



GBBC
Global Blockchain
Business Council

CHAIN REACTION: BLOCKCHAIN ENTERS THE MAINSTREAM

THE GBBC 2020 ANNUAL REPORT

SUPPORTED BY ACCENTURE



GBBC

SUPPORTED BY:



2020 **ANNUAL REPORT**

TABLE OF CONTENTS

Foreward.....	3
Introduction	4
Featured: Accenture	6
Financial Services.....	8
Digital Identity.....	18
Government.....	22
Business Processes & Insurance.....	24
Supply Chain	28
Energy.....	32
Social Impact.....	34
Arts & Media	38
Legal & Regulatory: Jurisdictions.....	42
Legal & Regulatory: Thought Pieces.....	72
Appendix.....	86
Conclusion.....	92

FOREWORD

TOMICAH TILLEMANN
CHAIR, GBBC



The 1920s were a time of extraordinary innovation. The commercialization of the automobile, airplane, and assembly line would transform the way citizens and society interacted and engaged in commerce. Now, a hundred years later, we are poised to experience something similar during the 2020s. A host of new technologies, including and perhaps especially blockchain, are moving out of the laboratory and into our lives — but not without a great deal of attendant effort and turmoil.

Just as the breakthroughs of the 1920s eventually shaped a century of investment in physical infrastructure, from interstate highways to intercontinental air travel and global manufacturing, the standards, principles, and practices that take root during the 2020s could once again guide a century of investment in digital infrastructure. More importantly, the systems built on these standards will shape and structure our economies, societies, and governments.

In 2019, the debate surrounding the future of blockchain innovation and regulation advanced rapidly from white papers to the White House and touched thousands of organizations and companies along the way. Breathless media coverage of crypto windfalls waned, and a deeper discussion about the digital platforms that will power the next century grew up in its place.

We must approach this debate with equal portions of humility and responsibility. Humility because the only certainty we have right now is that we don't possess all the answers. Responsibility because, if nothing else, we are beginning to grasp the magnitude of the questions ahead.

In the closing weeks of 2019, the GBBC came together with Members of the U.S. House and Senate in Washington for a remarkable demonstration day during which visionary leaders from industry showcased how blockchain is solving some of the most urgent challenges facing humankind. At a moment of crisis for many institutions, blockchain is helping rebuild trust, efficiency, and transparency in real-world applications that demand attention and respect.

At the same time, we have seen concerns about the misuse of technology reach unprecedented heights. Those fears, while often legitimate in their origins, threaten to suffocate a generation of new solutions just as they begin to mature.

It is because of the uncertainty on the horizon and the importance of the decisions confronting industry and government that the work of the GBBC has never been more vital. The Council's extraordinary executive team and members are engaging the private and public sectors to create clarity and common ground at a moment of division and disinformation. The GBBC's global network of ambassadors, eminent leaders drawn from over 50 countries, are building bridges of understanding over tides of mistrust.

This report provides a sampling of that work. The scope and urgency of these efforts will intensify in the months and years ahead. We look forward to collaborating with you and to deliver a decade of transformational breakthroughs during the 2020s. If we succeed, together, we can shape the next century of investment in global digital infrastructure and spread its benefits worldwide.



INTRODUCTION

SANDRA RO | CEO, GBBC

2019 — the year of proving blockchain is real and backing that up with real use cases to solve real problems.

And what have we learned matters the most in doing business? It is TRUST.

How do we help build and scale the next multi-trillion (insert your favorite crypto/digital asset/ fiat currency here) industry to create value and opportunities for the future? Trust.

What do we need to bring people and governments together in collaboration and help build sustainable, equitable societies? Trust.

Blockchain technology can help bring light to places where transparency is needed, where trust needs to be rebuilt. If trust is the bedrock on which humans develop relationships, drive innovation, and create opportunities for many, then blockchain technology's clear opportunity set (including the use of tokenization of assets and value) is as the trust enabler.

So, what did GBBC learn in 2019?

WE NEED SCALING:

Next level blockchain technology adoption requires massive scaling and some projects are stuck. We need all stakeholders to go to next level - motivated governments working in tandem with entrepreneurs, startups, and corporations. We also need sound legal frameworks, critical infrastructure, and mindset shifts to consider new paradigms and decentralized ways of restructuring organizations, processes, and power.

GOVERNMENTS AND BORDERLESS GROUPS (E.G. BITCOIN, ETHEREUM, SOCIAL NETWORKS, CONSORTIA) WILL BE KEY STAKEHOLDERS:

The demand for education and better understanding of practical use cases for emerging technologies, including blockchain, remains very high from governments around the world.

The GBBC conducted closed door sessions as well as public open-door forums for discourse and showcasing blockchain projects in 35 cities across 16 countries and 4 continents, including Bahrain, Kazakhstan, The Netherlands, and Japan.

EYES ON THE US — BEHIND THE CURVE BUT STILL AN IMPORTANT DRIVER

The GBBC's Capitol Hill event in July, bringing city, state, and federal government together for the first time to encourage blockchain and digital asset discourse across the US, was met with tremendous positive feedback. This led to Demo Day on the Hill in November, during which some of our members highlighted their use cases in front of members of Congress and their staffers.

The GBBC has not always spent a great deal of time on the Hill, but with increasing requests for education and partnership coming from the federal government, as well as states and cities like NYC and LA, we have added the US as a strategic regulatory focus. The GBBC has participated and continues to participate in hearings and briefings with regulators, Senate committees, as well as the State Department and others, all of which yield effective insights and discourse around the nature of cryptocurrencies, digital assets, and blockchain use cases.

MAIN TAKE AWAY:

The number one question when GBBC meets with government officials, regulators, and corporate executives around the world is: what are the real use cases in blockchain? This is usually followed by: who is really implementing it?

The good news is that there are many examples from which to draw, as provided in this Annual Report.

Furthermore, the rise of influence and power of social networks and grassroots groups should not be underestimated. We will see more in 2020 and beyond, and we are working with those associations and consortia which share similar missions and goals.

2020 NEXT STEPS:

The GBBC has launched an internal Advisory Services subsidiary to meet the demands of specialized pre-evaluation work with select governments to then launch requests for proposal to GBBC Members.

The new service offers additional business development opportunities to GBBC Members, as more and more governments look to implement their own blockchain use cases to improve the delivery of services to citizens, increase trust and transparency, and solve critical problems.

We remain focused on creating a democratized opportunity set for many and will prioritize delivering education and policy sessions in parts of South America, Southeast Asia, India, South Africa, and the Caribbean, as well as working closely with like-minded social networks and borderless groups.

2020: NEW DECADE — GROWING, MATURING INDUSTRY

The message that resonates the most, the message that we, the GBBC and its Members, supporters and Ambassadors are encouraged to share is this:

- Blockchain technology is a useful tool to enable and increase trust in a world where distrust, misinformation, and manipulation creates uncertainty, instability, and sometimes, chaos;

- Blockchain technology cannot solve all problems but it can shed light in areas where opacity or confusion over information reigns. The opportunities are staggering; coupled with other emerging technologies, blockchain has applications in nearly every industry - from media, to supply chains, to governments, to financial services, to NGOs and nonprofits.

There are plenty of skeptics who believe blockchain and crypto are dead or "blockchain good, crypto bad." Those of us who have been in the space for a long time know these arguments well.

In 2020, the bitcoin white paper will be 12 years old, the protocol 11; the underlying components of blockchain technology have been around for decades before that. Blockchain is not an unproven, theoretical technology, but rather one that is already being deployed and is critical in today's modern world to build the trust and transparency some parts of society desperately need today.

With deep gratitude to our many GBBC Members, Ambassadors, Observing Members, Sponsors, and supporters from around the world, thank you for dreaming of a better society, daring to be different, and collaborating with us to show the world humanity can use technology for good.

How do we get there? By sharing, speaking, and collaborating with each other. The profound paradigm shift blockchain enables is to a society with fewer zero-sum games and more collaboration.

Together, in 2020 and the decade beyond, we can spearhead change to create more secure, equitable, and functional societies around the globe.

FEATURED



NEW MONEY: HOW CBDC IS CHANGING HOW CENTRAL BANKS WORK

BY OUSMÈNE JACQUES MANDENG & DAVID TREAT

The architecture of money is changing. Major investments are being made in digital finance, and large players like global banks and social media companies are creating new ways to transfer value among ecosystems that aren't tied to traditional borders or currencies. Facebook's Libra, JPM Coin, and other initiatives by commercial banks signal an emerging demand for new types of money, underscoring the inadequacy of the status quo. As a result, central banks can no longer take for granted that their monies will be able to preserve the monopoly they have maintained for more than a century. To remain future-proof, central bank money must be modernized to meet the new demands and functionalities of our digital world.

THE SYSTEM MUST RISE WITH THE TIDE

Because central bank money is typically regarded as the most reliable source currency we have, economic and financial conditions depend on the efficient distribution of it. Yet, access to central bank money remains highly restricted due to the risk of adverse distributional effects.

Improving access to central bank money could produce a multitude of benefits. By promoting market inclusion and integration both domestically and internationally, it could bear important welfare gains in addition to supporting more efficient price formation and cross-market competition. In any case, central bank money must become more accessible to remain functionally relevant.

THE INNOVATION BEHIND CBDC: TOKENIZATION

Central banks today issue bank notes and reserves as a means of settlement. Central Bank Digital Currencies (CBDC) represent a third format offering new functionalities, scope, and possibilities, forming an integral part of the monetary base that is fully fungible with bank notes and reserves. The innovation around CBDC is the use of tokens—digital representations of value that provide several advantages over traditional formats of money:

- They're portable—they can exist outside the central bank in digital format for the first time and be deployed and used anywhere, anytime.

- They allow for the preservation of the existing two-tiered banking system, supporting financial stability while offering new payment functionalities.
- They can be embedded with smart contracts, where the rights and obligations of the bearer can be embedded in the asset, opening up new opportunities.

These properties allow central bank money itself to become a transferable bearer instrument in digital form, which in turn enables CBDC to expand access to money as well as its utility within the two-tier banking system.

Tokens can best be employed using blockchain and other types of distributed ledger technologies (DLT) to confirm authenticity, validation of transactions, and integrity of the network while addressing critical security, scalability, and privacy in payments.

INITIAL BENEFITS AT A GLANCE

CBDC will likely coexist with traditional central bank monies to improve payments at the retail, wholesale, and international levels.

- **Retail** — CBDC gives people the choice and flexibility to make online payments with central bank money in addition to credit/debit cards — effectively allowing them to transact in the digital world as though they were using cash, transferring value instantly. CBDC could be distributed to the end-user through commercial banks, just like cash.
- **Wholesale** — Large-value payments, such as securities trading, are normally settled through interbank clearing at the central bank. Token-based financial market infrastructures, however, could use CBDC to settle these transactions more efficiently, end-to-end, through token-for-token swaps.
- **International** — The reliance on a network of banks and third parties makes international

payments slow, expensive, opaque, and continually reliant on a small set of national currencies. CBDC establishes more direct monetary relations and can amplify the role of smaller currencies in settlement. It also supports integration by offering settlement in central bank money to a broader range of markets.

By expanding access and distribution of central bank money, CBDC fosters the creation of new business models and new, token-based financial ecosystems.

WHO'S LEADING THE WAY

While the adoption of CBDC seems inevitable, some central banks are more prepared than others. In December, Sweden's Riksbank awarded a public tender for a retail CBDC for the development of a pilot via its e-krona project, set to kick off in 2020. Also in December, Banque de France announced a call for CBDC projects to counter private sector initiatives like Libra as well as the dominance of the US dollar. In October, the Swiss National Bank stated it will launch a test to use CBDC for wholesale payments on the Swiss Digital Exchange (SDX). The People's Bank of China has repeatedly affirmed it has developed a CBDC and is expected to initiate adoption soon.

Despite its potential, many central banks are hesitant about the adoption of CBDC. This, in part, rests on the uncertainty of the effect of CBDC on the financial system and whether it may cause some crowding out of commercial bank monies. Wider access to central bank money may also be seen with some trepidation. However, the aim is not to disrupt financial intermediation, but rather to streamline access to central bank liquidity domestically and internationally — therein lies the potential.

2020 will be an important year for CBDC. Look to Accenture as we continue to develop the CBDC space alongside our clients and partners. To learn more, visit [Accenture.com/CBDC](https://www.accenture.com/CBDC).



FINANCIAL SERVICES



NIGHTFALL

Public blockchains like Ethereum and Bitcoin, which are the most widely used and accessible blockchain systems, do not in their native state support private transactions. All transactions are done in an entirely transparent manner. Blockchains, far from being anonymous, are in fact highly transparent. While individual users may enjoy a level of privacy as one small entry in a “sea” of transactions, for enterprise users, this lack of privacy makes adoption of public blockchains impractical for most applications: modern analytical tools would allow competitors to sift through the blockchain and discern business operations and strategy.

Private blockchains were created to provide enterprise users with a blockchain-like architecture while allowing for a level of privacy, but these systems are not decentralized, therefore, they lack the network effects, scale, and immutability of large public blockchains. We do not believe that centralized blockchains serve the public interest or are ever likely to achieve significant network effects. Consequently, EY created Nightfall to make it possible for enterprise users to transact securely and privately on the public blockchains.

Nightfall makes use of a mathematical innovation called a Zero Knowledge Proof (ZKP), which allows users to prove certain items are true without revealing the underlying information. This allows for provably secure, private transactions on public networks. While ZKPs have been available to consumers through specialized cryptocurrency transactions for some time, Nightfall is the first solution that allows any asset or token to be transferred in complete privacy and is designed for enterprise adoption.

EY has made Nightfall available as a public domain application — anyone can use it. The system is designed to support privacy with full regulatory compliance. Transaction data from Nightfall users can be integrated into EY’s Blockchain Analyzer for financial statement audits and transaction analytics. Users can also implement both white lists and black lists for allowed and blocked addresses to comply with regulatory requirements such as Know Your Customer (KYC) and Anti-Money-Laundering (AML) rules.



FIDELITY

Institutional investors are finding appeal in digital assets and many are looking to invest more in digital assets in the near term, according to 2019 research from Fidelity Investments®. In a survey of more than 400 U.S. institutional investors, about 22% have had some exposure to digital assets, with most investments having been made within the past three years. Four in ten respondents say they are open to future investments in digital assets over the next five years.

These findings are part of a study to better understand how institutions, advisors, and investors think about digital assets both overall, and as part of an investment portfolio.

- Almost half of those surveyed (47%) view digital assets as having a place in their investment portfolios. Nearly seven in ten cited certain characteristics of digital assets as appealing.
- Nearly half of respondents (47%) appreciate that digital assets are an innovative technology play
- 46% find digital assets' low correlation to other assets among the most appealing characteristic

Many ponder what is required to enable additional institutional adoption. We see progress as more institutional investors are engaging with digital assets, either directly or

through service providers, as the potential impact of blockchain technology on financial markets — new and old — becomes more readily apparent.

Analysis of on-chain data and network activity also demonstrates a steady increase over 2019 in key market metrics and signals, which are actively tracked and reviewed by a growing network of market researchers and analysts. Continued venture interest has fueled the ongoing maturation of necessary services and tools institutions require.

At Fidelity, we support further advancement of the ecosystem on many fronts. We began research and development efforts in 2014, started mining bitcoin in 2015, and tested our first digital asset storage solution with employees in 2016. We launched Fidelity Digital AssetsSM to service the unique needs of institutional investors. We look ahead to further progress in the digital assets ecosystem as critical components — such as custody — are addressed, enabling these markets and a new range of access vehicles to continue to develop.

METHODOLOGY:

Survey conducted for Fidelity by Greenwich Associates of 441 institutional investors. Surveys were collected by phone and digitally from November 26, 2018 to February 8, 2019.



Here's what institutional investors find appealing about digital assets

Innovative tech play
47%

Uncorrelated to other assets
46%

High potential upside
27%

Enable decentralization
25%



Services are provided by Fidelity Digital Asset Services, LLC (NMLS ID 1773897). The Fidelity Digital Assets logo is a service mark of FMR LLC © 2019 FMR LLC. All rights reserved. Survey conducted for Fidelity by Greenwich Associates of 441 institutional investors. Surveys were collected by phone and digitally from November 26, 2018 to February 8, 2019. 884957.1.0

Nearly half of institutional investors see a place for digital assets in their portfolios



Services are provided by Fidelity Digital Asset Services, LLC (NMLS ID 1773897). The Fidelity Digital Assets logo is a service mark of FMR LLC © 2019 FMR LLC. All rights reserved. Survey conducted for Fidelity by Greenwich Associates of 441 institutional investors. Surveys were collected by phone and digitally from November 26, 2018 to February 8, 2019. 884957.1.0

DIGINEX

Despite digital assets growing into a \$225 billion industry, institutional players have largely remained on the sidelines. The common challenge amongst large money managers, such as hedge funds and family offices, is where to safely and securely store large sums of digital assets.

While it may seem that there are many options in the market, quality has not always kept up with quantity. For the past decade, the search for a competent, trustworthy and secure digital asset custodian has been a challenge. That is why Diginex launched Digivault earlier this year, offering a solution that integrates institutional-grade custody storage with bank-grade technology and unparalleled security measures. This comes at a crucial time for the digital asset industry as losses from thefts, scams and misappropriation of funds totaled US\$4.26 billion in the first half of 2019.

To meet the exacting needs of sophisticated investors, Digivault's Kelvin solution offers secure, digital asset cold storage infrastructure inside the vaults of leading storage provider Malca-Amit. This cooperation enables Digivault to store client assets at the same standards as

precious metals, in vaults that meet the highest grades of bank-entrusted vault classification in select locations in Europe and Asia.

Digivault's completely air-gapped transaction process removes the need for conventional USB devices (or any other electronic device) to safeguard assets from the threat of hacks by eliminating the presence of WiFi, Bluetooth, and near-field communication capabilities. Digivault's solution is based on well-established methods using Hardware Security Modules to safeguard digital assets by way of securing private keys using physical objects, like key cards.

In order to develop this infrastructure, the Digivault team leveraged decades of experience in designing, developing, and delivering highly secure infrastructure solutions for the world's leading financial institutions, national defense, and security sectors.

At a time when cyberthreats, risks of human mismanagement, staff exploitation, and online attacks are abundant, Digivault has arrived to serve institutions who are eager for a top-caliber digital asset custodian that unfailingly brings them absolute peace of mind.

GENESIS GLOBAL TRADING

In 2019, Genesis, a worldwide leader in over-the-counter digital currency trading and lending, made its first-ever acquisition, proving itself an innovator in the virtual currency space. In September, Genesis announced the acquisition of the assets of Qu Capital, a New York-based quantitative investment and research firm. Founded in 2017, Qu Capital has developed state-of-the-art trading technology, including faster exchange connectivity, improved order routing, and advanced execution tools, and conducted quantitative research on the digital currency market. Qu Capital originally focused on applying statistical techniques to identify and trade inefficiencies across asset classes.

The acquisition bolstered Genesis's technology capabilities and intellectual firepower in order to better serve clients in an increasingly competitive marketplace. Genesis is committed to offering best-in-class trading and lending technology solutions to its institutional counterparties. The addition of the Qu Capital tools, which incorporate machine learning and other advanced methodologies into Genesis's existing technology stack and new product offerings, consolidates the company's innovative position in its industry. Genesis is initially leveraging the acquired technology to enhance trade execution for clients through improved price discovery. In

the future, Genesis could use the home-grown technology to build an integrated platform where users can access trading and lending through one clickable graphical user interface.

A broker-dealer registered with the Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA) and a BitLicense holder with the New York State Department of Financial Services, Genesis Global Trading is a pioneer in digital currency market making. It facilitates trades for institutional investors and high net worth individuals looking to buy or sell large sums of digital currencies. Genesis provides liquidity to its trading partners, along with same-day settlement, 24/7 trading, and deep institutional expertise developed from trading billions of dollars in digital assets since entering the industry in 2013.

Genesis is a wholly owned subsidiary of Digital Currency Group (DCG). In addition to Genesis, DCG is the parent company of Grayscale Investments, the largest asset manager in the digital currency industry, and CoinDesk, a leading media and events company. In 2018, Genesis launched its lending business, Genesis Capital, to provide a platform for borrowing and lending digital currencies. The lending arm of Genesis experienced significant growth in 2019.



QUORUM

Based on Ethereum, Quorum is an open source blockchain platform that combines the innovation of the public Ethereum community with enhancements to support enterprise needs. Quorum provides an end-to-end solution for building use cases and networks on blockchain. The Quorum team is global, with a strong presence across New York City, London, and Singapore.

Some of Quorum’s features that encourage enterprise adoption are:

- **Performance:** Design enables high throughput to support enterprise use cases.
- **Permissions:** Quorum offers roles-based access and rule-driven permissions to ensure control over which entities join the networks and what sort of access to information entities have.
- **Configurable consensus:** Multiple consensus options that are scalable, proven across 2000+ networks, and designed for permissioned environments. Users may also pick a consensus algorithm to suit their requirements: RAFT, IBFT, or Clique POA.

- **Privacy:** A unique privacy solution that is scalable, secure, and fully decentralized. The privacy solution has no single point of failure or third-party dependencies. Moreover, private information is never broadcast to network participants, and private data is encrypted and only shared directly with relevant parties.
- **Ethereum-based:** Quorum works with existing Ethereum tools, including: Truffle, MetaMask, Remix and OpenZeppelin (to name a few) — they’re ready to use and intuitive with the platform.

Enterprises across industries choose to adopt Quorum due to its robust feature set and simple integration that enables developers to seamlessly deploy applications. For example, J.P. Morgan and enterprise networks such as the Interbank Information Network (with over 300+ participating banks) use Quorum in a live production environment.

Most importantly, Quorum is always evolving. Dedicated researchers continuously bring the latest in privacy, consensus, and other technological developments to Quorum.



SORAMITSU

Soramitsu provides services to many financial institutions using blockchain-based solutions built on the Hyperledger Iroha blockchain platform. One prominent project is Bakong, a real-time gross payment system for the National Bank of Cambodia. This is the first blockchain-based retail payments platform in the world in use by a central bank. As of this writing, Bakong has thousands of users and has processed millions of dollars in transaction volume.

As a retail payments platform, Bakong presents an opportunity to improve access to banking and financial services, while increasing the efficiency of economic activity in Cambodia. In Bakong, Soramitsu leverages its open-source, private, permissioned blockchain protocol, Hyperledger Iroha, to create a retail payments system for a central bank and commercial banks. Moreover, by incorporating identity management within the transaction process system, central banks can benefit from increased safety, while reducing costs, and achieving a great user experience.

As almost 80 percent of Cambodian citizens are unbanked, the vast majority of financial transactions utilize US Dollars (USD) and Khmer Riel banknotes. Many physical bank locations are located in urban centers, which makes it difficult for those living in rural areas to access financial services. With the advent of expanded cellular networks and lower costs for smartphones, communications technologies are far more accessible by the populace than

banking services, thus providing an opportunity to give a wider demographic greater access to digital payments using existing communications technologies.

Through Bakong, anyone with a Cambodian phone number and a smartphone can access payments in USD or Khmer Riel. This can add an estimated 1-2 percent to the Gross Domestic Product (GDP) through increased efficiency, while creating new opportunities for both domestic and international trade. Bakong also creates immediate potential for lowering transaction fees and costs associated with compliance. Moreover, the potential for building a digital economy based around Internet commerce could have a profound impact on economic growth and the creation of new industries, as we have seen in developed nations. This will help broaden the opportunities for Cambodian citizens and lead to a higher quality of life.

Soramitsu designed the Bakong payment platform with the potential to evolve and adhere to future payments standards. The platform is modular and can be adapted to future use cases, as well as integrated efficiently with existing banking infrastructure. Soramitsu hopes to expand the geographic reach of Bakong by forging new partnerships in the near future, which will allow for further efficiencies with respect to cross-border payments and settlements.

Soramitsu (www.soramitsu.co.jp) is a boutique fintech company with over 70 employees in Japan, Switzerland, United States, Russia, and Cambodia. Specializing in providing applications for financial institutions that use blockchain technology, Soramitsu created Hyperledger Iroha, a private, permissioned blockchain platform that is part of the Linux Foundation’s Hyperledger Project.

REITBZ

THE CHALLENGE

While information, communication, music, and other forms of media are easily accessible on a global scale for users through a click of a button on a mobile app, ordinary investors are still restricted to a limited range of local investment opportunities.

For example, if a person in Kenya wants to invest in real estate assets in Brazil, this investor will most likely face huge upfront costs associated with developing a legal structure that allows them to have exposure to a foreign real estate asset. In practical terms, these costs are economically prohibitive for many investors, making it an economically unfeasible investment.

Consequently, ReitBZ was created to provide a service and an investment vehicle that enables investors from anywhere in the world to have democratic access to high-quality investments.

STRATEGY

Given that blockchain is a relatively new technology, business regulations for blockchain projects are nonexistent or unclear in many

jurisdictions. As a result, BTGPactual decided to set up ReitBZ in the Cayman Islands and limit token sales to a select list of countries.

The launch of ReitBZ comes at a time when the Brazilian economy is poised for investment in distressed real estate assets.

Moreover, the idea of tokenizing real estate assets was appealing both from an experimental perspective, but also given the associated benefits to the existing real estate business model, including global and pulverized distribution, transparency, ease of auditing, and cost efficiencies.

RESULTS ACHIEVED

ReitBZ's security token offering (STO) raised close to \$10 million (USD) in 3 months, reaching dozens of institutional and individual investors from America, Europe, Africa, and Asia.

