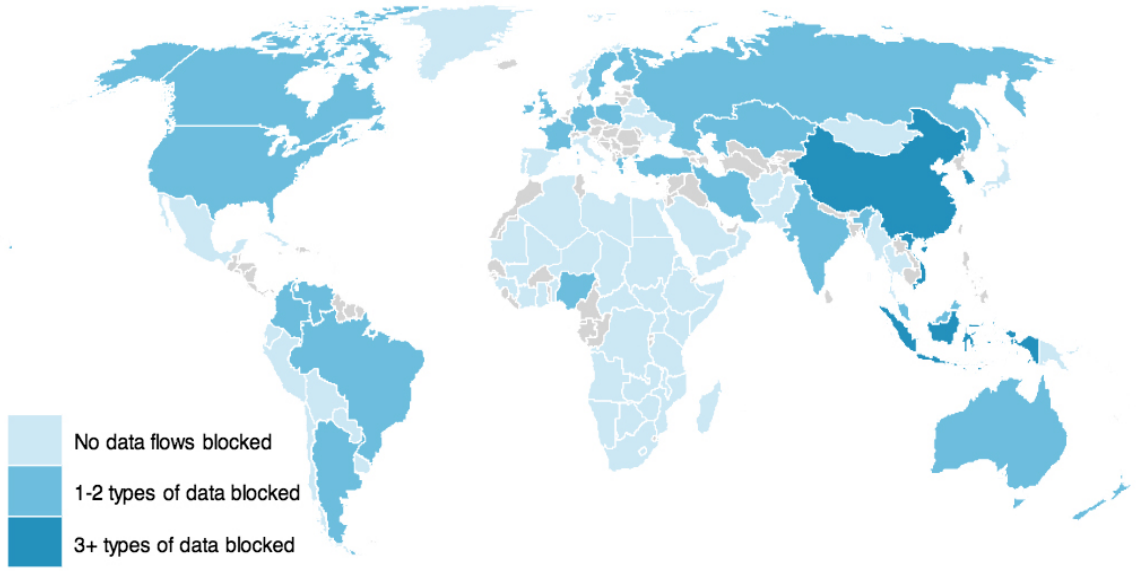

Figure 8: Transparency in Data Flow (Source: OECD)

Growth markets springing up around the world can mean a big opportunity for businesses willing to embrace globalization (See Figure 8). The Business Reality Check confirms that for the majority of business leaders, managing – not avoiding – cross-border regulation is the answer. Less than a quarter of business leaders seek to avoid cross-border regulations by reducing their global footprint.[15]

According to IFAC, businesses and banking institutions continue to view global harmonious laws created on the basis of cooperation and operational transparency as better than those created by international regulatory bodies. It is because the member countries have started to show a tendency towards focusing on domestic-first as opposed to the unwritten mandate of international bodies to create single market economies.

[14] https://www.ifac.org/publications-resources/regulatory-divergence-costs-risks-and-impacts-0
[15] http://35.170.55.184/in-brief-cross-border-regulations

Market Potential of Regulated end-to-end Asset Tokenization Lifecycle Management

Capital markets are still in the early phases of the adoption of blockchain and distributed ledger technologies (DLT). The industry continues to seek viable use cases. One broad category of such use cases is the end to end management of digitally tokenized assets (See Figure 9), in which the token either represents a property interest that exists only on the Blockchain (such as non-certificated securities) or represents an asset existing off the Blockchain.[16]

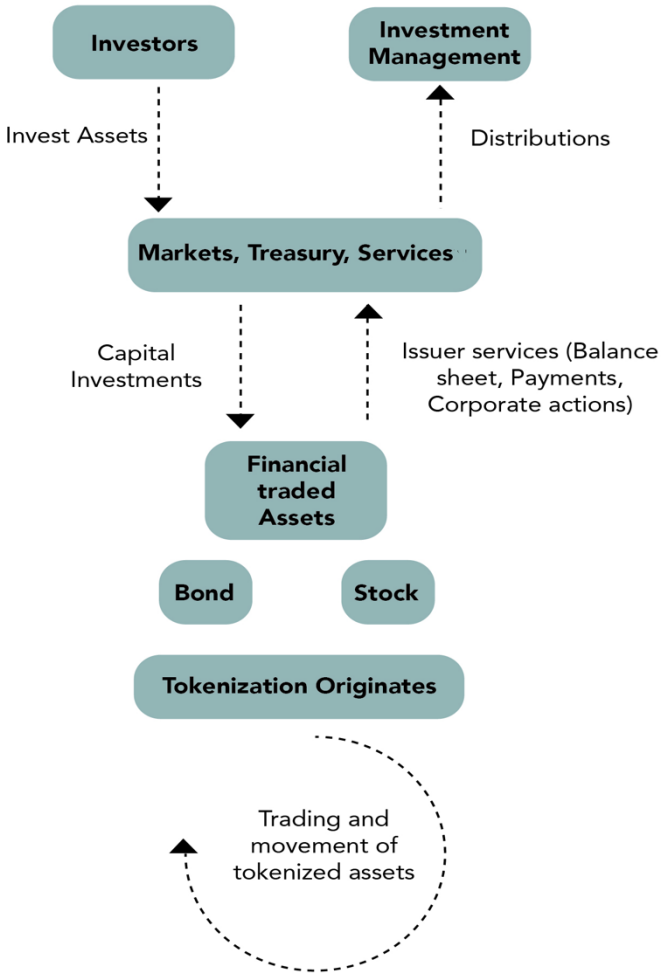

Figure 9: Asset Tokenization Lifecycle

The security token market size should grow to USD 2tn by 2030 with a 59% CAGR (See Figure 10) for the 2019-2030 period, amid steady improvement of the digital asset ecosystem. While mass institutional adoption should occur post 2025[17].

We are, however, already seeing the footprints of future institutional adoption. In 2015, NASDAQ launched LINQ, which deals with private equities based on blockchain technology. In 2018, Australia securities exchange ASX announced that they will replace their clearing and settlement system with a new blockchain-based system by 2021. JPX, the securities exchange of Japan, has been trying to implement blockchain technology to the clearing and settlement process of securities after constructing a consortium with finance and IT companies in 2016.

[16] https://www.bnymellon.com/us/en/our-thinking/tokenization-opening-illiquid-assets-to-investors.jsp
[17] https://www.finyear.com/attachment/1338789/

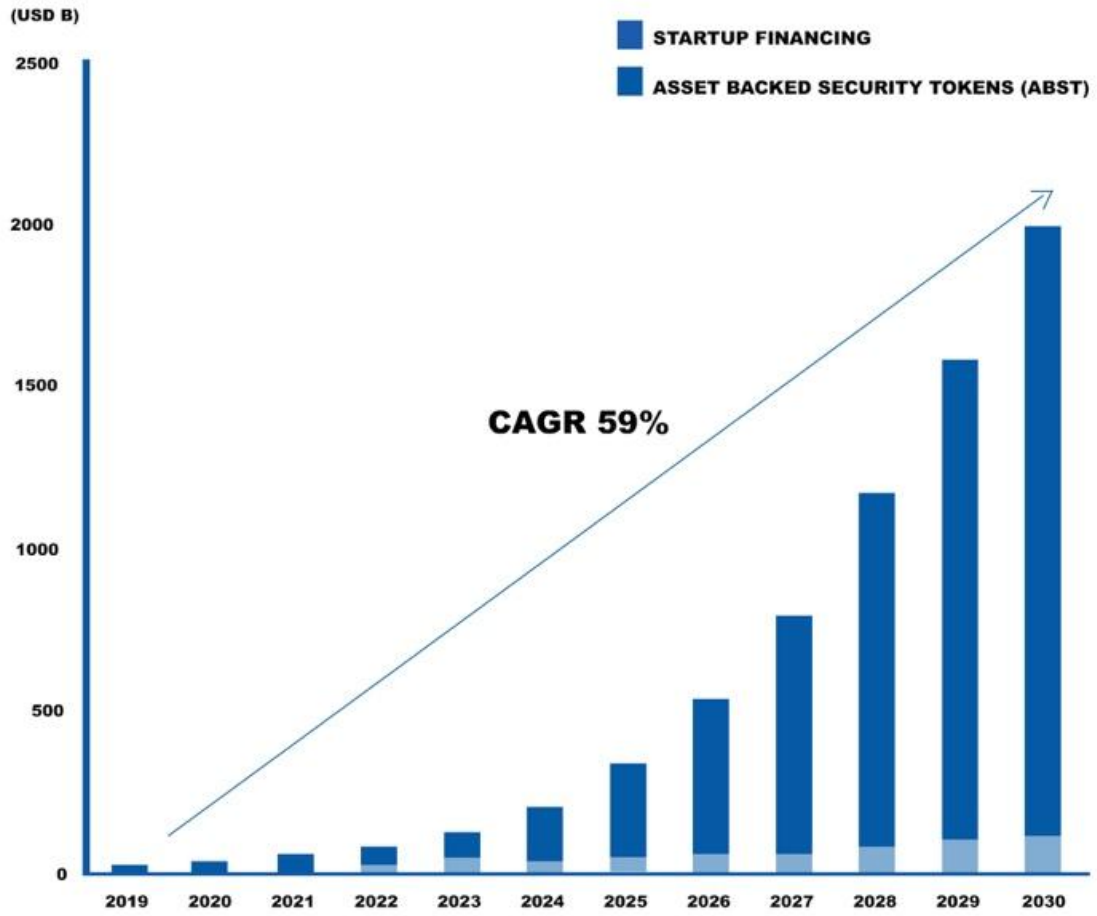

Figure 10: Growth of ABSTs (Source: Chain Partners)

In 2018, SGX, securities exchange of Singapore, developed DvP, which is a settlement solution for effective digital asset settlement across various blockchain platforms. KRX, the securities exchange of Korea, declared in 2016 that they will utilize blockchain technology at KSM[18].

Snippets on Market Potential of an Improved Regulatory Compliance Protocol

During 2017, Thomson Reuters Regulatory Intelligence captured 56,321 regulatory alerts from over 900 regulatory bodies averaging 216 updates a day (See Figure 11).

[18] Korea Startup Market

The scarcity and value of skilled compliance resources have been highlighted by both the expected increase in the cost of senior compliance staff and the continued use of outsourcing to respond to the continuous and increasing compliance requirements.

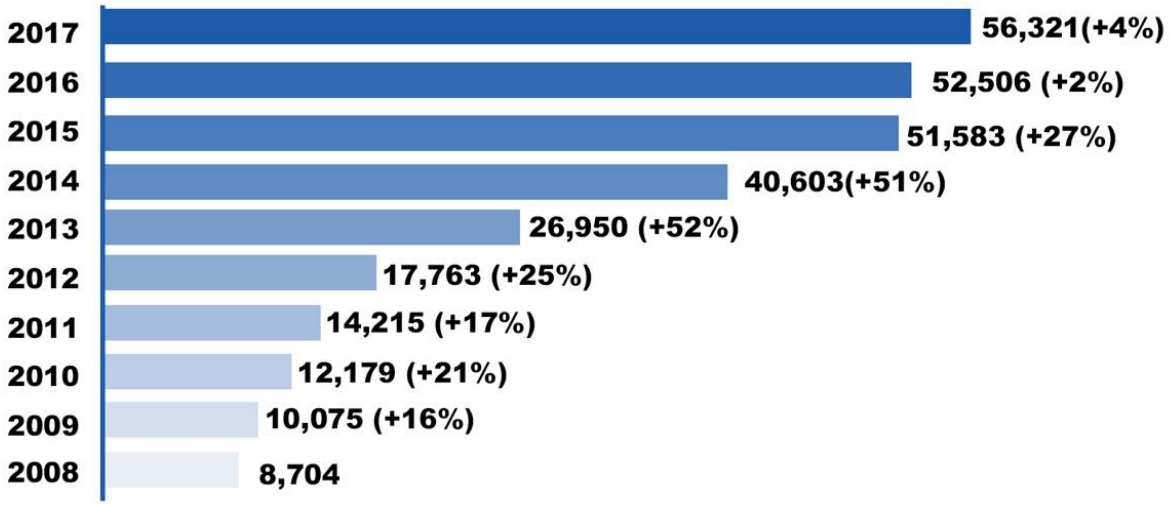

Figure 11: Total Yearly Alerts Raised (Source: Thomson Reuters)

Firms can seek to make the best use of in-house skills by optimizing the alignment, cooperation and coordination between the risk and control functions to ensure there is coverage of the key risks to the organization, and all associated reporting is consistent.

One area where firms and their compliance officers may be seeking to bridge a skills gap is with regard to evolving technology, notably in the shape of fintech developments and RegTech solutions.

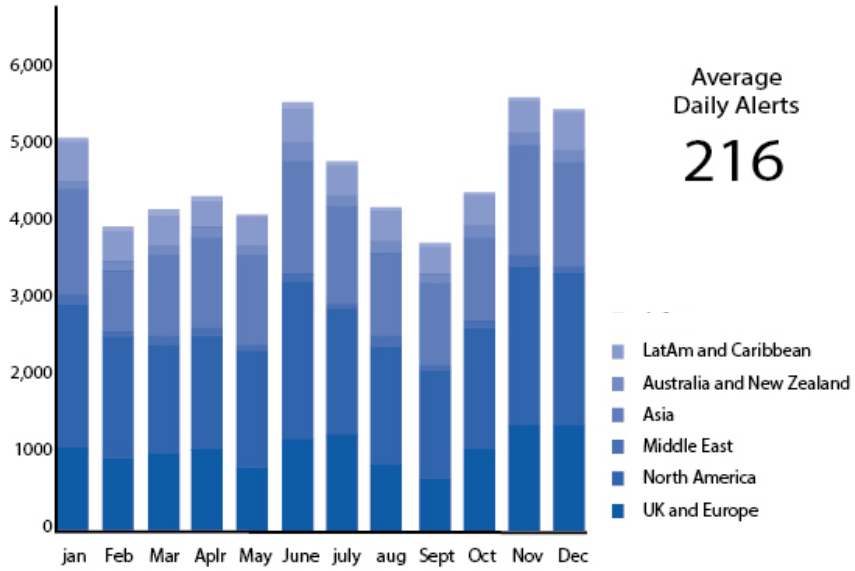

Figure 12: Regulatory Activities Tracked in 2017 (Source: Thomson Reuters)

Whilst it is encouraging that compliance functions have recognized any skills gap, firms need to keep the balance between in-house expertise and any outsourcing under review.

