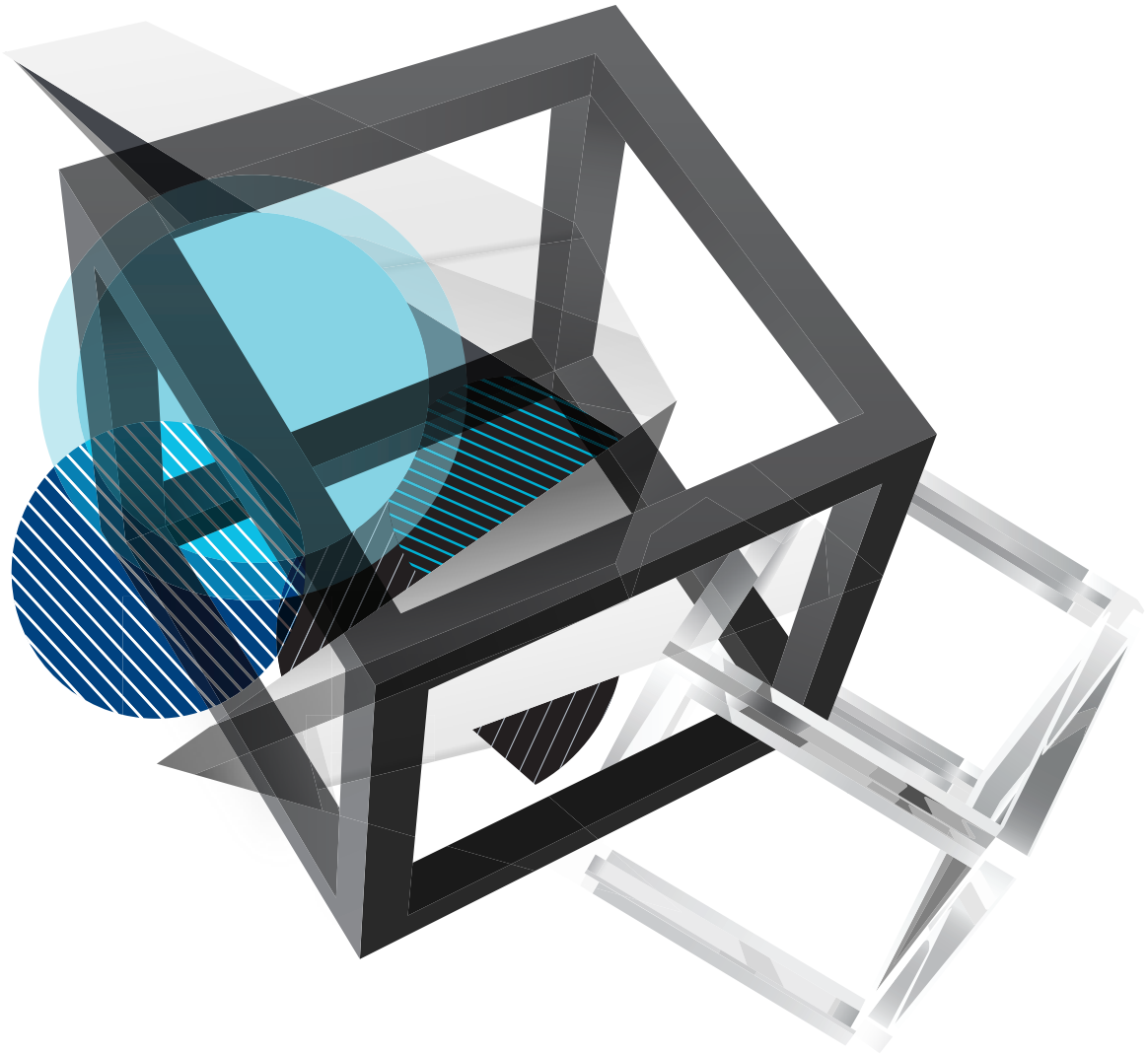
MARSH & McLENNAN COMPANIES

FireEye

CIRCLE

Crypto-Assets and Blockchain Technology

On the Brink of Legitimacy?



January 2019

Table of Contents

Executive Summary

It has been 10 years since the world was introduced to bitcoin and its underlying blockchain technology. Bitcoin has become a household name and has spawned hundreds of other crypto-assets. At its peak in January 2018, the total market cap of crypto-assets equaled one-tenth of the value of all the gold in the world.

Meanwhile, blockchain technology offers the potential to create new paradigms in virtually every industry, from financial services to health care, and to help solve intractable societal challenges like cybersecurity, privacy, and control of confidential data.

Yet, 2018 was a volatile, sometimes brutal, year for these linked innovations. Both are under the scrutiny that comes from high—and in some cases unrealistic—expectations. The price of bitcoin slumped more than 70 percent. And renowned experts, including the economist Nouriel Roubini, have denounced blockchain technology as "the most over hyped—and least useful—technology in human history."

