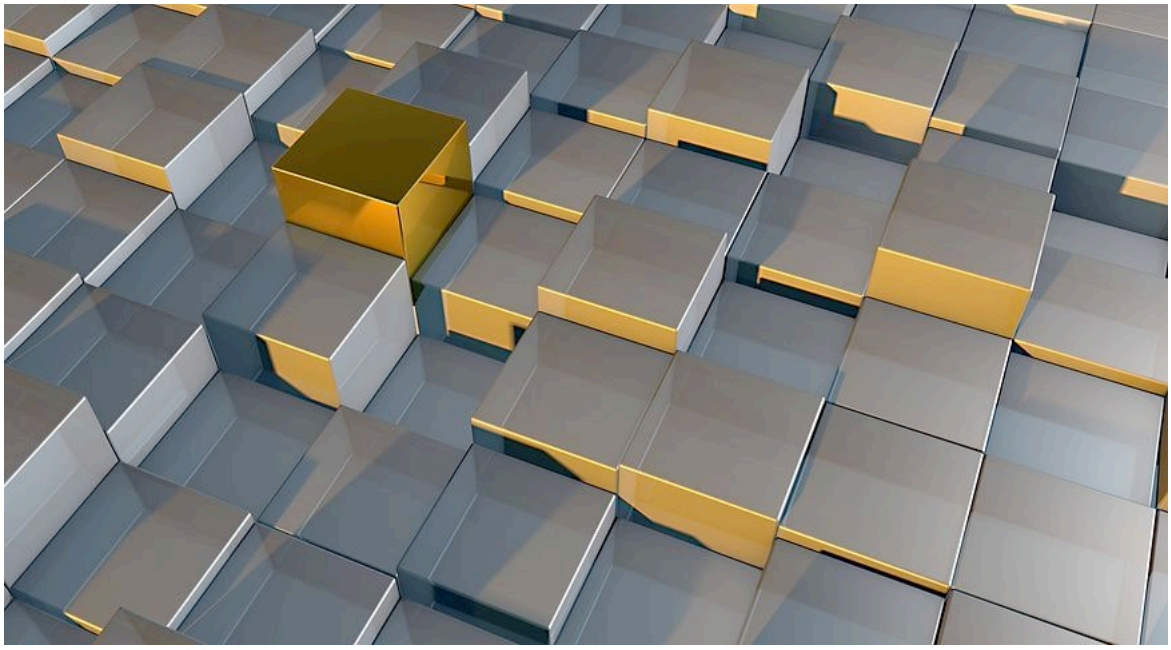
INTERNATIONAL INSURANCE SOCIETY

An affiliate of The Institutes | Risk and Insurance Knowledge Group

Regulatory Technology – the changing landscape

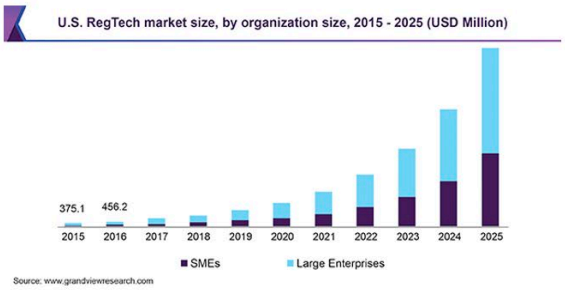


Abstract

Applying 20th century regulation for 21st century technology can impede innovation at a time where viable novel solutions should be out of the lab and into production quickly improving the world economy. There are significant increases in global regulatory responses to address growing market interest in Fourth Industrial Revolution [i], Web 3.0 [ii] and intangible digital assets leading to questions as to the future of money itself. Regulators are issuing taxonomy frameworks to classify types of tokenisation catalysed by cryptocurrency, blockchain and DeFi (decentralised finance) developments drawing fuel from unregulated permissionless, anonymous networks on the INTERNET in the public domain. The purpose of regulation is to protect the consumer from abject business processes and not regulating technology per se. Supervisory risk will emerge if technology is the direct focus rather than the nature of the asset and business processes that derive from it, as it will spread uncertainty between market stakeholders and regulators. Supervision in the 21st century must combine components of exponential technology into an inclusive strategy exploring how regulation can be embedded for economic benefits while preserving consumer privacy and data integrity. Having a separate regulation for each technology derives no benefit due

to pace of change so better to regulate the whole transaction flow to a safe conclusion. This way common themes are identified to conceive regulatory strategies in response. Regulatory technology spend will grow by 48 percent per annum – rising from $10.6 billion in 2017 to $76.3 billion in 2022 [iii].

Source: MarketsandMarkets Analysis



Source: www.grandviewresearch.com

Lack of standards and confusing taxonomy have kept regulation out of step with technological change. An issue that stands out is the difference between a digital and crypto asset. Digital assets, twin representations of the physical world, are familiar with existing legal concepts. Crypto assets are a new business model, founded on blockchain based programmable money and require compatible legal frameworks. Digital assets however are not exempt from regulatory innovation as a basket of rights, custody, ownership and privacy are encoded directly in the entities. The risk management model needs modernisation with regulators inside ecosystems interoperating across jurisdictions for cross border integrity.

This paper focusses on regulation becoming inclusive in the “world financial ecosystems” so regulators understand exponential technologies and formulate policy around that knowledge without trying to fit new technologies into existing regulations. The focus is FinTech, encompassing all financial services, with emphasis on insurance deriving benefits from progress of banking and payment sectors, themselves undergoing disruption. This resets and dovetails business sectors as they evolve to supervise control over customer personal data aggregation in a decentralized world of smart devices. This requires authentication, self-sovereign identity and evidence based data integrity as digital assets and crypto become the dominant internet business model. Data driven applications such as insurance underwriting offer self-executing infrastructures with performance-based regulations. The resulting regulatory technology can be divided into two pillars, one that serves financial institutions and one that serves regulators to support supervision using automation to check compliance.

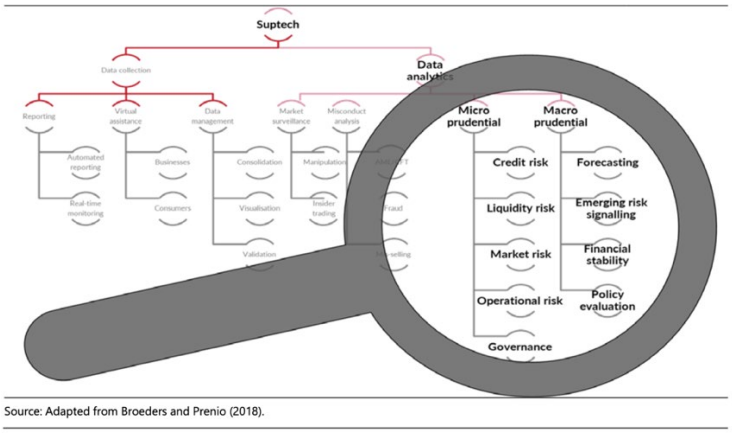
Definitions

Regulatory change is driven by blockchain in conjunction with other exponential technologies. **Blockchain and Distributed Ledger Technology (DLT)** are terms used interchangeably but blockchains are separated from distributed ledgers and do not store actual data (to preserve privacy/cyber security) but create a cryptographic hash key linking to identify the actual data stored in ledgers and data repositories. **Smart Contracts** are self-deploying contracts containing terms of legal agreements between two parties written into computer code directly connected to the blockchain. The code controls contract execution by

triggers and transactions are trackable, irreversible and immutable. **NFT** is “non-fungible token” which is a unique representation of an asset. “**Token”** is a term for a blockchain object such as a crypto coin or any token created on a blockchain. **On Chain** is where data is validated within a blockchain environment, **Off Chain** where data originates externally and **Cross Chain** is interoperability between different blockchain platforms. Data provenance is proving the origin of data and tracking the events of that data across it’s entire lifecycle.