Firms continue to invest in all aspects of their risk and compliance infrastructure, an essential part of which is the skills of the compliance function (See Figure 12).[19]

19 https://legal.thomsonreuters.com/content/dam/ewp-m/documents/legal/en/pdf/reports/cost-of-compliance-special-report-2018.pdf

The Prometheus Protocol – Compliance, Governance, and Digitized Issuance

Solution Overview

Simply put, the Prometheus Protocol is a highly flexible architecture comprised of interconnected layers that connect stakeholders, regulators, and technology to foster omnichannel transparent communication and compliance in a structured and cost-effective manner.

This makes the Prometheus Protocol an end-to-end regulatory compliance framework that acts as the connecting link between decentralization and regulation on an equal footing with equal weightage to both sides while addressing the concerns of both sides.

The Prometheus Protocol serves as the communications bridge between the stakeholders and all the actors within the Capital Markets' value-chain. It incorporates an open architecture for improved data governance and transparency between issuers and subscribers. It enables end to end cross-border compliance to regulatory authorities and a truly compliant-yet-customizable securities' issuance and trading in the secondary markets subject to cross-border regulation.

This makes the process of KYC/AML verification highly cost-effective and extremely fast for financial institutions (which spent over $47 MM in KYC in 2016 alone - Thomson Reuters[20]).

With the Prometheus Protocol, institutions will be able to perform KYC/AML/KYB[21]/DD[22] and such verifications faster and at a fraction of the existing cost (ZKP[23] can be used to perform such verifications instantly while preserving the privacy of Financial Institutions' clients). A consortium of validators (approved by the regulators and other stakeholders such as the institutions themselves) perform verification individually and only when they arrive at consensus will the verified data be committed to the *Data Registry*. This also serves as the facilitator of smoother cross-border regulatory harmonious action.

[20] https://legal.thomsonreuters.com/content/dam/ewp-m/documents/legal/en/pdf/reports/cost-of-compliance-special-report-2018.pdf
[21] KYB = Know Your Bank
[22] DD = Due Diligence
[23] ZKP = Zero Knowledge Proof

Robust Data Governance completely compliant to GDPR is the central tenet that underpins the Prometheus Protocol. The Prometheus Protocol is a comprehensive framework that includes all stakeholders in the regulatory, compliance, issuance, trading and post-trading ecosystem. From regulatory bodies and financial institutions such as Tier-II, Tier III investment banks, private banks, wealth managers, and asset managers to consulting agencies and tokenized issuance platforms that create solutions for their clients, the Prometheus Protocol has a role-based access control architecture to smoothen business flow both upstream and downstream.

In short, the Prometheus Protocol will become a connecting link between the tokenization forces and the regulatory forces and enable users to harness the best capabilities of both seamlessly.

Layers of the Prometheus Protocol

The Prometheus Protocol will be comprised of three key layers of communication to facilitate multidirectional data flow in a traceable, accountable, and regulated manner compliant with global, national, and local jurisdictions, as the case may be.

These three components are:

- **Data Governance Layer** - to ensure that all data collected, processed, and disseminated is completely compliant with regulatory requirements such as GDPR and MiFID II to ensure that both the privacy of the users and transparency of transactions, comply with the various regulations across the entirety of the Prometheus Protocol

- **Cross-Border Regulatory Compliance Layer (CBRCL)** - to ensure harmonious integration with existing legal and regulatory structures worldwide instead of removing them from the process. Compliance via Prometheus Protocol's cross-border regulatory compliance framework ensures complete regulatory oversight, legal recourse by relevant regulatory bodies, and upgradeability of smart contract logics by regulatory approval to continually comply with evolving regulatory landscape.

- **Security Issuance & Lifecycle Layer** - to ensure compliant tokenization of digital securities into digitized securities. The driving philosophy behind Prometheus Protocol is to ensure compliance from step 1 instead of as an after-thought or a slap-on.

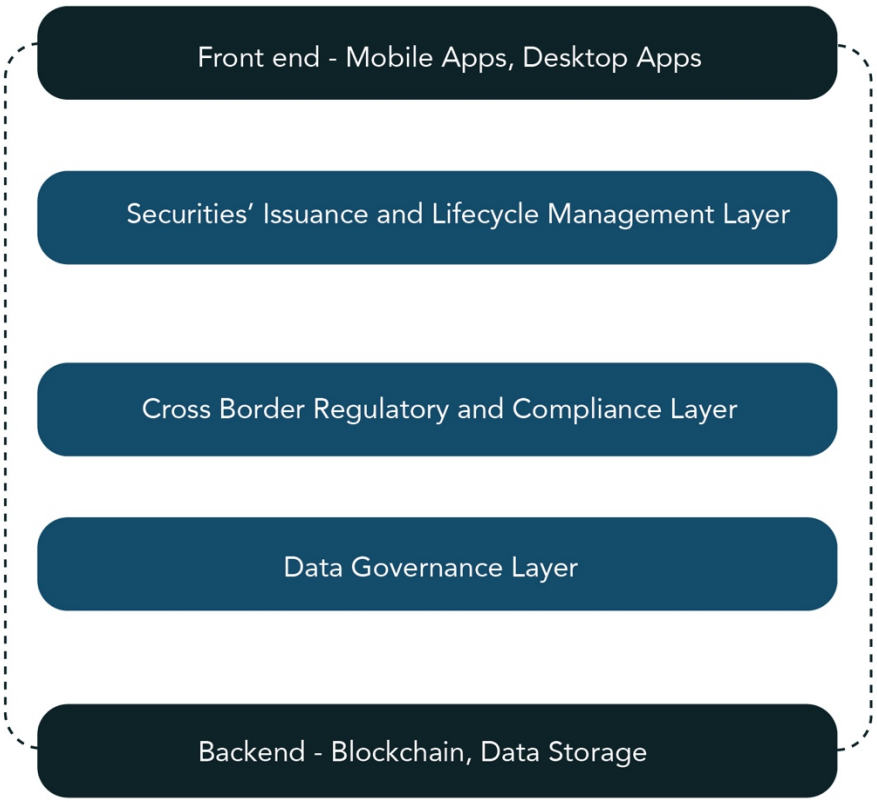

Figure 13: Layers of the Prometheus Protocol

The Data Governance Layer for Data Governance 3.0

Data Governance 3.0, as envisioned by the Prometheus Protocol, promises seamless and expedited regulated Data Governance across borders to ensure compliance with changing regulatory controls from one jurisdiction to the other.

It improves upon Data Governance 2.0 (which enabled seamless data governance within the same jurisdiction) which itself was an improvement upon Data Governance 1.0 (seamless data governance within the offices of an entity).

Data Registry

The Prometheus Protocol's Data Registry is the one-true trustless entity of all data components pertaining to the investors and the issuers. The data registry has multiple touchpoints with the Legal and Compliance Layer of the Prometheus Protocol whose mandate is to ensure 100% compliance of the entire system to the regulatory and legislative directives and laws.

Data stored on the Data Registry is:

1. KYC information of the investors and DD information of the legal entities (as value) linked to the hash (key) of the provided data
2. KYC and eligibility statuses of the investors
3. Legal ownership statuses of ***digitized*** securities on the Prometheus Protocol
4. Transactional data pertaining to trades between counterparties

The hashes are created on successful verification of the user's identity by the compliance-verification entity and can be updated on the presentation of new data but cannot be modified by any party unilaterally. The user's data wallet syncs to the Data Registry with Read-Only access to enable users to view their status but not modify it.

Data Fragmentation and Storage Architecture

Centralized storage is fraught with risks - censorship, single points of failure, and impermanence of data being the biggest among them. Decentralization (data transfer over peer to peer networks) has its problems too. Searching/Querying is painfully slow and unreliable at best.

This is where Decentralized Hash Tables (DHTs) come in.

What is a DHT?

A DHT is the decentralized version of a hash table. A hash table stores key(identifier) and value (content) pairs in an orderly manner. A DHT is the fundamental unit of IPFS storage. Data committed to the IPFS for storage and retrieval is stored within decentralized hash tables (DHTs)

Key (Header)	Value (Header)
001	“My Parameter”
002	“Is not”
003	“Ever Known”

The above table as a whole is a diagrammatic representation of a hash table. Now, in a DHT, the different key-value pairs (depicted by different colours and known as buckets) are stored in different locations. The same bucket can be stored at different locations. These locations are called ‘Peers’.

Each Peer has an identifier PeerID and stores a list of all of the peers who have a copy of the same bucket and also a list of the Peers who have copies of the other buckets created from the same DHT.

Content Commitment and Retrieval

Similar to the BitTorrent protocol, each content piece is hashed (to create a content address) before commitment to the IPFS and is chopped up into smaller pieces. Each chopped content piece has a content ID (CID) that points to the content ID of the piece preceding it and the piece succeeding it.

This is achieved by generating IPLD-Merkle-DAGs of the content piece. These smaller content pieces are then committed to the same or different DHTs where the CID serves as the key while the corresponding content piece is the value.

To retrieve a content piece, queries are raised using the content address instead of the content location. This acts as a security measure. Only those who possess the content address can request to retrieve it.

This content address query is relayed peer to peer to locate all of the CIDs and return the linked content pieces along the same path. Once the content pieces are received, the requesting party can verify their authenticity by hashing the content blocks and matching it with their CIDs.

Fragmenting Data Associations on the Prometheus Protocol (Work in Progress)

On the Prometheus Protocol, the Data Registry is the frontend of an IPFS-powered architecture. The Data Registry contains two major types of data -

- **Personally Identifiable User Data** - committed to Data Registry post consensus among KYC providers with respect to data validation

- **Transaction Data** - committed to Data Registry after verification by the CBRCL post-transaction execution

Once the data is created at the user level or at the institutional level, the transaction data and personally identifiable user data are treated differently. Wholesale encryption is typically an overkill (and very expensive) in many situations where some data is not sensitive per se; what is sensitive is their association with other data (Ciriani et al., 2010).

The Prometheus Protocol splits the data with minimal fragmentation and confidentiality constraints. The confidentiality constraints are the privacy requirements of that data and are used to segment the associations between the components of that data set.

This ensures that even if the data is stored on the same servers (low statistical probability), the fragments of the data will essentially be distinct pieces with an appearance of pointing to different sources and associations (if any). Only the data owners will possess the knowledge of :

1. Data's encryption keys
2. The storage location of the Data

Without having both the pieces of information, an actor cannot access the data or derive any of its associations. The queries issued by users with a full view are then translated into equivalent queries operating on the encrypted and fragmented data stored on the server(s). The translation process is executed by a trusted component, called a query mapping component, which is invoked every time there is a need to access sensitive information (Ciriani et al., 2010).

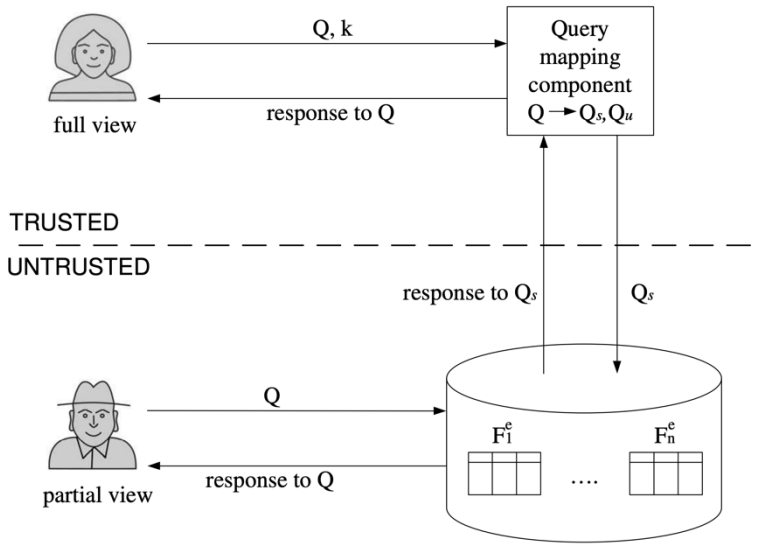

Figure 13: Interactions among users and server storing the fragments

The Prometheus Protocol uses this technology to build an open all-inclusive IPFS[24]-based public cloud system to enable sovereign ownership of user data to the users alone. Thus, users can validate their identities to multiple entities without exposing their KYC and such identity and compliance documents to every entity. It also ensures wider compliance with data privacy laws such as GDPR by ensuring complete deletion of user data - on demand, as opposed to accepting to leave digital breadcrumbs on the Blockchain as acceptable trade-offs[25].

The Prometheus Protocol uses data fragmentation and DHTs within the IPFS clusters to provide:

- Private and Secure data storage
- Trustless validation
- Right to be forgotten
- Conservation of power consumption

Prometheus Protocol's implementation includes a big IPFS pinset (as pinset manager) for sharing, to serve several virtual IPFS peers with just one running IPFS peer instance. This decreases users' resource consumption while also serving as a backend for IPFS clients. The protocol also includes a built-in fragmentation algorithm that can be called via APIs. The data fragmentation algorithm sits in between the users' data and the decentralized storage.

Financial consortiums can leverage the Prometheus Protocol to build their distinct private clouds with their own set of actors and operators but under the overall supervision of the regulatory and compliance layer.

Trustless Data Flow – Zero-Knowledge Proof for Validation

Access to the data registry is controlled via a Role-Based Access Control (RBAC) mechanism that allows read-only access to the users. It uses zero-knowledge proof driven validation of users' identities and eligibilities by the issuers and the trusted legal and regulatory entities.

Zero-Knowledge Proof[26] based validation ensures compliance with data privacy laws while simultaneously being error-proof. The Prometheus Protocol will implement zk STARK, an improvement of the zk SNARK for two main reasons:

[24] https://en.wikipedia.org/wiki/InterPlanetary_File_System
[25] https://www.linkedin.com/pulse/either-isnt-look-blockchain-gdpr-compliance-andres-pihor/
[26] Zero-knowledge proofs are methods of proving something while only divulging a very small amount of information about that something.

1. zk STARK is quantum computing resistant making it future proof to potential quantum encryption break
2. zk STARK does not require a trusted central setup to act as the intermediary between the decision-making arms (*Proof of Proximity)*

Example of Validation via Zero-Knowledge Proof

If an Investor Alice, who was on-boarded by Bank A, wants to invest in a security offering issued by Bank B, she needs to perform KYC again with Bank B by sharing her personal information with Bank B to prove that she is *eligible for and capable of* investing in Bank B's security's issuance.