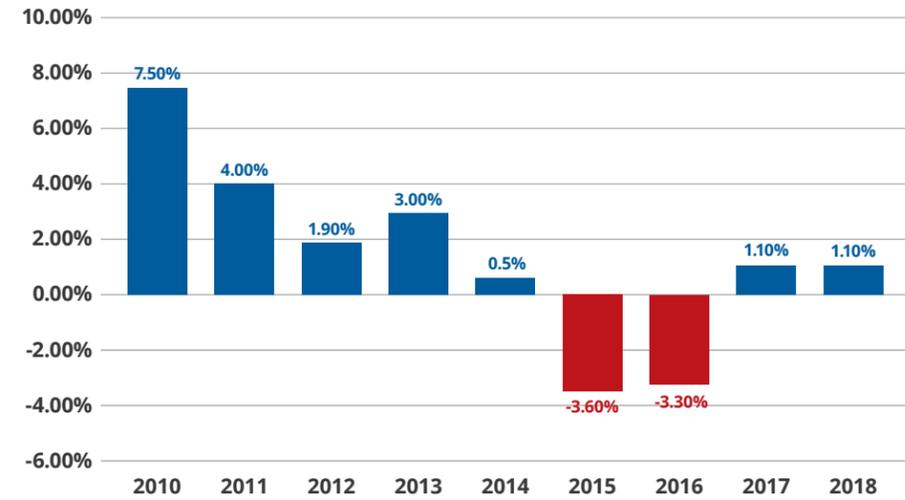


Figure 1. GDP year-on-year % change

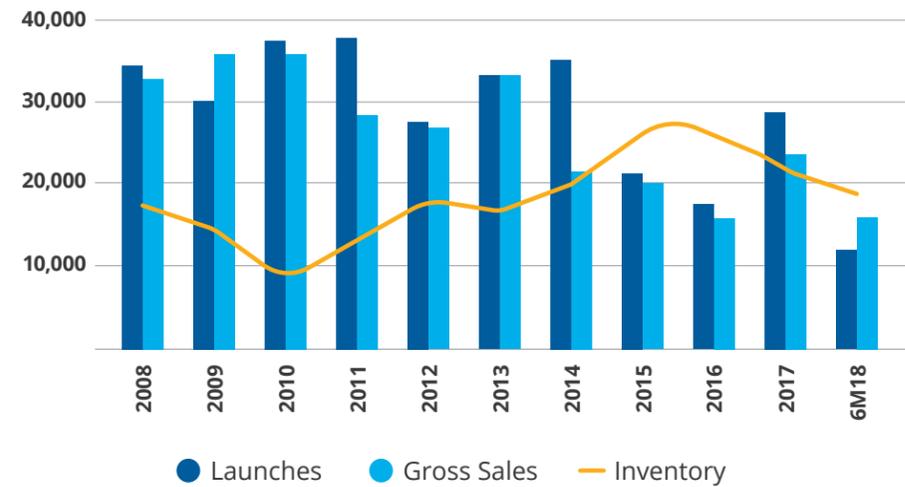


Figure 2. Housing inventories in São Paulo

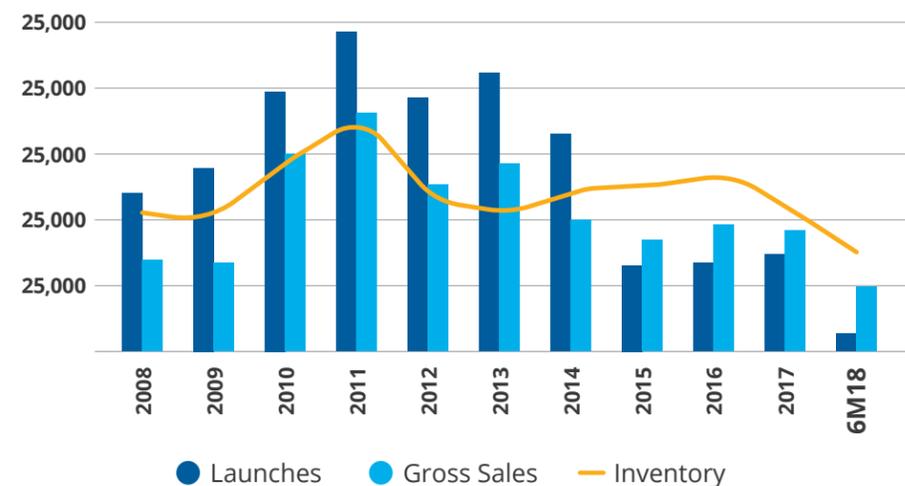


Figure 3. Housing inventories in Rio de Janeiro

DIGITAL IDENTITY



ACCENTURE

By 2030, international air arrivals are expected to reach 1.8 billion passengers, up 50 percent from 2016. This projected growth is far outpacing growth in airport capacity, putting the aviation industry under pressure to improve the flow of passengers through the world's airports — not only to improve the traveler experience, but also to mitigate potential increased risks to security, as more people cross international borders.

Known Traveller Digital Identity or KTDI (KTDI.org) is a World Economic Forum initiative that brings together a global consortium of individuals, governments, authorities and the travel industry to enhance security in world travel. The pilot, scheduled to go live in early 2020, leverages cryptography, blockchain technology and biometrics to allow cross-border travel

without presenting physical documents. This will accelerate the flow of passengers through airports, improving the passenger experience, and enabling authorities to better focus limited resources on critical risks.

In the future, KTDI would also allow passengers to consent to share their personal preferences and trusted identity data with other organizations — enabling a more personalized and meaningful experience.

For the KTDI concept to achieve its potential, the digital identity itself must be useful to the individual. That means it needs to be trusted and accepted by authorities and organizations globally. At the heart of KTDI is the importance of using international, open standards enabling

**UNWTO Tourism Towards 2030:
Actual Trend and Forecast 1950-2030**

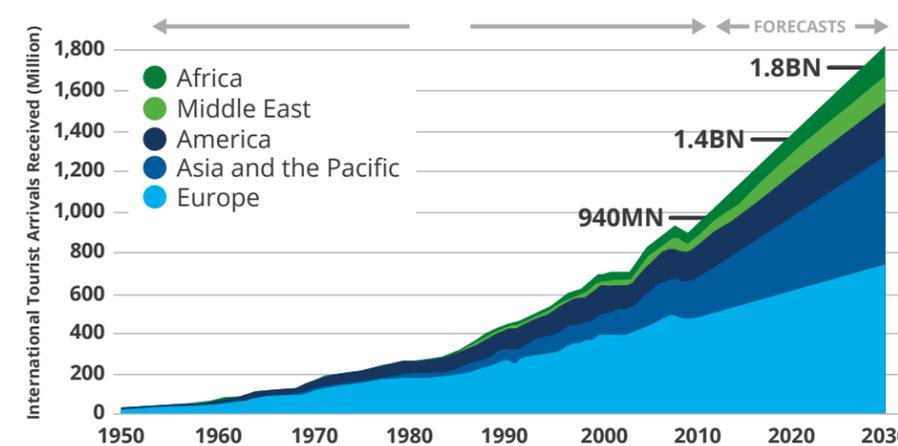


Figure 1: Actual trend and forecasts 1950-2030 for international arrivals, UNWTO1

interoperability across geographies, policy environments, and industries. The pilot group of roughly 5000 individuals will document and share lessons learned regarding policies, processes, technologies used, and how these can be improved to scale the KTDI concept across the travel and tourism sectors.

But this is just the start. It is estimated that we will each maintain an average of over 200 digital accounts by 2020. By expanding the concept

to support use cases across multiple industries that require a trusted, verifiable identity to conduct business (like banking, insurance, and healthcare) we can simplify more processes.

In addition, KTDI enables organizations to look beyond siloed identity models, focusing instead on collaboration in new ecosystems to unlock potential economic value, estimated to be worth between 3% and 13% of GDP depending on the country.

Through the course of the project, eID+ has constantly evolved, adding additional layers of security and features. The launch of eID+ v2.0 in early 2019 brought with it the integration of Futuræ's AI-assisted 2-factor authentication and Skribble's qualified electronic signature. Most recently, Procivis launched a pilot project in Schaffhausen leveraging Swisscom and Swiss Post's "Consensus as a Service" blockchain infrastructure for the issuance of tamper-evident

debt registry extracts. With the new service, citizens of the Canton of Schaffhausen can receive their debt registry extract immediately on their eID+ app, a process which used to take several days. The launch of the service also marked the start of a strategic partnership between Procivis and Swisscom to drive widespread adoption of blockchain-secured services for government.



eID+

Procivis AG was founded in September 2016 with the mission of empowering citizens with trusted digital tools to bring them closer to their governments. After an internally commissioned study that compared Switzerland and Estonia's e-Government efforts over twenty years, Procivis realized that a trusted digital identity is a necessary prerequisite for a digital society and that the market lacked such a solution. As a first step towards setting this mission in motion, Procivis developed its smartphone-based eID+ digital identity platform, secured by decentralized public key infrastructure (DPKI). Composed of three core features, e-Authentication, e-Signatures, and e-Payments, eID+ serves as a foundation for a host of eGovernment services.

In the summer of 2017, Procivis was mandated by the Swiss Canton of Schaffhausen to test eID+ in a pilot project. Over the course of the pilot, Procivis collaborated with academics from the Zurich University of Applied Sciences to continually evaluate eID+'s user experience, leading to a final product that is closely aligned with the needs of citizens and government officials. After successfully testing the solution over a six month period, the eID+ digital identity platform was rolled out to the citizens of Schaffhausen. Today, a year after the roll out, Procivis' eID+ enables the citizens of Schaffhausen to access over 100 eGovernment services through the Canton's eGov portal.



eID+ The Swiss Army knife for digital citizens

GOVERNMENT



INDIA'S BLOCKCHAIN DISTRICT, HYDERABAD

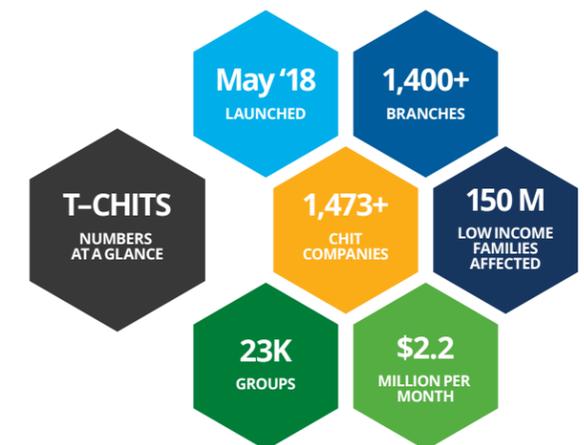
In 2018, India's provincial Government of Telangana recognized the potential of blockchain technology and resolved to establish Hyderabad as a blockchain hub. Hyderabad, the capital city of Telangana, is uniquely positioned to take a leadership role in the development of blockchain technology, due to the critical mass of industries leveraging blockchain technology located in Hyderabad, access to a robust talent pool, support of entrepreneurship, and collaboration with enterprises.

In the last 2 years, the Hyderabad Blockchain District has collaborated with IIITH (Renowned IT University of India), Tech Mahindra (Indian IT giant), CDAC (Central ministry's advanced computing arm), ISB (Renowned Indian B-School) and BitFury to facilitate and enable several initiatives such as developing a talent pool, incubating start-ups, investing in research and innovation, building local communities, and developing innovative blockchain-based government solutions to help citizens. The government is leading the way in implementing blockchain-based solutions, including land records, securing students' credentials, microfinance, anti-drug counterfeiting, peer-to-peer energy trading, credit financing, food subsidy supply chain, vehicle registrations, and law enforcement.

T-Chits is a use case unique to the Blockchain District, which aims to solve the problem of financial fraud in an Indian savings instrument known as Chit Funds. Chit Funds are key

instruments of financial inclusion in India, especially for those with little access to formal institutions. A group of individuals act as an informal financial institution which maintains a common fund. According to media reports, up to USD\$18 billion of savings belonging to 150 million low income families have been lost in 350 reported Chit Fund frauds in India.

Today, Blockchain District's T-Chits project is making Chit Fund credit financing accessible, credible, reliable, and rewarding. The solution at full scale implementation can potentially safeguard 150 million low income families against financial fraud. At present, 1473+ Chit Fund companies are registered, 198K+ transactions recorded, with over one million subscribers and \$2.2 million rotated per month.





BUSINESS PROCESSES & INSURANCE



ROBUST ACCESS CONTROLS — CRITICAL COMPONENTS FOR ENTERPRISE BLOCKCHAIN

A blockchain's distributed nature is an incredible benefit in engendering trust among a group of entities that do not fully trust each other; it creates an agreed upon shared source of truth. For permissioned blockchains, however, full data distribution and transparency can be problematic. For example, one could have multiple contractors to deliver packages from a central warehouse; the contractors may agree to share their fleet data with that company, but not with their competitors. In such a scenario, how does one manage access and visibility in a distributed business network?

We have observed two distinct needs regarding access controls. Static Access Controls refer to the securing of access to a resource in perpetuity; an individual has access to his/her digital ID, for example. Dynamic Access Control requirements are concerned with situational and time-based access rights, such as providing consent for a clinical trial only during a specific phase of the study.

To address Static Access Controls, Salesforce implements distinct policies and authorizations that define access to a resource by a participant. These policies are set upfront by the founder or consortium participants, depending on the

network set-up. Addressing Dynamic Access Controls is admittedly more complex and dependent on specific use cases. This is a critical confidentiality-preserving mechanism. Doing so, we not only define participant and access control policies, but also context-aware and time-bound permissions.

Let's take the example of clinical trial management for cancer patients. Patients sign their consent at each step of the trial to a variety of entities (genomic testing labs, clinical labs, pharmaceutical companies, research centers, etc.). Once the consent is received, the system keeps track of the consent and ensures that only authorized entities have access to patients' data and consent. In addition, some consent decisions are revisited and/or expire after some time. This is accomplished first by defining the participants and policies and then applying rules that respect the more specific limits defined by the consortium (e.g., lab A can only access information at a specific phase of the trial).

This is complex and crucial work, and will enable blockchain adoption at the enterprise level, not just for our customers, but more broadly across the blockchain ecosystem.



UNIVERSITY OF BAHRAIN

The national university of the Kingdom of Bahrain became one of the first universities globally to issue digital credentials anchored to the blockchain, using the Blockcerts open standard for creating, issuing, viewing and verifying any official record. The university is partnering with Learning Machine, the premier provider of Blockcerts credential issuing systems, to implement the initiative.

This blockchain credentialing initiative forms an integral part of the university's broader digitization strategy, which places digital security, ownership and portability at the center for globally mobile learners and workers. UoB issued over 400 credentials to students who recently graduated from the university's digital academy. UoB continues to play a crucial role in the regional entrepreneurship ecosystem. Hence, the credentials were endorsed by key partners, including Google Developers Group Manama and strategic partners Startup Bahrain.

The key pillars of blockchain are decentralization, transparency, and immutability; this project is innovative in that it takes the key pillars of blockchain and uses them within a university setting to serve students, employers, and other universities around the world. This initiative breaks tradition by using verified credentials to

students anchored to the blockchain, meaning students have them on their smartphone and for life. It allows governments to understand what qualifications and credentials are being gained in real-time, which can then be mapped against demand in the labor market. The initiative solves issues of fake and lost certificates, in addition to the time taken to validate with employers and universities anywhere.

During the issuance process earlier this year, students received invitations via email to download the Blockcerts Wallet on their mobile phones and add the University of Bahrain as an issuer. Then, another email was sent containing their digital credentials as a JSON (JavaScript Object Notation) file format, which provides the flexibility of sharing and validating through the Blockcerts portals and wallets. An acceptance rate of around 89.45% in one week was recorded during the issuance of the first batch of digital credentials. The students were excited and fascinated by the speed and accuracy with which credentials were distributed during the awards ceremony. The next issuance will take place within the coming few months and will target postgraduates from all colleges, which is around 200 graduates, then expand to the undergraduate level — about 20,000 students.

EVERTAS RISK SOLUTIONS

Evertas Risk Solutions is the world's leading expert on insuring cryptoassets and blockchain infrastructure. Our comprehensive risk assessment tool enables robust underwriting of this emerging asset class. We look at over twenty-one categories of risk and hundreds of potential exposure points to develop a comprehensive understanding of the insured's operations. In the last year, we have enhanced our tools with a new pre-screening module

which allows us to more rapidly assess the suitability of the insured. We are currently working on fully digitizing our application process to enable a more efficient and secure customer experience. Evertas Risk Solutions is continuing to build and expand its offering by seeking additional carrier capacity and more comprehensive coverage options to meet the needs of industry.



SUPPLY CHAIN

EVERLEDGER

EVERLEDGER

For the diamond industry, transparency is a two-way street. Information flows upstream, carrying insights about the origin and characteristics of the diamond or gemstone. Eventually, the customer at the head of the chain can make their purchase with a more thorough understanding of the jewelry's value.

Information is also sent back down the chain to help all stakeholders make better decisions. The overall impact is higher clarity in a complex supply chain, which results in closer adherence to the aims of the United Nations Sustainable Development Goals, including gender equality, decent work and economic growth, and responsible consumption and production.

Of course, it's not just information that flows up and down the transparency street. More than ever, consumers are voting with their wallets, favoring brands that can clearly demonstrate their ethical practices.

That is why, at Everledger, we don't see transparency as simply the end goal. It's

more than a 'state of mind' or a by-product of increased supply chain information. It's a potent force for change. Our purpose is to contribute greater clarity and confidence in the marketplaces where increased transparency is essential.

With information out in the open, we believe the value of many industries — from diamonds, to fine wine, to e-waste management — will be shared by all stakeholders throughout the value chain. We use a symphony of technologies to help our clients drive sustainability in the diamond industry. By combining blockchain technology with AI, IoT, and nanotechnology, we create a digital twin of every diamond, enabling traceability in a secure, unalterable, and private platform.

As transparency becomes more important for companies and consumers, we are ready to support industry partners in their efforts for social and environmental sustainability, compliance, and more equitable business practices in 2020 and beyond.



PROCTER & GAMBLE

P&G is exploring blockchain because we believe in the concept of Constructive Disruption. We are using new technologies, methods and processes to disrupt how we work in order to deliver superior and irresistible consumer experiences. Because of the varied feature set the technology affords — and its ability to combine with other emerging tech like IoT and AI — it has been at the precipice of innovation over the past year.

At P&G, we believe in partnerships and collaboration, especially where values and goals align and enable us to accomplish more for our consumers. This remains our guiding stick. This year, during the UN General Assembly week in New York in coordination with the GBBC, P&G sponsored a hackathon challenge to address the impending urban water crisis (Sustainable Development Goal #6). The hackathon brought together teams who designed blockchain-based solutions to connect urban households to water that is reusable, productive, and desirable. The room was filled with developers and strategists from around the globe, showing how we can tackle bigger goals more effectively when we work in partnership with others.

We operate across six business units and view blockchain distinctly through a consumer lens. Our interest is in how it can be used to help us deliver for consumers across the value chain. We are working with the global startup community

and longstanding partners who are equally interested in evolving consumer experiences for increased benefit. As an example, today's consumers are asking for ingredient transparency: they want to understand the content of their product, the people behind their products and the quality markers. We are piloting a blockchain-based solution that allows us to share how organic cotton was sourced for select period products. We look at the people who grow and purify it, which certifications guarantee it, and the time stamps that govern the phases. This is a first step in the consumerization of the supply chain — where markers of superiority in the value chain can be used as educational and informational methods. We see potential for expansion across global organizational units.

We are on a learning journey and believe strongly in educating people at all levels of the organization about this new technology. We now have learning paths about blockchain and other emerging technologies for employees and partners. We expect to see more efficiencies as processes are redesigned and different types of data are shared and secured.

2019 was about piloting and examining where we can tackle larger issues. To build upon this foundation, in 2020 we will experiment more deeply across vectors and put more learnings into practice.

ENERGY



RENEWABLE ENERGY CONTRACTS

Renewable energy certificates (RECs) are legal contracts created to represent the 'renewableness' of energy generation. Once created, these certificates can be purchased either voluntarily or to meet requirements set by state legislation. The process to purchase RECs is convoluted, expensive, and plagued by slow and outdated technology platforms.

Blockchain technology is being used to underpin a new, holistic solution that will address the pain points in the US REC market — improving data accessibility, reducing settlement times, and lowering transaction costs.

Power Ledger has partnered with renewable energy developer, owner, and operator Clearway Energy Group to develop a platform to trade RECs in the United States.

The market for RECs in the United States is estimated to be worth over \$3 billion annually and is often criticized for being opaque and inefficient. Our new integrated approach, supported by blockchain technology, will inject much needed transparency and efficiency into the ecosystem.

Whether companies are voluntarily meeting clean energy commitments or satisfying

regulatory requirements, there is a need to ensure that renewable energy credits are being purchased at the lowest cost — something made difficult by high prices for data access and for brokerage services.

Power Ledger's platform will integrate with existing REC registries to provide a real time marketplace for everyone, from large enterprise buyers to small use consumers. The platform will drive down brokerage costs and place control of energy data into the hands of users.

Power Ledger's partnership with Clearway will ensure a swift entry into the environmental commodity trading market due to the company's established footprint in renewable energy assets across the country.

Blockchain can significantly improve the efficiency of the REC market in the United States by linking transactional functions in a common platform. Power Ledger is excited to partner with Clearway to deliver a fully integrated, scalable, and low-cost solution.



SOCIAL IMPACT



NEW AMERICA/BTA

New America's Blockchain Trust Accelerator this year created the Blockchain Impact Ledger (BIL), a database of real-world social impact blockchain use cases aligned with the seventeen United Nations Sustainable Development Goals. Organizations can use the BIL to find detailed, vetted information about blockchain projects in specific thematic and geographic areas of interest.

Use cases that harness blockchain for social impact are among the most valuable, compelling applications for blockchain technology. However, public attention has focused primarily on cryptocurrencies and other FinTech applications. As a result, social impact organizations have struggled to share information that could promote innovation and iteration of successful solutions. Pilot projects tend to happen in isolation, and often repeat mistakes of earlier test projects or miss opportunities to coordinate with other aligned initiatives.

With support from the Social Alpha Foundation, the Blockchain Impact Ledger is gathering information from social impact initiatives

worldwide to accelerate the process of collective learning in the blockchain community. Projects profiled in the Ledger include the UN World Food Programme's use of Ethereum to provide Syrian refugees with access to financial services and direct aid transfers. This solution, called Building Blocks, has reduced transaction fees, boosted efficiency, and created a pathway for refugees to regain a legal identity and restart their lives. Another featured project, Plastic Bank, has combined efforts to combat poverty and reduce ocean plastic pollution. Their model uses IBM's Hyperledger to pay volunteers in Haiti, Indonesia, and the Philippines to clean up recyclable waste and deliver it to locations where it can be accumulated and sold as raw material.

The Blockchain Impact Ledger will encourage innovation and collaboration among the early actors in this promising field. We invite you to explore the first edition of the Ledger, provide feedback, and nominate projects for evaluation and inclusion. Together, we can identify opportunities to harness blockchain in solving the challenges of the 21st century.

ODYSSEY OPEN INNOVATION PROGRAM

Since 2017, over three thousand people from all over the world have been gathering once a year in Groningen, Netherlands. These people have come together for what has become known as “The Odyssey.”

This diverse group of people is growing each year. In 2019 alone, 100 teams and 100s of experts from 30 countries (1,500 people total) worked on 20 complex challenges. Within 48 hours, 100 working prototypes were co-created with corporate, governmental, regulatory, scientific, environmental, and civilian stakeholders at the table; GBBC’s CEO, Sandra Ro also participated in the distinguished role of “super accelerator.” Due to Odyssey’s programmatic approach, the best solutions moved towards real pilot implementations after the hackathon, supported by these ecosystems of stakeholders. The 2020 edition of Odyssey, being held on April 3-5, plans to host 2,000 participants, collaborating on 21 challenges to shape the 21st century.

In the past three years, Odyssey has delivered to its partners over 200 working prototypes. Over 30% of these prototypes are in development towards adoption, or have already been adopted.

The Odyssey Open Innovation Program is specifically tailored to co-create:

- **Community:** build collaborative ecosystems and adopt a shared digital public infrastructure, protocols, and governance;
- **Tools:** prototypes of digital public infrastructure, protocols, governance models, policy;
- **Narrative:** clearly articulating the benefits for all stakeholders.

SUCCESS STORY

In 2018, the reputable European company Kryha won with their prototype “GreX”: A Machine-to-Machine communication and collaboration platform. This platform enables machines to make decisions as a collective and operate in a truly autonomous manner. In 2019, their team created “Horizon”: A protocol for decentralized machine optimization. It sources the best compute service providers for your tasks and automatically handles container orchestration and payment in a fully decentralized manner.

PARTNERS

Vattenfall, Engie, KLM Cargo, Deloitte, VMWare, DAML, Loyens & Loeff, Dutch Central Bank, Dutch Authority for Financial Markets, Dutch Ministry of the Interior and Kingdom Relations, Dutch Ministry of Defence, IUCN, City of The Hague, City of Groningen, Dutch Chamber of Commerce, Visma, Outlier Ventures, Enexis, GridSingularity, Ocean Protocol and the European Union.



STHORM

Business and investment for impact has increased relevance in the global market and people are shifting their perspective on the role capital should play in our society. But most importantly, we are rethinking and redesigning some key components of our society: healthcare access, education, credit and wealth distribution, food and energy production, waste management, resources exploitation, supply chain efficiency and system structure.

Sthorm identified a need for a common platform to facilitate impact development and created CrowdHack, a blockchain-based digital marketplace of alternative funding methods to promote and finance impactful projects. Blockchain enables transparency, efficiency, reliability, collaboration, and decentralization in crowdfunding. Crypto-friendly, tech-curious, and social-minded individuals will find a variety of alternative ways to support campaigns such as collectible games, security tokens (STOs), initial coin offerings (ICOs), and other distributed ledger technologies (DLTs) developed for crowdfunding/investing. CrowdHack provides

real opportunities for impact-driven ideas and projects through an inclusive and human-centric system.