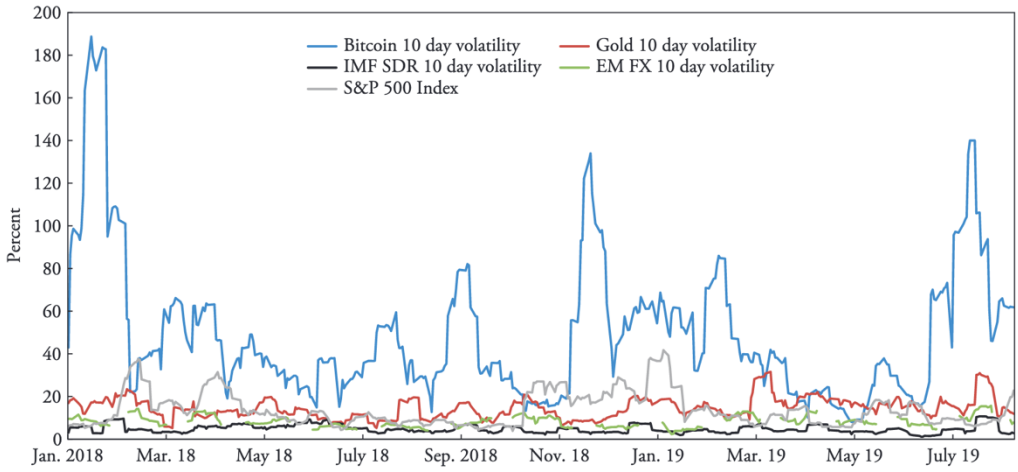
What is the new regulatory risk landscape

Operational issues pose the biggest risk and need dissection. Financial services risk market integrity and non-compliance due to legal uncertainty caused by pace of digital change plus lagging regulation polarised by legally imposed requirements limiting innovation. History shows regulatory arbitrage when the INTERNET first emerged, with business models operating in shaded areas facilitating avoidance of compliance via other jurisdictions. The inherent nature of insurance, sharing liability by stakeholders on a balance sheet, limits systemic risk or market destabilisation due to default of one particular company. Systemic risk can occur if a negative shock experience occurs with a large-scale, broadly used technology- based model undermining industry trust such as cyber-attacks and identity theft. Crypto assets may generate contagion which could introduce shocks warranting immediate regulatory responses. Smart contracts used to automatically pay insurance claims on a pre-arranged condition can fail due to non-correlation between loss events and performance of the underlying index aligning the payment. This increases basis risk [iv], losing consumer trust of unpaid claims. Design and provenance of smart contract triggers is paramount to mitigate risk. The operational risk of the current regulatory landscape shown below by the Bank of International Settlements (BIS) [v] needs to be disseminated with a relevant taxonomy. This adds an intangible aspect to operational risk, centred around data integrity, cybersecurity and crypto ecosystems across the whole financial services spectrum.



Source: Adapted from Broeders and Prenio (2018).

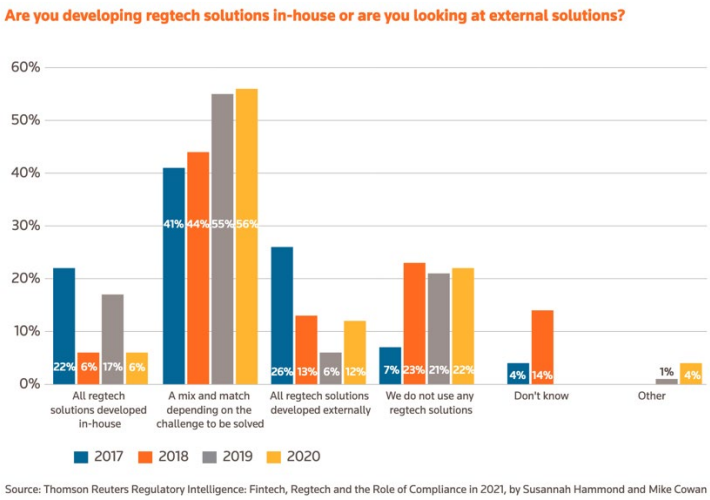
Crypto-investors and major crypto-asset service providers are exposed to high risks due to market volatility paired with customer anonymity. Risks incurred by investors include operational (smart contract failure), cyber integrity of e-wallet providers and crypto trading platform issues combined with market, credit, and issuer default risk. Digital and non-digital asset types comingle bringing asset liquidity risk in conjunction to market manipulation, mis-selling, money laundering, terrorist financing and fraud. The chart below shows prior volatility of crypto markets. Regulatory technology, risk modelling and new protection products are needed to address crypto especially smart contract failure and market volatility.



Source: Bloomberg data.

Regulatory Technology (RegTech) and Supervisory Technology (SupTech)

RegTech is a software innovation that enables corporations to configure against the onus of expanding regulatory reporting while remaining relevant, cyber secure and adopting real time information modelling. SupTech enables regulators to adjust rapidly to changes and accomplish goals of establishing trust in markets especially on financial transaction settlement in a crypto world. Innovative technologies, included by design, in a set of new supervisory guidelines allow future proof recommendations. Business need to stay compliant, is factored, to reduce current high costs of regulation. RegTech solutions today centre around regulated financial institutions, helping them to comply and improve risk management. Blockchain technology is a game changer leading to new breed of RegTech 2.0. Addressing interoperable smart contracts will automate regulatory reporting, make it more transparent, improving consistency, efficiency and data quality. Regulators will have real-time permissioned access to content of signed contracts and changes reducing compliance costs.



Source: Thomson Reuters Regulatory Intelligence: Fintech, Regtech and the Role of Compliance in 2021, by Susannah Hammond and Mike Cowan

A Deloitte report on the current RegTech universe is referenced [vi] showing how the status quo looks at compliance (tracking regulatory requirements), identity management (Know Your Customer/KYC, Anti Money Laundering/AML), risk management (data analytics),

regulatory reporting, end to end transaction monitoring and electronic trading platform controls. Currently regulators use a “sandbox” approach, hubs and accelerators as a controlled environment for regulated /unregulated institutions to test innovations for a group of customers over a set period under strict rules which incubates digital companies.

Emergence of exponential technologies means regulators can evolve to a forward-looking supervision with evidence based data integrity and predictive analytics eliminating manual processes in the aggregation and collection of data. SupTech will address granular, primary data adhering to new taxonomies, transforming the regulatory process by developing supervisory smart contracts bootstrapping blockchain technology. These smart contracts interact with RegTech compliance solutions by sending alerts to risk managers about impending regulatory changes automating the reporting process across the transaction flow. As SupTech automates repetitive tasks and analyses unstructured data by AI, augmentation should be applied to avoid relying completely on model output without human judgement. Regulators have to position for blockchain/DLT mainstream adoption and be there. The lack of taxonomy for digital and crypto assets is a barrier to their regulation and management in an international and multi-jurisdictional environment. The Cambridge Centre for Alternative Finance [vii] (CCAF) is addressing token taxonomies for near term adoption.

Blockchain/DLT Technology Effect on Embedded Supervision.