With Zero-Knowledge Proof verification, Alice does not need to share her personal information with Bank B. The only thing that Bank B needs to know is, whether Alice meets the eligibility criteria (KYC) to investment *and* has sufficient funds to invest in Bank B's securities issuance.

Here's how Zero-Knowledge Proof (ZKP) verification via the Prometheus Protocol helps Alice maintain her data privacy, Bank A stayed GDPR compliant in cross-border transactions; while providing Bank B with the necessary information to verify whether to subscribe Alice to the security's issuance or not. ZKP also enables banking consortiums to offer open finance to all their investors, *across jurisdictions and regulations*.

As an investor in Bank A, Alice's information is already stored with Bank A. Banks A and B are members of the same banking consortium. Bank A, after processing Alice's user data, uploads it to the data registry *post-encryption.* The data storage is in the form of a key-value pair with the hash of the data serving as the key to the user data serving as the value. The hash is committed to the DLT and a copy is stored on Alice's device (via the Prometheus Protocol's User-facing app), as well as, on the decentralized database in an encrypted manner.

Now, to prove her *eligibility for and capability of* investing in Bank B's security's issuance, Alice sends her access key (from the Prometheus Protocol's User-facing app) to Bank B which can simply query the data registry with it. The data registry returns the compliance and eligibility status of the provided hash, without divulging the user data. **This is the Zero Knowledge Proof Validation**.

If Bank B requires Alice's user data (to comply with regulatory requirements) or, if Alice wishes to conduct business with it, Bank B only needs:

1. Alice's express permission
2. Acceptance by Alice's jurisdiction *and* Bank B's jurisdiction as to the need of Bank B to access Alice's personal data

Once both conditions are met, an access key for Bank B is generated to access Alice's user data on the decentralized data registry.

If Alice wishes to stop doing business with Bank A, she can rescind access to her data on the data registry to Bank A rendering the previously generated access key invalid.

Prometheus Protocol and Comprehensive Data Governance

The Prometheus Protocol incorporates a strategic and comprehensive approach to achieve all-round robust data governance. Distinct from traditional data governance models that are bottlenecked at the board level due to Data Governance Boards acting slowly upon the advice of the Data Stewards, the Prometheus Protocol's data governance structure achieves:

1. Transparency in data processing and storage
2. Securing user privacy via zk STARK
3. Complete auditability with zero ability of data manipulation after recording

The Prometheus Protocol follows The Data Governance Institute recommended formal, documented, repeatable procedures for:

1. **Aligning Policies, Requirements, and Controls** -- via a comprehensive compliance layer that harmonises requirements of cross-border jurisdictions to ensure legal oversight over transactions

2. **Establishing Decision Rights** -- by ensuring that the decisions taken by the investors are dutifully carried to the issuers without possibility of tampering along the way

3. **Establishing Accountability** -- achieved by multi-directional and omni-channel traceability of all data with the help of the decentralized data registry

4. **Performing Stewardship** -- Legal and Compliance Trusted Entities ensure that data governance standards are always aligned to the regulatory and legislative requirements of all jurisdictions involved in the flow of the issue

5. **Managing Change** -- Amendments in the laws and regulations are transcribed into templates by the legal and compliance entities for automated and error proof encoding into the upgradeable smart contract logic representing that law as code instructions

6. **Defining Data** -- is easier with the DLT, decentralized data registry, the asset registry encrypting all user data and only storing hashes to ensure privacy

7. **Resolving Issues** -- is made possible by the installation of a grievance redressal entity to capture and collate all concerns raised by the stakeholders and transfer them to the relevant actioning authority

8. **Specifying Data Quality Requirements** -- is again easier with the incorporation of the DLT to store all hashed data on the decentralized data registry and pass only the status via zero knowledge proof

9. **Building Governance into Technology** -- by upgradeable smart contract logics to represent real world governance regulations as lines of code to automate the flow and still be upgradeable by relevant entities only

10. **Stakeholder Care** -- by ensuring all accruals and actions of the stakeholders are transparently, securely, and in a tamper-proof manner are transmitted across channels in compliance to the jurisdictional requirements

11. **Communications** -- are managed via secure app interfaces of the stakeholders and end to end encryption of messages to ensure safety from tampered instructions getting transmitted

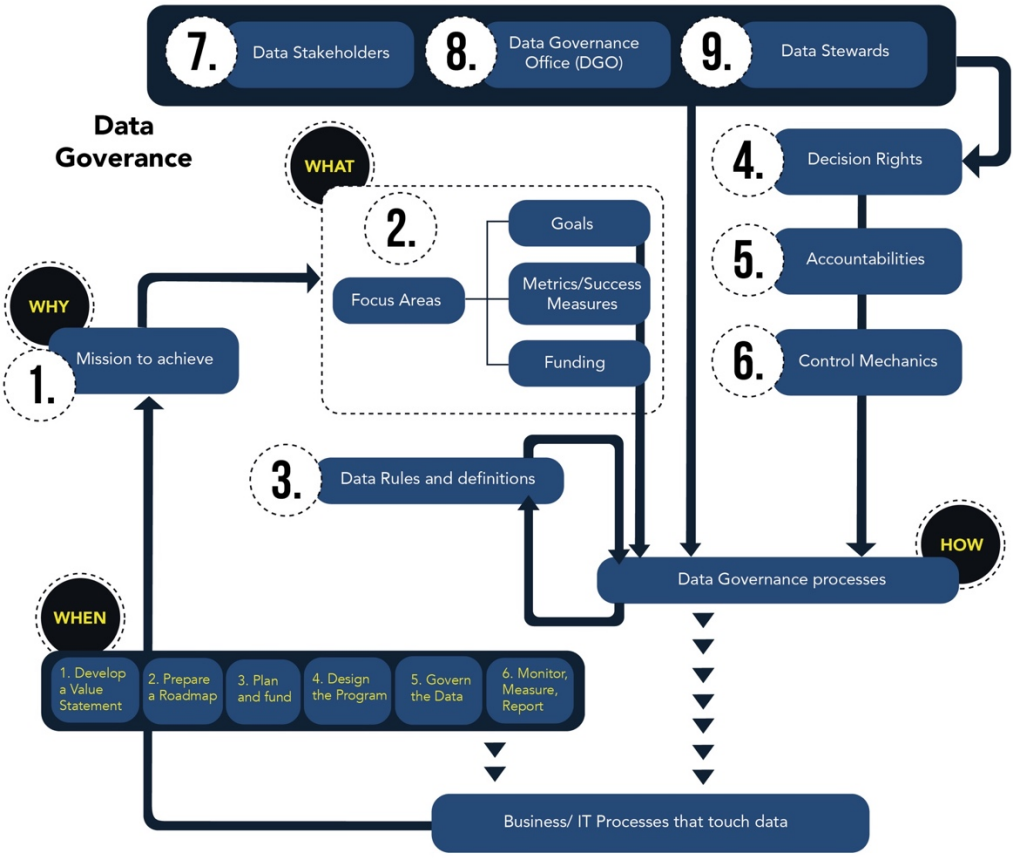

Figure 14: The Data Governance Framework (Source: Data Governance Institute)

Cross-Border Regulatory Compliance Layer – Transparent, Traceable, & Agnostic

The key issue is that data are not necessarily valid just because they are stored in multiple places. In today's compliance process, the data's trustworthiness is guaranteed by the legal system, the relevant authorities and the threat of legal penalties.

Transparent

On the Prometheus Protocol, the process of compliance and its monitoring is achieved via Consensus-Driven Compliance via the Cross Border Regulatory Compliance Layer that is directly actioned upon by legal and compliance entities in the event of addition, deletion, and/or amendment of the regulations governing the markets.

The Cross Border Regulatory Compliance Layer (CBRCL) of the Prometheus Protocol ensures:

1. Compliance Adherence by the Stakeholder Entities
2. Compliance Monitoring by the Legal and Compliance Entities

The CBRCL has an uninterrupted multidirectional communication channel with the data registry to ensure that any verified regulatory amendment is automatically and instantly incorporated and updated on the data registry.

Similarly, any changes that are queued for commitment into the data registry are first verified for compliance by the CBRCL.

In a nutshell, the Prometheus Protocol's Cross Border Regulatory Compliance Layer ensures regulator-driven compliance while also reducing the need for firms to actively collect, verify and deliver data by connecting both sides via its interface.

Any changes in compliance requirements are replicated directly at the layer-level by templatized amendment of the code by the representatives of the regulatory bodies themselves.

Traceable

The DLT bestows another benefit to the Prometheus Protocol in terms of end-to-end data traceability which can be utilized by a vast body of stakeholders.

For example, issuers create rules or create any form of communication for the investors and can send it across without fear of tampering or modification.

The investors also gain peace of mind on account of traceability since any modification done to the issuer's message will automatically raise a red flag before the investor can action it.

Data traceability on the Prometheus Protocol is not limited to unidirectional issuer to investor flow but can be easily implemented for a multi-stakeholder, omnichannel, and multi-directional flow of traceable information.

Each Blockchain event emission on the Prometheus Protocol is also captured on the database to enable faster querying in a localized environment without exposing the user identity to any of the validators or operator entities (except in cases where the identity needs to be divulged as part of the local regulatory requirements).

If the data is edited/modified by any of the recipients before transmission, it'll generate a new hash and not correspond to the hash on the data registry triggering a flag to prevent the transaction from proceeding further.

This will also automatically raise a flag that notifies the recipients of the modified message of the tampered status of the message and helps zero in on the source of the tamper by mala-fide intent or human error.

Thus, Compliance Monitoring and Adherence on the Prometheus Protocol is an overarching solution for enabling compliance to both:

1. Regulations and Laws created by jurisdictional legislations
2. Custom regulations for managing and auditing workflows within an Institution

Agnostic

The Data Registry is directly harmonized with the Cross-Border Regulatory Compliance Layer to update the regulatory requirements when required. Once a regulation is created/amended by the jurisdiction's legislature, one of the several 'Compliance and Legal Entities' on the Prometheus Protocol creates its corresponding rule (or rules) via standardized templates. Once this new rule is created, it must achieve consensus via concurring votes from the other Compliance and Legal Entities. If consensus is not achieved, the rule is discarded.

If consensus is achieved, the rule proceeds to the Rules Engine which converts rules into smart contract code. The logic of the smart contract is then deployed on the CBRCL to successfully implement the regulation/amendment within the Prometheus Protocol and it's live instantly.

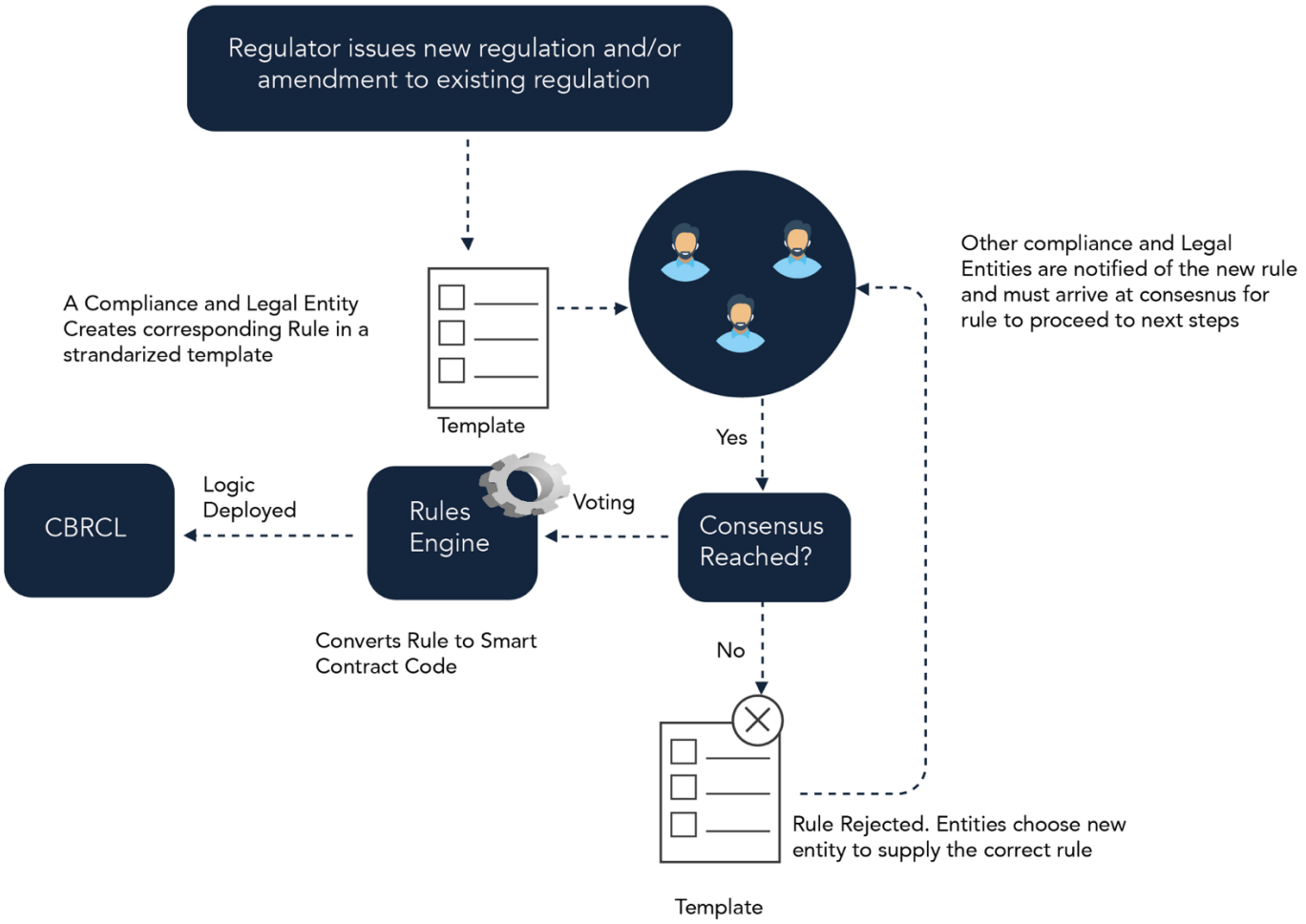

Figure 14: Cross Border Compliance Layer on the Prometheus Protocol

The CBRCL has multiple fail-safe channels of communication with the Data Registry to ensure consonance at all times. For example, if an investor's eligibility status changes or if a transaction is deemed invalid, it can be actioned almost instantly. It will also reflect on the Data Registry. This is a marked departure from the existing traditional siloed systems where such activities can take anywhere between days to months, depending on the jurisdiction in question.