Our first #viralcure campaign aims to crowdfund the research and development of neutralizing monoclonal antibodies for Zika and Dengue type 1, 2 and 3 viruses. The partnership with the laboratory Mabloc LLC based in Florida, U.S. ensures the necessary rigor and diligence for the scientific studies and tests of these antibodies. The alternative funding of this campaign will be achieved through the sale of collectible non-fungible tokens (NFTs) generated by an artificial intelligence named Theos from the inputs of inspiring individuals selected as ambassadors for the specific campaign.

CrowdHack is a promising example of a platform harnessing blockchain technology to make a traditionally opaque and centralized financing system open and available to the public, where users can actively participate in the campaigns. CrowdHack is shifting the power of change to individuals.



ARTS & MEDIA



BITFURY SURROUND

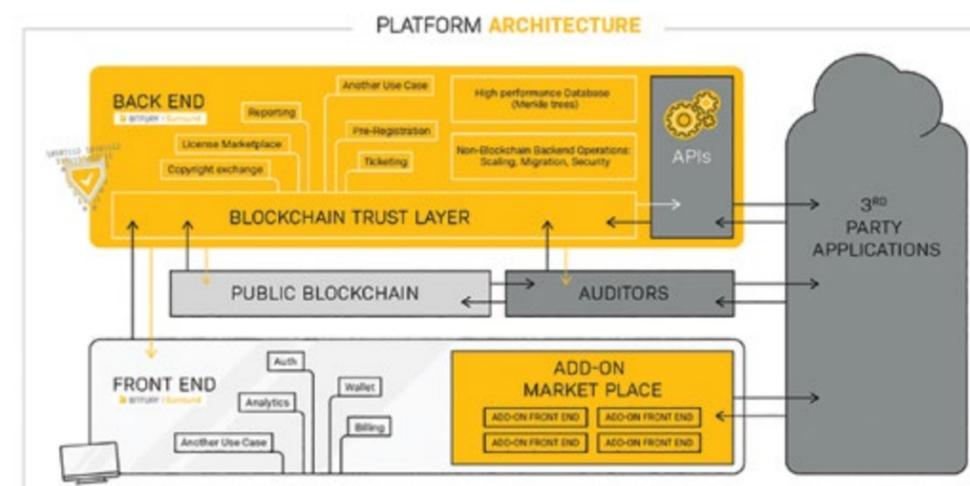
The Bitfury Group expanded its portfolio in 2019, becoming an emerging technologies company that builds cutting-edge solutions in AI, blockchain, high-performance computing, and digital currencies to improve the systems and services that people around the world use every day.

Our new AI division, led by veteran technologist Fabrizio Del Maffeo, uses the company's world-class hardware and software technologies to build integrated product solutions for AI at the edge, as well as AI cloud-to-edge enterprise solutions for corporations and governments. Our years of expertise building industry-leading hardware and software solutions for the blockchain industry equipped us with the expertise needed to build solutions for our increasingly AI-assisted world.

This year, we also launched Bitfury Surround, a music entertainment division that is designing blockchain solutions to boost the value of intellectual property for artists and other

stakeholders in the music industry. Led by seasoned music industry executive Stefan Schulz, Bitfury Surround's first initiative will be to create a music platform secured by the Bitcoin Blockchain. The Surround™ platform will encourage collaboration, foster fresh applications, and promote innovation within the industry. To do so, the platform will create a fully interoperable digital ecosystem for sharing and monetizing intellectual property and enhance economic opportunity by providing transparent management functions and trusted data.

The music and entertainment industry has evolved into a complex, competitive technology-driven environment that suffers from a serious lack of transparency. At Bitfury Surround, we want to champion artists and help incentivize the growth of the entire industry through collaboration and the creation of a blockchain-based ecosystem. Only an immutable layer of trust and open interoperability will provide more economic freedom for artists and opportunities for significant growth across the music industry.





ORBS

Orbs believes that public permissionless blockchains can add value to existing enterprise finance and, more importantly, to digital data solutions. Orbs is a permissionless blockchain for enterprise use based in Tel Aviv, Israel, building technology for existing data aggregators. One of our use cases is a rights management platform for digital content.

It is becoming increasingly difficult to verify who created digital content and whether that content is authentic, proving the need for a new form of digital rights management. Creators need both copyright protection and protection for how their content is used, which underscores the need to find a mechanism to definitively prove origin. While content creators wish to expose their work to the public and monetize it online, misuse and copyright violations are prevalent across the web. There are no open copyrights registries for images, and in case of infringement, proving ownership is both expensive and difficult.

Beyond rights management, image authenticity verification expands to identifying and fighting fake news, monetizing User Generated Content (UGC), verifying ownership of user-submitted

data for insurance apps, and facilitating compliance with General Data Protection Regulation (GDPR), especially the right to be forgotten.

The Hexa Foundation, Orbs' social impact arm, created an open-source proof of concept tool, Open-Rights, for digital content registration, starting with images. The platform-agnostic tool can be added to any app, and provides clear terms and conditions surrounding image ownership, storage, and sharing. For each image added to the service, a hash (unique identifier) is created and recorded on the Orbs blockchain, along with any relevant metadata, including owner information, a timestamp, geographic location, and licensing. This decentralized database allows creators to prove ownership of their images and allows any interested party to verify the authenticity and origins of an image by viewing the publisher's metadata.

In beta release alone, Open-Rights reached over 350,000 transactions per week, granting both content creators and viewers increased transparency in data and image origin.



NYC BLOCKCHAIN CENTER

An entrepreneur with a marketable idea meets a talented developer at a NYC Blockchain Center workshop, teams up to start a business, and is accepted into a blockchain accelerator program. All in the course of five weeks. A graduate student studying sustainability management walks into a Center community breakfast with an idea of combining blockchain and sanitation, but needs to learn more about blockchain. She joins a hackathon team less than two months later and wins. These are just two examples of the many success stories born at the NYC Blockchain Center.

GBBC partnered with the NYC Economic Development Corporation to open and operate the NYC Blockchain Center in 2019. This public-private partnership helped entrepreneurs grow their blockchain businesses, promoted diversity within the blockchain community, and deepened understanding of regulatory developments in the blockchain ecosystem.

The Center was an onramp for entrepreneurs and individuals alike. Start-ups demonstrated new products for peer review and prospective partnerships. Developer workshops, regulatory panels, product demonstrations, and community teach-ins were presented free of charge, ensuring that the economic status of individuals or cash position of start-ups were not barriers to participation.

The Center also provided unique networking opportunities. Drop-ins often included

international visitors and NYC newcomers. All-in-all, we held 136 events with almost 3,000 attendees, including entrepreneurs, executives, students and everyday New Yorkers.

The All Things Blockchain Conference, held during NYC Blockchain Week, invited top speakers from the industry to spend a day with a diverse group of participants at the Center. These were blockchain community members who might not otherwise have the opportunity to interact with such noted leaders in a small setting.

Our popular Community Breakfast Series provided a platform for in-depth discussions with experts on topics as diverse as tokenization, no-action letters, GDPR, and an entrepreneur's journey through blockchain. We even hosted a session with a cryptographer cited in three of the eight footnotes of Nakamoto's Bitcoin whitepaper.

The NYC Blockchain Center incorporated diversity and inclusion into every facet of our operations. We collaborated on special events with LatinX in Blockchain, Women in Blockchain, Blockchain for Schools, Black Girls Code, and the Crypto Community Project. We held Blockchain 101 courses in Harlem, Brooklyn, the Bronx, and Queens, along with Blockchain 101 en Español at the Center. We impacted the blockchain conversation, helped businesses grow, and the ecosystem prosper.

NORTH AMERICA

CANADA

NORTON ROSE FULBRIGHT | PATRICK CHOU

NORTON ROSE FULBRIGHT

Beginning 1 June 2020, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) will require businesses dealing with virtual currencies, including virtual currency exchanges, to register and comply with requirements previously applicable only to money services businesses. These requirements include registering with FINTRAC, complying with KYC and AML requirements, and monitoring and reporting certain types of transactions, such as transactions totaling \$10,000 CAD or more conducted by, or on behalf of the same person or entity within a 24-hour period, or any reasonably suspicious transaction.

Canada does not recognize virtual currencies as legal tender, but the Canada Revenue Agency has treated them as commodities since 23 December 2013 while the Canadian Securities Administrators (CSA) view virtual currencies as securities, having stated on 24 August 2017 that securities law requirements may apply to initial coin offerings, initial token offerings, cryptocurrency investment funds, and cryptocurrency exchanges. In response

to the collapse of Canadian cryptocurrency exchange QuadrigaCX, the CSA and Investment Industry Regulatory Organization of Canada issued Consultation Paper 21-402, Proposed Framework for Crypto-Asset Trading Platforms. Public consultations were solicited until 15 May 2019. On 31 October, the CSA formed a cryptoasset working group which aims to advise on the development of rules, guidance, and other policy matters related to the regulation of cryptoassets.

In March 2016, the Bank of Canada launched Project Jasper, which examines how DLT intersects with wholesale payment systems. Early phases focused on how DLT can improve clearing and settlements between banks, while phase 3 explored DLT applications involving foreign exchange, securities, and other assets. The Bank of Canada is also exploring a DLT-based securities settlement system using central bank money, and a cross-border, cross-currency settlement system in partnership with the Monetary Authority of Singapore and the Bank of England.

UNITED STATES | FEDERAL

STEPTOE & JOHNSON

Steptoe

REGULATION OF BLOCKCHAIN

- The United States does not currently have any law or regulation that comprehensively governs the use of blockchain and other DLTs. Industry-specific laws and regulations that govern products, services, and transactions, however, have application to blockchain technology, and guidance specific to blockchain

technology is beginning to emerge. Companies considering the use of blockchain technology must consider any laws or regulations that govern the underlying product, service, or transaction.¹ In addition, legislation that enables or explores the use of blockchain technology in certain contexts, or regulates certain aspects thereof, has been enacted in a growing num-

LEGAL & REGULATORY: JURISDICTIONS

ber of states. Twenty-eight states have introduced blockchain legislation and twenty-seven bills and resolutions were enacted or adopted². These new bills and laws cover, among other things, the recognition of blockchain records as electronic records with the same status as paper records³, the creation of task forces to study and evaluate the use of blockchain technology⁴, and the upkeep of corporate records on blockchain.⁵

- Federal and state agencies are actively exploring blockchain technology and its opportunities and risks, in areas such as supply chain management, digital identity and device authentication, customs compliance, and provenance of goods. These agencies are evaluating blockchain technology solutions with the goal of understanding how the technology works, whether the technology can streamline government and industry operations, and whether new regulations should be implemented or existing regulations modified.

REGULATION OF CRYPTOCURRENCIES

- No single U.S. regulatory agency regulates cryptocurrencies, and no comprehensive regulatory scheme exists in the U.S. regarding cryptocurrencies. However, federal regulations involving anti-money laundering and sanctions compliance, regulation of financial instruments and markets, taxation, as well as state regulations in areas such as money transmission, impact cryptocurrencies to different degrees.
- Two agencies of the U.S. Department of the Treasury, the Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC), directly regulate certain aspects of handling cryptocurrency.
 - FinCEN, which administers the Bank Secrecy Act — the primary US AML statute — has issued guidance since 2014 describing how certain types of businesses handling cryptocurrency may be considered regulated

financial institutions for the purposes of AML requirements. Specifically, entities that administer or exchange cryptocurrencies, as FinCEN has defined those terms, are subject to AML requirements, including a requirement to register with FinCEN.⁶ FinCEN enforcement actions as well as U.S. criminal proceedings have made clear that these requirements apply not just to U.S. entities but also to foreign entities that do business or service customers in the United States.⁷ Companies conducting ICOs or similar types of token issuances may also be required to register with FinCEN.

- In 2019, FinCEN issued an updated set of guidance, compiling and building upon its earlier framework.⁸ The 2019 guidance clarifies that FinCEN's rules apply to a number of specific business models including hosted wallet providers, certain decentralized applications (DApps), and certain token-based fundraising activities and similar token issuances, among other business models. The guidance also clarifies the scope of a number of exemptions from the rules, including exemptions for persons that provide only "the delivery, communication, or network access services used by a money transmitter to support money transmission services" and for persons providing money transmission only as an integral component of another non-money transmission service. According to the guidance, these exceptions may cover providers of anonymizing software, decentralized exchanges, and certain token issuers, depending on the facts and circumstances.
- The guidance also clarified FinCEN's long-standing position that the so-called "travel rule," requiring regulated financial institutions to obtain and transmit certain customer identity information applies to transfers conducted in cryptocurrency.

The U.S. also led an effort to include an extension of the travel rule to virtual asset service providers (VASPs) in the latest recommendations from the Financial Action Task Force (FATF), an international AML standards-setting body.⁹ Inclusion in the recommendations is likely to pave the way for adoption in other jurisdictions around the world, and has been matched with clear statements by senior Treasury officials that the U.S. expects VASPs to comply with the travel rule.

- Similarly, U.S. economic sanctions requirements apply to entities handling cryptocurrencies; OFAC has issued an executive order prohibiting U.S. persons from engaging in transactions with the Venezuelan government's cryptocurrency, the Petro,¹⁰ and included bitcoin wallet addresses in a blocking order relating to two Iranian individuals.¹¹ It would not be surprising to see OFAC take similar actions in the near future.
- The U.S. Commodity Futures Trading Commission (CFTC) considers bitcoin and other virtual currencies to be commodities under the U.S. Commodities Exchange Act, now specifically naming both bitcoin and ether as commodities. The CFTC also considers futures and options contracts and swap transactions to be subject to comprehensive regulatory oversight by the agency.¹² Although the CFTC lacks jurisdiction under the Commodities Exchange Act over spot and cash transactions, the CFTC has brought enforcement proceedings against cryptocurrency exchanges for actions involving margin trading. The CFTC has asserted its right to enforce anti-fraud and anti-manipulation authority over virtual currency transactions, and this assertion has been supported by at least one federal court.¹³ The CFTC also brought suit against a Nevada company for an alleged \$11M cryptocurrency fraud and misappropriation scheme.¹⁴ The CFTC issued a Customer Protection Advisory that warns customers to

be cautious of and avoid pump-and-dump schemes that can occur in thinly traded or new "alternative" virtual currencies, digital coins or tokens.¹⁵ The CFTC also included "cryptocurrency surveillance practices" in its 2019 Examination Priorities for its Division of Market Oversight (DMO).¹⁶

- The U.S. Securities and Exchange Commission (SEC) continues to issue guidance pertaining to cryptoassets, particularly tokens that are the subject of ICOs. The SEC has also brought enforcement actions involving token issuers, cryptocurrency exchange platforms, promoters, and other service providers, and issued guidance pertaining to investment funds holding cryptocurrencies and crypto-tokens.¹⁷ The SEC has so far declined to approve cryptocurrency-based Exchange-Traded Funds (ETFs).¹⁸
 - Following on from the SEC's report on the Decentralized Autonomous Organization token sale (DAO Report)¹⁹ and cease and desist proceedings involving the Munchie token,²⁰ the SEC continued messaging its view that, in general, ICOs have involved offerings of securities. In February 2018, in testimony before the Senate Banking Committee, SEC Chairman Jay Clayton affirmed his view that ICOs in general involve the offering of a security.²¹ However, in a well-publicized speech in June 2018, the Director of the SEC's Division of Corporation Finance, William Hinman, addressed the potential for a digital asset to start out as a security (for example, in a pre-sale) and, over time, become something other than a security. The speech identified a number of factors that parties could look to as part of a legal analysis of whether an asset meets the definition of an "investment contact" under the legal framework set forth in SEC v. Howey,²² the 1946 United States Supreme Court case defining investment contracts.²³ The Hinman speech also noted that Ether, like Bitcoin, would not be considered a security.²⁴

- In April of 2019, the SEC's Division of Corporate Finance released the Framework for "Investment Contract" Analysis of Digital Assets²⁵, which applied the Howey test to digital assets. While not exhaustive, the framework identifies factors market participants should utilize in evaluating whether a digital asset is being offered or sold as an investment contract, how a non-investment contract digital asset could change to an investment contract, and whether or when a digital asset is no longer a security.
- On the same day as the Framework's release, the SEC issued a no-action letter²⁶ to Turn Key Jet Incorporated (TKJ). TKJ tokens are used to pay for private jet charter service; the tokens are sold and remain at a fixed price throughout the life of the program, and are not traded on secondary exchanges. In June, a second no-action letter²⁷ was issued to Pocketful of Quarters Inc. allowing the platform to sell digital arcade tokens, known as quarters, for use across participating games and platforms. The letter confirms that certain classes of tokens, in this case available in unlimited quantities and at a fixed rate, are not subject to federal securities laws and do not need to be registered under Section 5 of the Securities Act and Section 12 of the Exchange Act since there is no expectation of profit.
- In June, the SEC filed a civil injunctive action²⁸ against Kik Interactive alleging that the company offered and sold their KIN digital token without registration or obtaining an exemption from registration — a violation of the Securities Act of 1933. The SEC also filed an emergency action and obtained a temporary restraining order against Telegram Group Inc. to stop Telegram from distributing pre-sold "grams" tokens in the US and making them available for sale on secondary exchanges.²⁹
- The SEC has also now issued a small body of settled orders concerning ICOs. In November 2018, the SEC settled charges against two ICOs that it determined were securities. In settlements with AirFox and Paragon Coin, the SEC required the companies to pay monetary penalties, register the tokens as securities, and file periodic reports with the Commission.³⁰ The SEC also required the companies to conduct a claims recovery process for investors who purchased the tokens in the illegal offerings. In a concurrent statement issued by the staff of the SEC Divisions of Corporation Finance, Investment Management, and Trading and Markets, these settled orders were identified as "a path to compliance with the federal securities laws going forward...."³¹ In September 2019, The SEC settled charges against Block.one for conducting an unregistered ICO that raised several billion dollars over one year.³² Block.one was assessed a \$24 million civil penalty for not complying with securities laws in conducting the sale of its ERC-20 security token; no remedial action was suggested with respect to the release of the EOS native protocol token. In December of 2019, the SEC also settled charges against Blockchain of Things Inc. (BCOT) for conducting an unregistered ICO of digital tokens.³³ Similar to Paragon Coin and AirFox, BCOT was ordered to return funds to investors who purchased tokens in the ICO and register its tokens as securities.
- In July 2019, the SEC and FINRA issued The Joint Statement Addressing the Broker Dealer Custody of Digital Asset Securities³⁴ addressing financial responsibility rules, non-custodial broker dealer models, the customer protection rule, and the maintenance of the books, records, and financial reporting rules.

- Entities handling cryptocurrencies may also be required to obtain licenses from regulators

in various states in which the entity conducts such activities. In many states, an entity may be required to apply for and obtain a money transmitter or equivalent license. New York is the only state to adopt comprehensive requirements for entities involved in cryptocurrency business operations, adopting its "BitLicense" regulations in 2015.³⁵ To date, only a relatively small number of entities have successfully obtained a BitLicense. However, the pace of new approvals has increased of late with 23 entities now authorized to engage in cryptocurrency business activity in New York, including both BitLicense holders and trust companies approved to conduct such activity.³⁶ New York has also begun increasing the array of activities such entities are authorized to engage in, including activity involving an increasing variety of digital assets, such as certain stablecoins.³⁷ In December 2019, New York announced proposed changes to the BitLicense regulations, focused on establishing a proposed coin listing policy framework and a list of New York-approved crypto-tokens that can be listed for trading or other regulated business activities by any entity holding a BitLicense without prior approval of the state.³⁸ By contrast, Wyoming has undertaken a multi-year effort to pass cryptocurrency-friendly legislation. In 2019, they enacted a series of blockchain laws that, among other things, create a fintech sandbox for innovators to test financial products and services,³⁹ allow a special purpose depository institution to provide basic banking services to blockchain,⁴⁰ and establish an opt-in framework for banks to provide custodial services for digital assets.⁴¹ Other states such as Utah passed regulations pertaining to the applica-

tion of state money-transmitter laws to virtual currencies.⁴²

- The Internal Revenue Service has increased its attention on cryptocurrency taxation. Since 2014, the IRS has considered cryptocurrency property for tax purposes. U.S. persons are subject to tax on worldwide income from all sources, including transactions involving cryptocurrency. Since 2014, the IRS has focused efforts on enforcement. In 2017, the IRS enforced a summons against Coinbase, obtaining data on approximately 13,000 taxpayers. In 2018, the IRS launched a Virtual Currency Compliance campaign to address noncompliance. In 2019, the IRS began sending letters to about 10,000 taxpayers with virtual currency transactions that potentially failed to report income and pay the proper amount of tax from virtual currency transactions, and the IRS appears to be stepping up criminal enforcement efforts as well. In October 2019, the IRS released new guidance addressing the tax treatment of a cryptocurrency hard fork and addressing the treatment of virtual currency transactions for investors.⁴³
- In 2018, the Office of the Comptroller of the Currency made available a federal fintech charter; however, many states challenged the availability of this charter on the grounds that it impermissibly intrudes on areas of responsibility retained by the states in the U.S. constitution.⁴⁴ In October 2019, a federal district court struck down the charter, ruling that the OCC exceeded its authority in making the charter available.⁴⁵

Many U.S. state legislatures have proposed or passed blockchain-specific bills. At least twenty-eight states introduced legislation relating to blockchain in 2019, and at least twenty-seven bills and resolutions were enacted or adopted.⁴⁶ This state legislation includes:

ARIZONA

In May 2019, Arizona Governor Doug Ducey signed into law HB 2747, appropriating \$1.25 million to be distributed in fiscal year 2019-2020

to applied research centers and institutes that specialize in blockchain.

ARKANSAS

In April 2019, Arkansas Governor Asa Hutchinson signed into law HB 1944, defining blockchain

distributed ledger technology, smart contracts, and other related terms.⁴⁷

CALIFORNIA

Current California law requires certified copies of births, deaths, and marriage records to be printed on chemically sensitized paper with various specified features. Proposed Senate Bill 373 has passed the California Senate, and

would enable counties to waive the physical requirements for these records until January 1, 2022, and instead issue records through a blockchain.⁴⁸

COLORADO

Colorado has sent a bill to the governor that directs the state’s commissioner of agriculture to convene an advisory group to study potential applications of blockchain technology in agriculture. The group is to report its findings

to the General Assembly in 2020.⁴⁹ Another bill that would have directed the Colorado Water Institute at Colorado State University to study potential uses of blockchain to manage a database of water rights is on hold.⁵⁰

CONNECTICUT

In 2019, Connecticut passed a bill requiring the Office of Policy and Management secretary to develop a plan to incorporate blockchain technology into the administrative functions of the state.⁵¹ Connecticut’s House also passed a

bill establishing a task force to study blockchain technology for use in managing elector registration.⁵² Three additional proposed bills are pending.⁵³

DELAWARE

Delaware proposed three blockchain-related bills in 2019. SB 89, SB 90, and SB 91 amend the Revised Uniform Limited Partnership Act (RULPA) to include definitions pertinent for the

blockchain industry and revise how the RULPA relates to other bills such as the Delaware Uniform Electronic Transactions Act.⁵⁴

FLORIDA

Florida passed two blockchain-related laws in 2019 and has another bill that is currently in

the House.⁵⁵ SB 1024 establishes the Florida Blockchain Task Force within the Department of

Financial Services, and HB 1393 establishes the Florida Blockchain Task Force within the Division

of the Treasury.⁵⁶

ILLINOIS

In 2019, the Illinois House passed bills HB 2540 and HB 3575 to create the Blockchain Business Development Act and Blockchain Technology Act, respectively.⁵⁷ The former bill would direct the secretary of state to recommend legislation

necessary to support the use of blockchains for public records, and the latter would permit the use of blockchain technology in transactions, with some limitations.

IOWA

In 2019, Iowa introduced a bill enabling the use of distributed ledger technology and smart

contracts to conduct electronic transactions.⁵⁸

KANSAS

Kansas’s Governor has signed into law a bill amending the Kansas Revised Limited Liability Company Act, Business Entity Standard

Treatment Act, and other statutes, to enable the use of electronic networks or databases to maintain records.⁵⁹

KENTUCKY

Kentucky has adopted “a resolution urging a comprehensive study of and subsequent plan to

deal with the growing blockchain technology.”⁶⁰

MAINE

Maine’s legislature passed a resolution in its first 2019 session that directs the Commissioner of Economic and Community Development

to establish a blockchain technology working group.⁶¹

MARYLAND

SB 136 was signed into law on April 30, 2019, amending the Maryland General Corporation Law. It permits corporations to maintain certain corporate records (including the company’s stock

ledger) and transmit certain communications (e.g. annual statements) on electronic networks or databases, including using blockchain technology.

MASSACHUSETTS

Massachusetts has proposed two blockchain-related bills. First, SB 1762 would amend the definition of “marketplace facilitator” for sales tax purposes to include businesses that

permit or require customers to use virtual currencies. Second, SB 200 would establish a special commission to study blockchain and cryptocurrencies.

MICHIGAN

On December 10, 2019, Michigan’s HB-4106 was enrolled — the final stage before being presented to the governor for signature. If signed into law, the bill would amend the penal

code to criminalize the alteration, forgery, or counterfeiting of records using distributed ledger technology, including blockchain.