Blockchain has been called the codification of the law with a capability of being fully decentralized with no central control. Self-deploying features of smart contracts and the immutable nature of DLT-based data repositories raises short term headwinds for regulators but fresh tailwinds for legally approved frameworks around self-regulation and multi-level governance. Debates between centralised and decentralised regulation will continue and vary by jurisdiction. A completely decentralised system will cause control problems so likely a hybrid will emerge as the middle ground. Digital currency blockchain developments in China, where the regulator is already a node on the network, shows China are way ahead on SupTech initiatives but with a centrally controlled policy, wary of cryptocurrency outside its own central bank digital currency, which may not prove to be economically competitive in the future. Fears exist globally as law and technology converge, that computer code could accidentally/deliberately override legal rules when regulating digital users on the INTERNET. In 2014 BITCOIN suffered distrust after Mount Gox [viii] serving as a reminder.

Regulating the transaction to finality with data integrity and proving provenance, while preserving customer privacy is the desired outcome. Cryptographic blockchain tools can be used to report accumulated financial exposures in real time without disclosing the underlying assets. This shifts from a legal system focussing ex ante on data breach financial penalties to a trusted/verifiable data integrity model, a priori, giving economic incentives based on an inclusive ecosystem approach. Regulators will promptly need to adjust to that premise.

Blockchain/DLT structures are classified as private (permissioned) or public (permissionless). Adoption of enterprise private blockchain is now mature and financial institutions look to leverage public permissionless blockchains so as to access locked in economic power delivered by DeFi and crypto now estimated at $2.5 T [ix]. The rise of NFT (emerging from collectibles), as a financial instrument tokenising, fractionising, collateralising, encapsulating ownership, draws parallels to when bitcoin was officially gaining acceptance as a balance sheet asset class. Through this development compliance platforms can emerge to better manage capitalization tables using a service for digital asset custody via wallets and pre-empting derivatives that may derive from digital strategies.

Public blockchains have a governance process call “forking” [x] which does not replace corporate governance, investor protection, or financial stability regulation. This blockchain democratic process where peers on a network vote to agree a change in a blockchain

protocol in decentralized fashion can result in new digital assets being created if denied. BITCOIN CASH [xi] emerged after the original BITCOIN forked. For private and permissioned blockchains ,such as Hyperledger Fabric [xii] forking is not a regulatory concern. Crypto mining, with communities of miners proving the validity of public on chain transactions, can have effect on capital market flows as miners expenses are paid domestically in local currency but revenue is received in cryptocurrency. Miners needed to be included as stakeholders in the financial services ecosystem as part of the interoperability process.

As financial institutions look to access public blockchains in the search for proven transaction settlement cross chain [xiii] supervision will look for integrity. Recent developments have separated public blockchain protocol into two architectural layers with a fully deployed production protocol such as ETHERIUM as a foundation layer guaranteeing settlement and a layer above which applies a concept known as “rollups” to get the scalability of transaction execution and to get interoperability to regulated private blockchains. This opens up enterprises to the whole available network so AML/KYC SupTech/RegTech solutions must be improved and upgraded. Scalability capability will be key to future developments.

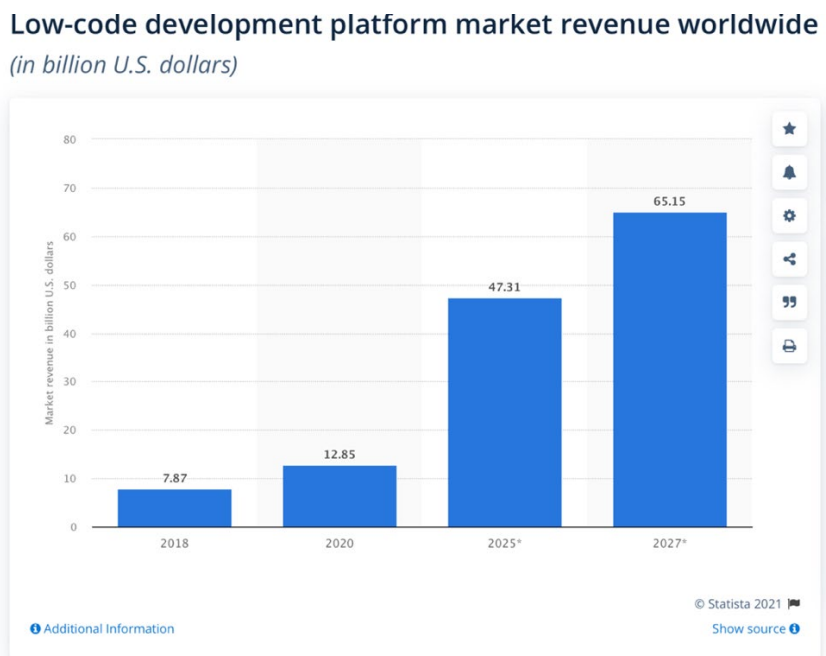
Ecosystems – embedding digital supervision

New technology emergence has given rise to the development of ecosystems consisting of like-minded affinity organisations that share data with permission, pool their ‘treasuries’ together to participate in electronic market places such as lending and reinsurance placement platforms. Data can be shared visibly without moving the data, creating trust and then moved to settle a transaction. As public blockchains are integrated into enterprise and more institutions join the ecosystem, more fragmentation will occur requiring cybersecurity cross chain and networks. Regulators need to be on the inside looking out to handle transaction regulation in real time and becoming influencers in promotion of trust models. Because of arbitrage, collaboration amongst peer regulators across borders is required. Self-regulation will become a ecosystem factor via smart contract automation and industry will prove out the Minimum Viable Ecosystem (MVE)[xiv]. MVE is an evolutionary process driving principle based regulations away from rule based creating new regulatory models within financial industry ecosystems and consortiums. Regulators act as another node on the network so to have permissioned access in real time to the ledger but regulators globally may in time have their own MVE. Ecosystem participants will benefit from a client on-boarding perspective by reducing the cost of KYC/AML compliance by only performing the registration once by one insurer/intermediary. Documentation already on chain is sufficient to confirm due diligence.

Low Code / No Code and Open Application Program Interfaces (API).

This emerging innovation can influence customer onboarding issues in regards to RegTech especially for insurance due to rigid legacy systems, slow product development and high customer onboarding costs. Legacy technology can delay onboarding time because of KYC take months to make regulatory changes. These offerings can give organizations the visual tools to manage compliance layers across regulatory regimes, testing outcomes of emerging risk and regulation using configuration only. An entity can be created in one location and adhere to compliance in multiple jurisdictions. Currently existing as middleware offerings they figure highly in the RegTech space and are a fulcrum for digital transformation.

No-Code Low Code solutions are pre-designed to avoid writing code or using minimal code. Graphical User Interfaces (GUI) provide users with visual interfaces to configure digital products or supervisory constructs. Pre-built multiple API’s address legacy integration. Software analysts predict that this development will account for 65% of all application development by 2024, with a potential to develop applications 10 times faster [xv].



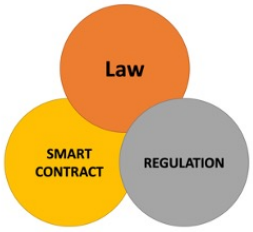
Using such development tools the regulation of financial inclusion, (denoting all insurance products/strategies targeted for the under-banked or underserved market), will benefit when combined with blockchain/DLT networks so villages and semi-urban areas can be nodes on a network redesigning cash and payment rail mechanisms. The term microinsurance is also a term used defined as insurance specifically designed and accessible by low-income populations. The technology now exists to implement social reinsurance [xvi] which despite great efforts has been difficult to do prior to this time. Regulations using digital technology has been most successful when the supervision was proportional, as in the Philippines [xvii]. The global underserved financial sector has an estimated market of over 2 billion people.