Security Issuance & Lifecycle Layer: Digitization of Assets

Background: Lifecycle of a Security

Securities can be defined as tradable financial assets that have monetary value. The legal definition varies by jurisdiction but broadly speaking a security can be:

- **Bearer** - recognize the holder of the security certificate as the rightful owner. (For example - bearer cheques)

- **Non-certificated** - also known as dematerialized, book-entry or electronic - recognize the entity or individual whose name appears on the security register maintained by the issuer or an intermediary. (For example, equity shares)

Bearer securities are risky in the sense that if you lose it, it's literally "finders' keepers". Additionally, it's harder, if not impossible, to keep track of such a security.

On the other hand, the non-certificated/book-entry securities do not suffer from untraceability, but the trade-off here is that such securities can be traded only within the jurisdiction of the issue *and* with a trusted intermediary entrusted with the task of updating the book entries in case of trades.

These intermediaries are known as **Central Securities Depositories (CSDs)** and simply put they are directly involved in[27]

- the process of issuing securities, by holding issue accounts and handling the initial registration of securities.
- the management of the book-entries (notary service) on behalf of the issuer throughout the life of the security
- the -at least- daily reconciliation of the number of securities in the issue account versus the outstanding number of securities

the access to participants in a given market to invest in securities issued in other jurisdictions through their link to other CSDs.

The entire process above is part of the lifecycle of a security and is replete with multiple trusted entities acting under the supervision of regulatory entities installed by local jurisdictions to ensure compliance with jurisdictional regulations governing the trading of assets.

[27] there are some variations per jurisdiction

The Story of Non-Bankable Assets

Traditionally, assets have been, either liquid (like equities - traded on exchanges) or illiquid/non-bankable (like a painting - buyers and sellers need to find each other, gain each other's trust, involve their lawyers, and only then, can transact).

Book-keeping for non-bankable assets is highly fractured and highly manual leaving it susceptible to human errors, either intended or unintended.

Why Digitization of Assets?

The Prometheus Protocol's approach via its Data Governance Layer, the Cross-Border Regulatory and Compliance Layer, and the Securities Issuance and Lifecycle Management Layer work in tandem to ensure:

- **Simplified and Regulated Trading of Assets across jurisdictions** unlocking markets and opportunities for both issuers and subscribers

- **Simplified Tokenization of Assets** unlocking the potential of bankable and non-bankable assets and entrepreneurs looking to crowdfund against equity, utility, or a combination thereof

What is a Digitized Asset?

The Prometheus Protocol's Securities' Issuance and Lifecycle Management Layer (SILMA) takes traditional securities, non-bankable assets, and other financial innovative products, and converts them into Digitized Assets.

Here's what happens in the background:

In the case of Traditional Securities (such as equities):

Here, a banking institution has taken care of the issuance, underwriting and trading on behalf of the issuer while a depository - CSD takes care of the book-keeping with respect to the transfer of ownership following transactions.

The Banking Institution can leverage the Prometheus Protocol to digitize their securities which automates the compliance of trades to both jurisdiction of the Issue and the jurisdiction of sale.

For CSDs, the book-keeping part becomes automated too while also providing transparency, immutability, and automated compliance validation of both, the eligibility of the counterparties and any additional requirements that the issuer wants to govern trades

For jurisdictions that have digital CSDs, it continues to perform its depository mandate while leveraging the Prometheus Protocol to maintain the registry and ensure compliance. If the jurisdiction does not have digital CSDs, the issuers can install a custodian of choice to perform the depository functions of the digital CSDs for the digitized assets.

In both cases, the Prometheus Protocol allows for the automation of corporate actions, from dividend payments, coupon payments, stock splits all the way to voting, collapsing multiple layers between the end investor and the issuer.

For Non-Bankable Assets and New Issue;

The Prometheus Protocol enables digitization of not only traditional securities but also of other assets that have colloquially been labelled as non-bankable assets because they could never find a large enough number of buyers due to their non fungibility, lack of liquidity and related costs.

First, the issuer figuratively divides the non-bankable asset into smaller and cheaper digitized (tokenized) securities and then sells ownership, legal rights, or a combination thereof to the eligible buyers.

Tokenization practically increases the number of potential buyers by making the newly created security (backed by the non-bankable asset) fungible and affordable to a larger number of individuals.

The Prometheus Protocol enables issuers to file term sheets, prospectuses, and cap tables, etc. securely and without the need to print on paper, to the regulatory bodies governing the new Issue.

On successful filing, the Asset Registry is populated with the new digitized asset and the rules governing trades, eligibility of counterparties, and other issuer-specific rules are encoded into smart contract logics that perform eligibility checks before allowing trades to proceed.

Here too, the digital CSDs (if present), act as depositories and if not present, the Prometheus Protocol possesses the capabilities to enable the installation of a suitable and verified entity to act as the custodian to perform the activities of the digital CSDs in its absence.

Technical Architecture

Actors within the Prometheus Protocol

The Prometheus Protocol connects all stakeholders in the issuance and data governance space comprehensively. The actors are:

1. **Financial Institutions** - are banks, private banks, asset management companies, etc, that wish to conduct tokenized issuance or access unbankable assets etc. in a completely regulated manner and foster faster and safer communications within their branches and consortiums. Their *key requirements* - speed, costs, security, and compliance to facilitate a smoother experience for their customers

2. **Data Processors** - are entities that collect, collate, process, manage, and/or store the data collected at various entry points of the financial ecosystems. Their *key requirements* - clarity in terms of data governance and data privacy laws so that they may adhere to them properly.

3. **Legal and Compliance Entities** - are entities tasked with the mandate to oversee the compliance to financial and legal regulations laid down by the government and regulatory bodies. Their *key requirements* - ensure adherence to regulations and modify them as per the law of the land to prevent nefarious activities such as terror financing and money laundering.

4. **Book-keeping Entities** - are essential infrastructure for the proper functioning and security of financial markets and are entities such as depositories and digital custodians that maintain authentic records of transactions between parties and a history of legal ownership over the assets held by them in trust. Their *key requirements* - Faster arrival of transactional data in a standardized manner to expedite transfers of ownership of assets while ensuring the integrity of the issue.

5. **Technology Provisioning Entities** - are service and product providers that enable secure communication and transfer of information between the stakeholders. Their *key requirements* - a standardized protocol/framework of rules and requirements to help them flesh out their best practices.

6. **Issuer-Investor Entities** - are the issuers and subscribers of the digitized asset and are the key actors around which the remaining actors are arranged. Their *key requirements* - hassle-free transaction of business with faster processing times and cheaper transaction costs.

Functional Components - Definitions and Roles

Component	Definition	Functional Designing
Data Registry	Single entity implemented on DLT for immutable and decentralized storage to provide resilience and ownership.	Tracks and regulates access to user data and transaction data. Data once entered by its owner and validated by regulated third parties become immutable. Data owner can grant/revoke access to their data, as well as, expunge it from the Data Registry.
Regulatory services	Regulate the capacity of all users to enter into transactions. The governing regulatory rule for each transaction is determined by multiple variables (underlying security, jurisdiction, type of user etc…) The value of the variables is accessed through the Data Registry.	Are multiple third-party solutions plugging into the Prometheus Protocol to implement and update regulations while integrating with the Data Registry for source of truth of Client and Transaction Data. Regulatory Services can be implemented as: 1. Blockchain services within the local network of the Data Registry 2. Blockchain services in other networks via cross-chain integrations 3. Off-chain services integration via oracles.
Securities	Represent digitized (for those using a traditional CSD) or tokenized (for those using a digital CSD) securities. Are regulated by the Regulatory Service and recorded in the Data Registry.	Securities are independent smart contracts extending existing tokenization functionalities to integrate with Regulatory Services and the Data Registry. In Ethereum-compatible networks this means a smart contract extending ERC20, but for other Blockchain networks or off-chain platforms other implementations are expected.
Issuance	To create new digitized or tokenized securities following standard financial processes. Subscription to an issuance is regulated by the Regulatory Service and recorded in the Data Registry.	Multiple issuance platforms can coexist within the Prometheus Protocol and are integrated to the Data Registry and Regulatory Services. They can digitize or tokenize securities within the Prometheus Protocol's compliant regulatory environment.
Market	To enable secondary trade in Securities. Trades are regulated by the Regulatory Service and recorded on the Data Registry.	Multiple markets can coexist integrated with the Data Registry and Regulatory Service. Both centralized markets (with an off-chain component) and fully decentralized markets can plug in to the Prometheus Protocol for full traceability of transactions and compliance of all trades with relevant regulatory bodies.

Figure 15: Definitions and Roles of Prometheus Protocol Components

Inter-Component Communications

Traceability of Transactions and User Data

The primary function of the Data Registry is to track all *state changes* of all components integrated to the Prometheus Protocol. For DLT components this is achieved by following the principle – **All State Changes Shall Emit an Event**[28]. The Prometheus Protocol extracts these events into a user-friendly database where they can be queried.

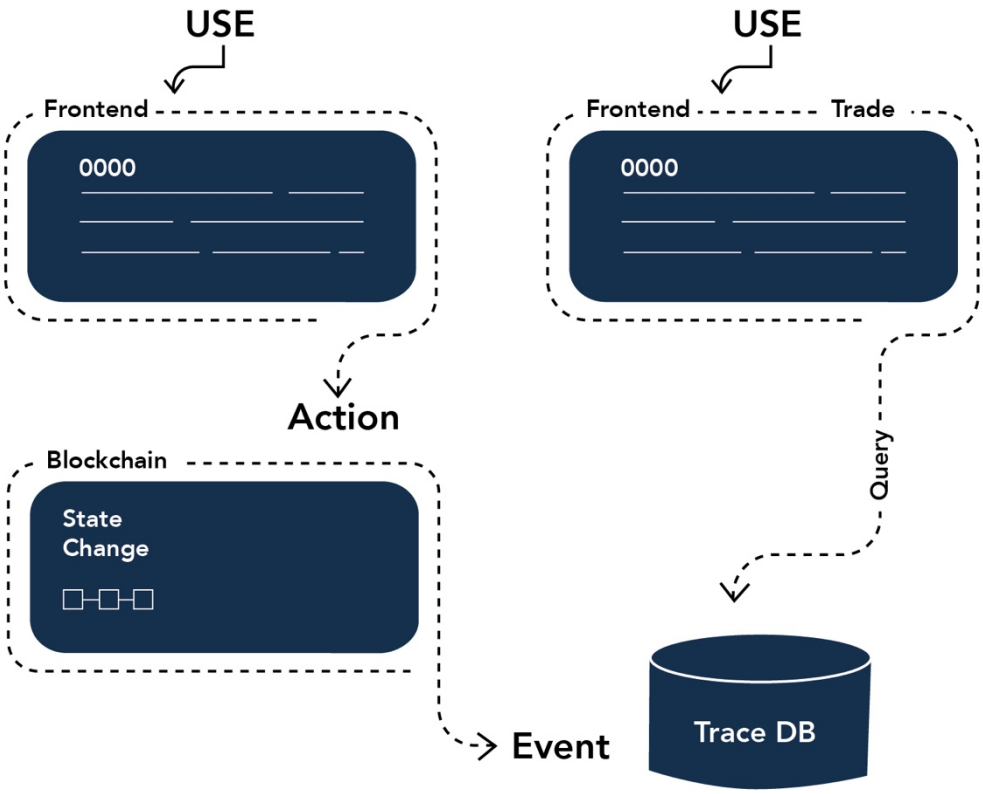

Figure 16: Traceability of Transactions and User Data Flow

For components on the same consortium but different Blockchain, an **Oracle** interface is implemented to allow them to record their state changes via a simple contract that will generate events with the information to be tracked.

[28] Events are recorded in the Blockchain as a default feature of all Ethereum-compatible networks,

Encrypted Storage of Users' Legal Documents

The first step towards automated validation of user data across borders and jurisdictions on the Prometheus Protocol is the secure upload and encrypted storage of a user's legal documents followed by their validation by Legal and Compliance Entities.

All verified documents are recorded in the data registry – decentralized storage (for public systems) and private clouds (for permissioned systems) for future reference.

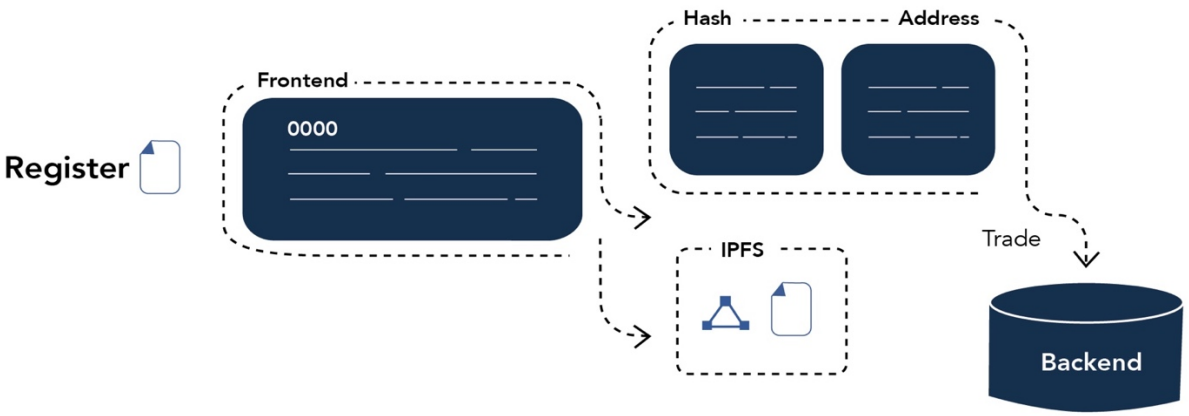

Figure 17: Encrypted Storage of Users' Data Flow

During the upload to the Data Registry, key identifier attributes of the legal documents are appended to its hash (as a trace identifying pattern) to enable downstream traceability at all times such as:

- Was the document uploaded?
- When was the document uploaded?
- Who is/was the document attributed to?
- Who uploaded the document?