MINNESOTA

In May 2019, legislation was introduced in the House regarding the use of bitcoin in campaign finance. If passed, HB 2884 would prohibit an individual, political committee, political fund,

MISSOURI

Missouri copied Wyoming's law defining certificated shares as "a representation of shares that are stored in an electronic format and contains information entered into a blockchain or other secure, auditable database, linked to or

NEBRASKA

Nebraska has introduced several bills relating to blockchain and cryptocurrency. LB 284, which was approved by the governor in March 2019, would expand the definition of "marketplace facilitator" to include persons or businesses who provide virtual currency that buyers are required or allowed to use for the purposes of

NEVADA

Nevada's AB 533 creates an advisory commission with the purpose to "study the feasibility of the use of emerging technologies, including, without limitation, blockchain and systems that use a single source of truth, as a means of collecting data or efficiently and effectively handling transactions electronically to reduce or eliminate the handling of cash."⁶³ SB 162, SB 163, and SB 164 create a definition for "public blockchain," permit corporations and other organizations

NEW HAMPSHIRE

In January 2019, New Hampshire introduced a bill that would require the state treasurer to "develop an implementation plan for the state

NEW JERSEY

In August 2019, the New Jersey legislature approved SB 2297 to establish "the New Jersey Blockchain Initiative Task Force to study whether state, county, and municipal governments can benefit from a transition to a blockchain-based system for record keeping and service delivery." Two additional bills, AB 3768 and SB

principal campaign committee, or party unit from soliciting or accepting donations or contributions of any digital unit of exchange, including bitcoin.

associated with the certificate token, and able to be transmitted electronically to the issuing corporation, the person to whom the certificate token was issued, and any transferee."⁶²

sales tax. LB 9 would prohibit cities, counties, and villages from taxing or regulating distributed ledger technology, as defined in the legislation. In May 2019, resolution LR 164 was introduced to create an interim study to examine the need to update insurance laws in light of technological advancement.

to maintain certain records via blockchain, and exempt virtual currency from personal property taxation by classifying it as intangible personal property.⁶⁴ Additionally, SB 488 was introduced in March 2019 and would create an Emerging Technologies Task Force within the Department of Business and Industry to develop strategies and recommendations regarding the development of blockchain technology.⁶⁵

to accept cryptocurrencies as payment for taxes and fees beginning July 1, 2020."⁶⁶

2462, were introduced in 2018 that would allow corporations to use blockchain technology for certain recordkeeping requirements. Finally, effective as of the end of 2018, New Jersey will treat virtual currency as intangible property and subject to sales tax, per AB 4496.

NEW YORK

New York — which established its "BitLicense" in 2015 — introduced various blockchain-specific bills in 2019. In 2018, New York adopted AB 8783, which created a task force charged with evaluating cryptocurrencies' impact on financial markets. Two bills expanding the size of the task force and further defining its mandate were introduced in 2019.⁶⁷ In 2019, New York also introduced AB 2213, which proposes a financial technology regulatory sandbox program to test "cryptocurrency business activity" and other fintech products.⁶⁸ AB 1683 and SB 4142,

NORTH DAKOTA

In 2019, North Dakota Governor Doug Burgum signed into law two pieces of legislation relating to blockchain technology. First, HB 1048 creates a program requiring the Department of Information Technologies to "research and develop the use of distributed ledger enabled platform technologies, such as blockchains, for computer-controlled programs, data transfer and storage, and program regulation to protect against falsification, improve internal

OHIO

In 2018, Ohio amended the definitions of "electronic record" and "electronic signature" to include blockchain technology, allowing the validation of transactions by blockchain

OKLAHOMA

In April 2019, Oklahoma adopted SB 700, which modifies certain definitions relating to blockchain to allow contracts, signatures, and records on a blockchain to be recognized as valid electronic

OREGON

The Oregon House introduced three pieces of legislation in 2019 pertaining to blockchain. HB 2487 proposes that the Oregon Department of Administrative Services examine the use of blockchain technology in state administrative

passed in the Senate in April 2019, would allow signatures, contracts, and records obtained via blockchain to be recognized as valid electronic forms, and would "allow smart contracts to exist in commerce."⁶⁹ Other legislation, if enacted, would establish a task force to examine the use of blockchain technology for state administrative purposes⁷⁰ and an "office of financial resilience" whose responsibility, among other things, would be to advocate for certain kinds of blockchain companies.⁷¹

data security, and identify external hacking threats."⁷² The second bill, HB 1045, relates to the inclusion of blockchain technology, smart contracts, and electronic signatures in the state code. Additionally, North Dakota adopted resolution HCR 3004 in March 2019, which requests Legislative Management to examine the potential of blockchain in state government administration.⁷³

technology. Additionally, the House introduced a bill in April 2019 that would allow the government to use distributed ledger and blockchain technology.

records.⁷⁴ The Senate also introduced SB 843, which, if enacted, would state when securities exemptions would apply to a blockchain token.⁷⁵

services.⁷⁶ HB 2179, introduced on the same day, would establish a task force to study the "status and development of blockchain technology" and investigate its potential use in economic development and business transactions.⁷⁷

PENNSYLVANIA

In January 2019, the Pennsylvania Department of Banking and Securities published guidance clarifying that, generally, virtual currency trading platforms are not money transmitters under state law. Similarly, entities operating virtual

currency kiosks, ATMs, and vending machines are not considered money transmitters because “there is no transfer of money to any third party.”⁷⁸

RHODE ISLAND

In February 2019, the Rhode Island House proposed a comprehensive bill, 2019 RI HB 5776, to regulate virtual currency. Rhode Island’s

House also passed HB 5683, which enables the use of electronic networks and databases for corporate records.

SOUTH CAROLINA

This year, South Carolina enacted SB 738 and SB 4351, the “South Carolina Blockchain Industry Empowerment Act of 2019,” which

seeks to establish the state as an incubator for technology industries seeking to develop innovation by using blockchain technology.

SOUTH DAKOTA

In March 2019, the governor signed into law SB 1859, which included a definition of blockchain

technology for certain purposes.

TENNESSEE

In March 2018, Tennessee passed SB 1662, which recognizes the legal authority to use blockchain technology and smart contracts in

electronic transactions and recognizes that smart contracts are legally binding.

TEXAS

In 2019, Texas adopted SB 64, which encourages state agencies and local governments to use blockchain and cryptocurrencies, and SB 1859, which included blockchain technology into

the state’s Business Organizations Code as an “electronic data system.” In March 2019, the House introduced HB 4517, a bill to establish a blockchain working group.

UTAH

In April 2019, Utah adopted SB 213, which exempts those who facilitate the creation, exchange, or sale of certain blockchain technology-related products from the Money Transmitter Act and creates a legislative task force to study the potential applications of blockchain technology to government services.

Also adopted in April 2019, SB 168 states that a person or business will be a “marketplace facilitator” for purposes of state sales tax law if that person “provides a virtual currency for a purchaser to use to purchase tangible personal property, a product transferred electronically, or service offered for sale.”

VERMONT

In May 2018, Vermont enacted SB 269, which allowed for the creation of “blockchain-based limited liability companies (BBLLC)”. The bill describes these businesses as “limited liability

compan[ies] organized... for the purpose of operating a business that utilizes blockchain technology for a material portion of its business activities.” In order to set up a blockchain-based

company, applicants must “specify whether the decentralized consensus ledger or database utilized or enabled by the BBLLC will be fully decentralized or partially decentralized and whether such ledger or database will be fully or partially public or private.”

VIRGINIA

A Joint House Resolution, HJR 153, was introduced seeking to establish a one-year joint subcommittee consisting of seven legislative and five non-legislative members to study the potential implementation of blockchain

In June 2019, the governor signed HB 536, which defines a “marketplace facilitator” as a person or business who provides “a virtual currency that purchasers are allowed or required to use to purchase products from sellers.” Virtual currency is also explicitly included in the definition of “property” in Vermont’s Revised Uniform Unclaimed Property Act, per HB 550.

in state recordkeeping. Another Joint House Resolution, HJR 677, attempted to establish a “joint subcommittee to study the emergence and integration of blockchain technology in the economy of the Commonwealth.”

WASHINGTON

In previous years, the state passed legislation that places virtual currency exchange operators under the state’s money transmitter rules and requires them to comply with the same licensing requirements as traditional money transmitters. In addition, the Washington Department of Financial Institutions proposed rules and amendments to the Uniform Money Services Act, which further incorporates virtual currency into the money transmission regulations. In 2019, Washington passed a bill, SB 5638,

which recognizes and protects the legal status of electronic records pertaining to distributed ledgers like blockchains. The law includes a clause that prevents discriminating against electronic records that have in some way been part of a distributed ledger and provides legal definitions for the terms “blockchain” and “distributed ledger.” SB 5638 expands the Electronic Authentication Act to include “encouraging the development of distributed ledger technology.”

WYOMING

Wyoming has passed the most comprehensive blockchain-specific legislation to date. Wyoming has enacted more than a dozen “blockchain-enabling laws.”⁷⁹ A new law passed in 2019 “establishes the legal nature of digital assets

within existing law, dividing these assets into three categories of intangible personal property and classifying these assets within the Uniform Commercial Code (UCC).⁸⁰

CENTRAL AND SOUTH AMERICA

SULLIVAN & WORCESTER



ARGENTINA

The regulatory focus of Argentina has been limited to KYC/AML requirements and taxation of cryptocurrency. Presently, Argentina does not generally regulate the issuance, exchange

or use of cryptocurrencies. Accordingly, cryptocurrencies are not illegal in Argentina and no general prohibition exists on the sale of cryptocurrencies such as Bitcoin.

Similar to statements issued by regulatory bodies in other countries, the Argentine Securities and Exchange Commission issued an investor advisory on the potential risks of participating in ICOs. The regulatory body noted that while ICOs are generally not expected to

BRAZIL

Brazil does not generally regulate the issuance, exchange or use of cryptocurrencies other than to recognize that cryptocurrencies do not constitute legal tender. Both the Brazilian Central Bank and the Brazil Security and Exchange Commission have issued various statements warning consumers about potential risks arising from transactions in cryptocurrencies. In particular, like other countries, the securities

MEXICO

Unlike other South and Central American countries, Mexico has been quite active in implementing legislation with respect to cryptocurrencies. Mexico enacted the Financial Technology Institutions Law (FTIL) that both defines cryptocurrencies and regulates their use. Under the FTIL cryptocurrencies are defined as digital assets represented by electronically registered value that can only be transferred by electronic means. The intent of the FTIL is to provide regulatory oversight of crowdfunding involving digital assets, digital wallets, and the use of regulatory sandboxes.

be subject to capital markets regulations, the structure and characteristics of a particular ICO could nevertheless bring the ICO into the realm of applicable securities regulations, particularly in the case of fraud.

regulator noted that, depending on the facts and circumstances, certain ICOs could be considered to be securities offerings.

In 2019, a bill was introduced in the Brazilian House of Representatives that would clarify that cryptocurrencies are not securities and are freely issuable and tradeable.

The FTIL requires that Banco de México (the “Central Bank”) first authorize any digital assets that are to be used by Financial Technology Institutions and other financial institution entities. In granting such approvals, the Central Bank will take into account the extent to which the digital assets are intended to be used as a means of exchange, the various agreements, rules, and protocols that will govern the digital assets, and the treatment other countries are giving to the type of digital asset under consideration. Transactions in approved digital assets will not be regulated on the same basis as other traditional financial transactions.

CARIBBEAN

SULLIVAN & WORCESTER

BRITISH VIRGIN ISLANDS

The British Virgin Islands (BVI) Financial Services Commission has acknowledged that it is lawful to create investment funds focused on Bitcoin and Ether. As a result, 2019 saw a growing number of third-party service providers offering ICO-related services for BVI funds. The BVI has not, however, otherwise provided any

regulatory advice or guidance with respect to ICOs or cryptocurrencies in general. While the government has indicated its intention to create a legal framework for cryptocurrencies and other financial technologies, no legislation was proposed in 2019.



Although it appears that the government is waiting to see what steps are first taken by other jurisdictions, it is generally believed that most ICOs will not be subject to securities

CAYMAN ISLANDS

Other than KYC/AML requirements, the Cayman Islands does not presently regulate cryptocurrencies or other digital assets. However, the Cayman Islands Government previously announced that it is in the process of considering industry working group proposals on the potential adoption of regulatory measures and governance standards for the marketing

regulations, although, like other jurisdictions, a subset of ICOs could be subject to securities regulations depending on the applicable facts and circumstances.

and trading of cryptocurrencies and other digital assets both inside and outside the Cayman Islands. Any such future regulations are likely to be based on whether or not existing regulations could already apply and the nature of the transactional activity for which cryptocurrencies and digital assets are being used.

EUROPE

EUROPEAN UNION

COVINGTON & BURLING

COVINGTON

REGULATION OF BLOCKCHAIN

In 2019, the European Commission (EC) has continued to express support for blockchain technology and DLT. According to the EC, this technology promotes trust, making it possible to share online information, as well as agree on, and record transactions in a verifiable, secure, and permanent manner.⁸¹

Since trust is becoming the most valuable commodity in the digital economy, and perhaps even society, the EC places blockchain at the heart of its future strategy for the European Union (EU).⁸² Furthermore, the EC aims to spearhead a common approach on blockchain technology also in the international arena.

The EU is not rushing to regulate blockchain technology and DLT, but rather wants to lay down the right conditions and appropriate legislative framework to ensure the socially

beneficial development of the technology, and the reduction of legal uncertainties.

In April 2019, the EC launched the International Association for Trusted Blockchain Applications (INATBA), which is a multi-stakeholder organization based in Brussels.⁸³ INATBA brings together suppliers and users of DLT with representatives of government organizations and standard setting bodies from all over the world. INATBA promotes transparent governance, interoperability, legal certainty, and trust in services enabled by blockchain and DLT. The EU Blockchain Observatory and Forum also published a number of important reports on blockchain and DLT in 2019:⁸⁴

- In March, it issued a report on “Scalability, interoperability and sustainability of blockchains”.⁸⁵ The report analyzes the current and

projected future state of blockchain in Europe through the lens of large-scale blockchain platforms.

- In May, a report on “Blockchain and legal identity” indicated that it is now possible to build new identity frameworks based on the concept of decentralized identities — potentially including an interesting subset of decentralized identity known as self-sovereign identity.⁸⁶ The report also explains how such concepts might

REGULATION OF CRYPTOCURRENCIES

In January 2019 both the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) issued reports concerning the regulation of cryptocurrencies.

EBA published its advice for the EC on crypto-assets.⁸⁹ In this report, EBA generally indicated that pure cryptoassets fall outside the scope of EU financial services regulation (although there are cases in which cryptoassets may qualify as electronic money or its operators as payment service providers), and, that “specific services relating to crypto-asset custodian wallet provision and crypto-asset trading platforms do not constitute regulated activities under EU financial services law”.⁹⁰ EBA also expressed concerns that divergent approaches to the regulation of these activities are emerging in Member States. Therefore, EBA recommended that the EC carry out a cost/benefit analysis to assess whether EU-level action is appropriate and feasible at this stage to address the potential issues.

ESMA issued its advice to the EU institutions on ICOs and cryptoassets, calling for a common EU-wide approach to ensure investor protection.⁹¹ The advice clarifies the existing EU rules applicable to cryptoassets that qualify as financial instruments, and provides ESMA’s position on any gaps and issues in the current EU financial regulatory framework for consideration by EU policymakers.

work specifically in the European context.

In September 2019, it examined the intersection of blockchain with EU law and regulation as it relates specifically to smart contracts.⁸⁷

The EU continues to provide substantial financial support for the development of projects that promote the use of blockchain. The EC has been active in setting up “*Proof of Concepts, Pilot Projects and EU initiatives to explore, test and understand legal, regulatory, policy, research and funding needs related to blockchain and DLT*”.⁸⁸

On 10 October 2019, Valdis Dombrovskis, the EC’s new Executive Vice President for the portfolio concerned with an “Economy that Works for People”, said that the EU needs a common approach on cryptoassets, such as the Libra, and that he intends to propose new legislation.⁹² The scope of the proposal remains unclear. It is expected that the EC will try to find a balanced approach between regulation and continuous innovation in the EU.

Lastly, in December, the Council of the EU and the EC adopted a joint statement on stablecoins,⁹³ noting opportunities but also the “multifaceted challenges and risks related for example to consumer protection, privacy, taxation, cyber security and operational resilience, money laundering, terrorism financing, market integrity, governance and legal certainty.”⁹⁴ The Council and the EC concluded that no global “stablecoin” arrangement should begin operation in the EU “until the legal, regulatory and oversight challenges and risks have been adequately identified and addressed”.⁹⁵ The Council of the EU and the EC noted that the ECB and other central banks and national competent authorities will continue working on exploring further the ongoing digital transformation of the payment system (in particular, the consequences of initiatives such as stablecoins).

BELGIUM

NORTON ROSE FULBRIGHT | ANNA CARRIER



In Belgium there is no national legislation that regulates the use of blockchain, the status of cryptocurrencies or platforms offering trading in such cryptocurrencies. Trading in cryptocurrencies in Belgium is not illegal, and gains generated by such activity may be subject to the national income tax. In addition, both the National Bank of Belgium and the Belgian Financial Services and Markets Authority (FSMA) actively monitor the market for any activities involving potentially fraudulent offerings of cryptocurrencies. The FSMA regularly publishes customer warnings against fraudulent activities involving provision of cryptocurrencies or trading activities in such assets. The FSMA’s list of suspicious cryptocurrencies trading platforms, compiled mainly on the basis of complaints

received from consumers, at the end of 2019 totals 131 websites.

Finally, the Belgian government is yet to transpose to national law provisions of the 5th Anti-Money Laundering Directive that extends anti-money laundering and counter-terrorism financing requirements to transactions in “virtual currencies” and “custodian wallet providers”. This is expected by means of amendments to the Law of 18 September 2017 on the prevention of money laundering and terrorist financing, and on the restriction of the use of cash. The deadline to transpose the provisions of this directive into national laws of EU Member States is 10 January 2020.

FRANCE

NORTON ROSE FULBRIGHT | ROBERTO CRISTOFOLINI; SONIA AÏT AMMAR



For several years there has been a desire for the French Autorité des Marchés Financiers (AMF) and other French authorities to regulate financial activities linked to blockchain technology. This year, the PACTE (Action Plan for Business

Growth and Transformation) law established a framework for ICOs, digital assets services providers, and investment by funds in digital assets.

BLOCKCHAIN⁹⁶

- Under French law, the term used to refer to blockchain is “distributed ledger technology”. A distributed ledger technology is a system for recording an issue or transfer of (i) digital assets or (ii) a number of securities (minibons and securities that are not admitted to a central securities depository).

- A distributed ledger technology must be designed and implemented in such a way as to ensure the recording and integrity of recordings and to allow, directly or indirectly, the identification of the owners, and the nature and number of securities held.

ICOS⁹⁷

- At present, France is one of the only European countries with regulated ICOs. ICOs are permitted and are not subject to approval by the AMF. However, the new regime set out by the PACTE law provides for an optional prior

approval of the AMF. Issuers of tokens seeking to carry out an ICO in France may submit, in advance to the AMF, the information document in relation to the ICO (commonly called a “white paper”) to obtain AMF approval. The advantage

of this AMF approval is that only ICOs which obtained the approval by the AMF may carry out canvassing of investors in France.

DIGITAL ASSETS SERVICES PROVIDERS⁹⁸

- Under French law, “digital assets” include
 - tokens (as defined above); and
 - cryptocurrencies as defined by French law.
- The provision of digital assets services can be freely provided except safeguarding of digital assets or accessing digital assets and buying or selling digital assets using currencies having legal tender, which are subject to registration

INVESTMENT IN DIGITAL ASSETS BY FRENCH FUNDS⁹⁹

- Under French law, professional specialized investment funds (fonds professionnels spécialisés) and professional private equity

• To grant its approval, the AMF will check if the ICO complies with the requirements for a public offer.

- with the AMF by the digital assets services providers.
- However, if they so wish, digital assets services providers may obtain a license and place themselves under the supervision of the AMF. The advantage of this optional license is that only licensed digital asset service providers may carry out canvassing of clients in France.

investment funds (fonds professionnels de capital investissement) are allowed to invest in digital assets.

GERMANY

NORTON ROSE FULBRIGHT | RALF KOSCHMIEDER



CURRENT STAGE

Germany is known for its prudent approach regarding regulatory oversight to protect market participants. However, the German legal framework was not designed to address the specifics of emerging technologies such as blockchain and cryptocurrencies. From a regulatory point of view, the German regulator (BaFin) considers cryptocurrencies as units of account (Rechnungseinheiten), which qualify as financial instruments within the scope of the German Banking Act. In its circular, BaFin points out that the mere use of cryptocurrencies and the mining thereof

does not require a license under the German Banking Act, however, intermediary functions may be subject to licensing requirements.¹⁰⁰ In a further statement,¹⁰¹ BaFin pointed out that it has to be assessed on a case by case basis whether the activity requires a license or is subject to prospectus requirements, based on the different features and use cases of crypto-tokens (currency coins, security coins, and utility coins). The German supervisory law is technology agnostic and token-based operations must not be discriminated against.

PATH TOWARDS A LEADING TOKEN ECONOMY

On the 18 September 2019, the German government adopted its blockchain strategy,¹⁰² taking a holistic approach to growing Germany's leading position as a token economy. This includes:

- opening up German law for electronic securities
- establishing a regulatory framework for public offerings of certain crypto-tokens

- piloting blockchain-based identities
- regulating money on the blockchain as a means to synchronize legal transactions between the virtual and real world but not as an alternative state currency
- reviewing company law in consideration of possible blockchain applications

The German government states that it is very conscious that German legislation should be

CONCLUSION

Germany is adopting the approach that every business activity requires a well-designed and elaborated legal framework that creates trust among participants. To this end the

in line with the harmonized European legal framework but, nevertheless, is determined to take the lead to align German law to the requirements of the token economy. In this regard, the German government transposed the amendments of the Fourth Anti-Money-Laundering Directive into German law in a way that regulates custodian services of cryptoassets as financial services under the supervision of the regulator, effective as of 1 January 2020.

German government is proactively creating an environment conducive to a token economy accompanied by a reliable legal framework.

GIBRALTAR

COVINGTON & BURLING

COVINGTON

Gibraltar has understood the value of blockchain and DLT technologies and has been extremely open and progressive in its attitude towards the technology. Indeed, Gibraltar was the first jurisdiction to implement a framework regulating businesses using DLT.

In 2014, a Cryptocurrency Working Group (an initiative of the private sector) was established. In 2016, the Working Group, together with the Government of Gibraltar began working on a paper that led to the creation of the Distributed Ledger Technology Regulatory Framework

(the “DLT Framework”). The Framework, which includes the Financial Services (Distributed Ledger Technology Providers) Regulations, entered into force in January 2018. The DLT Framework aims to lay out a regulatory regime for companies using DLT for either the storage or transmission of value in or from Gibraltar.

As a supplement to the DLT Framework, the Government of Gibraltar also published a consultation paper on the regulation of token sales. It has since published a draft bill that would implement its proposals in this area.

MALTA

COVINGTON & BURLING

COVINGTON

In 2018, the Government of Malta launched public consultations on the digitization of Malta's economy. Malta's Parliamentary Secretariat for Financial Services, Digital Economy and

Innovation and the Malta Financial Services Authority (MFSA) have together taken steps towards the fulfillment of Malta's ambition to be known as “Blockchain Island.”

In July 2018, three acts, known together as the Digital Innovation Framework, came into force. Through these acts, businesses using blockchain technologies may be established in, or operate from, Malta, while the applicable regulatory and legal framework offers more legal certainty.

Further, in 2019 MFSA launched a strategy called “Vision 2021”, which aims to position Malta as a leader in FinTech. It is based on six pillars: (1) regulations; (2) ecosystem; (3) architecture;

NETHERLANDS

NORTON ROSE FULBRIGHT | FLOORTJE NAGELKERKE, PARTNER

In the Netherlands, there is no national legislation that regulates the use of blockchain, the status of cryptocurrencies, or platforms offering trading in such cryptocurrencies. Trading cryptocurrencies in the Netherlands is not illegal, and gains generated by such activity may be subject to the national income tax.

Both the Dutch Central Bank (DNB) and the Netherlands Authority for the Financial Markets (AFM) actively monitor the market for any activities involving potentially fraudulent offerings of cryptocurrencies. Both regulators regularly

QUALIFYING CRYPTOS

It is undisputed under Dutch regulatory law that cryptocurrencies are not considered to qualify as a current account, savings account, insurance, or premium pension entitlement.

AML LEGISLATION

To address the risk of financial crime associated with cryptocurrencies, the Netherlands amended its AML laws. Starting 10 January 2020, the Act implementing the amendments will hold requirements for providers of exchange services between virtual currencies and fiat currencies and custodian wallet providers. Once the Act enters into force, these parties must register with DNB. Also, DNB will become the supervisory

(4) international links; (5) knowledge; and (6) security. At the same time, MFSA launched a public consultation on Malta’s FinTech Strategy. One of the main goals of the FinTech Strategy is the creation of a “regulatory sandbox” for fintech in Malta, providing companies with a space where they can operate and test their businesses. This strategy also envisions that Malta would provide accelerator programs for startups in the field.

publish customer warnings of fraudulent activities involving provision of cryptocurrencies or trading activities in such assets.

DNB also carries out experiments based on blockchain technology to gather knowledge and assess the usefulness of the technology in improving payments. The blockchain solutions they tested so far fail to meet the high demands made of financial market infrastructures. However, their research shows that blockchain technology is promising, and could be applied in the future.

Cryptocurrencies also do not qualify as an investment object, electronic money, credit, or a financial instrument. This has been confirmed by both Dutch financial regulatory authorities.

authority for these service providers. DNB published a number of factsheets on its website with the aim of assisting crypto service providers in assessing whether they will need to register themselves with DNB and, if they do, what the registration process will entail for them. DNB notes that the information contained in the fact sheets (and any other information to which reference is made) is on the basis of the wording

of the proposed Implementing Act amending the Fourth Anti-Money Laundering Directive of 1 July 2019, which is yet to be adopted by the Dutch Parliament and subsequently by the Dutch Senate, and therefore subject to changes that may result from amendments adopted during, for example, parliamentary debates.