Open APIs allow financial institutions to open up internal IT systems/data for programmatic access by third-party service providers (TSP) in an open, secure manner facilitating exchange of information and across disparate networks. These APIs allow applications developed by TSP to integrate seamlessly with the overall enterprise system of an organisation. Blockchain networks utilise external transactional structures called oracles to act as API's and these act as triggers for parametric insurance especially for agriculture and natural catastrophe management utilising smart contracts providing transparency, self-governing and provenance. This allows performance based regulations where incentives are given to reduce regulatory cost. use API's for transparency, self-governing and auditing plus integrating on chain and off chain capabilities with data integrity.

Smart Contracts are the Harbinger of Change

Smart Contracts are parametric vehicles and a constant element in all blockchain/DLT based information making them a regulatory magnet. They consist of programmable code and trigger actions automatically on an event based on data parameters. The diagram below shows the lines between law, regulation, and computer code become blurred posing questions such as "is the code the law or is the law the code" (LESSIG) [xviii] signifying the manner in which smart contracts are coded for financial contracts. SupTech/RegTech will protect the public from the emergence of "ponzi scheme" [xix] smart contracts self-executing in the financial space, using AI to detect such structures. The nature of cyberspace generates need for international and regional institutions exercising a balance of law-making and authority over financial activity across jurisdictions. Standards emerging are not yet

regulations so SupTech/RegTech can use the same technology like for like for economic importance.



The economic or market dimension needs to be added to the equation when legal and regulatory questions are debated. How does a legal system responds to key economic practices that are enabled when innovation such as tokenisation improves market capitalisation. The whole framework must actively utilises new technologies to achieve economic benefits.

Economic benefit drives development here so the smart contract process requires a degree of self-regulation to govern the code. Risk management platforms for cryptocurrency lending are looking to on chain data triggers to govern the process using the blockchain immutable and trust properties. The close alignment to parametric insurance means if any external off chain claim triggers (oracles) are used then they need to be validated for provenance. All parties need to trust these sources of information and they must possess cyber integrity.

WEF published a paper on navigating crypto regulation [xx] for data delivery to financial supervision. Creation of **NFTs** is a potential game changer and will benefit the economy for anyone who lends, insures, trades or provides financial services. Due to cryptocurrency volatility issues stability is needed so pooled NFT assets interact with **stablecoins** [xxi],crypto asset tokens with value pegged to fiat currencies, commodities or another type of crypto asset. This enables collateralized asset life cycle management, ownership and sovereign identity , interoperating with electronic wallet management for currency conversions operating across borders. With low code software technology, digital payment gateways, and multi device capability the operational pathway for RegTech is clear. NFTs will act as a payment to transfer value, an investment into low-volatility assets and a user interface to link the users wallet providers providing collateral. Both NFT and stablecoin tokens are smart contracts so transparency exists as on chain collateral can be automatically verified.

Insurance claims are transformed as a built in voting and governance mechanism aids claim payment. The legal system validates on chain/off chain data triggers creating an evidence based parametric insurance mechanism. This automates a large part of claims-handling, limiting the scope for disagreement between parties and reduce settlement times and claims handling expenses. Claim events are recorded on a blockchain and primary data entered into smart contracts, with information being accessible to (re)insurers, rating agencies and regulators in real-time on a permissioned basis. Data can be verified by the blockchain for modelling, audits, and compliance checks with automated notification to relevant parties.

The Decentralised Autonomous Organization (DAO) Regulatory Dilemma

A DAO is an internet-native-entity with no central leadership governed by a member community organized around a specific set of rules enforced on a blockchain network with smart contracts. Plainly speaking this is a mutual digital corporation that has no “company house” registration as exists for limited companies today. DAO accounts are embedded and

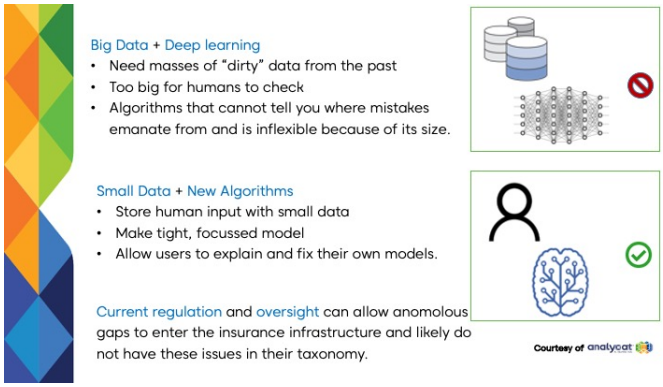
only updated with member approval. Decisions are made on chain by voting and are fully autonomous and transparent. They are built on open-source blockchains and anyone can audit their code or their funds as the ledger records all financial transactions. The smart contracts must be extensively tested for cybersecurity. Regulatory concerns exist about their legality, structure and arbitrage risk as they can be distributed across multiple jurisdictions without a legal framework using self-governance and reward tokens. DAO's are deployed for decentralized finance (DeFi) governance, fundraising, real estate in a growing list of usage. The classification and regulation of DAO's is a dilemma that cannot be ignored.

A development occurred on July 1st 2021 when Wyoming legally recognized DAO's [xxii] in a law intended to close the gap between formalized corporate structures and unincorporated groups governed by rules coded in smart contracts. This takes the first steps towards formulating regulatory standards and practices for DAO-based corporate operations. If other jurisdictions take these steps RegTech/SupTech can be used to counter arbitrage and cross border regulatory requirements. The law allows evaluation and verification of blockchain transactions and smart contracts as legitimate proof of ownership and transfer allowing data provenance to stand up in a court of law. This will assist in the addressing the disconnect between regulators and decentralized protocols where the current sole regulatory focus is on AML/KYC. Wyoming provides DAO members with the same limitations on individual liability afforded to members of limited liability companies (LLCs) thereby creating a level playing field between traditional and emerging financial markets.

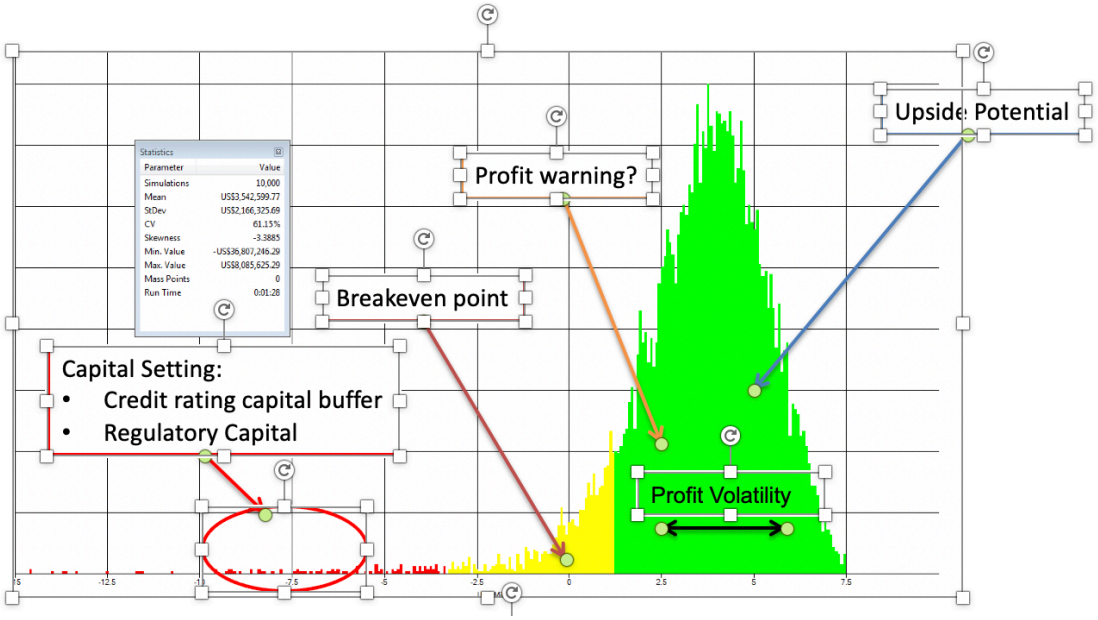
Data Analytics and use of Artificial Intelligence (AI)