Due to the trace identifying pattern, multiple Legal and Compliance Entities can verify the validity of the legal documents via zk STARK (with zero-knowledge proof), simultaneously or in succession.

Document Verification Status Validation

To verify submitted documents, its hash is calculated, and the database is queried. This database is a continuously synced replica of Blockchain events corresponding to the hashes of the user data and transaction data on the Prometheus Protocol.

If the submitted documents' hash gets a positive match, it is an indication that the submitted document has already been validated and was found compliant to the applicable regulatory frameworks.

If the submitted documents' hash does not match, the Prometheus Protocol will highlight on what basis it has been rejected, redirect them to the registration flow of the institution or end the flow.

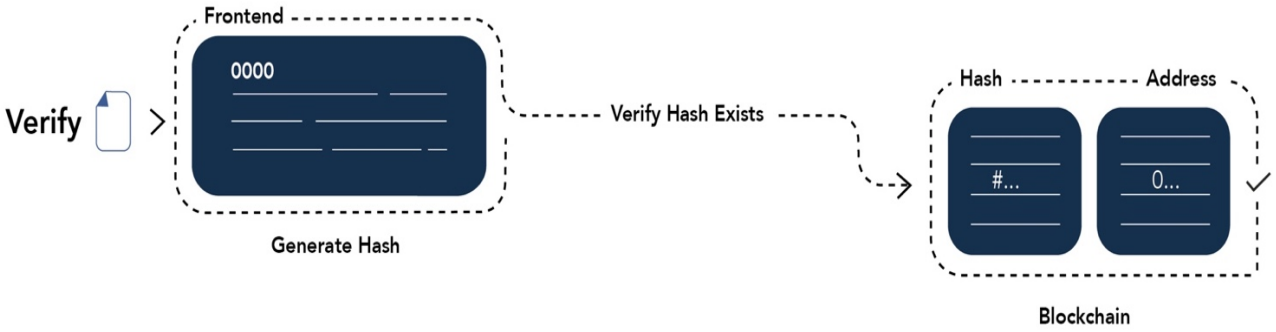

Figure 18: Document Verification Validation Flow

If the user data changes, for example, a change in the permanent residence of the user, this needs to be updated in their legal documents and similarly updated in the data registry on the Prometheus Protocol. For this, the user needs to send their new legal documents for re-verification and validation.

These new legal documents update the user's status with the new information while preserving the traceability of the user data from the latest version to the oldest version that was uploaded first on the Prometheus Protocol.

User Validation

All actors in the Prometheus Protocol are recorded in a hierarchical and dynamic Blockchain structure that identifies them as authorized to perform specific actions on specific functions.

An authorized operator can update the profile of any user and change its user profile. These changes are only effective after being checked for compliance with the pertaining regulatory processes.

The **Permissions Hierarchy** is dynamic. New users and securities categories can be created by authorized operators. Existing or new rules will then apply to these new categories based on existing regulatory processes.

As for any other *state change* in the Prometheus Protocol, all operations that result in a change for the profile of any actor are recorded in the Data Registry and can be queried.

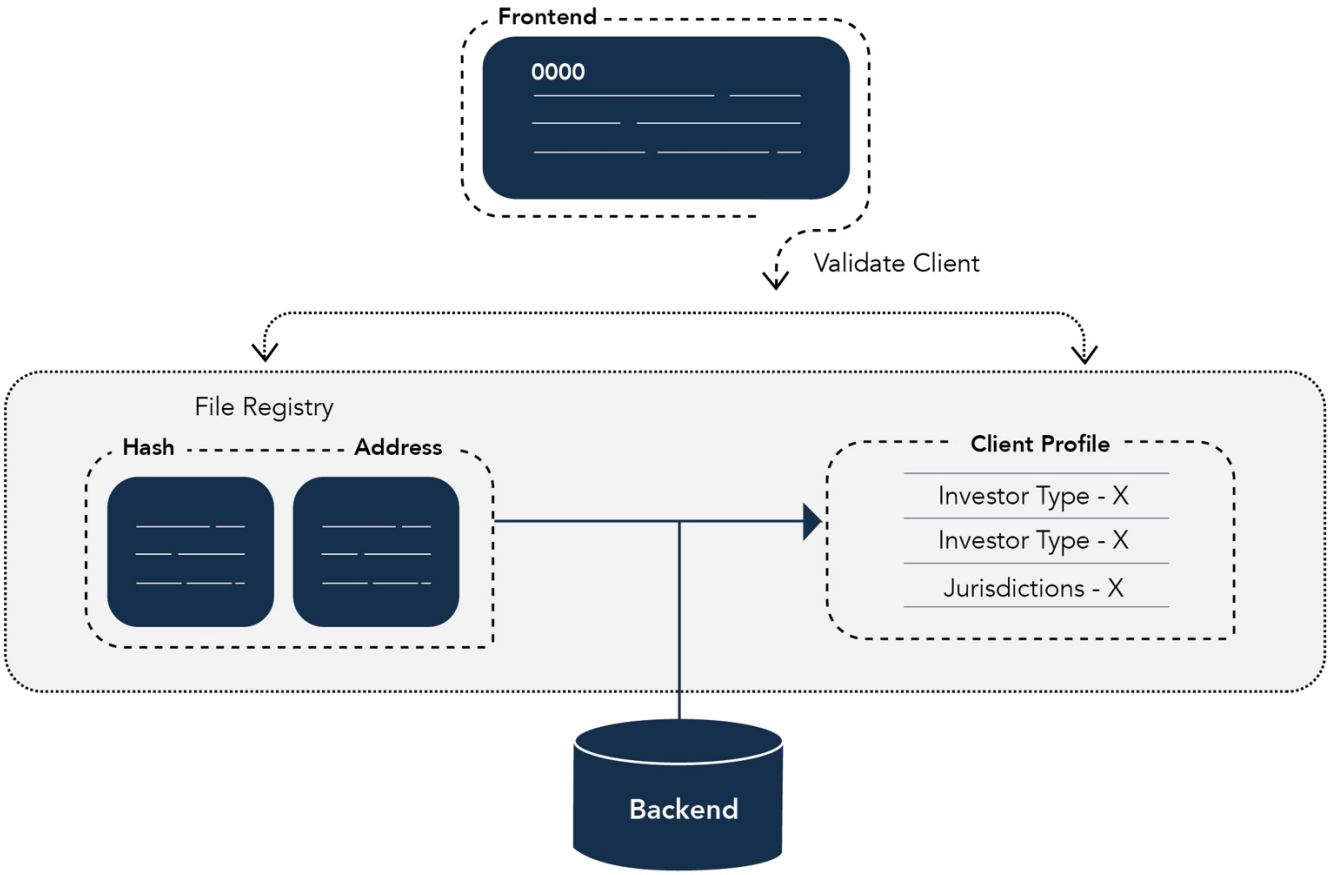

Figure 19: User Validation Flow

Regulatory and Compliance Services

Every security on the Prometheus protocol is associated with at least one regulatory service and any state change generated with respect to that security is subject to the consequence of the regulatory service's rules.

The CBRCL sits upstream of the transactions, therefore all of the rules are applied upstream. Meaning, the regulatory service pre-matches the profiles of all transacting counterparties against its own internal rules as well as other conditions that need to be met. This allows for checks to be done pre-trade and in layman's term it means users can only access transactions/actions that corresponds to their profile. The CBRCL will automatically grey out and deny access to transactions/actions that do not comply with the following:

1. Rules governing the eligibility of transacting counterparties
2. Rules created to govern transactions

It is only after both these regulatory checks that the transaction/action will be available to the investor, and once processed, will be committed to the Data Registry.

For example, if during an issuance, the regulatory service governing the ownership of the issued security has an embedded rule that citizens of country X cannot own these securities; all citizens of country X will be able to see (greyed out) but not access any of these securities.
If the investor is not a resident of country X, the transaction will be actionable and once it proceeds, will emit a Blockchain event (assuming that there are no other regulatory rules). In a real-world scenario, there will be multiple regulatory rules that will need to be activated to ensure compliance with the jurisdiction of the issuer and that of the investor.

Regulatory Services can be third party modules implemented and maintained by specialized parties. As regulations change, the regulatory services are updated with immediate effect on subsequent transactions.

Schematic Representation – Proof of Concept

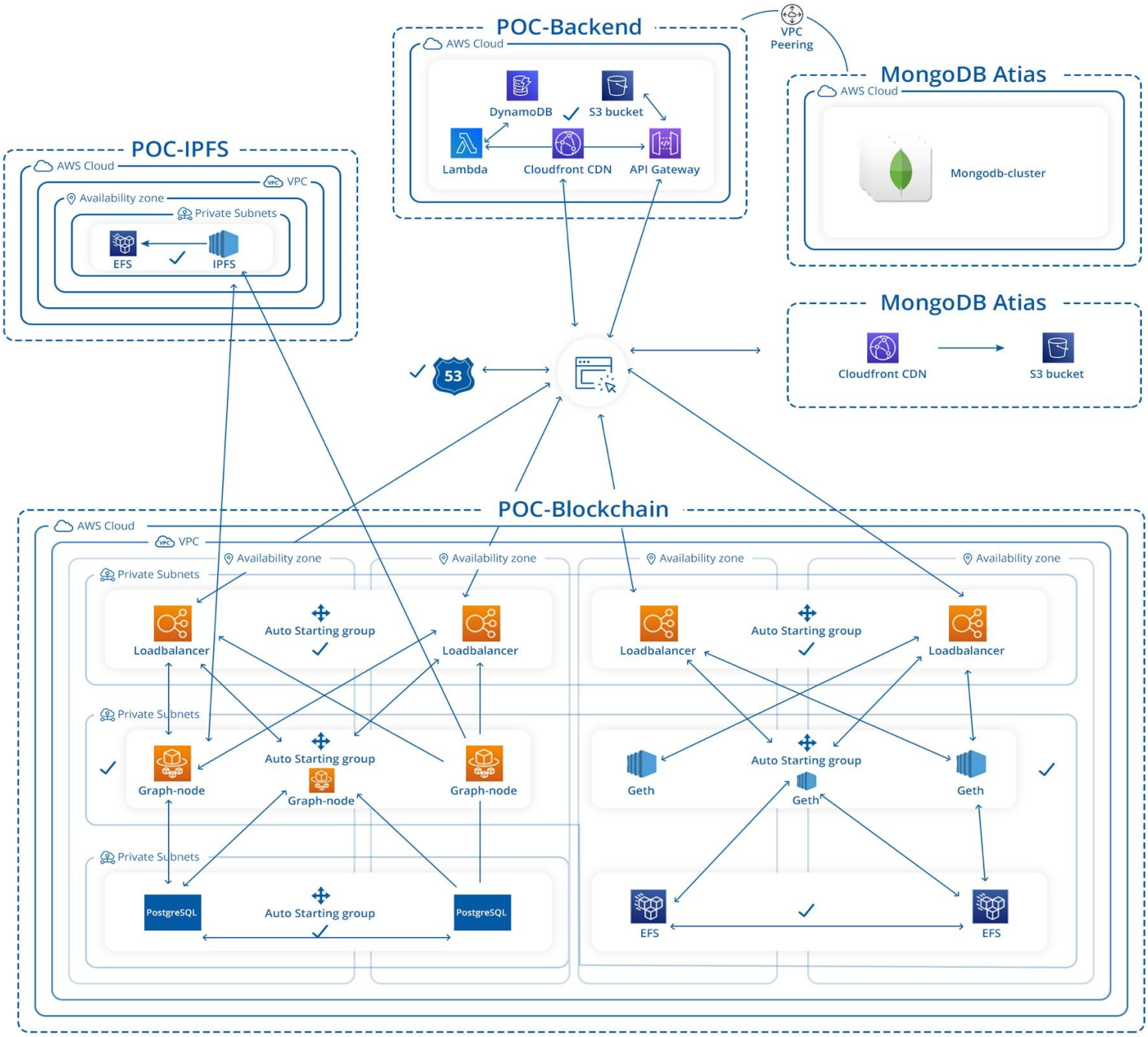

Figure 20: Prometheus Protocol - PoC Architecture (Detailed)

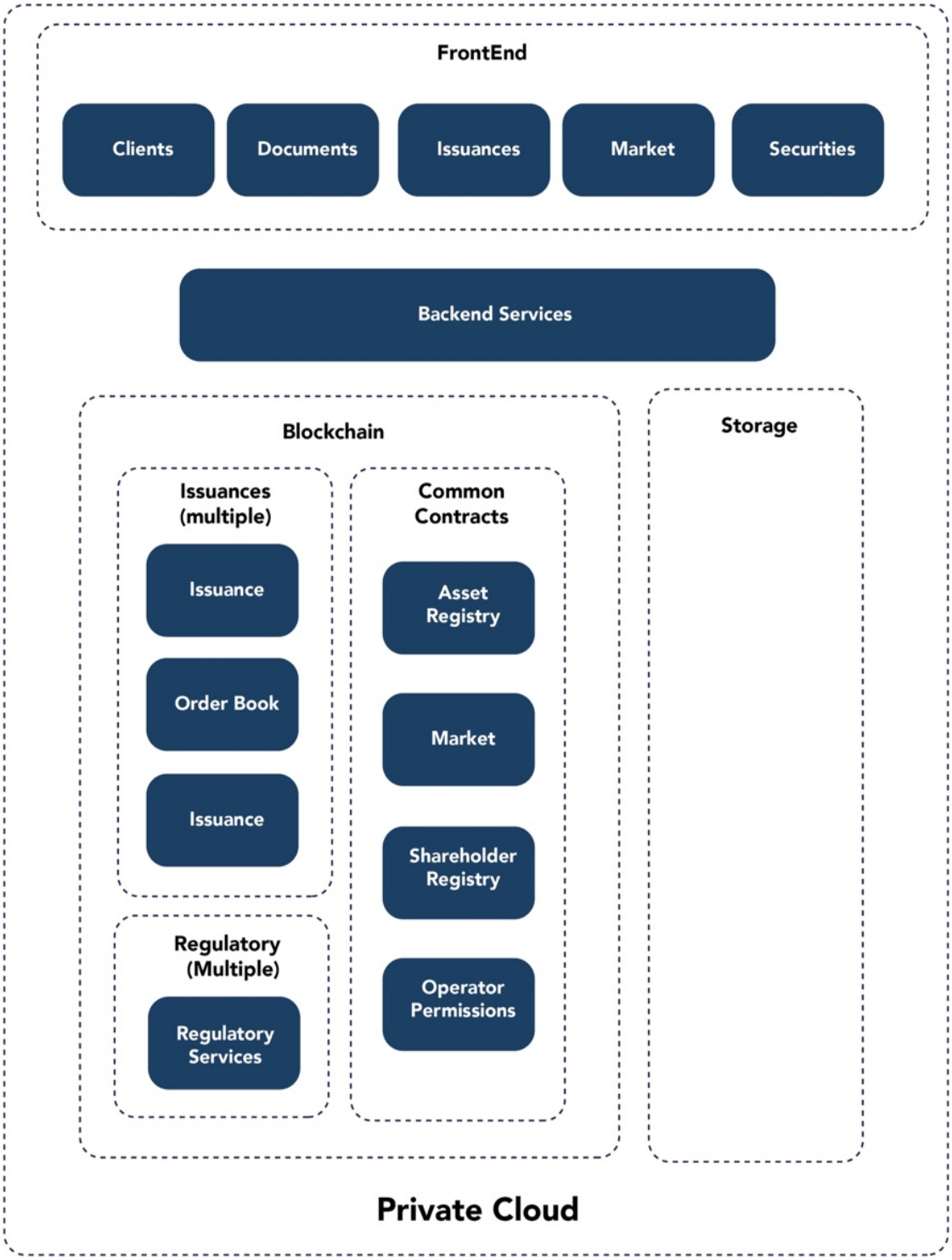

Figure 21: Prometheus Protocol - PoC Architecture (Overview)