SWITZERLAND

COVINGTON & BURLING

Swiss regulators are widely regarded as particularly open, and positively disposed, to blockchain technology. This is especially true for innovations in the financial and financial technology sectors.

Switzerland is looking to position itself as an innovative, yet trustworthy and first-in-class regulator of blockchain technologies. Perhaps nowhere was this ambition, and its payoffs, as visible as in the decision by the Libra Association, the member-driven stablecoin payment network, to establish itself as a not-for-profit in Geneva, governed by Swiss law. The Libra Association’s decision was supported by a specifically tailored, and generally supportive, assessment by the Swiss Financial Market Supervisory Authority (FINMA) with respect to the applicable regulatory framework.¹⁰³ The Libra Association has since applied for a payment system license in Switzerland.

FINMA has also published guidance on how AML rules apply to blockchain technologies under its supervision,¹⁰⁴ and in August 2019 it issued banking and securities dealers’ licenses to two pure crypto banks. The licenses allow for the

The relevant forms that will need to be completed for registration will be published on DNB’s website. DNB is currently in the process of preparing its Digital Supervision Portal, which will be used by crypto service providers to submit their applications for registration.

offering of innovative banking services that have blockchain at their core. At first, these will only be available to institutional and professional clients and FINMA is set to closely monitor this situation, thereby further developing its status as an experienced regulator.

Even though Switzerland does not have “regulatory sandbox” exemptions specifically designed for blockchain technologies, it offers a series of simplifications for fintech startups that can also cover blockchain-based innovation. For example, it is possible to apply for a “simplified” fintech license, which allows the holder to accept deposits up to 100 million CHF provided that the deposits are neither invested nor bear interest.¹⁰⁵

Overall, the Swiss regulatory approach emphasizes technological neutrality and a proactive and adaptive legal landscape. In March 2019, Swiss legislators published a draft for a specific distributed ledger technology law (the “Draft DLT law”), with the aim to improve the regulatory fit for blockchain technologies with existing rules on privacy, financial markets, and insolvency.¹⁰⁶

COVINGTON

UNITED KINGDOM

SHEARMAN & STERLING



- The UK Financial Conduct Authority (FCA) published final Guidance on Cryptoassets, clarifying its expectations for firms carrying on cryptoasset activities within the UK and providing insight as to whether certain cryptoassets are within the FCA's regulatory perimeter or otherwise regulated. The FCA highlights that firms should use the Guidance to understand the regulatory status of their cryptoasset activities, but assessing whether a cryptoasset or related activity is within the regulatory perimeter can be done only on a case-by-case basis.
- On 10 January 2020, the FCA will become responsible for supervising the anti-money laundering and counter terrorist financing of UK cryptoasset businesses. However, the exact scope of the activities under the FCA's remit is uncertain until HM Treasury publishes the final laws implementing the European Union's (EU) Fifth Money Laundering Directive (5MLD). HM Treasury proposed extending the scope of the UK laws beyond that provided for in 5MLD by extending the requirements to crypto-to-crypto exchange service providers, peer-to-peer exchange service providers, cryptoasset ATMs, ICOs, and the publication of open-source software.
- The FCA is proposing to restrict the sale, marketing and distribution of derivatives and

exchange-traded notes (ETNs) that reference certain types of unregulated, transferable cryptoassets to all retail clients. The proposed prohibition would cover contracts for difference, futures, and options relating to crypto-assets and would apply to products sold, distributed, or marketed in or from the UK to retail clients, including sales to UK retail clients by other firms within the European Economic Area, and outbound sales of these products from the UK. The FCA's final rules are expected in early 2020.

- A UK court recently granted an asset preservation order over Bitcoin stolen in a "spear phishing" attack on a major crypto-currency trader. The decision confirms that proprietary claims over Bitcoin constitute issues to be tried in the courts. It is believed that this is the first time the English courts have considered the nature of cryptocurrencies as property. Subsequently, the UK Jurisdiction Taskforce (UKJT) published a legal statement providing the UKJT's view of the principles applicable under English and Welsh private law for determining when a cryptoasset will be considered property and when an enforceable contract is concluded through a smart contract. UKJT is part of the LawTech Delivery Panel, an industry-led group that aims to identify barriers and opportunities for growth.

AFRICA

COVINGTON & BURLING

COVINGTON

KENYA

Kenya is often seen as a hotbed of innovation in Africa — high internet penetration, a

vibrant tech start-up economy, sophisticated infrastructure, and a high literacy rate support

this reputation.¹⁰⁷ The government has demonstrated a keen interest in creating an enabling environment for the adoption of technologies to address some of the region's biggest challenges and opportunities. In 2018, the Ministry of Information, Communications and Technology established a "Blockchain and Artificial Intelligence Taskforce" (the "Taskforce") with the mandate to assist the government in exploiting technology development. Academics, researchers, some regulatory bodies, local blockchain startups, as well as large corporations are participating.¹⁰⁸

The Taskforce has made a number of proposals which demonstrate Kenya's ambitions to exploit blockchain opportunities for macroeconomic benefit. These include ways to add efficiency in

public sector processes, allocating resources for research, as well as to explore ways to solve some of Kenya's socio-economic challenges through blockchain technology.¹⁰⁹ A good example includes the public health sector exploring the creation of a blockchain hub for the collection and management of key patient data, as well as providing medical advisory services to rural communities.¹¹⁰

In Kenya, the business community is taking full advantage of the enabling policy environment. The start-up scene is vibrant and innovative, and business ideas range from blockchain being used to improve agro-manufacturing to the provision of mobile money services across the country.¹¹¹

SOUTH AFRICA

Over recent years, the South African government has explored ways to regulate the cryptocurrency industry. This has been both necessary and critical given the unprecedented growth and innovation in the fintech sector, which has challenged the existing regulatory framework.¹¹²

Compared to its neighbors in the region, South Africa is viewed as highly progressive and actively engaged in new technologies, with existing legislation currently under review to match these technological advances.¹¹³ Overall, regulators are cautious in their deliberations and highlight the "risks", as well as the "threat(s) to traditional financial institutions", which they state include "opportunities for money laundering and financing terrorism."¹¹⁴

Cryptocurrencies are largely unregulated in South Africa. In 2014, the South African Reserve Bank (SARB) issued a Position Paper on Virtual Currencies, outlining its policy position on what it referred to as "virtual currencies" (VCs) and

"Decentralized Convertible Virtual Currencies" (DCVCs).¹¹⁵ The paper made it clear that the SARB is not responsible for overseeing, supervising or regulating the virtual currency landscape,¹¹⁶ as SARB's mandate is limited to notes and coins issued by a bank.¹¹⁷ The paper further states that all "activities involving the acquisition, trading or use of virtual currencies are performed at the sole risk of the end-user."¹¹⁸

The paper does not object to the use of cryptocurrencies. To the contrary, section 2.1 of the paper, while careful to signal that its position is not legally binding, recognizes the use of DCVCs as mediums of exchange, etc.¹¹⁹

Similarly, other South African authorities are rolling out several policy initiatives to explore risks and opportunities. These include the establishment of the Intergovernmental FinTech Working Group (Working Group). The Working Group's mandate is to develop policy and regulatory alignment for the fintech sector,

and to unpack its implications for the overall economy.¹²⁰ It is composed of representatives from several government departments including the SARB, National Treasury, the Financial Sector Conduct Authority, and the Financial Intelligence Centre. Over the years, the Working Group has released a number of policy positions, calling for public comment and involvement in defining the trajectory of blockchain regulation in South Africa.

Taxation is an increasingly topical theme in the regulatory landscape for blockchain and cryptocurrencies. Given the current budget deficit, effective taxation could assist the South African Revenue Services with increasing the revenues it collects.¹²¹ The National Treasury has not taken a position on this point.

MIDDLE EAST & NORTH AFRICA (MENA)

COVINGTON & BURLING

COVINGTON

BAHRAIN

The government of Bahrain also appears intent on placing the country at the cutting edge of fintech innovations. Khalid Al Rumaihi, CEO of the Bahrain Economic Development Board (its inward investment agency), has previously stated: “the ability for blockchain to be adopted at country level is a huge opportunity for Bahrain to move into the spotlight as a pioneer in this space”.¹²²

In February 2019, the Government of Bahrain unveiled its preliminary “regulatory sandbox” for cryptocurrency companies. The sandbox allowed 28 companies to operate in the country under a preliminary regulatory regime. Not long after,

the Bahrain Central Bank issued a new (English) cryptocurrency regulation. Executive Director of Banking Supervision of the Central Bank, Mr. Khalid Hamad, said in a statement: “We will continue to enhance our regulatory framework in order to keep pace with the innovations taking place in the major financial centres around the globe. The [Central Bank’s] introduction of the rules relating to cryptoassets is in line with its goal to develop comprehensive rules for the fintech ecosystem supporting Bahrain’s position as a leading financial hub in the MENA region.” How these rules will impact the operation of the “regulatory sandbox” is still to be seen.

MOROCCO

Since 2017, l’Office des Changes, part of Morocco’s Ministry of Economic Affairs, has prohibited transactions effectuated through virtual currencies.¹²³ Violations of this prohibition are subject to penalties and fines. At the same

time, the Office warned of investor risks linked to the use of virtual systems of payment that are outside the regulatory scope of the supervisory authorities.

Nevertheless, Morocco is looking at other options to expand access to financial services. In November 2019, Abdellatif Jouahri, Governor of Morocco’s Central Bank, said at the Africa Blockchain Summit in Rabat that: “Morocco will deploy financial technology to enhance access to

financial services.” He continued that blockchain technology could offer “all businesses and individuals equal access to financial services and products in a bid to endorse social and economic inclusion.”

SAUDI ARABIA

Banking, currency, and payment and settlement systems are regulated by the Saudi Arabian Monetary Authority (SAMA), and the provision of cryptocurrency-related services fall within SAMA’s remit. While Saudi authorities are looking to provide a regulatory framework for blockchain, the trading of cryptocurrencies is currently illegal.

Nevertheless, in January 2019, the central banks of Saudi Arabia and the UAE jointly launched a digital currency trial, called “Aber,” to facilitate blockchain-based financial settlements between the two countries.¹²⁴ The goal of the experiment is to examine whether the nations can reduce remittance costs.

UNITED ARAB EMIRATES

The United Arab Emirates (UAE) stands at the forefront of blockchain developments in the Middle East and North Africa region. In 2019, crypto transactions accounted for over \$210 million, more than in the US and the UK.

Banking, currency, and payment and settlement systems are regulated by the UAE Central Bank. Oversight over the UAE’s financial and commodities markets is shared by the UAE Central Bank Securities and Commodities Authority (SCA). The latter is the principal authority tasked with regulating and supervising the markets of cryptoassets. Previously, this authority warned investors about investor protections and that ICOs are not supervised by the authority.

In October 2019, the SCA published a draft regulation for “Issuing and Offering Crypto Assets”.^[125] The draft regulation would govern the promotion, offering, and trading

of cryptoassets and related activities, such as token issuance requirements, trading and safekeeping practices, information security controls, technology governance norms, and business conduct requirements for all market intermediaries. The standards set by the draft regulation are addressed to investors, custodians, crypto-trading platforms, brokers and promoters engaged in the cryptoasset industry.

It is likely to remain uncertain how this planned regulation will apply to free-financial zones, such as the Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Market (ADGM). Oversight of their financial and capital markets is done, respectively, by the Dubai Financial Services Authority (DFSA) and the Financial Services Regulatory Authority (FSRA). These zones have different regulatory frameworks. For example, in the DIFC a system based on English common law is in place, while English common

law itself applies in the ADGM. The ADGM already has an established regulatory framework in place to accommodate for digital assets, such as cryptoassets, digital securities, fiat tokens, and derivatives over digital assets.¹²⁶ Uniquely, the

DIFC also launched the world's first blockchain court in 2018. The project experiments with how blockchain can help verify court judgments outside of the DIFC.

ASIA PACIFIC

LATHAM & WATKINS

LATHAM & WATKINS LLP

AUSTRALIA

- On 30 April 2019, the Australian Taxation Office announced that it would collect data from Australian cryptocurrency designated service providers for its data matching program in the regime of tax compliance. The data, which is to be collected on an ongoing basis, includes cryptocurrency purchase and sale information. The data collection and matching strategies are intended to help prevent cryptocurrency from being used to move funds within the black economy and/or for the purpose of hiding money offshore.
- On 30 May 2019, the Australian Securities and Investment Commission published updated

guidelines on compliance requirements for initial coin offerings and cryptocurrency trading. The updated guidelines specify that token issuers and investment advisors dealing in tokens that are deemed to be financial products must have an Australian Financial Services license. Exchanges managing tokens that are characterized as financial products also would be subject to licensing requirements, and cryptocurrency miners may fall within the licensing perimeter if they are deemed to be part of the clearing and settlement process for tokens that are considered to be financial products.

HONG KONG

- On 12 May 2019, the Hong Kong Monetary Authority (HKMA) and the Bank of Thailand (BOT) signed a MoU on collaboration of joint projects, as well as sharing of knowledge and experience gained from their Central Bank Digital Currency (CBDC) research studies, namely Project LionRock of the HKMA and Project Inthanon of BOT. In November 2019, following the MoU, the HKMA and the BOT carried out a joint project called Project LionRock-Inthanon, aiming to facilitate Hong Kong dollar and Thai

baht payment-versus-payment among banks in the two territories using blockchain-backed tokens. Under the project, tokens will first be issued to Hong Kong banks and such banks will then distribute the issued tokens to their corporate customers for cross-border payments. Such a settlement platform allows companies in the two territories to settle payments more efficiently, as multiple layers of intermediaries are no longer involved. A report on the Project LionRock-Inthanon is expected to be released

in the first quarter of 2020.

- On 6 November 2019, the Securities and Futures Commission (SFC) issued warnings to investors regarding the risks associated with the purchase of virtual asset futures contracts. In particular, their highly volatile prices, complexities in valuation, and highly leveraged nature pose risks for average investors. In addition, some of the platforms for trading virtual asset futures contracts are subject to market manipulation and abusive activities. The SFC reminded investors that it has not licensed any person in Hong Kong to offer or trade virtual asset futures contracts. Purchasing virtual asset futures contracts also may be construed as gambling activities in Hong Kong, which is unlawful unless it is expressly authorized under the Gambling Ordinance (Cap. 148).
- On 6 November 2019, the SFC published a position paper announcing a new regulatory approach for virtual asset trading platforms (VATPs). VATPs that operate in Hong Kong and trade at least one virtual asset that is considered to be a "security" under the Securities and Futures Ordinance (Cap. 571) will need to apply to the SFC to be licensed for the regulated activities of "dealing in securities" (Type 1) and providing automated trading services (ATS) (Type 7). Once licensed, a VATP will be placed in the SFC's Regulatory Sandbox for close supervision where it will be subject to more frequent reporting, monitoring and reviews.
 - The SFC has clarified that even if a VATP's business consists mostly of the trading of non-security virtual assets (e.g., Bitcoin or Ether, which are unregulated) such activities will still be subject to the SFC's regulatory ambit as long as a VATP trades at least one virtual asset that is a 'security'.
 - A VATP will only qualify to be licensed by the SFC if it is operating a centralized platform in Hong Kong and its security virtual

assets are (i) asset-backed; (ii) approved or qualified by, or registered with, regulators in comparable jurisdictions; and (iii) have a post-issuance track record of at least 12 months. In addition, VATPs will need to meet a range of robust regulatory standards that are comparable to the standards applicable to traditional securities brokers and ATS providers. Under the key licensing conditions that will be imposed on licensees, a VATP operator must:

- only offer its services to "professional investors" (i.e., the general public will not be able to trade on SFC-licensed VATPs);
- have stringent criteria for the inclusion of virtual assets to be traded on its platform;
- obtain the SFC's prior written approval for any plan or proposal to add any product to its trading platform;
- submit monthly reports to the SFC on its business activities;
- engage an independent professional firm acceptable to the SFC to conduct an annual review of its activities and operations and prepare a report confirming that it has complied with the licensing conditions and all relevant legal and regulatory requirements;
- only provide services to clients who have sufficient knowledge of virtual assets;
- not conduct any offering, trading, or dealing activities of virtual asset futures contracts or related derivatives;
- adopt a reputable external market surveillance system to supplement its own market surveillance policies and controls; and

- ensure that an insurance policy covering the risks associated with custody of virtual assets is in effect at all times.

JAPAN

- On 15 March 2019, Japan's Financial Services Agency (FSA) submitted a bill to the National Diet to amend both the Payment Services Act (PSA) and the Financial Instruments and Exchange Act (FIEA) relating to regulations of the purchase and sale of cryptocurrencies in Japan. Proposed amendments include: (1) certain types of cryptocurrencies to constitute "securities" for purposes of Japanese securities regulations, which would be exclusively regulated by the FIEA; (2) the provision of "custody services" regarding cryptoassets to become subject to the PSA and require that entities providing such services register as a "Crypto Asset Exchange Service Provider" (the "Exchange Provider"); (3) providing designated methods regarding the safe keeping of customer cryptoassets by Exchange Providers; (4) Exchange Providers to be required to notify the FSA prior to conducting transactions with respect to each particular cryptoasset; and (5) Exchange Providers to be required to implement internal rules consistent with the rules adopted by the Designated Association of Crypto Asset Exchange Service Providers, a

self-regulatory body authorized under the PSA, which is currently the Japan Virtual Currency Exchange Association (the "JVCEA").

- On 25 June 2019, the JVCEA published a draft self-regulatory rule and guideline regarding initial coin offerings (ICOs) for Virtual Currency-type tokens, titled "Rules for Selling New Virtual Currency" (the "Rules"). The Rules distinguish between two types of ICOs: (i) an Exchange Provider who issues new tokens and sells such tokens by itself; or (ii) a token issuer who delegates to Exchange Providers to sell newly issued tokens. For each type of token, the Rules require: (1) maintenance of a structure for review of a targeted business which raises funds via ICO; (2) information disclosure of the token, the token issuer's purpose for the funds or the like; (3) segregated management of funds raised by ICO; (4) proper account processing and financial disclosure of funds raised by ICO; (5) safety assurance of the newly issued token, its blockchain, smart contract, wallet tool and the like; and (6) proper valuation of newly issued tokens.

KOREA

On 23 July 2019, the Ministry of SMEs and Startups designated Busan, South Korea's second-most populous city, as a regulation-free zone for blockchain technologies. It is expected that Busan will be a testbed for developing and applying blockchain technology in various sectors, ranging from finance and payment solutions to tourism promotion and fisheries.

Such application of blockchain technology was

made possible by the government granting, on a limited basis, alleviation of regulations currently applied to blockchain, in particular those relating to personal information data protection. Korea has strict rules relating to protection of personal information, and such rules were deemed to be in conflict with the nature of blockchain, where information may be stored indefinitely. For Busan, this restriction was alleviated by regarding storage of personal information "off-

chain" (in a separate server) and subsequent destruction of such personal information as satisfying the requirements under Korean data protection laws.

However, the program will not allow ICOs and will not include cryptocurrency related products, other than digital vouchers to be issued by the Busan government for use in certain

designated outlets. South Korea has taken a conservative approach towards cryptocurrency and ICOs. While there has been press coverage of the Financial Supervisory Service preparing to legalize ICOs and cryptocurrency trading, it remains to be seen whether an effective regulatory framework will be adopted in the near future.

NEW ZEALAND

In June 2019, New Zealand became the first country to legalize payments of salaries and wages in cryptocurrencies, provided that the payments are (1) for services performed under an employment contract, (2) for a fixed amount, and (3) regular remuneration. According to the Inland Revenue Department, the cryptocurrency must be convertible into fiat currency, and pegged to the price of one

or more fiat currencies. In terms of taxation, wages and salaries paid in cryptocurrencies will be treated as Pay as You Earn (PAYE) income payments. Under the PAYE scheme, the employer deducts taxes before distributing payments to employees. The ruling excludes self-employed taxpayers from changing their income to cryptocurrencies. The new law went into effect on 1 September.

SINGAPORE

- On 2 May 2019, the Monetary Authority of Singapore (MAS) and the Bank of Canada (BoC) announced they had conducted a successful experiment on cross-border and cross-currency payments using central bank digital currencies. This announcement follows the linking of MAS and BoC's respective experimental blockchain-based payment networks, Project Ubin and Project Jasper. Following this collaboration, MAS and BoC jointly published a report that proposes different design options for cross-border settlement systems and discusses the technical aspects of implementing distributed ledger technology for cross-border, cross-currency, cross-platform high-value payments.
- On 11 November 2019, the MAS announced the successful development of a blockchain-based prototype that enables payments

to be carried out in different currencies on the same network. The prototype network, developed by MAS in collaboration with J.P. Morgan and Temasek, marks another milestone for Project Ubin, which in its fifth phase aims to determine the commercial viability and value of the blockchain-based payments network. A project report is expected to be published in early 2020, which will describe the blockchain use cases that would benefit from the prototype network, as well as additional features that the network could provide.

- On 20 November 2019, the MAS published a consultation paper on its proposed regulatory approach for derivatives contracts that reference payment tokens (e.g., Bitcoin, Ether) as underlying assets. Currently, a derivative is regulated under the Securities and Futures Act (SFA) if its "underlying thing" falls into one

of the categories prescribed in the SFA (e.g., currencies, commodities, etc). However, since payment tokens are not usually characterised as any of the prescribed “underlying things”, derivatives contracts referencing payment tokens fall outside of the MAS’ regulatory perimeter. The MAS proposes to add payment tokens to the definition of “underlying things” under the SFA and payment token derivatives can then be listed and traded on “approved exchanges” in Singapore. To reduce the ampli-

fication of losses experienced by retail investors, regulated financial institutions will have to collect from retail investors 1.5 times the standard amount of margin required for contracts offered by “approved exchanges”, subject to a floor of 50%. The 1.5x margin requirement applies to both listed and over-the-counter payment token derivatives. The margin requirement will be supplemented with other measures such as tailored risk warnings and restrictions on advertising.

THAILAND

- In July 2019, the BOT published a report on the completion of Phase II of Project Inthanon, the wholesale CBDC experiment between the BOT and leading financial institutions. The report detailed the successful use of DLT for interbank bond repo and trading, facilitating third-party funds transfer, and enhancing the monitoring of regulatory compliance activities.
- Phase III of Project Inthanon, which focuses on interoperability, particularly in the area of

cross-border payments and settlements, sees the BOT collaborating with the HKMA. The two authorities will explore linking the BOT’s Project Inthanon with the HKMA’s Project LionRock via a corridor network to achieve atomic PvP with reduced settlement layers. According to the BOT’s press release, Phase III aimed to be completed by the fourth quarter of 2019 and a joint project report with the HKMA is expected in the first quarter of 2020.

THE PEOPLE’S REPUBLIC OF CHINA (PRC)

- In July 2019, the Hangzhou Internet Court issued a ruling which recognizes Bitcoin as digital property, despite it not possessing the legality of official currency. In other words, Bitcoin obtained by legal means shall be protected by PRC laws. The People’s Bank of China (PBoC), the central bank of PRC which oversees financial institutions across the country, has confirmed the ruling. While this local ruling has yet to become national law of the country, it is still regarded as a milestone that has set a positive precedent for future cases and regulations regarding cryptocurrencies.
- In August 2019, the PBoC announced that it is creating a digital currency that they refer to as

the Digital Currency Electronic Payment (DCEP). Planning for the DCEP project has been underway since 2014, when the original objective of DCEP project was to safeguard China’s currency sovereignty, in part because of the growing popularity of Bitcoin, but also because two Chinese private sector payment systems accounted for 96% of China’s mobile payments market share, making them systemically important payments infrastructures. This concentration risk concerned the PBoC, because if there were any problems with those private sector service providers then the PBoC must be prepared to assist, and, without its own digital form of cash, offering immediate assistance would be difficult.

- The DCEP coin is targeted at the retail sector, not at wholesale payments. The distribution model will be two-tier: the PBoC will issue DCEP coins to commercial banks and certain other institutions, and those banks/institutions will distribute the DCEP coins to the general public. To avoid disintermediating the financial system, the PBoC will not be issuing DCEP coins to the public directly.
- DCEP coins are a substitute for existing M0 currency (i.e., paper notes and coins). No interest will be paid for holding DCEP, and there also should be no implications for inflation and no impact on the PBoC’s monetary policy.
- All existing rules on cash and foreign exchange management must be observed, together with other applicable rules relating to anti-money laundering and counter-terrorist financing.
- The DCEP project is decoupled from traditional bank account ownership so it will enhance financial inclusion, particularly in China’s rural areas. Customers will be able to open a digital wallet and receive DCEP coins without any linkage to a bank account. Therefore foreign visitors to China will also be able to open a digital wallet and have access to digital payments in China without a local bank account.
- It is not clear the extent to which blockchain technology will be incorporated into the DCEP project – statements by the PBoC indicate that digital currency will not rely entirely on blockchain because it cannot handle the enormous volume of retail transactions.

Instead, it seems likely that the PBoC will use the same governance structures it uses in coordination with commercial banks to release fiat currency into circulation -- meaning that the issuance will be controlled and governed not by decentralized stakes or proof-of-work but rather by the same mechanisms that currently exist for domestic fiat currency. Patents filed by the PBoC also indicate that the PBoC plans to deploy some of the security features popularized by cryptocurrencies, including private keys and multi-signature authentication.

- In October 2019, President Xi described blockchain technology as a “core technology” and called upon the country to take the lead in blockchain development. President Xi pointed out a number of areas in which blockchain technology could be usefully employed, including supply chain management, food safety, healthcare, and public services. Despite the PRC government’s support for blockchain technology, it remains skeptical towards cryptocurrencies due to fears relating to cybercrime and fraud; crackdowns on crypto exchanges and ICOs continue to take place.
- Shortly after President Xi’s announcement, the PRC’s National People’s Congress passed a new Cryptography Law, introducing a framework to facilitate the cryptography industry and promote cyber-security. This new law categorizes cryptography into core, common and commercial cryptography. It requires state secrets to be stored using the core and common encryption and non-state secrets to be stored using the commercial encryption. The law went into effect on 1 January 2020.