Data is a common theme to all technologies so an encompassing data integrity and provenance strategy leading to a full transparency approach is required. Data analytics using real time granular data and AI can give outcome-based predictions and regulatory reporting across jurisdictions. Parallels can be drawn to the early days of financial and catastrophe models where solutions were considered black box solutions with a risk of over dependence on modelling. Regulators require explanation of how AI programs reach a decision and to isolate and change exact data points that caused a problem. Black box algorithms without explanations will not survive scrutiny. Data explosion phenomena brings the anomaly of questionable data and spawns debate about the promise of big data for improved risk assessment as generating larger datasets maybe codified in law or used for enterprise datafication. Particular attention needs to be given to data information risk from sensors via smart contracts that trigger machine to machine interaction without human involvement as in Internet of Things (IOT) scenarios where standards and OEM regulations are still emerging.

So there is a strong case to take a smaller dataset AI approach to fix bad data and give an easier interpretation for regulatory reporting including a search for counterfactuals asking for missing data and unthought of outcomes (aka unknown unknowns). Adi Hazan [xxiii], a mathematician who has developed an AI solution that is completely transparent says: "The current regulatory framework seems to live in a separate context from current technologies. I have yet to hear a regulator deal with AI vulnerabilities, the impossibility of diagnosing what has caused an AI error or the dangers of missing data."



SupTech is also creating opportunities for supervisory agencies to collect and analyze unstructured data (i.e., data that is not organized in databases) with greater efficiency, which could relieve regulators from time-consuming tasks in data collection. Equally important is the use of data analytics to apply risk adjusted return predictions, capital modelling and holistic enterprise risk management that complies with regulatory solvency regimes such as SOLVENCY II, RBC, C-ROSS, BASEL) and apply it across various jurisdictions to enhance decision making using a stochastic approach. An example is used of such an approach to shows the distribution of an insurer's profit in context of regulation courtesy of URS [xxiv] utilising a current in production use of a no code/low code software approach to RegTech. The technology uses mathematically produced scenarios to align risk and regulation and the increased use of this technique for correlating intangible risks for solvency is paramount.



The challenge is interoperability between emerging ecosystem data analytics and the current RegTech approaches. Financial authorities use SupTech tools for a range of activities, including data analytics to automate of certain repetitive tasks in prudential supervision. Growth of non-traditional data sources that can have a bearing on a firm's risk profile will drive new and existing FinTech analytical tools to help process and analyse data – such as artificial intelligence and machine learning linked by Open API's to existing systems.

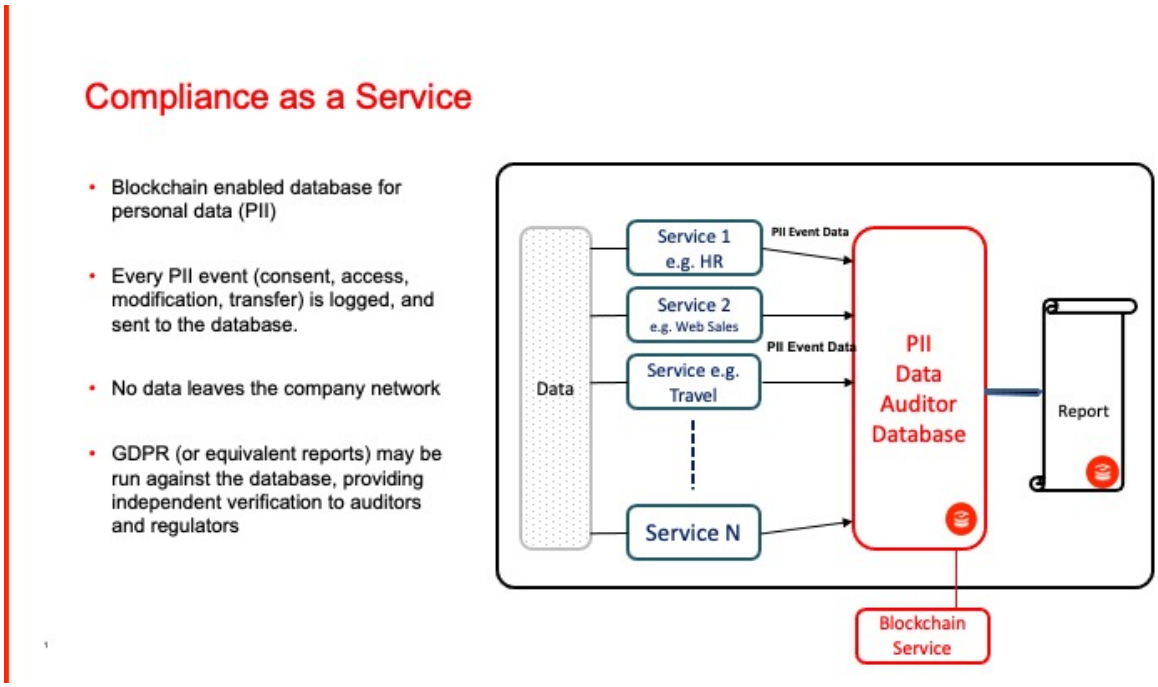
Privacy by Design

Data privacy cannot be an afterthought. Systems that process personal data should be designed to ensure privacy protection for risk mitigation. Regulators are including this

principle in regulatory frameworks such as GDPR [xxv]. Dynamic approaches are required responding to privacy threats from future technological innovations such as quantum computing. regardless of how technology evolves. Data are an intangible economic asset requiring regulation and governance ensuring future prosperity of the world economy.

Holding pools of stand -alone data without associated properties of trust, integrity and provenance is largely worthless, hard to manage efficiently, impeding company performance as data inconsistency and tampering is allowed to go undetected. Digital information is extracted, refined, valued, bought and sold differently to other resources. It changes the rules for markets and demands new approaches from regulators. Market forces alone cannot be relied upon to advance the data economy because of a lack of transparency in data usage. Strengthening data protection will improve trust in the emerging digital economy

Personal data today, is held on many disparate systems and affects multiple workflows (i.e. applications, processes, and services). Integrating these systems is a major challenge for tracking PII (personally identifiable information) use. However, all PII related transactions can be continuously registered in the blockchain, providing an immutable history for auditors, tracking all transactions associated with each workflow. Business processes can be instrumented with minimal integration issues, avoiding a major rewrite of existing infrastructure. Over time, deeper integration can be undertaken where appropriate to further strengthen immutability at a core system level. This creates a compliance as a service approach as shown below in a GDPR example courtesy of Guardtime [xxvi].