Contract Architecture - Proof of Concept

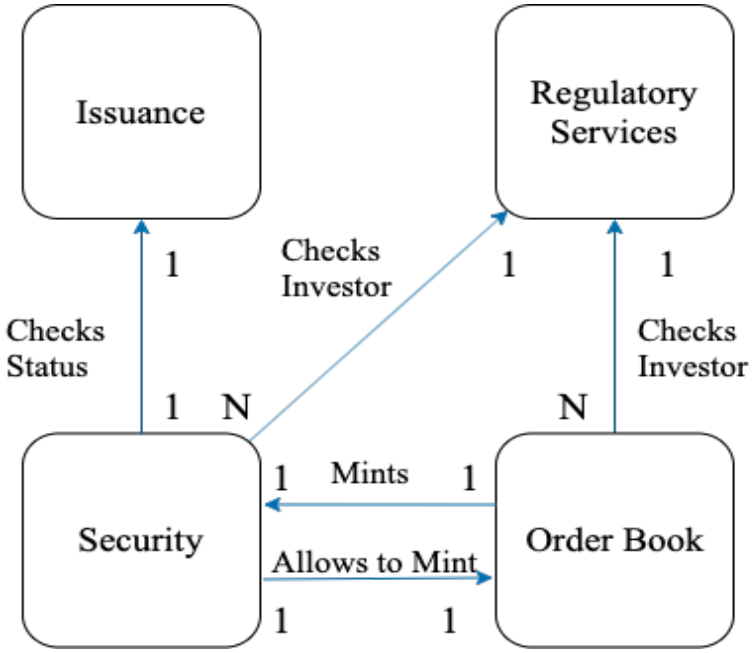

Figure 22: Issuance Process

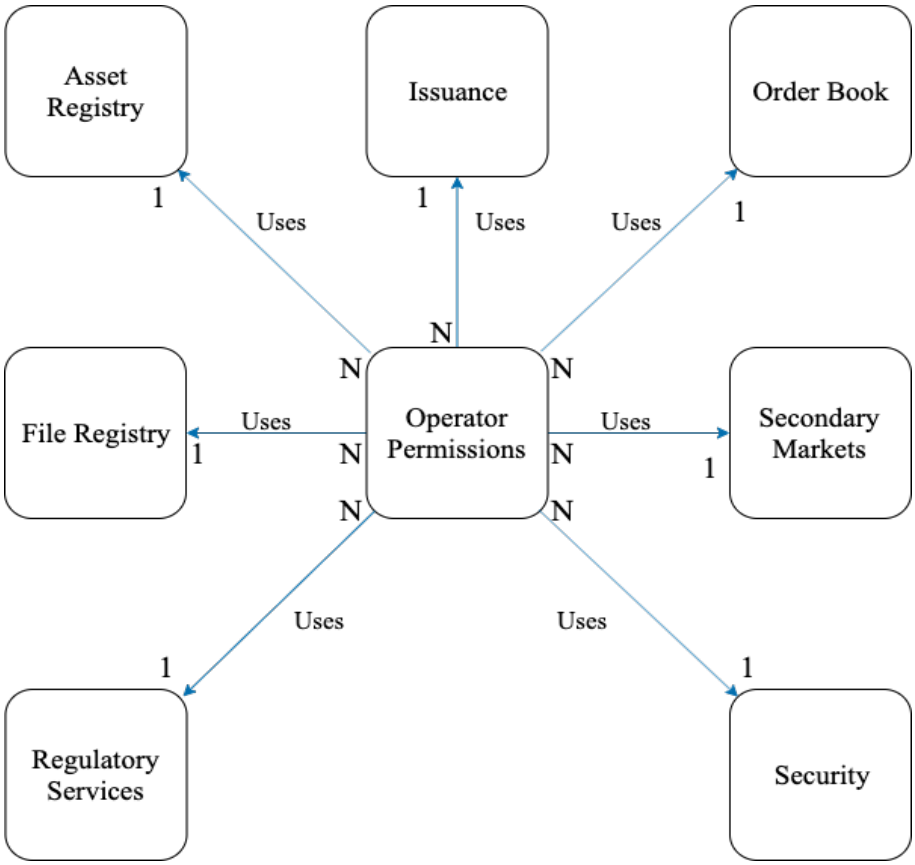

Figure 23: Operator Permissions

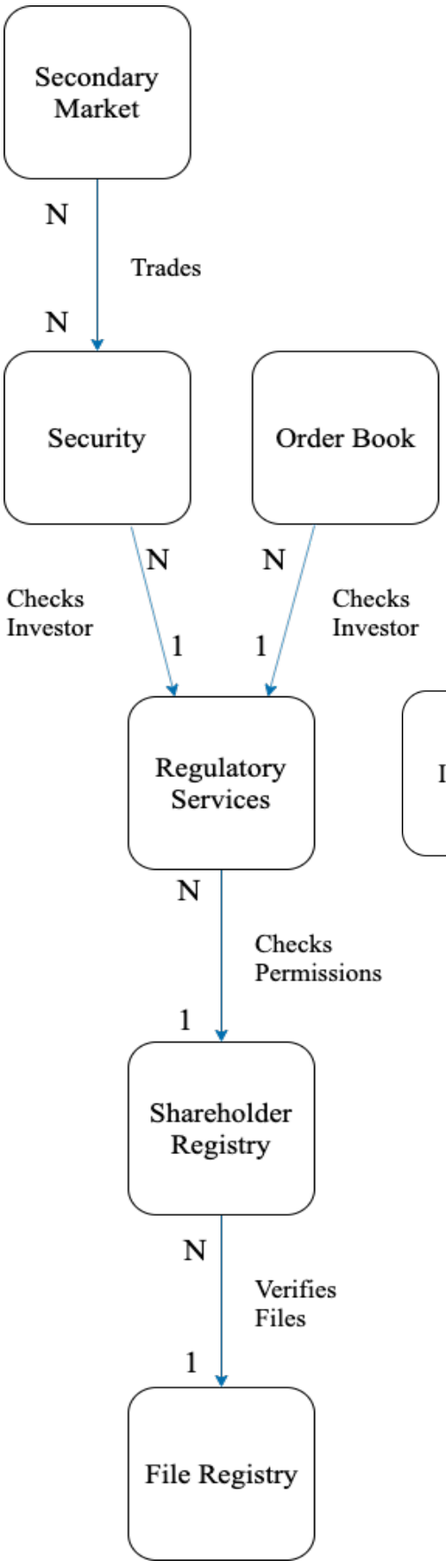

Figure 24: Shareholder Registry

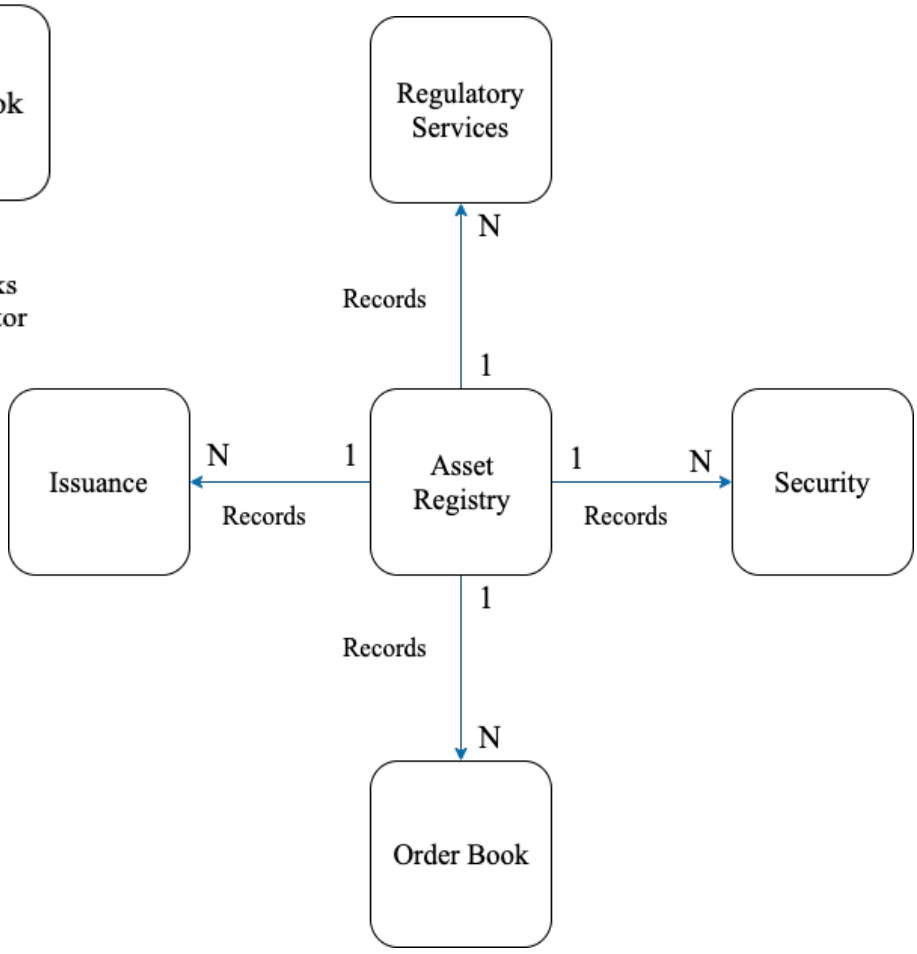

Figure 25: Issuance Registry

On-Chain - Off-Chain Data Split

	Purpose	On-Chain	Off- Chain
Operator Permissions	Manage System Permissions	Role Ids Account => Role	Role Description Account Details
File Registry	Manage File Registrations	Document Hash => Account	Document Details
Shareholder Registry	Manage Regulatory Permissions	Role IDs Account => Role (Account => Role) => Document	Role Description Account Details
Regulatory Service	Third Party Rules	Role Ids	Nothing
ERC20	Currency Features	Account => Balance	Nothing
Security	Security Features	Security Parameters Transaction Data	Nothing
Order Book	Pre-Issuance Investing	Investing Parameters Regulatory Service Contract Address Account => Commitment	Nothing
Issuance	Issuance Data and Flow	Issuance Parameters Investing Parameters Security Parameters Issuance Data Hashes Investing Data Hashes Security Data Hashes	Issuance Data Investing Data Securities Data
Assest Registry	Issuance Factory	Issuance Contract Addresses	Nothing
Secondary Market	Security Market	Security Contract Addresses Account => Trade	Nothing

Figure 26: On-Chain - Off-Chain Data Split

Use Cases

A Regulated Securities Offering

- **Issuance Commencement**

The issuer creates the proposal and undergoes regulatory compliance for approval by the regulators from within the protocol itself. If the jurisdiction of the issuer has a digital CSD, the security is issued in the digital CSD while a concurrent entry into both the *Shareholder Register and Asset Registry* are created.

All transactions pertaining to this asset will be captured within the *Asset Registry*. Both, the issuer and the compliance entities have read access to the *Asset Registry.*

If the jurisdiction of the issuer does not offer a digital CSD, the Prometheus Protocol will enable a communication channel between:

- the traditional CSD
- the digital custodian
- the *Asset Registry,*
- the regulatory-compliance entities
- the issuer, and;
- the investors

to directly facilitate the updating of the status of the security's ownership (in case of jurisdictions that have traditional CSDs), a digital custodian is required.

- **Whitelisting of Potential Subscribers and KYC**

Central to secure data governance on the Prometheus Protocol is the *Data Registry* that contains encrypted statuses of the KYC, the users' legal documents, and compliance details of the users registered on the Protocol.

The validation of these data is done via consensus among a set of KYC providers. Institutions, while onboarding customers perform KYC. Directly committing this data to the data registry is fraught with certain hazards, namely:

1. Data pollution and duplication that could arise due to minor spelling diversions
2. Entities might not be open to accepting KYC verification by other entities as it might expose them to potential liabilities.

Thus, on the Prometheus Protocol, the commitment of user statuses such as KYC/AML/KYB/DD etc to the Data Registry is subject to consensus among the KYC and verification entities. The data processing agencies such as the KYC and verification entities become such operators by fulfilling the conditions and requirements set forth by regulators, participating entities (such as banks), and other data processing agencies on the Prometheus Protocol.

However participating entities such as banks can pre-approve validators/providers but also invalidate them based on their internal requirements, banks will provide a DNC (Do Not Comply) list with validators/providers that do not match their internal requirements. In this case, if approval is reached by the majority of the validators/providers while all these validators/providers are on the DNC list of a certain bank for example, this particular KYC for this particular bank will be considered not valid.

Users can download their records maintained on the *Data Registry* and can even request its complete deletion, should they wish to unenroll themselves. The obvious benefit of the Prometheus Protocol to the user is that if he/she wishes to conduct business with another bank, the new bank will not have to perform the entire KYC process again. *(Keeping in mind the DNC list for each bank)*

The new bank, if a member of the Prometheus Protocol, can query the *Data Registry* via the *Role-Based Access Control* mechanism and receive the result of that user's KYC status. This makes KYC verification – faster, cheaper, and less prone to data mismanagement, either accidentally deliberately.