LEGAL & REGULATORY: THOUGHT PIECES

PRIVACY

COVINGTON & BURLING

COVINGTON

As with any new technology, attempting to align blockchain with existing legal norms poses many challenges. Much has been said about aligning the unique features of blockchain — such as its immutability and decentralised nature — with existing privacy legislation. More specifically, some have questioned whether real-world applications of blockchain can comply with the EU's General Data Protection Regulation (GDPR). A recent study from the European Parliament has once again brought these issues to light.

This article notes at a high-level some of the privacy issues that blockchain raises, and sets out some solutions that have been proposed — solutions that will need to be explored further by policy makers, regulators, and industry experts. Such legal certainty is greatly needed to ensure that these challenges do not hinder the adoption of a new technology that is set to revolutionize whole industries.

BLOCKCHAIN VS. PRIVACY

Issues with respect to aligning blockchain and the GDPR range from questions about the responsibility for, and enforceability of, GDPR obligations, to the application of international data transfer rules to blockchain scenarios. In this wide field of issues, two of the most salient are the following:

- **Immutability.** Blockchain is an immutable ledger, meaning that once information is uploaded to the network, it cannot be deleted or modified. This runs counter to some key principles and rights outlined in the GDPR, including that personal data should not be retained for longer than is necessary (the “minimisation” principle), and that individuals have a right to correct and delete their personal data.
- **Decentralisation.** Blockchain is decentralised, meaning that no one entity controls the net-

work, and many different actors can access and use it. The GDPR, however, has been drafted with a fundamentally different conception of how information systems operate. Rather simplistically, it divides the world into entities that control the processing of personal data (controllers) and entities that merely process personal data on behalf of others (processors). Unhelpfully, blockchain participants do not fit nicely into these preconceived categories, making it challenging to apply the GDPR's substantive rules and liability provisions.

The extent to which any given blockchain will engender privacy issues will vary from case to case, depending on the purpose of the blockchain, the extent to which personal data is associated with it, and the particular features of the blockchain network (e.g., public vs. private and permissioned vs. permissionless). The European Parliament conceded in a recent study that “it is impossible to state that blockchains are, as a whole, either completely compliant or non-compliant with the GDPR”. It is widely accepted by commentators and policy makers that public and permissionless blockchain networks will raise the greatest privacy challenges, as access and use of these blockchain networks is unrestricted.

POSSIBLE SOLUTIONS

The use of blockchain solutions will not necessarily lead to a breach of data privacy laws. However, as outlined above, there are some areas where issues are likely to arise. Commentators and policy makers have suggested a number of solutions:

- **Keeping personal data off the network.** Some argue that personal data should not be stored on blockchain networks, but instead in a separate database. However, for many use cases, avoiding the use of personal data in a

blockchain network itself may be difficult. As such, this solution seeks to avoid the issues to the detriment of the technology's promise, as opposed to addressing them head-on.

- **Greater regulatory guidance vs. updating legislation.** Lawmakers appear to lack the motivation to update existing regulation to address blockchain technologies. Instead, there has been more focus on policymakers and regulators releasing coordinated guidance to help address the issues raised above. This could allow for a more flexible, nimble approach – subject of course to those recommendations not reducing blockchain's potential.

- **Technical solutions.** More cross-disciplinary research is required to understand the intersection of blockchain and law, and to find practical and innovative technological solutions. For example, the development of more advanced encryption and anonymization techniques could lower privacy concerns around information stored on blockchains.

In order to ensure legal certainty for businesses wishing to adopt blockchain solutions, clarity on how to address these tensions is desperately needed. The solutions provided above must be explored further by policy makers, privacy regulators, and industry experts, as a matter of urgency.

CRYPTOASSETS AND PAYMENT SERVICES

SHEARMAN & STERLING | BARNABAS REYNOLDS; MATTHEW HUMPHREYS



INTRODUCTION

Various different approaches have been taken by regulators to address the risks presented by cryptoassets to consumers, as well as money laundering/terrorist financing threats and wider financial stability concerns. These range from simple warnings to consumers about the risks posed by cryptoassets, to partial or outright bans. Some regulators, such as the UK Financial Conduct Authority (FCA), have adopted a “regulatory sandbox”, allowing for market entrants to test innovative products and services in a controlled environment, with support in assessing the regulatory treatment of the proposed business model.

In the UK, the FCA has considered how cryptoassets and related activities may be dealt with by existing regulation, which was not designed with such assets in mind. This short note considers how existing UK payment services regulation could apply to crypto-related business activities, taking into account recent guidance published by the FCA.

CRYPTOASSETS AND PAYMENT SERVICES

Many of the innovative business models leveraging cryptoassets are in the payment services space. One example is the use of cryptoassets to facilitate international money remittance. On this model, a customer hands over an amount in one currency to their payment service provider, with the intention of an equivalent amount in another currency being made available to a recipient. The payment service provider converts the fiat funds into a cryptoasset, which is then converted into the desired currency of the recipient. The use of cryptoassets to intermediate the conversion of one currency into another is intended to facilitate low cost cross-border, cross-currency payments, but that may not always be achieved.

Wherever a business uses cryptoassets to facilitate payment services, there is a possibility of the activities falling within the scope of UK payment services regulation. If so, the business may require UK authorization as a payment institution. The relevant UK regulations (which

derive from EU-wide rules) capture a number of different types of payment services including, among others, money remittance, the provision of payment accounts, and the execution of payment transactions.

The FCA has confirmed that activities relating purely to cryptoassets, such as the operation of a cryptoasset account or the transmission of cryptoassets, are not within the scope of UK payment services regulation, which governs activities relating to “funds”, defined as “banknotes and coins, scriptural money and electronic money”. However, the use of cryptoassets to facilitate a service involving traditional money, for example transferring money overseas using cryptoassets as an intermediary mechanism, may still be captured by regulation.

Electronic money (e-money) is a related area of regulation that may apply to the use of cryptoassets in a payment services context. Businesses that issue cryptoassets that constitute e-money under the relevant regulations would need to obtain authorisation as an e-money institution, unless an exemption applies or the business already has an acceptable regulatory status (for example, authorisation as a bank).

A contemporary example of a crypto-asset that may qualify as electronic money is a “stablecoin”. Stablecoins are effectively electronic stores of monetary value and, depending on the circumstances, their issuance may therefore be

regulated. On the other hand, “[c]ryptoassets that establish a new sort of unit of account rather than representing fiat funds are unlikely to amount to e-money unless the value of the unit is pegged to a fiat currency”, according to the FCA guidance referred to above. Enhanced regulatory scrutiny towards stablecoins is likely to emerge in the future given the significant financial stability implications and monetary policy risks identified by the G7 Working Group on Stablecoins in their October 2019 report. Firms leveraging cryptoassets to facilitate payment transactions, building payment networks using cryptoassets or issuing cryptoassets should consider whether the ultimate service provided to clients constitutes a regulated payment service or the issuance of e-money. Without the required authorisation, they may be subject to a fine or (for an individual) a custodial sentence.

OTHER ISSUES

Firms engaging in activities related to cryptoassets should always seek legal advice as to potential regulatory and other legal issues that may apply to ensure that they do not engage in cryptoasset activities that constitute UK regulated activities without the appropriate regulatory authorisation. Firms will also need to comply with applicable AML laws. The Fifth EU Money Laundering Directive is due to come into effect in January 2020 and brings crypto exchanges and crypto wallet providers into the scope of the AML obligations. These businesses will need to carry out customer due diligence on prospective clients, among other requirements.

CUSTODY OF DIGITAL ASSETS

NORTON ROSE FULBRIGHT | HANNAH MEAKIN; RONALD D SMITH; ETELKA BOGARDI; GLEN BARRENTINE; ALBERT WEATHERILL; AMY CHUNG



The cryptocurrency custody market has had an interesting year. A greater institutional presence, new and innovative financial

products referencing a range of cryptoassets and an increasing desire for secure and stable infrastructure to support an often volatile asset

class have come together to push demand for institutional-grade custody offerings. And where there is demand, there is usually supply. A number of global financial institutions, such as Fidelity and Nomura, have entered the market over the course of the last year, adding to solutions provided by cryptoassets stalwarts such as Coinbase, Gemini and Bakkt. This article provides a short update of the key developments impacting the burgeoning industry of custodying cryptoassets.

LEGAL CHANGES IN THE MARKET

In many jurisdictions, key legal questions as to the true status of cryptoassets as a matter of law remain unanswered. These are often fundamental as they determine how a cryptoasset can be transferred, whether a trust can be established in respect of a cryptoasset and how a cryptoasset can be stored by a custodian. In recognition that adoption is being hindered by these uncertainties, the past year has seen increased focus from various governments, courts and the broader legal community to try to address these issues. Notably, in a recent decision of the Singapore International Commercial Court, the judge held that cryptoassets (in this case BTC and ETH) may be treated as a form of property capable of being held on trust. The UK Jurisdictional Taskforce also published a report in November identifying cryptoassets as a “third-kind” of property which cannot be possessed and does not embody any enforceable rights. The Taskforce also expressed the view that private keys connected to wallets constitute information as opposed to a form of property in and of themselves, potentially calling into question the ownership of private keys. Whilst these developments help to add clarity to the legal assessment of cryptoassets across jurisdictions, uncertainty still remains.

REGULATORY FRAMEWORKS BEGINNING TO TAKE SHAPE

2019 also saw regulators begin to enhance

and confirm their respective positions on cryptoassets, providing additional clarity for custodians operating in this space. In the UK, the FCA confirmed that cryptoassets such as BTC and ETH are not regulated instruments, meaning custodying those forms of cryptoassets is not, in isolation, a regulated activity requiring a licence.

In Hong Kong, the Securities and Futures Commission recently launched a new “opt-in” regulatory regime for cryptoasset exchanges under which any client assets of a cryptoasset exchange are required to be held on trust for its clients through a company that is licensed to carry on a trust or company service provider business in Hong Kong, meaning that the custody of such cryptoassets will be brought within the remit of a regulator.

In the US, regulation relating to the custody of digital assets is a work in progress, particularly at the federal level where regulators are still studying issues related to the custody of digital assets. As a result, the only regulated entities that currently offer custody services with respect to digital assets are state registered trust companies. State registered trust companies may meet the definition of the term “bank” for purposes of the federal securities laws and, as such, may also be a “qualified custodian” that can hold funds and assets for investment advisers pursuant to the custody rule applicable to investment advisers.

As to broker-dealers, the U.S. Securities and Exchange Commission, in a joint statement with the Financial Industry Regulatory Authority, raised a number of concerns relating to custody by broker-dealers of digital assets, including those relating to fraud and theft, the loss of private keys, and the inability to record or replace lost property or correct errors. The Joint Statement makes it clear that they currently view digital securities as incompatible with a broker-dealer’s obligations under the custody provisions of the customer protection rule to which broker-

dealers are subject. Accordingly, broker-dealers that transact in digital assets or currencies for themselves or their customers may currently do so only on a non-custodial basis.

On the AML front, as of 10 January 2020, crypto custodians established in the European Union will need to be fully compliant with the provisions of the 5th Money Laundering Directive. For non-financial institutions active in the crypto custody market, this is the first time that many have been subject to any form of regulatory supervision and it will be interesting to monitor the enforcement trends in this space in the year ahead.

OPERATIONAL TRENDS

A variety of operating models have arisen across the market, reflecting both legal and commercial considerations. A form of custody that has proven popular is that of bailment. More traditionally utilized for physical goods, such as freight and the vaulting of metals, bailment is where a party takes a possessory interest in property without acquiring any legal or beneficial interest in it. The alternative to this structure is the traditional English law custody model, whereby the custodian or a nominee is

recorded as the legal owner of the assets, with the beneficial interest in the assets remaining with the depositor or its underlying client.

Likewise, the extent of custody services remains varied. In some contexts, custody has been determined to constitute the holding of private keys, rather than the cryptoassets themselves, whereas in other contexts custodians are providing wallet functionality and holding the assets. Within the latter model, some custodians have implemented segregated wallets and sub-wallet structures, whereas others have been adopting the omnibus account structure more typically seen in traditional custodial arrangements. In all such instances, as the custodian is maintaining books and records as to ownership interests in cryptoassets, many have sought to provide trade execution services in cryptoassets and support settlement cycles through regular reconciliations and a combination of off and on-chain transactions.

Finally, a handful of crypto-custodians have been able to secure insurance for cold storage solutions. Insurers tend to remain skeptical of less robust models.

these projects should be regulated.

WHAT IS A STABLECOIN?

A stablecoin is a crypto-asset designed to have low volatility and consistently reflect the value of a reference asset or assets with identifiable value (such as currencies, commodities or securities). By seeking to achieve price stability, stablecoins aim to overcome the significant volatility which is a key limitation preventing cryptoassets being adopted as a means of exchange or a store of value (rather than a means of speculation). To achieve price stability, stablecoins employ a

STABLECOINS

LATHAM & WATKINS

LATHAM & WATKINS LLP

STABLECOINS: GLOBAL REGULATORY OVERVIEW¹²⁷

An important global trend continuing from 2018 is the emergence and proliferation of stablecoins.¹²⁸ Given their inherently data-centric and financial nature, stablecoin projects face various legal and regulatory hurdles, some quite unique from traditional cryptocurrencies. In particular, the more recent development of “global stablecoins,”¹²⁹ which have the potential to disrupt traditional payments systems and other financial services, has provoked increased governmental and regulatory scrutiny of how

range of stabilisation methods. Typical structures include:

- **Currency-backed:** a stablecoin backed by, and redeemable for, funds held by an issuer or custodian.
- **Asset-backed:** a stablecoin backed by traditional assets (such as commodities or securities) held by an issuer or custodian, or decentralised assets, which is either redeemable or held in a manner designed to reduce the value volatility.
- **Algorithmic:** a stablecoin with a price that reflects holders' expectations about the future purchasing power of their holdings, which does not require the custody of any underlying asset. For example, the value of a stablecoin 'pegged' to an index or other measure of value may be stabilized using an algorithm that expands and contracts the circulating supply of the stablecoin in response to market behaviour.

REGULATORY TREATMENT: STRUCTURE MATTERS

Governments are grappling with the implications of stablecoin usage, including potential consumer fraud or loss, financial crime and tax evasion, competition issues, and even reduced sovereign control of monetary policy and supply. As a result, regulators face questions regarding how to apply laws and regulatory regimes that did not contemplate the technology underpinning stablecoins or their uses, and legislators are also forced to consider whether to tweak existing, or implement new, legislative frameworks to accommodate such technology and uses.

That said, it is clear from a regulatory perspective that the structure of a stablecoin (including the stabilisation method used) matters. For example, in most major jurisdictions, whether a stablecoin is to be regulated as a security, a derivative, a stored value product, or an unregulated

instrument turns on these facts. Generally speaking, currency-backed and asset-backed stablecoins¹³⁰ will be regulated as a security, derivative or stored value product. As a result, issuers and intermediaries may be required to register with, or be licensed by, regulators, and the stablecoin may need to be traded through regulated channels.

It is critical to assess the regulatory treatment of the stablecoin at the outset of a project as the conclusions will drive a number of significant legal and regulatory dependencies including whether the stablecoin issuer or other intermediaries (such as exchanges or wallet providers) require licenses, whether there are restrictions on the marketing and sale of the stablecoin, and whether (or how) the project will need to interact with regulated financial markets infrastructures (e.g. existing payment, clearing or settlement systems). Unfortunately, at present, legal uncertainty continues to exist in various jurisdictions regarding the treatment of stablecoins; further, little regulatory alignment exists across jurisdictions. Stablecoin developers must reconcile whether and how their project may operate under the laws and regulations of each jurisdiction in which they will operate or in which the stablecoin will be distributed.

KEY DEVELOPMENTS

The emergence of stablecoins has prompted national and international reactions.

At a national level, for example, the UK Financial Conduct Authority has provided specific regulatory guidance on the application of the UK regulatory framework to stablecoins. A number of jurisdictions (e.g., Gibraltar, Malta, and Hong Kong) have gone further, developing technology-specific regulatory frameworks for digital assets that may apply to stablecoins. Regulators in the US are still grappling with the treatment of stablecoins and how they may differ from other crypto-assets.

At an international level, the Group of Seven Working Group on Stablecoins released a report Investigating the Impact of Global Stablecoins (G7 Report), published in tandem with a report by the Financial Stability Board (FSB) on the Regulatory Issues of Stablecoins (FSB Report). Taken together, these reports provide insight into how some of the world's most advanced economies view digital assets and stablecoins, particularly those with the potential to launch and quickly scale on an established private-sector global network.

The G7 Report highlights many concerns regarding the development of global stablecoins that are linked to a basket of real-world assets or sovereign currencies, including the possible threats to global financial stability and national monetary sovereignty. The FSB Report acknowledges that a stablecoin payment system could benefit the global financial system and broader economy, but potentially entail material risk to systemic financial stability due to rapid scalability of stablecoins, the interconnectedness

of the payment ecosystem, the impact on existing financial infrastructure, and various market integrity and cybersecurity concerns.

The policy considerations raised in both the G7 Report and the FSB report are likely to provide the foundation for further work by governments and regulators in relation to stablecoins. Much of the work is expected to be the development of legislative and regulatory frameworks that clarify stablecoin regulation and address risks associated with stablecoin projects. However, the emergence of possible global stablecoins may also be the impetus for governmental and international bodies to develop publicly issued and controlled stablecoins that digitally represent fiat currency. Two notable projects of this kind are underway, with the People's Bank of China announcing a project to issue the world's first national digital currency in 2020, and the European Central Bank announcing that it is analyzing the technical aspects of a digital currency to assess the desirability and feasibility of a publicly issued cryptocurrency in the EU.

AT THE VERGE OF REGULATION: TRADING SIGNALS AND COPY TRADING IN SWITZERLAND

FRORIEP | CATRINA LUCHSINGER; RONALD KOGENS

FRORIEP

The hype around ICOs and new DLT-protocol launches has calmed down. The technology has proven its ability to revolutionize the financial market industry, as well as other industries, by serving as an infrastructure where physical and digital assets or financial instruments can be tokenized in rivalrous cryptographic tokens and exchanged in a secure, cost-efficient and reliable manner. The next stage for DLT to enter into full productivity is to have built the surrounding infrastructure, tools, and service providers. Trading signals and copy trading are among such additional tools. Trading signals are trading ideas or trade suggestions to buy or sell a particular cryptographic asset at a certain price

and time. These trade signals are generated manually by experienced, professional traders, or automatically by algorithmic bots. Copy-trading goes one step further. It enables a holder of cryptographic assets not only to receive buy or sell indications but also to automatically copy transactions made by another experienced trader on an ongoing basis. The use of these two terms in practice is not consistent. Sometimes trading signals can also be applied directly to balances of cryptographic assets on exchange-platforms, whereby procedure becomes copy trading.

Trading signals and copy trading have

similarities to professional asset management and investment advice known from the old economy, but with a different mission: reduction of intermediary costs and expenses as well as the democratization of asset management and investment advice.

As with every new tool, be it infrastructure or services surrounding DLT, questions arise if and how the tool falls under existing financial market law regulation. As of 1 January 2020, financial services are mainly regulated in the Financial Market Services Act (FinSA) that seeks to enhance the reputation and competitiveness of Switzerland's financial market. FinSA applies to financial service providers, client advisers, producers and providers of financial instruments. In terms of cryptographic tokens, it is only relevant for tokens qualifying as securities.

The term "financial services" in accordance with article 3 (c) FinSA is defined broadly. It includes the acquisition and sale of financial instruments for the account of clients (article 3 [c] [1] FinSA). Mere brokering of transactions in financial instruments (article 3 [c] [2] FinSA) as well as portfolio management and investment advice are also considered to be financial services. Portfolio management is deemed to comprise all activities for which the financial service provider is given power of attorney to invest assets for the account of the clients (article 3 [c] [2] FinSA). By contrast, if the financial service provider recommends the purchase or sale of financial instruments to specific clients, this constitutes investment advice. No personal recommendation and thus no investment advice is given if a financial services provider merely communicates to its client the general expectations of its institution or third parties regarding the development of certain financial instruments. Such references do not refer to financial instruments in client portfolios.

Trading signal providers in our view simply communicate to the signal receivers general expectations of its institution or third parties regarding the development of certain security tokens (financial instruments). Signal providers do not have access to the portfolios held by the signal receivers on third-party exchanges. They also do not have any information in this regard. The relationship is impersonal (anonymous) and the signals do not take into account in any way personal characteristics of the signal receivers such as their preferences, risk appetite, and financial situation. In our opinion trading signals, therefore, do not qualify as financial services as there is no customer/provider relationship. It is possible that the signals relate to security tokens which the signal receiver does not even own or are not traded on the third-party exchanges for which she/he has wallets. To publish a trading signal is only to grant a use right (no different than the purchase of an app) where only the purchaser can decide whether or not the software tool is of use to him or not.

We believe that the same must apply to copy trading. With copy trading, expert traders only allow others to obtain information about the trades they are executing and give them the opportunity to copy such trades. The expert traders likewise do not have access to the portfolios held by the copying individuals on third-party exchanges. They can also not adjust signals to the existing constituents contained in any one exchange account. The relationship is again impersonal/anonymous. The expert traders act in their own name and own account and only consider their own interests and preferences. Interests and preferences of copying individuals are not known to the expert traders; in fact, they do not care about the interests and preferences of copying individuals. As stated, trading signals and copy trading have similarities to asset management and investment advice, however, their functioning includes key

distinctive characteristics. These characteristics should not be ignored and in our view must result in the non-application of the Financial

Market Services Act; the Swiss Financial Market Supervisory Authority will have a say in how these tools will be treated.

TAXATION

STEPTOE & JOHNSON | LISA ZARLENGA; JOHN COBB

Steptoe

The Internal Revenue Service (IRS) has been paying increasing attention to the taxation of cryptocurrency transactions over the past couple of years. Thus far, the IRS approach to cryptocurrency has been somewhat divided — with the enforcement side of the IRS (both civil and criminal) jumping out ahead, developing centralized expertise and a coordinated effort to root out noncompliance and outright evasion. The guidance side of the IRS (i.e., the Chief Counsel office), though it acted first back in 2014 (issuing Notice 2014-21), seemed to slow down after that. Recently issued guidance and identification of additional guidance on virtual currency on the IRS's Priority Guidance Plan (PGP) suggest a renewed effort on the guidance side in the coming year.

IRS CRYPTOCURRENCY ENFORCEMENT EFFORTS

The IRS's public-facing cryptocurrency enforcement efforts began in earnest in November 2016, when the Department of Justice filed an action seeking an order to serve an IRS John Doe summons on Coinbase. After a year-long fight, the District Court for the Northern District of California ordered Coinbase to turn over the name, address, taxpayer ID number, birthdate, transaction logs, account statements, and invoices for U.S. customers engaging in transactions of at least \$20,000. Coinbase informed approximately 13,000 affected customers that it expected to send their information to the IRS by March 16, 2018.

In July 2018, the IRS Large Business and International Division (LB&I) announced a new

audit campaign to address tax noncompliance related to the use of virtual currency. LB&I campaigns direct the IRS's audit resources to specific areas the IRS believes have the greatest risk of noncompliance. The IRS's announcement means that taxpayers who failed to report virtual currency transactions face an increased risk of an audit.

At the same time, the IRS announced a joint international coalition to investigate cryptocurrency-related tax crimes and money laundering, including agencies from Australia, Canada, the Netherlands, and the United Kingdom. The coalition will work together to gather information, share intelligence, conduct operations, and build the capacity of tax crime enforcement officials.

In July 2019, the IRS began sending letters to about 10,000 taxpayers with virtual currency transactions that potentially failed to report income and pay the proper amount tax from virtual currency transactions. There were three variations of the letter with increasing degrees of firmness, with the strongest one requiring that the taxpayer file either an amended return or a written response.

At the same time, the IRS also appears to be stepping up criminal enforcement efforts. In July 2019, Don Fort, Chief of the IRS's Criminal Investigation Division stated in a speech that the Division is building a number of cryptocurrency-related criminal tax cases, and that details about those cases may soon become public. A detailed presentation, prepared by the Criminal

Investigation Division, regarding the use of cryptocurrencies in cybercrimes also became public in July. The presentation included a suggestion to investigators to consider issuing grand jury subpoenas to companies such as Google for the subject's download history or to financial institutions or PayPal for the subject's transaction history.

IRS GUIDANCE EFFORTS

The IRS's initial guidance on cryptocurrency, Notice 2014-21, concluded that convertible virtual currency is treated as property for tax purposes. Many tax consequences follow from characterization as property, including that "spending" cryptocurrency is treated as a taxable exchange. However, as pointed out by various stakeholders, many questions remain. Just this past October, the IRS released new guidance for the first time since 2014. The guidance included Revenue Ruling 2019-24, which addresses the tax treatment of hard forks, and a series of FAQs covering a variety of topics that expand on Notice 2014-21.

Revenue Ruling 2019-24 concludes that when a taxpayer receives units of new cryptocurrency "as a result of an airdrop of a new cryptocurrency following the hard fork," the taxpayer has ordinary income because he has experienced an accession to wealth. According to the Revenue Ruling, the income arises at the time of the airdrop, when it is recorded on the distributed ledger, because the taxpayer is, at that time, able to exercise dominion and control over the forked cryptocurrency.

The Revenue Ruling's analysis on this point appears to be based on some misconceptions about how units of a new cryptocurrency are accessed by holders of a pre-fork cryptocurrency, and confusion about the relationship between forks and airdrops. Because of this apparent confusion, the Revenue Ruling creates some uncertainty and practical issues for taxpayers. Nevertheless, the guidance

might be read as saying that a taxpayer will recognize income whenever the taxpayer gains dominion and control over a new cryptocurrency following a hard fork (i.e., the ability to dispose of the new cryptocurrency). Although the guidance does not technically apply to an airdrop without a fork, the reasoning would likely make that taxable as well.