From a legal and data privacy perspective there is a risk that the combination of large amounts of historic data about a consumer or a group of customers may result in an indirect use of sensitive data otherwise not allowed by laws. Given that records on the blockchain are largely tamper-resistant and immutable, the adverse impact on compliance with certain GDPR provisions, such as the right to be forgotten and data erasure requirements, needs to be carefully considered. Any privacy regulation can be defined as code and compliance enforced and proven through blockchain providing adherence with the law.

Healthcare and RegTech

American Hospital Association who put out a report of the cost of healthcare regulation [xxvii] found that healthcare providers in USA alone spend nearly $39 billion a year and this is the business case for RegTech to automate processes to free up resources for patient care and efficiency for insurers/payers. Patient data is highly sensitive and use of wearables increases obligations in respect of data protection and privacy by design. This is not an easy landscape to navigate which is why healthcare RegTech lags behind financial services. The use of AI will be paramount to remove repetitive tasks around compliance and to get doctors to train models to answer questions as the experts. All healthcare workers would work to an even, dynamic standard of care to make consistent better decisions to save lives including the difficult decisions where technology augmentation would give relief to care workers. This robotic process automation, for compliance, can also automatically access multiple information systems and compile records increasing the efficiency of regulatory audits.

Open Source Regulation

Open source is software code that is publicly available and constantly reviewed for credibility and flaw detection by communities before release. A recent hack December 2021 on the Apache open source logging library (Log4J) [xxviii] has affected millions of devices and applications worldwide. A fix had been applied to the flaw and this can be taken as a positive wake-up call for the future cyber integrity of open source. Accelerated attention is now being paid to the Open Source Security Foundation (openssf.org) [xxix] to address community based regulation security improvements in the future. Regardless of this event regulatory bodies and the financial services industry have an opportunity to redesign the traditional regulatory framework using open source technology. Currently many RegTech /SupTech solutions on the market are expensive and use inefficient proprietary code.

A recent development for the insurance industry is a collaboration between The Linux Foundation [xxx], a non profit organization enabling mass innovation through open source, and the American Association of Insurance Services (AAIS) [xxxi] known as the openIDL [xxxii] (Open Insurance Data Link platform). This provides a standardized data repository streamlining regulatory reporting and analytics across insurance organizations reducing the cost of compliance and a connection point for third parties to deliver new applications to members. openIDL has onboarded some of the world's largest insurance companies to advance a common distributed ledger platform for sharing information and business processes across the insurance ecosystem. The first use case for the openIDL network is regulatory reporting in the Property and Casualty (P&C) insurance industry. openIDL leverages the trust and integrity inherent in distributed ledger networks. The secure platform guarantees to regulators and other insurance industry participants that data is accurate and complete. It leverages open source code and a community open governance network for objective transparency and accountability among participants.

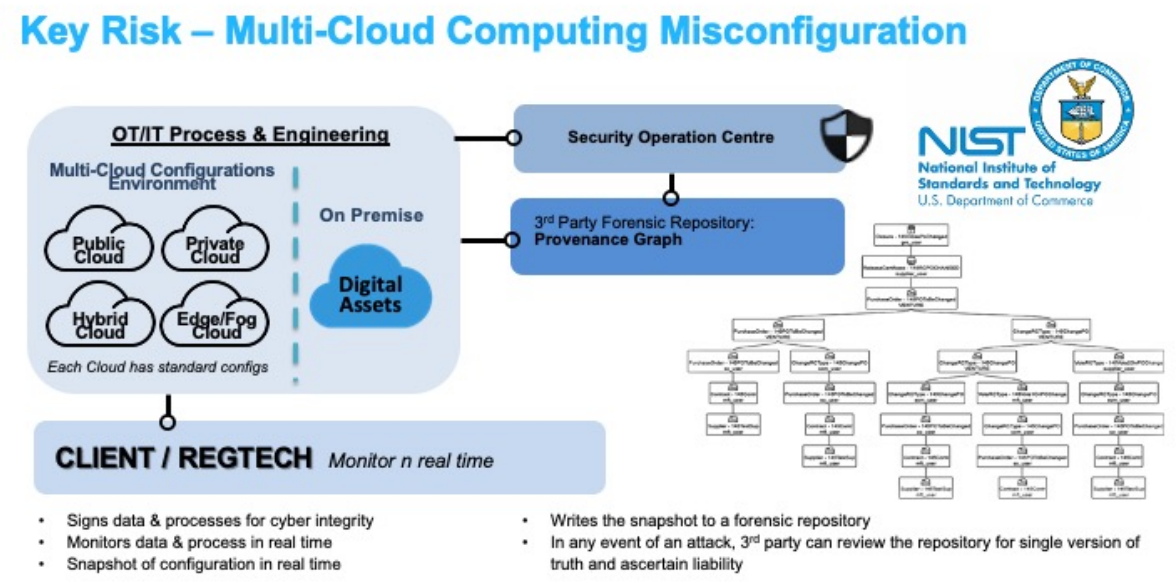
The FINOS Regulation Innovation Special Interest Group [xxxiii] is a community creating open source solutions for regulatory and compliance issues in financial services. Launched in September 2020 and approved by the FINOS Governing board in October 2020, they recently announced an Open RegTech [xxxiv] initiative, which expands open collaboration models built between financial institutions, FinTech/Insurtech firms, regulators and RegTech companies alike combine to establish an open source model for the regulatory community.

Cloud Computing Security Regulation

Global use of cloud computing is a vital economic and climate change benefit but has well-documented security and governance problems. Cloud services require you to trust the

cloud service provider (CSP) and data are only as secure as the CSP implementation of data integrity. Everyone is an insider in the cloud so in event of breach knowing who is liable can be an obstacle. Major cloud services pose an attractive target for attackers due to global access to many high-value customers. Even when cloud services are secure, misconfiguration and administrative errors frequently create security holes so RegTech adoption is fast growing. Paradigms for cyber security are largely perimeter control but this breaks down in the cloud as running on someone else's infrastructure there is no perimeter to protect.

Regulators have supported cloud security standards and certifications confirming the compliance of a cloud service at the point of audit but do not provide ongoing compliance in real time for platform services that are constantly renewing and updating. Automated solutions for controlling cloud and edge computing are required, allowing the security team to verify the integrity of security control policies and the actual state of data and services, reflecting the reality of the infrastructure across cloud environments. Using a cryptographically enforceable policy real-time breach detection and incident response dynamic attestation of compliance for external auditors occurs. As new resources and services are subscribed they are automatically enrolled into existing monitoring. This pulls together security information across multiple cloud services, agencies, deployments under a into a single pane of glass. A data integrity layer is built specifically to address data access management, cyber security, and data monitoring. It can manage billions of log events each second for data monitoring and distribution/management operations. It is interoperable with existing IT platform investments and does not require the movement of any customer data to the blockchain. Trusted cloud in an era of digital sovereignty. As can be seen in the following diagram a data provenance repository is created that can be monitored in the case of breach.



Important New Developments involving RegTech

RegTech innovations emerging from Asia in parallel with the USA/EU form a new global standard framework. Both Singapore and Hong Kong are developing risk management hubs.

USA The BIS Innovation hub has advanced a strategic partnership with the Federal Reserve Bank of New York (NY FED) by creating the New York Innovation Centre (NYIC) [xxxv] in order to launch new financial technology products and services for the central bank community. NYIC will focus on five opportunity areas: SupTech/RegTech, Financial Market Infrastructures, Future of Money, Open Finance, and Climate Risk. In addition federal regulators are allowing credit unions to hold digital assets via third parties [xxxvi].