The onboarding of the investors, after KYC/AML/DD/KYB, is again verified against the Cross-Border Regulatory Compliance Layer to ensure compliance with the issuer and investor's jurisdictional regulations.

The modification of the rules governing transactions on the CBRCL are conditional to consensus of a multiplicity of Legal Trusted Entities. Once consensus is reached, the modification/addition is committed to the "Rules Engine" which is then converted to Smart Contract Code and the logic deployed to the CBRCL.

Simultaneously, on the issuer side, once the Legal Trusted Entities prepare the term sheets, cap tables, prospectuses and other relevant information, the issuance is triggered only after a concurrent green light from the CBRCL. This entire step is digitized and does not require any filings to be done via paper submissions.

These double checks with the Cross-Border Regulatory Compliance Layer ensure that issuers, investors, and other stakeholders are compliant right before, during, and after the issuance process.

- **Investing in Issued Securities**

Once the proposal has been accepted and its records created in the *Asset Registry* and *Shareholder Register,* the eligible investors will be able to view the available investment opportunities on their devices and can proceed to the next steps via the app itself.

If an investor not registered on the Prometheus Protocol wishes to subscribe to the offered security, they can get their KYC status verified by the *trusted entities* within the Prometheus Protocol.

Once verified, the new potential investor's KYC data is added securely to the *Data Registry* in an encrypted manner from where the issuer can verify their KYC status via the *Role-Based Access Control* mechanism.

The Cross-Border Regulatory Compliance Layer is also the driving regulatory compliance check over the digitized securities environment that includes the digitized securities themselves, exchanges, CSDs, Digital CSDs, and Digital Custodians.

The digitized securities' ownership records and their corporate actionable items are stored on the Data Registry and are updated only after concurrence with the Cross-Border Regulatory Compliance Layer.

- **Secondary Trading of Securities**

The completion of a trade on an Alternate Trading Systems (ATSs) or Securities' Trading Platforms will automatically change the ownership of the digitized security to the new owner and automatically update the shareholder register in the digital CSD.

For traditional CSDs, we are partnering with various CSDs in order to seamlessly allow them to update their registers.

- **Corporate Actions**

Corporate actions processing has long been plagued by inefficiencies and has been written off as multiple complex processes that are unsystematic, abstruse and difficult to automate. One of the reasons has been the multitude of intermediaries sitting between an issuer and its investors. The Prometheus Protocol aims to create more standardized and automated corporate actions. These include dividend payments, coupon payments, withholding taxes, voting, stock split, stock buyback etc. To activate a corporate action such as dividend distribution etc, the issuer sends the instruction via the app which performs a concurrence check with the Cross-Border Regulatory Compliance Layer and the digitized securities environment.

Once everything checks out, digitized securities environment connects to the Shareholder Register and the Data Registry to give effect to the corporate actions by providing direct transfer of funds and/or instructions from the issuer to the investor and vice versa.

The Prometheus Protocol ensures that despite trustless networks and the litany of financial institutions in the fray, the corporate actions are straightforward encrypted private conversations or instructions between the issuers and their subscribers.

- **Legal Recourse Mechanism Layer (LRML)**

As previously described, the CBRCL pre-checks any trade or transaction, meaning that no trade or action can go through if it doesn't comply with its respective regulatory requirements.

However, as an added safeguard and in case regulations or client status changes unexpectedly, or even in case of a genuine erroneous mistake (with no losses to the other party) trades that can be deemed invalid and can be easily reversed on the Prometheus Protocol by regulator-driven action.

Once a member of the Regulatory Service deems a transaction invalid, the trusted legal-regulatory entity or Regulatory Services' representative on the Prometheus Protocol or the Issuer can request the reversal of the transaction and *status quo ante* is restored.

This prevents mistaken trades from causing loss to the investor while also ensuring compliance with the AML norms as subscribed to and interpreted by the respective regulators.

Figure 27: A Regulated Issuance on the Prometheus Protocol

Consortia for Private Banks and Wealth Managers

Prometheus Protocol enables large consortiums such as those comprised of Private Banks and Wealth Managers, to create permissioned channels to foster lightning-fast and tamper-proof data flow, trading and communication.

These private communication channels enable internally transparent, auditable, and access-controlled transaction of business; as opposed to the opaque flows that plague the traditional system.

Such permissioned networks have their own data registries and 'trusted entities' entrusted with the responsibility of enforcing the regulations of the issuer entity. The data registries are the one true repository of all validated user data and issuance data) within their consortia.

The issuing entity can also implement *global* rules for the consortium to expedite the compliance with the issuing entity's internal compliance protocols and/or to the delegated authority. The trusted entities ensure compliance to the *global* rules of business decided upon by the consortium members.

It is pertinent to note here that the customization of rules of business can only function under the CBRCL overall regulatory framework that is backed up by an effective legal system and supporting institutions[29].

The internal rules' implementation is subject to compliance with the CBRCL because its compliance with regulation is not just external, but also internal. Issuers can obviously create additional compliance requirements for their issues. But these are restricted to just that issue and may have no bearing on other issues by other issuers.

The Prometheus Protocol allows for flexibility in terms of access, degree of access, and the addition of additional entities such as Legal Recourse Mechanism Layer, arbitration, and mediation, to name a few.

[29] https://www.bis.org/publ/work811.pdf

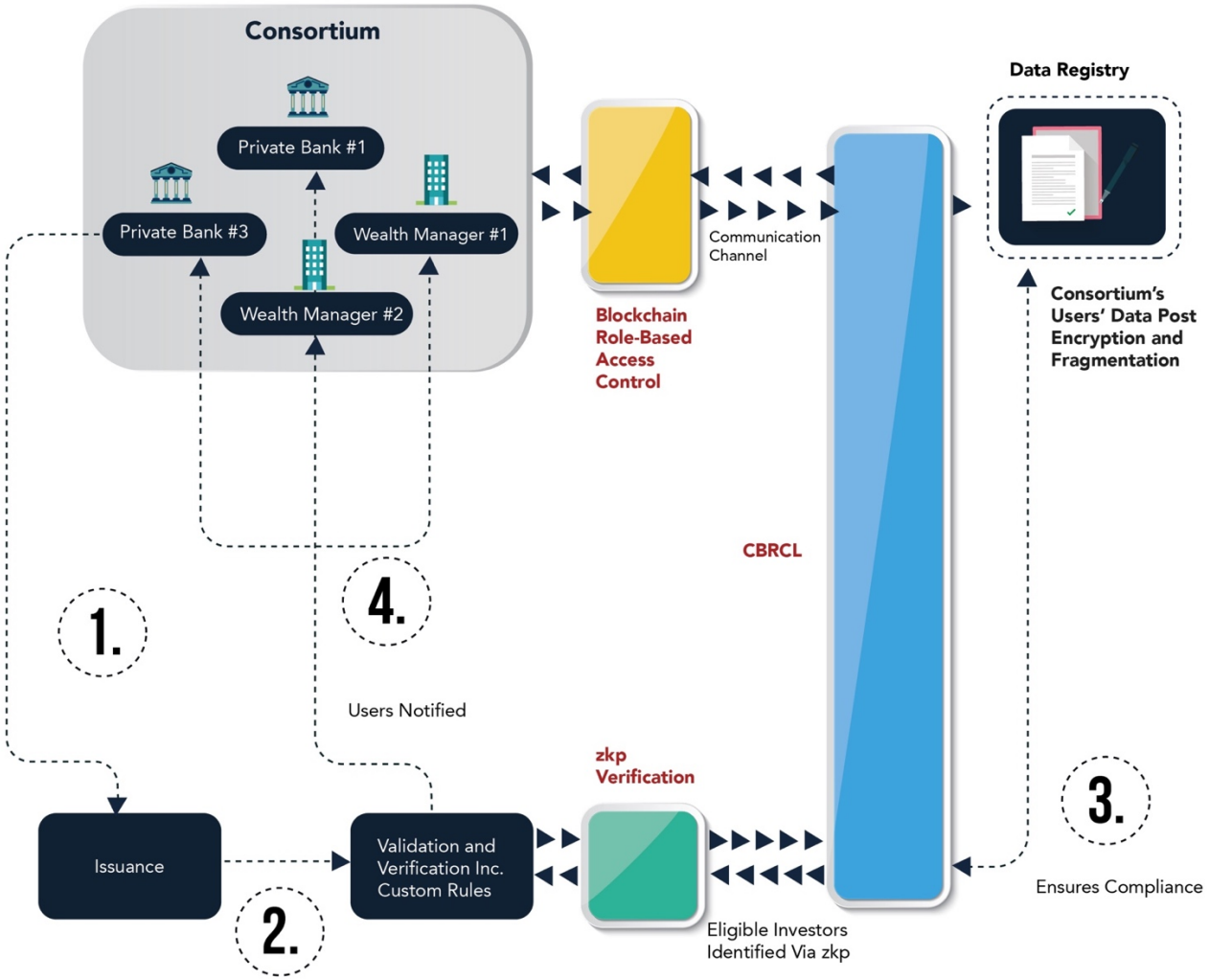

Figure 28: Flow in Consortia of Private Banks, Wealth Managers etc.

Consolidated Reporting of Financial Exposure for Regulation

Data gaps are the inevitable price paid by financial institutions as they seek to keep the costs of compliance within limits. But the cost of such gaps can be devastating, as the snowball effect of the collapse of Lehman Brothers in 2008 showed.

At the time, the worlds' major financial institutions were not able to compute their consolidated exposure to the many subsidiaries of Lehman, so that "what would have been systemic risk morphed into systemic uncertainty" (Haldane et al (2015).

For example, Citibank, a multinational bank, faced a lot of criticism from a section of the regulators and the public due to its troubles with consolidated reporting of its financial exposure. Here, the problem was two-fold:

1. Regulators were unaware of Citibank's financial exposure
2. Citibank had trouble consolidating this data due to its large sprawl

The Prometheus Protocol offers such financial institutions and institutional consortia the ability to place consortium-wide or a tiered financial exposure rules to minimize systemic risks. Non-adherence to these financial exposure limits is flagged and the relevant entity and/or the supervisory entity is notified of the flag.

Compliance-checks, consolidations, and even reporting becomes easier due to large-scale automation and easy verification, tabulation, and rectification by leveraging the data registry. Consolidated Reporting on the Prometheus Protocol is also fully compliant to local jurisdictions' regulations such as MiFID II, Basel 3, etc

In a multinational setting, such as in the example of Citibank, the Prometheus Protocol's CBRCL (cross-border regulatory and compliance layer) ensures that all three, namely:

1. The transacting counterparties
2. The Asset being transferred
3. The transaction itself

are compliant at all points of time with successful-transaction-triggered Blockchain event serving as the trusted reference over trustless networks. This reporting of an institution's aggregated financial exposures to the supervisor does not require entities to disclose its underlying individual transactions (data privacy compliance).

A Truly Compliant Open Finance Solution

Open Finance is the next logical step to Open Banking[30] which enables the use of open APIs for third-party developers to develop apps and services leveraging a financial institution. Open Finance envisages leveraging multiple financial institutions in multiple jurisdictions. *The Prometheus Protocol is a pioneer in Open Finance.*

The investor data is stored post-encryption on the decentralized data registry and its hash (also acting as the key of the key-value pair) is stored not only in the data registry but also on the user's devices. If the investor wishes to grant access to their information to any third-party entity, they simply need to share their access key with the entity.The entity will then leverage the Prometheus Protocol's API to query for the user data which will be provided post a successful check by the Role-Based Access Control Mechanism (RBAC) of the Prometheus Protocol. The entity shall prove its compliance, as well as, its requirement of the user data, to gain access to the user data.

This secondary check by the Prometheus Protocol's RBAC ensures that the user is protected by phishing, hacking, and honey potting attacks from nefarious actors. Even if the nefarious actors gain unauthorized access to the investor's hash, they'll be prevented from using it to unlock the user's data by the RBAC. Since such actors do not possess qualifying credentials (for e.g. *private key*), they'll be denied access to the investor's data.

Access to investor data via APIs across jurisdictions will involve a tertiary but automated verification of the requesting entity's credentials by the Cross-Border Compliance Layer of the Prometheus Protocol for compliance to the following two jurisdictions:

1. Jurisdiction of the Investor
2. Jurisdiction of the Requesting Entity

Thus, the strict adherence to data governance and compliance regulations coupled with technological advancement enables the Prometheus Protocol to provide Open Finance in its undiluted form - *across jurisdictions and entities.*

The Prometheus Protocol's APIs will be amongst the pioneers in the open finance space and will enable wider access to partnered institutions to develop their own apps. These apps can enable not just banking and financial institutions, but also other service provisioning companies to develop innovative solutions such as a single app to manage all bank accounts on partnered institutions.

[30] https://en.wikipedia.org/wiki/Payment_Services_Directive

Embedded Data Traceability and Tokenized Content Management

In an age where fake news is at the forefront of our social media and more and more so traditional media, data traceability on the Prometheus Protocol can enable a simplified implementation mechanism for data creators such as writing agencies, individual bloggers, and news processing companies to tokenize their content and achieve end-to-end visibility into data quality.

This is achieved on the Prometheus Protocol by hashing the content piece and appending the creator's public key to it for verification. The hash of this amalgamation is stored on the decentralized data registry and also on the data wallets of the content creators.

The content creators can go a step further and tokenize the entire content piece directly from their devices. Therefore, every time this content piece is referenced, downloaded, and/or processed for elucidation, tokens are generated and appended to these secondary works, acting as the tenets of data traceability.

In the event of a data piece being modified or a third party is interested in looking up the data source, the indexed token-driven architecture allows complete visibility from any given point to the point of provenance i.e. the content creator. Its immutable traceability constitutes proof of the data's authenticity.

If the data is tampered with, let's say, by a blogger who misunderstood some of the content within a tokenized content piece on the Prometheus Protocol and changes a figure, effectively rewriting it. In this case, the token generated at this blogger's data wallet will represent a fork away from the line of data traceability and act as the proof of divergence from the original piece.

Thus, this modified data is automatically and transparently flagged as a deviation/modification of the original piece. This flag is also appended to the future transmissions of this modified piece so that the recipients downwards are notified of its modified status without having to depend on third-party centralized fact-checking organizations but be notified automatically by the Prometheus Protocol itself.