The FAQs mostly just elaborate on Notice 2014-21, though there are some welcome expansions, such as clarifying that soft forks and transfers between wallets of a single taxpayer are not taxable and that the basis of cryptocurrency may be allocated using first-in-first-out assumptions if specific identification is not possible.

NEXT STEPS FOR CRYPTOCURRENCY TAX GUIDANCE

The IRS's 2019-2020 PGP identifies as a priority, for the first time, "guidance concerning virtual currency." The fact that virtual currency has made it to the PGP suggests an increased guidance focus.

In addition, the PGP lists a project regarding information reporting on virtual currency under the broker reporting rules of section 6045. These rules — which currently apply to brokers and dealers that affect sales of securities, commodities, options, and other financial instruments on behalf of U.S. customers — provide for information reporting on Form 1099-B. Information reporting would be a big step forward because it creates a compliance system. Other income that is subject to information reporting enjoys much higher compliance rates.¹³¹ The information returns help inform taxpayers of the need to pay tax on their cryptocurrency transactions, and they help the IRS identify taxpayers with cryptocurrency transactions.

CONCLUSION

New technologies are often used by criminals before becoming mainstream. This happened

with the internet and has happened with cryptocurrency. The IRS's focus on cryptocurrency has reflected this trend, with enforcement gearing up before substantial guidance is issued. However, the fact that the IRS

is beginning to shift towards a guidance focus and implement an information reporting regime suggests that U.S. cryptocurrency tax regulation may be turning the corner from enforcement to guidance.

ICOS ARE DEAD... LONG LIVE THE IEO... MAYBE?

SULLIVAN & WORCESTER | JOEL TELPNER; MARI TOMUNEN



Initial coin offerings (ICOs) had a spectacular rise in 2017 and 2018 and an equally spectacular fall as we moved into 2019. Are ICOs dead? No. On life support? Depending on who you ask, very likely. ICOs were perceived as a quick and easy way to raise funds through the issuance of new cryptocurrencies or tokens. Unfortunately, many ICO issuers believed - wrongly so - that ICOs were subject to little or no regulatory oversight. The documentation used to sell tokens in ICOs was inconsistent at best, scammers jumped into the space to make a quick buck, and many of the developers behind cryptocurrency projects overpromised and underdelivered. By some estimates, the tokens issued during the ICO frenzy have in the aggregate lost over 90% of their value.

In many cases the ICO issuer argued that the token being sold in the ICO was a so-called "utility token." That is, a token that either was not subject to regulation at all or, at the very least, was a means to raise capital that did not constitute the sale of securities. Of course, governments do not define and regulate securities in a uniform manner. In an effort to attract new blockchain businesses, some countries went so far as implementing new legislation giving recognition to the sale of cryptographic tokens that could, in certain cases, fall outside of that country's securities regulatory regime. We saw in 2017 and 2018 a number of ICO issuers engaging in "forum shopping," looking for the most regulatory friendly jurisdiction from which they could stage their

ICO. A false narrative existed in the ICO market that as long as an issuer picked the right location for staging the ICO, the issuer could avoid the regulatory requirements of the countries where investors were located.

Lack of transparency and unfulfilled promises, combined with some unscrupulous issuers and regulatory crackdowns in various countries, all put severe downward pressure on the ICO craze. As the market moved away from ICOs, alternative financing structures began to emerge in 2019. Security token offerings (STOs) were a response to this regulatory pressure, particularly from the U.S. STOs recognize that in many cases, when an issuer is selling a cryptographic token to raise funds to build a business or platform or protocol, the issuer is selling a security. Therefore, STOs are theoretically structured to comply with applicable securities laws disclosure and selling requirements. As a result, STOs involve a more complex selling process than existed with ICOs and require an appropriate infrastructure for ongoing compliance, such as regulated trading platforms to facilitate secondary trading.

Perhaps the more direct successor to ICOs are initial exchange offerings (IEOs). IEOs emerged in 2019 as a next generation ICO and are intended to address some of the problems that hobbled the ICO market. In a typical ICO, the issuer structures the terms of the token sale, often seeking out investors directly, without intermediaries. In contrast, in an IEO, a token issuer teams up with a third-party crypto

exchange or trading platform to issue its tokens.

Like ICOs, IEOs come in different flavors. In a typical IEO, an issuer must apply to a crypto exchange and pay a listing fee and in return, the exchange assumes the responsibility of issuing the issuer's tokens and raising funds for the token project. Because an exchange is expected to undertake due diligence on the potential token issuer and project, investors theoretically benefit by relying on the exchange's due diligence to weed out questionable projects. Of course, the comprehensiveness of any such due diligence may vary significantly from one exchange to another and the results of the due diligence may not be shared with potential investors. Additionally, as was the case with ICOs, there is no standardized minimum disclosure requirements on which potential investors can rely.

The token issuer in an ICO determines who is permitted to participate in the ICO and purchase tokens. We know that with many ICOs of securities, ICO issuers failed to apply appropriate regulatory limits on who qualified to purchase tokens. Similarly, those token issuers also failed to place appropriate restrictions on ongoing trading of the tokens once sold. Many in the market believe that IEOs solve these problems but that is not necessarily the case.

It is true that in an IEO, eligible investors are limited to those who have already been onboarded and have been given access to the exchange. That is, only whitelisted investors can participate in an IEO. This typically means that eligible investors would have been subject to whatever level of KYC/AML due diligence the exchange requires. Presently, however, there is no consistency among platforms

as to minimum KYC/AML standards or the process by which investors must satisfy those requirements. Additionally, the extent to which an exchange may impose secondary trading restrictions, if at all, varies significantly from one exchange to another. Therefore, to the extent that a regulator, such as the SEC, were to determine that a token sold pursuant to an IEO was a security, the procedures imposed by the exchange in the IEO process would likely not satisfy regulatory requirements for selling a security. Further, given the continued regulatory uncertainty in the U.S. and other jurisdictions, exchanges simply do not have the ability to determine that a token it is about to sell in an IEO is or is not a security under the laws of various jurisdictions.

There may be some clear benefits for IEOs over ICOs. Many believe that there may be efficiencies in investing through an exchange as opposed to creating a separate digital wallet for each ICO investment. Also, depending on the terms of the IEO, an exchange may impose milestones on the token issuer as a condition to releasing funds to the issuer that were raised in the IEO. These potential investor benefits may be offset, however, by the fact that the exchange receives a series of revenue streams including a listing fee, commissions on every token sale, potential revenue from undisclosed market making activities, and revenue created from increasing demand for the exchange's native token that may be required in order to participate in the IEO. Therefore, the exchange's own interests may be inconsistent with the interests of potential investors.

In 2020, we will see whether IEOs become a core method for fundraising in the cryptocurrency space or just another passing fad.

APPENDIX

THE STATE OF VOTING IN THE USA: PROBLEMS, POTENTIAL SOLUTIONS, AND RISKS — CAN TECHNOLOGY HELP DEFEND DEMOCRACY?

PART I OF THE GLOBAL BLOCKCHAIN BUSINESS COUNCIL'S 'OPEN SOURCE IDEAS': STATE OF GLOBAL VOTING SYSTEMS, TECHNOLOGY, AND GOVERNMENT

INTRODUCTION

Congratulations! You have decided to vote for the first time. But before you can cast your ballot, a lot of pieces need to come together. To start, you need to give yourself enough time to register because only 21 states allow for same day registration (SDR)¹³² and some states (including Ohio, Pennsylvania, and South Carolina) require registration at least 30 days before an election.¹³³ Next, you'll have to determine how to register. As of this writing, 13 states (including Michigan, New Jersey, North Carolina, and Texas) still do not allow online voter registration.¹³⁴ As you are filling out the paperwork, you will be asked if you are already registered to vote in any other states. Assuming you moved away from the state where you first got your driver's license, this might be a difficult question: did you check the box asking you if you would like to register way back when?

Once you have completed and submitted your registration, you wait. Depending on your state, you may be able to check a government website

to see if your registration was successful; but in many states you can only confirm your status by calling or visiting an election office.

Finally, you wake up on Election Day, excited to participate in the democratic process for the first time. You head to your polling place before work, hoping to beat the crowd. But there is already a line. You decide to come back after work so as not to arrive late and draw the ire of your not-very-understanding boss.

Throughout the day you check social media and are bombarded by reports of long lines at polls across the country. But you are not easily dissuaded (as this process has shown) and you travel back to your polling place after work to find the line just as you left it. You wait and finally get to cast your vote, which is stored on the voting machine to be tallied and delivered to a central location.

As polls across the country start to close,

election results start trickling in; races are called in favor of one candidate or another. Then your state is called with only 1% of precincts reporting — you know your vote *technically* matters, but it doesn't feel that way.

At times, the very structure of the U.S. voting system can seem designed to dissuade you from casting your ballot. The process is so archaic and disconnected that even the most modest reforms could have a significant impact. When examining the existing system — from registration to casting a vote v] — it is easy to see how a potential voter can become a discouraged non-voter or how a one-time voter can become a never-again voter.

Looking to more agile countries that have leveraged new technologies to improve the process shows the massive opportunity for improvement in the U.S. For the purposes of this report, we will examine the voting process in three distinct stages:

- (1) identity and voter registration;
- (2) casting votes; and
- (3) verification, accuracy, and security.

I. IDENTITY AND VOTER REGISTRATION

Voter registration and roll management processes vary significantly from state to state and have not been significantly altered since the passage of the National Voter Registration Act of 1993 (NVRA). NVRA requires states to offer voter registration at motor vehicle agencies and by mail-in application. A 2014 study found that about 24 million voter registrations in the U.S. are “no longer valid or are significantly inaccurate,” more than 1.8 million deceased individuals are still listed as voters, and about 2.75 million individuals are registered in more than one state.¹³⁵

In response to inaccurate voter rolls, some states have adopted controversial voter purge laws. Notably, in 2017, Georgia removed over 500,000

voters from its rolls, 107,000 of which were “purged because they had decided not to vote in previous elections and they failed to respond to mailed notices from the state.”¹³⁶ In June 2018, the U.S. Supreme Court upheld Ohio's “use-it-or-lose-it” voting law, which gives the state power to remove from its voter rolls anyone who does not respond to a mailed address confirmation form (which may or may not be received/seen by the individual) and does not vote for four years.¹³⁷ Using data from the federal Election Assistance Commission (EAC), the Brennan Center found that at least 17 million voters were purged between 2016 and 2018 and that purge rates were significantly higher in jurisdictions with a history of voting discrimination (as identified in the Voting Rights Act).¹³⁸

Estonia

To date, states have not properly leveraged technological advances to improve voter registration and roll management; blockchain technology¹³⁹ could be part of the solutions to both issues. Blockchain-based digital identities have already been deployed in places like Estonia, which has revolutionized its governance with digital solutions secured on the KSI Blockchain.¹⁴⁰ In Estonia, citizens are provided an ID-card with a chip that grants digital access to all government e-services, and can be used for voting and digital signatures, as a health insurance card, and to check medical records and submit tax claims, among other uses.¹⁴¹ Citizens may also obtain a special mobile SIM card to use their mobile phone as a secure digital ID. Estonia's i-Voting system is secured on the blockchain and leverages the country's digital ID system to save voters an estimated 11,000 working days each election.¹⁴² Estonia's e-governance and digital ID system has contributed to the country becoming the 18th-least corrupt nation¹⁴³ and growing its GDP per capita from US\$4,070 in 2000 to \$22,927 in 2018.¹⁴⁴ Estonia is a small, largely homogeneous country and is thus not a perfect template for the United States, though it is not the only

country innovating in the area of digital identity.

Switzerland

In 2018, the Swiss Canton of Schaffhausen and digital identity firm ProCivis successfully completed a pilot phase of its eID+ electronic identity solution and began to roll it out for the entire canton. Schaffhausen's eID+ allows citizens to create an electronic identification on their mobile phones that is then validated by a government registration office. This government-verified and blockchain-secured digital ID allows citizens to easily verify their personal information for a range of government services. As of this writing, eID+ has enabled e-Authentication, which allows users to "engage in trusted interactions with third parties," e-Signature, and e-Document, which allows citizens to review, sign, and submit official government documents, all from their mobile device. ProCivis and the Schaffhausen government are also moving to add e-License (to digitally store licenses and permits), e-Company (to simplify the founding of companies), e-KYC (to improve know-your-customer processes), and e-Health (to provide direct access to health platforms). They are also currently developing e-Data, which will allow citizens to control and monetize their personal data. These solutions, whether revolutionizing or streamlining government processes, are made possible by Schaffhausen's robust and secure blockchain-based digital ID solution.¹⁴⁵

Sierra Leone

This summer, nonprofit organization Kiva and the government of Sierra Leone announced that they will be building a national blockchain-based digital ID solution using biometric data that was previously collected by the government. According to President Julius Maada Bio, this project "guarantees that Sierra Leoneans are not excluded from... the global digital economy," by utilizing digital ID to allow citizens to build and prove credit history.¹⁴⁶ While the project was developed with financial inclusion rather than voting in mind, it shows that digital ID can be

attractive to governments, NGOs, and companies for a variety of reasons.¹⁴⁷

ID2020 Alliance

Companies and organizations, including Microsoft, Accenture, and the Rockefeller Foundation, created the ID2020 Alliance to provide digital identities to refugees around the world. The Alliance believes that effective digital ID is crucial for at-risk populations and notes that it is nearly impossible to access government services or vote without a recognized form of ID.¹⁴⁸ Most recently, the Alliance announced that it is partnering with the City of Austin, TX to develop MyPass, a blockchain-powered digital ID solution for people experiencing homelessness.¹⁴⁹

Digital Identity in the United States

The introduction of a robust digital ID system for U.S. citizens would make registering to vote easier for the average citizen. Further, keeping voter rolls on a blockchain could potentially allow voters to use their own private key (essentially a very secure password) to confirm they are registered and ensure their information is correct. Tying registration to a private key would also reduce or eliminate issues surrounding voters with the same name, as "minority voters are more likely to share names than white voters, potentially exposing them to a greater risk of being purged."¹⁵⁰ Some innovative jurisdictions like Schaffhausen and Estonia have implemented blockchain-based digital ID and begun building on it; meanwhile, projects like those in Austin, TX are crucial for identifying problems, improving solutions, and ultimately convincing some skeptics that digital ID is worth the implementation cost.

However, many questions remain open and in development regarding the type of digital identity from country to country. Is self-sovereign digital identity with government-based verification the ideal model? Who should act as the verification nodes in a blockchain-based identity network? How can any system scale?

Who will develop common taxonomy and/or standards language? And do we need a global solution or country-specific solutions?

II. VOTING

It is a well-known fact that the U.S. has lower voter turnout than most other developed democratic countries; in 2016 just 55.7% of the voting-age population voted, compared to 77.92% in South Korea and 62.12% in Canada.¹⁵¹ Perhaps most shocking, the Department of Defense estimates that only 7% of the 3 million eligible overseas voters voted in 2016.¹⁵²

In-Person Voting

While national average voting times declined from 14 minutes in 2008 to 8 minutes in 2016, there remain extreme outlier districts with significantly longer wait times. For example, in 2008 the average wait time in South Carolina was 62 minutes and in 2012 the average wait time in Florida was 45 minutes.¹⁵³ In 2016, some voters in Maricopa County, Arizona (home of Phoenix) waited over 5 hours to vote – the average wait time was over 2 hours.¹⁵⁴ According to *The Arizona Republic*, most counties had an average of 2,500 eligible voters per polling place; Maricopa County had about 21,000 eligible voters per polling place.¹⁵⁵ Most recently, non-partisan advocacy organization Common Cause Georgia stated the average wait time in 2018 in the Atlanta metro area was an astonishing three hours because of "locations not opening on time, broken voting machines, and issues with the state's exact match rules."¹⁵⁶ While there is a dearth of research in this area, studies by the Brennan Center¹⁵⁷ and Dartmouth¹⁵⁸ found statistically significant positive correlations between precinct proportion of minority voters and wait time.

Overseas Voting

Overseas voting is even more unreliable, with the DoD's Federal Voting Assistance Program (FVAP) estimating that if obstacles to overseas voting were removed, the voting rate would

increase from 6.9% to 37.5%. FVAP also found that "in countries with the highest estimated voting obstacles, those who receive their ballot electronically are approximately 50% more likely to have a vote recorded in administrative records than those receiving a ballot by mail."¹⁵⁹ Electronic submission of ballots is critical to engaging overseas voters in the democratic process.

Voting in the USA

There are reforms that could be implemented to boost voter turnout (e.g. compulsory voting, automatic registration, making Election Day a national holiday, etc.), but in recent years there has been increasing advocacy for blockchain-based mobile voting. Notably, a top Democratic candidate for president (as of this writing) believes that "Americans should be able to vote via their mobile device, with verification done via blockchain. This could significantly increase participation in all elections, whether local, state or federal."¹⁶⁰

In the U.S., blockchain voting pilots have been tested in multiple jurisdictions, most notably West Virginia. In a 2018 pilot project, individuals covered by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)¹⁶¹ were able to cast ballots using their mobile phones, each "ballot submitted was encrypted and stored on a geographically distributed and redundant network of blockchain servers managed by the two largest cloud infrastructure providers."¹⁶² Of the 183 eligible UOCAVA voters, 144 submitted ballots, for a voter turnout rate of 78.6%. This is a remarkable improvement over the DoD's estimated 7% voter turnout for overseas voters. It is important to note that the FBI is currently conducting an investigation into an attempted hack of the platform during this election, though the U.S. Attorney for the Southern District of WV has stated that "there was no intrusion and the integrity of votes and the election system was not compromised."¹⁶³ Jurisdictions have not been dissuaded by the hack attempt, as Jackson

and Umatilla Counties in Oregon announced in October 2019 that they are moving forward with pilot projects.¹⁶⁴

Russia

Russia has experimented with online voting for years, most recently offering about 450,000 citizens of Moscow the opportunity to cast blockchain-secured online ballots in the 2018 Moscow City Duma election. On its website, the Moscow city government claims that its “electronic elections guarantee complete anonymity and observance of ballot secrecy. The voter identity can not be connected with the ballot he/she made.”¹⁶⁵ However, shortly after the government released the code on GitHub, a French researcher found a critical encryption flaw that could be cracked “in a matter of minutes with easily available resources.”¹⁶⁶ After the flaw was published, the government corrected the issue and promised to pay its highest bug bounty, about US\$15,000. Next, a Harvard researcher identified another vulnerability that “can be used for counting the number of votes cast for a candidate.” Finally, after the votes were tallied, a Russian researcher found that there were significant statistical abnormalities between the online and offline votes; for example, one candidate supported by the ruling party received 47.1% of electronic votes and only 28.1% of paper ballots.¹⁶⁷ Russian journalists found that in “all three districts that used online voting, voters who chose pro-regime candidates submitted their ballots in the morning... at noticeably higher rates than voters who chose independent candidates.”¹⁶⁸

As demonstrated by the projects in West Virginia and Russia, it is crucial that online voting projects are conducted in a thoughtful and cautious manner; developers, government officials, and citizens should be aware that the use of blockchain technology does not necessarily make a voting system secure.

Blockchain Voting

Furthermore, while the prospect of mobile voting secured on the blockchain is exciting, many election security experts have cautioned against its broader implementation. Generally, they believe that while blockchain is secure, transmitting votes over the internet comes with inherent risks that have yet to be appropriately addressed.¹⁶⁹ The U.S. Vote Foundation wrote an extensive report on internet voting with input from “experts in election integrity, election administration, high-assurance engineering, and cryptography.”¹⁷⁰ This report states that “public elections conducted over the internet must be end-to-end verifiable (E2E-VIV)... No internet voting system of any kind should be deployed for public election before end-to-end verifiable in-person voting systems have been widely deployed and experience has been gained from their use.”¹⁷¹ And further, it “is currently unclear whether it is possible to construct an E2E-VIV system” that is sufficiently secure, usable, and transparent.

Currently, blockchain-based voting presents the greatest opportunity for overseas voters, many of whom already use return ballots electronically. Given the significant technological challenges associated with creating a blockchain-secured mobile voting system, more pilot projects and innovations will be necessary before the technology can be deployed on a wider scale. Blockchain-based voting projects must be conducted carefully and should generate paper backups and undergo rigorous post-election risk-limiting audits, which can determine whether votes were counted correctly.¹⁷²

III. VERIFICATION/ACCURACY

The patchwork of voting systems around the U.S. means that vote count and certification systems also differ. Generally, the process goes as follows: (1) wait for polls to close; (2) shut down voting machines and download votes; (3) deliver the votes by phone, modem, or hand; (4) count overseas, absentee, and provisional ballots; and

(5) certify the votes.¹⁷³ This entire process can take weeks; elections are usually decided by the time the overseas, absentee, and provisional ballots are counted. There have also been shocking reports, most recently in Texas¹⁷⁴ and Mississippi,¹⁷⁵ of voting machines changing votes.

There is room for innovation in these arenas and blockchain technology presents a promising solution. If votes were verified as a matter of record on a blockchain, voters would be able to confirm that their vote was included in the official result. Relevant state, federal, and local authorities could be included as trusted nodes on the network, granting them the ability to audit vote tallies and spot irregularities in real time. It would also be possible to count and include overseas and absentee ballots on Election Day, rather than tallying them days after.

CONCLUSION

The promise of an effective, digital, blockchain-backed voting system is not some far away dream — it’s already being used in various countries around the globe. Let’s take a moment to imagine what that might look like in the U.S.

You’ve decided to vote for the first time. You wake up on Election Day and log in to your state’s voting portal using your private key. Here you link your government-issued digital ID to register to vote or update your information. You fill out your ballot and securely cast your vote, all before leaving for work.

While it will be a long time before this full vision becomes a reality, there remains plenty of opportunity for technology-minded states to take incremental steps to dramatically improve the U.S. voting process. Voter registration, roll management, voting itself, and verification of votes are all processes that are ripe for improvements. It is encouraging to see forward-thinking jurisdictions thoughtfully leverage blockchain to overhaul government systems and voting systems due for a revamp. Further, the

slow and measured progression of bold voting reforms like the National Popular Vote Interstate Compact suggests there is an appetite for overhauling election systems.

Countries like Estonia and Georgia have shown that governments can use blockchain for the betterment of all citizens. Perhaps it is time for the U.S. to lead a transformation of traditional voting systems with the aim of increasing access, expanding engagement, and improving the health of its democracy.

All American citizens should be certain that their vote counts, and blockchain technology, along with other technologies, can be used to restore faith in democratic processes and the government as a whole. Today, there are too many inaccuracies, acts of voter suppression, questions of fraud, and inefficiencies surrounding the single most important function of a democratic government.

It’s time for the voting process in the U.S. to be reexamined and reformed to create a secure, equitable, and trustworthy system.

CONCLUSION

Turning the staggering potential presented by emerging technologies into substantive solutions that move our world in a positive direction is the collective challenge that galvanizes our community. Over the last year, we saw this promise improve the lives of refugees, empower consumers, redefine the way we produce and use electricity, inform new regulation, encourage corporate responsibility, and begin to reshape the landscape of traditional and digital news and print media. Conversations surrounding the creation of new systems aimed at facilitating the more efficient, effective movement of resources across borders for all sectors of society were highlighted during the most prominent forums around the globe. And established players embraced new models of decentralization and openness with resolve and enthusiasm. The power of dedicated ingenuity cannot be understated. We continue to see it first-hand.

And transformational, cross-industry, global change will continue be a generational effort. The litany of new solutions inspired by the attributes of blockchain and other emerging technologies are beginning to create an

infrastructure of transparency and trust desperately needed in every industry and every corner of the globe. They are establishing standards for more sustainable, rational, and ethical behavior — for individuals, communities, corporates, and governments. But building good infrastructure takes time, and requires thoughtful, sustained, multi-stakeholder engagement.

The GBBC is dedicated to continuing to support this work. With a new year, we anticipate the emergence of essential data points which will enable us to test the efficacy of new tools — whether we are building back better, and whether we are indeed moving past the “hype” of emerging technologies.

We remain inspired by the diversity, resilience, and capacity of our community and their commitment to creating a more fair, functional and efficient world. We welcome 2020 as a year of collaboration and look forward with renewed vigor to cataloging our community's collective progress.



The Global Blockchain Business Council is grateful for the extraordinary people that have contributed to the creation of this report.

We extend special thanks to:

Sierra Lewis, Riyad Carey, Mercina Tillemann, Sandra Ro, Sofia Arend, Alfredo Oballos Diaz

Thank you for joining us as we advocate for circumspect regulation, targeted solutions, and meaningful partnerships around the globe.