Hong Kong Monetary Authority (HKMA) launched an AML RegTech Lab (AMLab) [xxxvii], in collaboration with Cyberport [xxxviii] to further encourage the use of RegTech under a "Fintech 2025" [xxxix] strategy. AMLab will strengthen banks capabilities to protect customers from fraud and financial crime losses, reduce risk displacement across the banking sector and raise the overall effectiveness of the AML ecosystem. AMLab focuses on using network analytics to address the risks of fraud-related mule accounts, enhancing data and information sharing through public-private partnership efforts. AMLab series will provide a collaborative platform for ongoing peer group sharing of operational, hands-on experience of Regtech approaches, focusing on solutions such as machine learning in transaction monitoring process, low/no code workflow automation solutions.

ASEAN FUSANG Exchange [xl] is a fully-licensed digital securities exchange focused solely on digital assets. This can facilitate the primary issuance and secondary trading of security tokens such as digital securities, cryptocurrencies and fiat currencies. This is licensed as a Securities Exchange and not as a cryptocurrency platform operator or broker/dealer.

China launched the Blockchain-based Service Network (**BSN**) [xli] a global network supporting future central bank digital currencies (CBDC) from multiple countries. This is effectively creating the next generation of the internet, supporting and interconnecting multiple public and private blockchains in an international network. The Chinese version of the network supports only enterprise blockchains and is payment driven with UnionPay [xlii] as founder. If the BSN is adopted at scale, it could have a significant role in setting the standards used by others even if the invention of the component parts is done elsewhere.

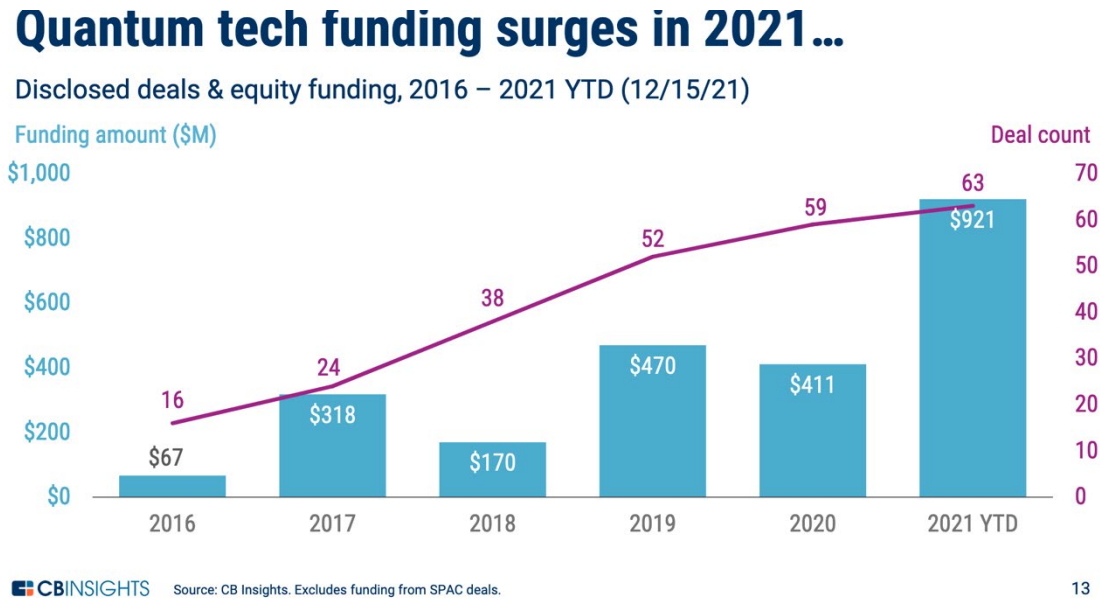
Europe the European Banking Authority (EBA) [xliii] is advancing RegTech//SupTech amidst an already advanced prudential supervisory environment.

What is the Future for REGTECH

Re-thinking corporate governance for the 21st century is an opportunity. The **DAO** presents challenges as it introduces trustless organizations on the INTERNET combining ownership and control of new stakeholders, not been seen before in traditional mechanisms of corporate governance. A blue shift will occur when corporate law, regulation and IT governance merge and investor decisions are implemented by computer algorithms rather than by humans.

Quantum computing provides regulatory challenges and an effective first step is to educate supervisors on the technology outcomes. This will lead to creation of a global standard reducing the risks and opening international discussion on regulatory perspectives. The foremost challenge is around privacy as the encryption system in place today will become vestigial by the increased speed of calculation algorithms and offered as a sacrifice to the innovations that will emerge with a greater number of probabilities and predictions being made about how markets are likely to perform using AI and machine learning. Advances are being made by the US National Institute of Standards and Technology (NIST) [xliv] who are addressing encryption threats that quantum computing poses and other global institutions are expected to follow. In 2017, the NIST launched a Post-Quantum Encryption

Standardization which is not a legal foundation but should encourage legislators and privacy authorities worldwide to start the necessary process of reforming existing and introducing new regulatory frameworks Data protection and privacy laws that hinge on encryption as a technical measure to prevent breaches must be reimagined for quantum computing.



Cybersecurity is logged as the world's short term highest risk but the global financial services industry is witnessing enormous attention to climate change. According to Bloomberg, by 2025 ESG assets may reach as high as $53 trillion [xlv], representing a third of global AUM. As financial institutions upgrade their capabilities regulators will codify frameworks and take steps to encourage companies to become more environmentally and socially conscious. RegTech improves transparency and consistency of regulatory processes around ESG and meeting new climate related obligations in this long term risk.

Regulation in the tokenised crypto world has seen many unregulated mechanisms being addressed well after their implementation as posed consumer risk but at the same time impeded innovation. The innovation is the **IGO** (Initial Game Offering) [xlvi] hosting gaming projecting using NFT's is predicted to move in to the DeFi space very quickly in 2022.

Conclusions and Putting it all Together

21st century regulation is dealing with an intangible asset world where data, intellectual property, cyber, decentralized finance, smart devices and cloud computing dovetail and require an inclusive strategy. Today 90% of corporation assets are intangible The regulatory environment for governments and businesses has never been more challenged due to the exponential scale of technology. Businesses are exposed to regulatory oversight across their lifecycle and as these multiple technologies come together, regulation must be technology neutral with emphasis on regulating the data provenance of cradle to grave settlement of financial transactions across disparate networks. Regulating this new world ecosystem lies within the technology itself to bootstrap for equal exchange of ideas.

A tipping point exists between decentralized finance and retaining a centralized regulation. Technology advances now allows a truly decentralised, mutual, trusted, democratic model where participants can operate peer to peer utilising self-governance with performance based incentives. Without any form of centralised regulation this process will be totally

automated and concerns lie with the custody and KYC of the assets plus a dilemma, cutting across existing data privacy acts, of a loss of ability to back out a transaction once it has been agreed as the smart contracts deployed on blockchain are immutable and final when they execute.

Digital transformation has accelerated after the pandemic and digital assets for the most part represent recognised assets in the physical world with some existing central regulation such as laws around security tokens (STO) [xlvii] which followed initial coin offering (ICO) [xlviii] by regulatory intervention which detractors said stifled innovation. Cryptocurrency assets on the other hand are a completely new business model and if regulators favour centralised control it could have an effect on the market economics of new asset classes bringing larger returns and hedging in a deflationary world. The market debate is highly jurisdictional with Central Bank Digital Currency (CBDC) [xlix] driving centralisation as in China. Historically financial market regulation especially derivative structures, has tended to favour centralized solutions and as crypto grows in strength this approach could inhibit the development of decentralized systems and consequently delay ways to improve stability in financial market infrastructure. There is a need to strike a proper balance between the emergence of stablecoins and CBDC.