Writing Agencies such as satire magazines that routinely process news for their purposes can be granted special flags that notify the recipients downstream of its modified status, for satire, so that readers understand that it is not fake news per se.

The Team Behind the Prometheus Protocol

Executive and Management Team

Rachid Ajaja
(Co-Founder)

Rachid is a serial entrepreneur with an obsession for modelling, analytics development, quantitative analysis and data science. For the last decade, he has been developing and implementing models and methodologies to help organizations with forecasting and risk management. In 2017, he completed the building and deployment of a highly scalable deep learning models in artificial intelligence applied to computer vision. His impressive work received accolades from VINCI which commissioned him to help orchestrating the ambitious “smart highways and smart cities” project, combining AI and Blockchain. He holds an engineering degree in Computer Science and Signal Processing, and a Masters degree in Probability Theory, Stochastic Process and Quantitative Finance.

I. N. Amber Ghaddar, PhD
(Co-Founder)

Before co-founding AllianceBlock, Amber was a fixed-income trader at JP Morgan in London. She started her career in Global Investment Research at Goldman Sachs and moved from there to the Cross Asset Solution team at JP Morgan in 2012, where she worked on structured and exotic products across Equities, FX, Rates, Credit and Commodities. During this time she build the JP Morgan UK MultiAsset franchise. Later, she spearheaded the Macro Systematic Strategies effort at JP Morgan, focusing on dynamic risk premia trading strategies. She is one of the masterminds behind Participative Capitalism and has been invited to various events and universities to give talks on the subject. She graduated from HEC in 2011 with a Masters in International Risk Management. Previously, she spent most of her early career in Neurophysiology and Nanotechnologies. She obtained her B.Sc in Science & Technology from McGill University in Canada, graduated with two masters (Neurosciences and Microelectronics & Nanotechnologies) from Universite Aix-Marseille in France and read for a PhD in Molecular Medicine at Vita Salute in Italy.

Matthijs De Vries
(Co-Founder)

Matthijs has managed the product development of one of the largest Dutch companies: PostNL. There, he was responsible for several software development departments and related departments in order to lead an entire software development chain before switching companies to lead the development of several unique AI products amongst which a ground-breaking chatbot. He has an extensive and varied background as a software developer himself. He has developed a full-blown workflow management suite and analytical algorithm in the field of veterinary diagnostics, among various other projects, before growing into a managerial role. He knows what is important for a developer to be able to thrive and deliver high end products. Besides hands-on software development experience and management, Matthijs has founded and managed three other companies, thereby gaining plenty of entrepreneurial experience in the process.

Strategic Advisors

Chris Laurent (Vertical Lead FinTech/Kickstart)

Swiss Zurich-based passionate participant in the global Fintech (incl. Blockchain) community as Vertical Lead @ Kickstart, Europe's leading innovation program and Non-executive board member @ Achiko ltd, a Swiss listed Fintech, South East Asia 20 years of experience at board level in various corporates and startups also as entrepreneur, with 10 years dedicated to the financial industry, including one direct listing at the Swiss Stock Exchange in Nov. 2019. MBA x2 (incl. IMD program), MSc x2, most recently Google "Square" Academy graduate 2015. Beside general management, competencies include marketing, business development and fundraising (>10m raised)

Christian Marchand (Head of (Wealth-), (Fin-), (Global-) Tech Enthusiast & Events co-Organizer)

After a banking education quickly supplemented by an IT training, Christian Marchand has evolved for over 30 years with "one leg" in the bank, and the other one in IT Banking Industry at various positions. In 2009, he became an independent consultant, first in the field of "Sustainable ICT", but also in the field of new financial technologies (FinTech), which combine his initial orientations. Advice, fundraising, coaching, organization of events (among others Geneva WealthTech Forum & GlobalTech Summit Lausanne, editorial contributions are now his daily. He is also certified for GDPR since 2018.

Christen Oesterbye (Executive Director SEBA AG)

Serial entrepreneur of Danish origin with strong international experience focused on scaling and building successful companies and teams in the Technology and Fintech space. Initial career with IBM Software Group in Corporate Finance and later leading the EMEA region for Safenet Inc. a leading global IT security vendor listed on NASDAQ prior to being acquired by Vector Capital, a San Francisco based Private Equity company. Strong cross functional general management skills operating at Board and Executive level. Known for being very "hands-on" at the critical growth phase to drive companies to success. Most recently involved with SEBA Bank AG and IOV42 Ltd in executive roles. Currently supporting a number of startups in Switzerland and abroad. Bachelor and Master degrees in Economics and Business Administration from Denmark, UK and Norway.

Alexander Seel
(Director Legend Holdings)

International career with 20 years of experience in investment management, investment banking and consulting with a focus on financial institutions. Investment management track record includes private equity investments across the financial institutions sector on behalf of a Middle Eastern sovereign wealth fund as well as a Hong Kong listed Chinese investment company. Hands-on entrepreneurial experience in setting up three start-up companies (two of them fintech companies) and personal early-stage investments in two other fintech companies. Bachelor's degree in mechanical engineering and MBA from IESE Business School

Luke Lombe
(Co-Founder of MYNTD)

Luke Lombe is the Co-Founder of MYNTD, a capital access firm specialising in digital securities, and Founder of Echelon One, a boutique tech-focused start-up and scale-up consultancy. with a range of clients including blockchain projects, Grammy-winning production studios, government, mining, VR, real estate, and tech firms. Luke is a 2 x TEDx speaker, panellist, keynote speaker, MBA lecturer, and has been featured in a variety of media including Huffington Post, Forbes, Sky News TV, The Daily Telegraph, Wall Street Journal, Network HR Magazine, Hackernoon, and Shanghai Daily. Luke holds an MBA, B.Com, and Dip. Fin.

David Atkinson
(Current roles: Exec team at Holochain, Co-Founder Blockleaders, Advisor)

David loves to help people and businesses driven by purpose and a deep understanding and love of what they do. He is a member of the leadership team of Holo & Holochain where he focusses on business, community and ecosystem growth, and service delivery. He is also a co-founder of Blockleaders, a media platform telling human stories that power the world of blockchain. Prior to that, David was COO of Mind Gym, a behavioural change consultancy. During his tenure, Mind Gym grew revenue 3x in 4 years, and now has a market cap of ~£150m. David is driven to provide clarity (insight, simplification, story, vision/ambition, contribution, diagnosis), consideration (teaching, theory, provocation, recalibration, consultation), creation (prototypes, propositions, products/services) and containers (frameworks, mental models, systems) for those he works with.

David has a longstanding advisory experience including his time as a Strategy Consultant at Marakon, where he worked with companies like Heineken, DONG energy and the Nuclear Decommissioning Authority, as an ICO Advisor where he is known for his understanding of economic, strategic, ecosystem and currency landscapes, as Investor Director at Up Learn and as a relied upon Business Mentor and Advisor to >50 businesses since 2017. David is a co-founder of Blockleaders, Fetchhcup and Men In Therapy.

Pranav Sharma
(Current roles: Co-founder & Managing Partner - Woodstock Fund)

Pranav has over a decade & a half year leadership experience covering Business Development, Sales & Distribution, Asset Management, Private Equity & Insurance. He is passionate about Entrepreneurship, Technology and Renewable Energy. He has always taken challenging roles covering wide gamut of area like Cutting tool & Wind Power Sales as an Engineer (India), Private Equity in Renewable energy Sector (Philippines), Strategic initiatives in Financial Services (in India, Dubai, Singapore and Korea). He has worked with Sandvik Asia, Suzlon Energy, Alternergy Pte & Aditya Birla Group. In Aditya Birla Group he was part of Young Talent & leadership program and has been with Aditya Birla Chemicals (Thailand), Corporate Strategy (Mumbai) & Aditya Birla Financial Services Group.

Pranav has a deep understanding of SME context on business & financial services side. On one hand, he has helped SMEs raise funds & take Insurance cover. On the other hand, he has built pioneering institutional infrastructure like SME Counselling, SME University & tied up with over 15+ SME associations, over 3000+ SMEs outreached, over 800+ SME Distributors trained & 30+ SME Workshops

Partners

HOLOCHAIN

Table of Figures

References

Americas FS Regulatory Center of Excellence, K. (2017). *Ten key regulatory challenges Facing the financial services industry in 2017*.

Bellamy, P. and Andrade, D. (2019). *Data governance: securing the future of financial services*. [online] Ey.com. Available at: https://www.ey.com/Publication/vwLUAssets/EY-securing-the-financial-future-with-data-governance/%24File/EY-securing-the-financial-future-with-data-governance.pdf

Buterin, V. (2017). STARKs, Part I: Proofs with Polynomials. Retrieved 7 November 2019, from https://vitalik.ca/general/2017/11/09/starks_part_1.html

DGI Data Governance Framework Components - The Data Governance Institute. Retrieved 7 November 2019, from http://www.datagovernance.com/fwk_dgi_data_governance_framework_components/

Ciriani, V., Vimercati, S., Foresti, S., Jajodia, S., Paraboschi, S., & Samarati, P. (2010). Combining fragmentation and encryption to protect privacy in data storage. ACM Transactions On Information And System Security, 13(3), 1-33. doi: 10.1145/1805974.1805978

Domingo, C., Finkelstein, S., & Sarna, J. (2018). DS Protocol - Securitize's Digital Ownership Architecture for Complete Lifecycle Management of Digital Securities. Retrieved 7 November 2019, from https://securitize.sfo2.digitaloceanspaces.com/whitepapers/DS-Protocolv1.0.pdf

English, S., & Hammond, S. (2018). COST OF COMPLIANCE 2018. Retrieved 7 November 2019, from https://legal.thomsonreuters.com/content/dam/ewp-m/documents/legal/en/pdf/reports/cost-of-compliance-special-report-2018.pdf

Enterprise Information Management: Best Practices in Data Management. Retrieved 7 November 2019, from http://egovstandards.gov.in/sites/default/files/oea-best-practices-data-gov-400760.pdf

Gowravaram, N. (n.d.). *Zero Knowledge Proofs and Applications to Financial Regulation*. [online] Nrs.harvard.edu. Available at: http://nrs.harvard.edu/urn-3:HUL.InstRepos:38811528

Inc, M. (n.d.). *Open Banking platform strategy: Modernize customer engagement with APIs*. [online] MuleSoft. Available at: https://www.mulesoft.com/lp/whitepaper/api/open-banking-platform

Koverko, T., & Housser, C. (n.d.). POLYMATH THE SECURITIES TOKEN PLATFORM. Retrieved 7 November 2019, from https://daks2k3a4ib2z.cloudfront.net/5a46fad33472ef00014b540a/5a46fad33472ef00014b54d0_Polymath%20Whitepaper.pdf

Labs, M. (n.d.). *matter-labs/awesome-zero-knowledge-proofs*. [online] GitHub. Available at: https://github.com/matter-labs/awesome-zero-knowledge-proofs#comparison-of-the-most-popular-zkp-systems

Lukas, J. (n.d.). *The Leading Security Token Issuance Platforms: A Summary Comparison*. [online] Medium. Available at: https://medium.com/@jaronlukas/the-leading-security-token-issuance-platforms-a-summary-comparison-ac8d42290f98

McLellan, L. (n.d.). Fintech finally at the capital markets gates. Retrieved 7 November 2019, from https://www.globalcapital.com/article/b1hlqyd81qwvgm/fintech-finally-at-the-capital-markets-gates

News, O. (n.d.). [online] Pinsentmasons.com. Available at: https://www.pinsentmasons.com/out-law/news/uk-moving-from-open-banking-to-open-finance [Accessed 6 Nov. 2019].

News, O. (n.d.). [online] Pinsentmasons.com. Available at: https://www.pinsentmasons.com/out-law/news/payments-rules-present-a-barrier-to-open-finance

Pandit, V., & Dayama, P. (n.d.). Privacy in blockchain collaboration with zero knowledge proofs - Blockchain Pulse: IBM Blockchain Blog. Retrieved 7 November 2019, from https://www.ibm.com/blogs/blockchain/2019/01/privacy-in-blockchain-collaboration-with-zero-knowledge-proofs/

Pribanic, E. (2018). *Top Regulatory Compliance in Financial Services by techFunnel*. [online] Techfunnel. Available at: https://www.techfunnel.com/fintech/top-regulatory-compliance-in-financial-services/

Rijvenam, M. (n.d.). How Zero Knowledge Proof Will Enable Trustless Transactions and Increase our Privacy. Retrieved 7 November 2019, from https://www.linkedin.com/pulse/how-trustless-society-improve-our-privacy-mark-van-rijmenam

Remeika, B., Amano, A., & Sacks, D. (2018). The Regulated Token™ (R-Token™) Standard. Retrieved 7 November 2019, from https://harbor.com/rtokenwhitepaper.pdf

Sasson, E., Bentov, I., Horesh, Y. and Riabzev, M. (n.d.). *Scalable, transparent, and post-quantum secure computational integrity*. [online] Eprint.iacr.org. Available at: https://eprint.iacr.org/2018/046.pdf

Stringfellow, A. (2018). *NGDATA | 3 Data Governance Best Practices for Banks & Financial Services Companies*. [online] NGDATA. Available at: https://www.ngdata.com/data-governance-best-practices-for-banks-financial-services-companies/

Thomas, H., Kimber, A. and Brown, W. (n.d.). *How regulation is unlocking the potential of open banking in the UK*. [online] Ey.com. Available at: https://www.ey.com/en_gl/banking-capital-markets/how-regulation-is-unlocking-the-potential-of-open-banking-in-the-uk

Timpert, A., Wyss, R., Ouschan, D. and Azzouz, Z. (2017). *Compliance 2025*. [online] Abti.ch. Available at: https://www.abti.ch/pdf/ch-en-fs-compliance-2025-dna-evolution.pdf

T-REX (Token for Regulated EXchanges) The token standard allowing ownership transfers of tokenized securities. Retrieved 7 November 2019, from https://tokeny.com/wp-content/uploads/2018/12/t-rex-whitepaper.pdf

Traulsen, S. and Tröbs, M. (2019). *Implementing Data Governance within a Financial Institution*. [online] User.tu-berlin.de. Available at: https://www.user.tu-berlin.de/komm/CD/paper/050141.pdf

Zuenko, A. Zero-Knowledge Explained: Part 1. Use Cases. Retrieved 7 November 2019, from https://stratumn.com/thinking/zero-knowledge-explained/