Thank you to our members who contributed:

Accenture	Government of Telangana	Proclivis
Bitfury	JP Morgan – Quorum	Procter & Gamble
BTG Pactual	Latham & Watkins	Ropes & Gray
Covington & Burling	New America – Blockchain	Salesforce
Diginex	Trust Accelerator	Shearman & Sterling
Everledger	Norton Rose Fulbright	Soramitsu
Evertas Risk Solutions	NYC Blockchain Center	Stephens & Johnson
EY	Odyssey	STHORM
Friorep	Orbs	Sullivan & Worcester
Genesis Global Trading	Power Ledger	University of Bahrain

- 1| For example, the Electronic Fund Transfer Act, 15 U.S.C. §§ 1693 et seq., and Regulation E, 12 C.F.R. Part 1005, prescribe requirements for electronic fund transfers, such as the use of ATM cards and other electronic access devices. These requirements would likewise apply to an electronic fund transfer process that leveraged the use of blockchain or another DLT.
- 2| See National Conference of State Legislators (NCSL), Blockchain 2019 Legislation (July 23, 2019).
- 3| Bills passed at least one house of the legislature in Michigan, California, and New York, and were enacted in Nevada and Illinois.
- 4| Bills were enacted in Connecticut, Florida, Nevada, New Jersey, New York, and Oregon.
- 5| Bills were enacted in Maryland and Rhode Island and passed the state House in Kansas.
- 6| See FinCEN, FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013).
- 7| See Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 9, 2018).
- 8| FinCEN, FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 9, 2019).
- 9| FATF, The FATF Recommendations (Updated June 2019), Interpretive Note to Recommendation 15.
- 10| Executive Order 13827, Taking Additional Steps to Address the Situation in Venezuela (Mar. 21, 2018).
- 11| See FinCEN, FIN-2018-A006, Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System (Oct. 11, 2018); U.S. Department of Treasury Press Release, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses (Dec. 21, 2018).
- 12| See CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets (Jan. 4, 2018).
- 13| See, e.g., CFTC v. Patrick K. McDonnell and Cabbagetechnology, Corp., Case No. 18-CV-0361 (E.D.N.Y. Mar. 6, 2018).
- 14| <https://cftc.gov/PressRoom/PressReleases/8053-19>
- 15| See CFTC Release Number 7697-18 *CFTC Issues First Pump-and-Dump Virtual Currency Customer Protection Advisory*
- 16| See CFTC Release Number 7869-19 *CFTC Divisions Announce Examination Priorities*
- 17| See, e.g., *In the Matter of TokenLot, LLC, Lenny Kugel, and Eli L. Lewitt*, SEC Docket No. 3-18739 (Sept. 11, 2018)
- 18| See, e.g., Self-Regulatory Organizations; NYSE Arca, Inc.; Order Disapproving a Proposed Rule Change to List and Trade the Shares of the ProShares Bitcoin ETF and the ProShares Short Bitcoin ETF, SEC Release No. 34-83904 (Aug. 22, 2018)
- 19| <https://www.sec.gov/litigation/investreport/34-81207.pdf>
- 20| <https://www.sec.gov/litigation/admin/2017/33-10445.pdf>
- 21| <https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission>
- 22| <https://www.loc.gov/item/usrep328293/>
- 23| <https://www.sec.gov/news/speech/speech-hinman-061418>
- 24| *Id.*
- 25| SEC, *Framework for "Investment Contract" Analysis of Digital Assets*
- 26| SEC, Response of the Div. of Corp. Fin. Re: Turnkey Jet, Inc. Letter dated Apr. 2, 2019
- 27| SEC, Response of the Div. of Corp. Fin. Re: Pocketful of Quarters, Inc. Letter dated July 25, 2019
- 28| Complaint, SEC v. Kik Interactive, Inc. (Kik), Case No. 1:19-cv-05244 S.D.N.Y. June 4, 2019
- 29| Complaint, SEC v. Telegram Group Inc. and Ton Issuer Inc. ECF Case 19 Civ. 9439 (PKC)
- 30| <https://www.sec.gov/news/press-release/2018-264>
- 31| <https://www.sec.gov/news/public-statement/digital-asset-securities-issuance-and-trading>
- 32| SEC, SEC Orders Blockchain Company to Pay \$24 Million Penalty for Unregistered ICO (September 30, 2019)
- 33| SEC, Issuer Settles Unregistered ICO Charges, Agrees to Return Funds and Register Tokens (December 18, 2019)
- 34| J SEC, *Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities* July 8, 2019
- 35| New York is the only state with a license available specifically for cryptocurrency providers. It has been particularly focused on cryptocurrency exchange's vulnerabilities to fraud. This concern was spurred by an inquiry launched by the New York Attorney General, which resulted in the Virtual Markets Integrity Initiative Report (Sept. 2018), which concluded in part that protections for customers on cryptocurrency exchanges are often limited.
- 36| See New York Department of Financial Services, Financial Services Superintendent Linda A. Lacewell Announces Grant of DFS Trust Charter to Enable Fidelity to Engage in New York's Growing Virtual Currency Marketplace (Nov. 19, 2019).
- 37| See, e.g., New York Department of Financial Services, Superintendent of Financial Services Linda A. Lacewell Announces Approval of First Gold-Backed Virtual Currency in New York State (Sep. 5, 2019).
- 38| https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/pr_guidance_regarding_listing_of_vc
- 39| Enrolled Act NO. 34, Original House Bill NO. HB0057, 65th Leg., Gen. Sess. (Wyo. 2019)
- 40| Enrolled Act NO. 47, Original House Bill NO. HB0074, 65th Leg., Gen. Sess. (Wyo. 2019)
- 41| Enrolled Act NO. 39, Original Senate File NO. SF0125, 65th Leg., Gen. Sess. (Wyo. 2019)
- 42| In March of 2019, the governor of Utah signed into effect a bill that clarified blockchain related terms and exempted a person who facilitates the creation, exchange, or sale of certain blockchain technology-related products from Title 7, Chapter 25, Money Transmitter Act
- 43| See IRS Rev. Rule 2019-24 and IRS Frequently Asked Questions on Virtual Currency Transactions
- 44| See OCC, Policy Statement on Financial Technology Companies' Eligibility to Apply for National Bank Charters (July 31, 2018); OCC, Considering Charter Applications From Financial Technology Companies (July 2018).
- 45| *Lacewell v. Office of the Comptroller of the Currency*, No. 18-cv-8377 (Oct 21, 2019)
- 46| *Blockchain 2019 Legislation*, National Conference of State Legislatures, <http://www.ncsl.org/research/financial-services-and-commerce/blockchain-2019-legislation.aspx> (Blockchain 2019 Legislation).
- 47| HB 1944 — *An Act Concerning Blockchain Technology; and for Other Purposes*, State of Arkansas General Assembly, <http://www.arkleg.state.ar.us/assembly/2019/2019R/Acts/Act1061.pdf>.

- 48] SB 373 — *An act to add and repeal Section 103526.7 of the Health and Safety Code*, relating to vital records, California Legislature, http://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=20190200SB373.
- 49] *HB 1247 - Concerning A Study by The Commissioner of Agriculture on The Potential Applications for Blockchain Technology in Agricultural Operations*, General Assembly of the State of Colorado, http://leg.colorado.gov/sites/default/files/documents/2019A/bills/2019a_1247_enr.pdf.
- 50] *SB 184 - Concerning a Grant of Authority to the Colorado Water Institute to Study Potential uses of Blockchain Technology*, General Assembly of the State of Colorado, http://leg.colorado.gov/sites/default/files/documents/2019A/bills/2019a_184_01.pdf.
- 51] *SB 1032 - An Act Requiring the Secretary of the Office of Policy and Management to Develop a Plan to Incorporate Blockchain Technology in the Administration of a State Function*, State of Connecticut Senate, <https://www.cga.ct.gov/2019/FC/pdf/2019SB-01032-R000384-FC.PDF>.
- 52] *HB 5417 - An Act Establishing a Task Force to Study the Use of Blockchain Technology to Manage Elector Information*, State of Connecticut House of Representatives, <https://www.cga.ct.gov/2019/FC/pdf/2019HB-05417-R000081-FC.PDF>.
- 53] *SB 1033 - An Act Concerning Noncompete Agreements in the Blockchain Technology Industry*, State of Connecticut Commerce Committee, <https://www.cga.ct.gov/2019/TOB/s/pdf/2019SB-01033-R00-SB.PDF>; *HB 6062 - An Act Establishing a Task Force to Study Online Voting*, State of Connecticut Public Safety and Security Committee, <https://www.cga.ct.gov/2019/TOB/h/pdf/2019HB-06062-R00-HB.PDF>; *HB 7310 - An Act Authorizing The Use Of Smart Contracts*, State of Connecticut Commerce Committee, <https://www.cga.ct.gov/2019/TOB/h/pdf/2019HB-07310-R00-HB.PDF>.
- 54] *SB 89 - An Act To Amend Chapter 17, Title 6 Of The Delaware Code Relating To The Creation, Regulation, Operation And Dissolution Of Domestic Limited Partnerships And The Registration And Regulation Of Foreign Limited Partnerships*, Delaware State Senate, <http://legis.delaware.gov/json/BillDetail/GenerateHtmlDocument?legislationId=47447&legislationTypeId=1&docTypeId=2&legislationName=SB89>; *SB 90 - An Act To Amend Chapter 15, Title 6 Of The Delaware Code Relating To The Creation, Regulation, Operation And Dissolution Of Domestic Partnerships And The Registration And Regulation Of Foreign Limited Liability Partnerships*, Delaware State Senate, <http://legis.delaware.gov/json/BillDetail/GenerateHtmlDocument?legislationId=47448&legislationTypeId=1&docTypeId=2&legislationName=SB90>; *SB 91 - An Act To Amend Chapter 18, Title 6 Of The Delaware Code Relating To The Creation, Regulation, Operation And Dissolution Of Domestic Limited Liability Companies And The Registration And Regulation Of Foreign Limited Liability Companies*, Delaware State Senate, <http://legis.delaware.gov/json/BillDetail/GenerateHtmlDocument?legislationId=47449&legislationTypeId=1&docTypeId=2&legislationName=SB91>.
- 55] *HB 735 - An act relating to blockchain technology; providing legislative findings; establishing the Florida Blockchain Task Force in the Department of Financial Services; providing for membership and duties of the task force; requiring the task force to submit a report to the Governor and the Legislature and make presentations; requiring the department to provide support staff and other assistance to the task force; providing for termination of the task force; providing an effective date*, Florida Senate, <http://www.flsenate.gov/Session/Bill/2019/735/BillText/c1/PDF> (proposing, if passed, to establish the Florida Blockchain Task Force in the Department of Financial Services)
- 56] *HB 1393*, Florida Senate, <http://www.flsenate.gov/Session/Bill/2019/1393/BillText/er/PDF>; *SB 1024*, Florida Senate, <http://www.flsenate.gov/Session/Bill/2019/1024/BillText/er/PDF>.
- 57] *HB 2540 - Blockchain Business Development Act*, State of Illinois General Assembly, <http://www.ilga.gov/legislation/101/HB/PDF/10100HB2540lv.pdf>; *HB 3575 - Blockchain Technology Act*, State of Illinois General Assembly, <http://www.ilga.gov/legislation/101/HB/PDF/10100HB3575lv.pdf>.
- 58] *SF 137 - An Act relating to electronic transactions by permitting the use of distributed ledger technology and smart contracts*, <https://www.legis.iowa.gov/docs/publications/LGI/88/SF137.pdf>.
- 59] *HB 2039*, Legislature of the State of Kansas, http://kslegislature.org/li/b2019_20/measures/documents/hb2039_enrolled.pdf (signed by the Governor); see also *HB 2105*, Legislature of the State of Kansas,
- 60] *HR 171*, Kentucky Legislature, https://apps.legislature.ky.gov/recorddocuments/bill/19RS/hr171/orig_bill.pdf.
- 61] *LD 909 - Resolve, Directing the Commissioner of Economic and Community Development to Establish a Blockchain Technology Working Group*, Maine Legislature, <http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=HP0673&item=1&snum=129>.
- 62] Blockchain 2019 Legislation; referring to *HB 1109*, State of Missouri Legislature, <https://house.mo.gov/billtracking/bills191/hrbills/pdf/2265H.011.pdf>.
- 63] AB 533, 2019 Leg., 80th Reg. Sess. (Nev. 2019).
- 64] SB 162, 2019 Leg., 80th Reg. Sess. (Nev. 2019); SB 163, 2019 Leg., 80th Reg. Sess. (Nev. 2019); SB 164, 2019 Leg., 80th Reg. Sess. (Nev. 2019).
- 65] Blockchain 2019 Legislation, referring to Nevada SB 488.
- 66] HB 470, Gen. Court, 166th Sess. (N.H. 2019).
- 67] SB 1194, 242nd Leg., Reg. Sess. (N.Y. 2019); SB 4562, 242nd Leg., Reg. Sess. (N.Y. 2019).
- 68] AB 2213, 242nd Leg., Reg. Sess. (N.Y. 2019).
- 69] SB 4142, 242nd Leg. (N.Y. 2019).
- 70] AB 1371, 242nd Leg., Reg. Sess. (N.Y. 2019).
- 71] AB 2239, 242nd Leg., Reg. Sess. (N.Y. 2019).
- 72] HB 1048, 66th Leg. Assemb., Reg. Sess. (N.D. 2019).
- 73] Blockchain 2019 Legislation, referring to North Dakota HCR 3004, Chapter 539.
- 74] Blockchain 2019 Legislation, referring to Oklahoma SB 700.
- 75] SB 843, 57th Leg., 1st Reg. Sess. (Okla. 2019).
- 76] HB. 2487, 80th Leg. Assemb., Reg. Sess. (Or. 2019).
- 77] HB 2179, 80th Leg. Assemb., Gen. Sess. (Or. 2019).
- 78] <https://www.dobs.pa.gov/Documents/Securities%20Resources/MTA%20Guidance%20for%20Virtual%20Currency%20Businesses.pdf>.
- 79] Caitlin Long, *What Do Wyoming's 13 New Blockchain Laws Mean?*, Forbes, Mar. 4, 2019, <https://www.forbes.com/sites/caitlinlong/2019/03/04/what-do-wyomings-new-blockchain-laws-mean/#3edd9f5fde> (last visited Jul. 23, 2019) (describing the highlights of Wyoming's new blockchain laws and stating "Wyoming has now enacted a total of 13 blockchain-enabling laws, making it the only US state to provide a comprehensive, welcoming legal framework that enables blockchain technology to flourish, both for individuals and companies. These laws enable innovation and creativity, and are meant to bring capital, jobs and revenue into Wyoming).
- 80] SF0125 — Digital assets-existing law, State of Wyoming Legislature, <https://www.wyoleg.gov/Legislation/2019/SF0125>.
- 81] See <https://ec.europa.eu/digital-single-market/en/blogposts/question-trust-eus-blockchain-challenge>.
- 82] *Ibid.*
- 83] See <https://inatba.org/organization/>.
- 84] See <https://ec.europa.eu/jrc/en/facts4efuture/blockchain-now-and-tomorrow>.
- 85] See <https://ec.europa.eu/digital-single-market/en/news/convergence-global-blockchain-congress>.
- 86] The EC launched the EU Blockchain Observatory in February 2018 with the purpose of mapping key initiatives, monitoring developments, and involving private stakeholders and public authorities in technical and regulatory discussions about the future of blockchain in the EU. For more information see <https://ec.europa.eu/digital-single-market/en/eu-blockchain-observatory-and-forum>.
- 87] See <https://www.eublockchainforum.eu/reports>.
- 88] See <https://www.eublockchainforum.eu/reports>.
- 89] See https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf?width=1024&height=800&frame=true.
- 90] The EC indicates that "Around EUR 200 million have already been allocated to blockchain related projects in H2020 with new opportunities for research and innovation coming up in the Work Programme 2020". See <https://ec.europa.eu/digital-single-market/en/investing-blockchain>.
- 91] See <https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1>.
- 92] *Ibid.*
- 93] See https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.
- 94] See <https://www.europarl.europa.eu/news/en/hearings2019/commission-hearings-2019/20190910STO60708/valdis-dom-brovskis-latvia>.
- 95] See <https://www.consilium.europa.eu/en/press/press-releases/2019/12/05/joint-statement-by-the-council-and-the-commission-on-stablecoins/>.
- 96] Articles L.211-3 to L.211-7 of the CMF, L. 223-12 to L.223-13 of the CMF and R. 211-9-7 of the CMF.
- 97] Articles L.552-1 to L.552-7 of the CMF, 711-1 to 715-2 of the General Regulation of the AMF (RGAMF) and AMF Instruction DOC-2019-06.
- 98] Articles L.54-10-1 to L.54-10-5 of the CMF and D.54-10-1 to D.54-10-1 to D.54-10-9 of the CMF.
- 99] Articles L.214-160 and L.214-154 of the CMF.
- 100] Cf. BaFin as of 28.04.2016 available at https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html
- 101] Cf. BaFin GZ: WA 51-Wp 7100-2019/0011 and IF 1-AZB 1505-2019/0003, available at https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/WA/dl_wa_merkblatt_ICOs.html
- 102] Cf. German finance ministry, available at https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Financial_markets/Articles/2019-09-18-Blockchain.html
- 103] FINMA, *Supplement to the guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)* (11 September 2019), available at <https://www.finma.ch/en/~media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/FinTech/wegleitung-stable-coins.pdf?la=en>
- 104] FINMA Guidance 02/2019 "Payments on the blockchain" (26 August 2019).
- 105] Daniel Haerberli, Stefan Osterhelt, and Alexander Wherlock, *Blockchain & Cryptocurrency Regulation 2020 | Switzerland*, Global Legal Insights, available at <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/switzerland>
- 106] *Ibid.*
- 107] Karanja, J. "How blockchain can help to tackle sub-Saharan Africa's challenges", (2018) https://www.ey.com/en_gl/digital/tackling-sub-saharan-africa-s-challenges-with-blockchain.
- 108] Kenyan WallStreet, (2018) "Kenya Govt Sets up Blockchain and Artificial Intelligence Taskforce", <https://kenyanwallstreet.com/kenya-govt-sets-blockchain-artificial-intelligence-taskforce/>.
- 109] *Ibid.*
- 110] "Blockchain and Cryptocurrency in Africa: A comparative summary of the reception and regulation of Blockchain and Cryptocurrency in Africa".
- 111] Darko, E. (2018) "Why Kenya is the Bedrock of Blockchain Technology in Africa", <https://icowatchlist.com/blog/kenya-bedrock-blockchain-technology-africa/>.
- 112] Khoza, F. (2016) "The Blockchain revolution and financial regulation in South Africa", <https://www.golegal.co.za/blockchain-revolution-financial-regulation-south-africa/>.
- 113] ICE3X.com (2018) "New Cryptocurrency Regulations coming to South Africa", <https://ice3x.co.za/crypto-policy/>.
- 114] Business Tech (2019) "Reserve Bank proposes stricter cryptocurrency regulations in South Africa in 2019", <https://businesstech.co.za/news/technology/293594/reserve-bank-proposes-stricter-cryptocurrency-regulations-for-south-africa-in-2019/>.
- 115] Issued by the National Treasury as a joint initiative with the South African Reserve Bank, the Financial Services Board (now the Financial Sector Conduct Authority), the South African Revenue Service and the Financial Intelligence Centre.
- 116] Geral, D., Tibane, B and Kern, K. (2019) "FinTech in South Africa: overview", <https://www.bowmanslaw.com/wp-content/uploads/2018/05/FinTech-in-South-Africa-overview.pdf>.
- 117] The South African Reserve Bank, "Policy Paper on Virtual Currencies", Section 3.2.3 [https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem\(NPS\)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20Final_02of2014.pdf](https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20Final_02of2014.pdf).
- 118] *Ibid.*, Section 4.3.5.2.
- 119] *Ibid.*, Section 2.1.
- 120] Itzikowitz, A and Meiring, I. (2018) "Blockchain & cryptocurrency regulation 2020: South Africa", <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/south-africa>
- 121] Vanmali, C. (2018) "Cryptocurrency transactions", <https://www.golegal.co.za/cryptocurrency-transactions/>.
- 122] See <https://www.arabianbusiness.com/bahrain-in-talks-with-sin-gapore-on-blockchain-pilot-665012.html>.
- 123] See <http://www.oc.gov.ma/portal/sites/default/files/actualites/communiqu%C3%A>.
- 124] See <http://www.sama.gov.sa/en-US/News/Pages/news29012019.aspx>.
- 125] See <https://www.sca.gov.au/en/regulations/drafts.aspx#page=1>.
- 126] See the FSRA's Guidance to Crypto Asset Activities in ADGM, <https://www.sca.gov.au/en/regulations/drafts.aspx#page=1>.
- 127] The definitions of the terms used in this article, as well as other blockchain and cryptocurrency industry-related terms, may be found at https://www.lw.com/admin/Upload/Documents/Book_of_Jargon_Cryptocurrency_Blockchain_Technology.pdf

- 128| For example, the European Central Bank estimates that the total value of stablecoins almost tripled from €1.5 billion in January 2018 to more than €4.3 billion in July 2019. It also estimates that there are over 50 stablecoin initiatives in existence, and in the first half of 2019, the average volume of stablecoin transactions was €13.5 billion per month.
- 129| Global stablecoins are generally understood to be those that may enable cross-border payments and have the ability to scale rapidly to create a global (or substantially international) footprint.
- 130| According to a recent study by the blockchain research group Blockdata, such stablecoins make up 95% of all active stablecoins. <https://download.blockdata.tech/blockdata-stablecoin-report-blockchain-technology.pdf>.
- 131| Tax compliance is approximately 93 percent with information reporting, but the IRS estimates that it is as low as 37 percent without information reporting or withholding. "Understanding The Tax Gap And Taxpayer Noncompliance," Testimony of The Honorable J. Russell George, Treasury Inspector General for Tax Administration before the House Ways & Means Committee, at 2 (May 9, 2019).
- 132| <http://www.ncsl.org/research/elections-and-campaigns/same-day-registration.aspx>
- 133| <https://www.vote.org/voter-registration-deadlines/>
- 134| <http://www.ncsl.org/research/elections-and-campaigns/electronic-or-online-voter-registration.aspx>
- 135| https://www.pewtrusts.org/~media/legacy/uploadedfiles/pcs_assets/2012/pewupgradingvoterregistrationpdf.pdf
- 136| <https://www.npr.org/2018/10/22/659591998/6-takeaways-from-georgias-use-it-or-lose-it-voter-purge-investigation>
- 137| <https://www.npr.org/2018/06/11/618870982/supreme-court-upholds-controversial-ohio-voter-purge-law>
- 138| <https://www.brennancenter.org/blog/voter-purge-rates-remain-high-analysis-finds>
- 139| <http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html>
- 140| <https://e-estonia.com/solutions/security-and-safety/ksi-block-chain/>
- 141| <https://e-estonia.com/solutions/e-identity/id-card>
- 142| <https://e-estonia.com/solutions/e-governance/i-voting/>
- 143| <https://www.transparency.org/cpi2018>
- 144| <https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=LT:UA:LV:EE>
- 145| <https://procivis.ch/2018/06/06/canton-of-schaffhausen-officially-launches-procivis-electronic-id-solution-following-a-successful-pilot-phase/>
- 146| <https://www.reuters.com/article/us-leone-kiva/san-francisco-crowdfunder-kiva-sets-up-sierra-leone-credit-data-base-idUSKCN1VB262>
- 147| <https://www.kiva.org/blog/kivas-next-frontier-kiva-protocol>
- 148| <https://id2020.org/digital-identity#approach>
- 149| <https://medium.com/id2020/welcome-the-city-of-austin-to-the-id2020-alliance-76b0e6e6776>
- 150| <https://www.brennancenter.org/blog/voter-purge-rates-remain-high-analysis-finds>
- 151| <https://history.house.gov/Institution/Election-Statistics/2016election/>
- 152| <https://www.fvap.gov/info/news/2018/9/12/dod-releases-biennial-study-of-us-voters-abroad>
- 153| <https://medium.com/mit-election-lab/insights-into-voting-wait-time-from-the-2016-elections-performance-index-6693576e9b99>
- 154| https://www.brennancenter.org/sites/default/files/analysis/Long_Voting_Lines_Explained.pdf
- 155| <https://www.azcentral.com/story/news/politics/elections/2016/03/22/live-arizona-primary-coverage-presidential-preference-election/82096726/>
- 156| <https://thehill.com/homenews/campaign/415275-average-wait-time-to-vote-tops-3-hours-in-atlanta-metro-area-watchdog-group>
- 157| <https://www.brennancenter.org/publication/election-day-long-lines-resource-allocation>
- 158| <http://www.dartmouth.edu/~herron/closingtimes.pdf>
- 159| <https://www.fvap.gov/uploads/FVAP/Reports/FVAP-2016-OCPA-FINAL-Report.pdf>
- 160| <https://www.yang2020.com/policies/modernize-voting/>
- 161| <https://www.justice.gov/crt/uniformed-and-overseas-citizens-absentee-voting-act#prov>
- 162| <https://blog.voatz.com/?p=721>
- 163| <https://www.cnn.com/2019/10/01/politics/fbi-hacking-attempt-alleged-mobile-voting-app-voatz/index.html>
- 164| <https://www.prnewswire.com/news-releases/mobile-voting-is-coming-to-local-oregon-elections-300939320.html>
- 165| <https://www.mos.ru/en/city/projects/blockchain-vyborny/>
- 166| <https://golovnev.org/papers/election.pdf>
- 167| <https://tjournal.ru/analysis/115536-elektronnoe-golosovanie-v-moskve-vygrali-kandidaty-ot-vlasti-v-oflayn-golosovanii-u-nih-net-takogo-perevesa>
- 168|
- 169| <https://www.technologyreview.com/s/611850/why-security-experts-hate-that-blockchain-voting-will-be-used-in-the-midterm-elections/>
- 170| <https://www.usvotefoundation.org/E2E-VIV>
- 171| https://www.usvotefoundation.org/sites/default/files/E2EVIV_full_report.pdf
- 172| <https://www.verifiedvoting.org/resources/post-election-audits/risk-limiting-audits/>
- 173| <https://www.vox.com/2018/11/6/18066350/midterm-elections-2018-vote-counting>
- 174| <https://www.dallasnews.com/news/2018/10/26/company-blames-texas-voters-problems-on-user-error-saying-its-machines-dont-flip-straight-ticket-ballots/>
- 175| <https://www.washingtonpost.com/nation/2019/08/28/mississippi-election-machine-changes-votes-video/>



DC LOCATION:

700 PENNSYLVANIA AVENUE SE
WASHINGTON, DC 20003

GENEVA LOCATION:

20 RUE DE-CANDOLLE
1205 GENEVA