Now is the time for businesses to brainstorm their response to regulatory change, be influential and challenge outdated regulation in light of the growing mismatch between traditional financial markets and the mainstream adoption of cyberspace parenthesised by preservation of data privacy and consumer protection. The crypto industry will not wait around for regulators to act and that is obvious by the amount of assets under management and the body of software that supports it. Self- regulatory standards are being formulated for trading, custody and other functions without a recognised taxonomy in place. A number of regulators have issued classification frameworks for digital assets, generally functionally token-oriented and significantly inspired by open and permissionless networks defining, payment/exchange tokens, utility tokens, and security tokens. Existing taxonomies of digital assets have failed to fully capture the true nature of digital assets and novelty introduced by cryptoassets. Many crypto platforms are now looking at how to future proof their technology to pre-empt against regulation to avoid issues when regulation catches up with innovations. A good example is claims reserving in insurance and creation of reinsurance derivatives.

Adoption of blockchain may not change the underlying risks but there are always emerging risk and counterfactuals, however but it opens new ways of supervising these risks. Instead of engineering to fit crypto-assets into existing regulations, which were formulated long before the advent of blockchain emphasis should be on how to use smart contracts to better monitor risks in financial markets. The FinTech landscape is fecund with start-ups which are new entrants do not operate like traditional banks or insurers and have not been subject to the risk management regulations that govern the status quo. With the emergence of NFT's and global stablecoin arrangements in parallel it stresses the need for cross-border cooperation and information-sharing arrangements that mitigate arbitrage and fraud. The use of AI is going to play an important role both for RegTech/SupTech so companies and regulatory teams would have more time to spend on pre-emptive and early supervisory actions.

The DAO is going to be a pathfinder into the future as they are completely decentralized entities self-governed by technology but are the digital equivalent of a "company house" registrations. Regulators in certain jurisdictions are starting to accept these legally and the degree of international adoption will certainly address the Defi (decentralized finance) and CeFi (centralized finance) balance. CAOs (centralized autonomous organizations on a network) will emerge governed by smart contracts. The DAO will remain as a marker along

the path to the future of blockchain, smart contracts, and the corporations of the 21st century.

An unregulated crypto ecosystem could lead to financial instability so regulators need to combine to develop global standards around the economic benefit and risks posed by this new model. Counterfactuals (missing data gaps) need to be assessed in this regard. So the hard two questions that will be asked by regulators will be firstly how much automation using blockchain and smart contracts is too much and what balance of centralization is needed to avoid inhibit the need for new asset classes? Secondly with the use of AI what extent will machines substitute human judgment in supervision and while removing repetitive tasks what degree of augmentation is needed?

There is a lot of work required by regulators in 2022 and beyond to address arbitrage and potential financial crime from the decentralized world in conjunction with all the new innovations emerging of economic importance including healthcare. The key thing that emerges is that the solutions to the regulation of a new digitized world exist within the properties of the exponential technology itself and not from outdated legal systems, lowering the cost of financial services and making them faster and accessible across borders.

References

[i] https://www.weforum.org/focus/fourth-industrial-revolution
[ii] https://www.investopedia.com/web-20-web-30-5208698
[iii] https://www.marketwatch.com/press-release/regulatory-technology-regtech-market-2021-growing-rapidly-with-modern-trends-development-investment-opportunities-share-revenue-demand-and-forecast-to-2030-2021-11-16
[iv] https://www.indexinsuranceforum.org/faq/what-basis-risk
[v] https://www.bis.org/
[vi] https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html
[vii] https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/
[viii] https://en.wikipedia.org/wiki/Mt._Gox
[ix] https://gadgets.ndtv.com/cryptocurrency/news/cryptocurrency-market-cap-usd-2-5-trillion-2580254
[x] https://en.wikipedia.org/wiki/Fork_(blockchain)
[xi] https://www.investopedia.com/tech/bitcoin-vs-bitcoin-cash-whats-difference/
[xii] https://www.hyperledger.org/use/fabric
[xiii] https://www.leewayhertz.com/blockchain-interoperability-crosschain-technology/
[xiv] https://medium.com/work-futures/minimum-viable-ecosystem-53ae03d43cbf
[xv] https://www.gartner.com/en/newsroom/press-releases/2021-02-15-gartner-forecasts-worldwide-low-code-development-technologies-market-to-grow-23-percent-in-2021
[xvi] https://elibrary.worldbank.org/doi/abs/10.1596/0-8213-5041-2
[xvii] https://us.milliman.com/-/media/milliman/pdfs/2021-articles/12-9-2015-ria-mi-ph-report.ashx
[xviii] https://cartorios.org/wp-content/uploads/2020/11/LESSIG._Lawrence_Code_is_law.pdf
[xix] https://www4.comp.polyu.edu.hk/~csxluo/SADPonzi.pdf
[xx] https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf
[xxi] https://www.investopedia.com/terms/s/stablecoin.asp
[xxii] legally recognized Decentralized Autonomous Organization (DAO)
[xxiii] https://analycat.com/adi-hazan-addressed-the-old-library-in-lloyds/
[xxiv] https://www.ultirisk.com/
[xxv] https://gdpr-info.eu/
[xxvi] https://guardtime.com/
[xxvii] https://www.aha.org/system/files/2018-02/regulatory-overload-report.pdf
[xxviii] https://thehackernews.com/2021/12/new-local-attack-vector-expands-attack.html
[xxix] https://openssf.org/

[xxx] https://www.linuxfoundation.org/
[xxxi] https://aaisonline.com/
[xxxii] https://www.linux.com/news/what-is-openidl-the-open-insurance-data-link-platform/
[xxxiii] https://github.com/finos/open-regtech-sig
[xxxiv] https://www.linuxfoundation.org/press-release/finos-launches-open-regtech-initiative-as-it-receives-record-high-number-of-open-source-contributions/
[xxxv] https://www.newyorkfed.org/aboutthefed/nyic
[xxxvi] https://www.bloomberg.com/news/articles/2021-12-21/credit-unions-seek-regulator-approval-to-hold-crypto-assets
[xxxvii] https://www.hkma.gov.hk/eng/news-and-media/press-releases/2021/11/20211105-6/
[xxxviii] http://www.cyberport.hk/en
[xxxix] https://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20210608e1.pdf
[xl] https://www.fusang.co/
[xli] https://bsnbase.io/g/main/index
[xlii] https://en.wikipedia.org/wiki/UnionPay
[xliii] https://www.eba.europa.eu/
[xliv] https://www.nist.gov
[xlv] https://www.bloomberg.com/professional/blog/esg-assets-may-hit-53-trillion-by-2025-a-third-of-global-aum/
[xlvi] https://coinmarketcap.com/alexandria/glossary/initial-game-offering-igo
[xlvii] https://www.investopedia.com/tech/2018-year-security-token/
[xlviii] https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp
[xlix] https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp

1.2022

David Piesse
CEO, DP88

About the Author:
David Piesse is CEO of a family office, DP88, specialising in InsurTech initiatives in Asia - www,DP88.com.hk. David has held numerous positions in a 40-year career including Global Insurance Lead for SUN Microsystems, Asia Pacific Chairman for Unirisx, United Nations Risk Management Consultant, Canadian government roles and staring career in Lloyds of London and associated market. David is an Asia Pacific specialist having lived in Asia 30 years with educational background at the British Computer Society and the Chartered Insurance Institute.