Marsh & McLennan, FireEye, and Circle, each a leader in their respective industries, have collaborated to cut through the hype surrounding crypto-assets and blockchain technology. The goal of this white paper is simple—to frame three key challenges that must be overcome if the promise of these emerging technologies is to be achieved.

- Can a credible institutional market infrastructure be created for crypto-assets?
- Can governments coalesce around a common regulatory framework for this new asset class?
- Can blockchain technology prove itself as a secure network for the exchange of value at scale?

There is no better place to engage in this debate than at the World Economic Forum in Davos. Switzerland, long a global financial hub, has emerged as a clear leader in crypto-assets and blockchain technology. Just two months ago, the SIX Swiss Exchange authorized the first-ever exchange-traded crypto-asset product. The "Amun Crypto Basket Index" ETP invests its assets in Bitcoin, Ethereum, Ripple, Bitcoin Cash, and Litecoin, tracking the performance of the top five crypto-assets. Switzerland has also invested heavily in blockchain research and hosts the highly-regarded Crypto Valley Summit outside of Zurich.

We hope that this report helps you separate fact from fiction.

Peter Beshar
EVP, Marsh & McLennan

Kevin Mandia
CEO, FireEye

Jeremy Allaire
CEO, Circle

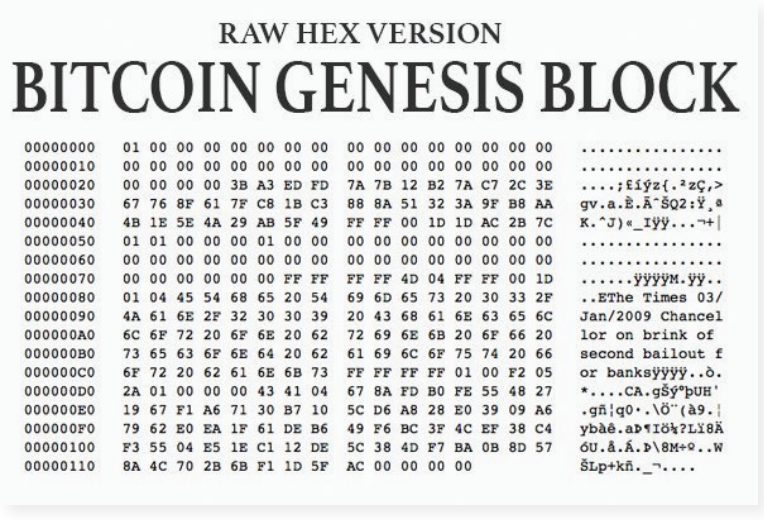
From the Depths of the Financial Crisis, the Birth of Bitcoin and Blockchain Technology

A decade ago, an anonymous person or group using the name "Satoshi Nakamoto" published a seminal nine-page paper titled: "Bitcoin: A Peer-to-Peer Electronic Cash System."

At the time, panic was engulfing the financial markets, and the global economy was convulsing. As asset prices plunged, central banks struggled to maintain public confidence in financial institutions, markets, and currencies. Nakamoto proposed a new digital currency that would be created and traded solely among users without explicit government oversight.

Bitcoin promised something radically different: an entirely new digital money ecosystem that was cryptographically secured, decentralized, and, perhaps most important, did not involve any central bank or government. Rather than top-down and "command and control," it was bottom-up and peer-to-peer. It suited the times—with a nascent populism emerging from widespread distrust of financial institutions and governments.

In January 2009, Nakamoto created the first 50 units of Bitcoin, stamping them with a message that served as a statement of purpose: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." The reference was to *The Times'* headline that day about the British government's moves to prop up wobbly financial institutions.



RAW HEX VERSION

BITCOIN GENESIS BLOCK

```
00000000  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E  ....;£íýz{.²zÇ,>
00000030  67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA  gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040  4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C  K.^J)«_Iÿÿ...¬+|
00000050  01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D  ......ÿÿÿÿM.ÿÿ..
00000080  01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F  ..EThe Times 03/
00000090  4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C  Jan/2009 Chancel
000000A0  6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20  lor on brink of
000000B0  73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66  second bailout f
000000C0  6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05  or banksÿÿÿÿ..ò.
000000D0  2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27  *....CA.gŠý°þUH'
000000E0  19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6  .gñ¦q0·.\Ö¨(à9.¦
000000F0  79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4  ybàê.aÞ¶Iö¼?LÏ8Ä
00000100  F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57  óU.å.Á.Þ\8M÷º..W
00000110  8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00           ŠLp+kñ._¬....
```

The "Wild West" Years of Bitcoin

At first, bitcoin attracted a sometimes motley assortment of early internet architects, anarchists, "cypherpunks," futurists, encryption experts, government skeptics, and later, criminals. But over time the technology that drove bitcoin, known as blockchain, proved to be remarkably durable. With that foundation, the initial adopters began to give way to a broader and more traditional population of users.

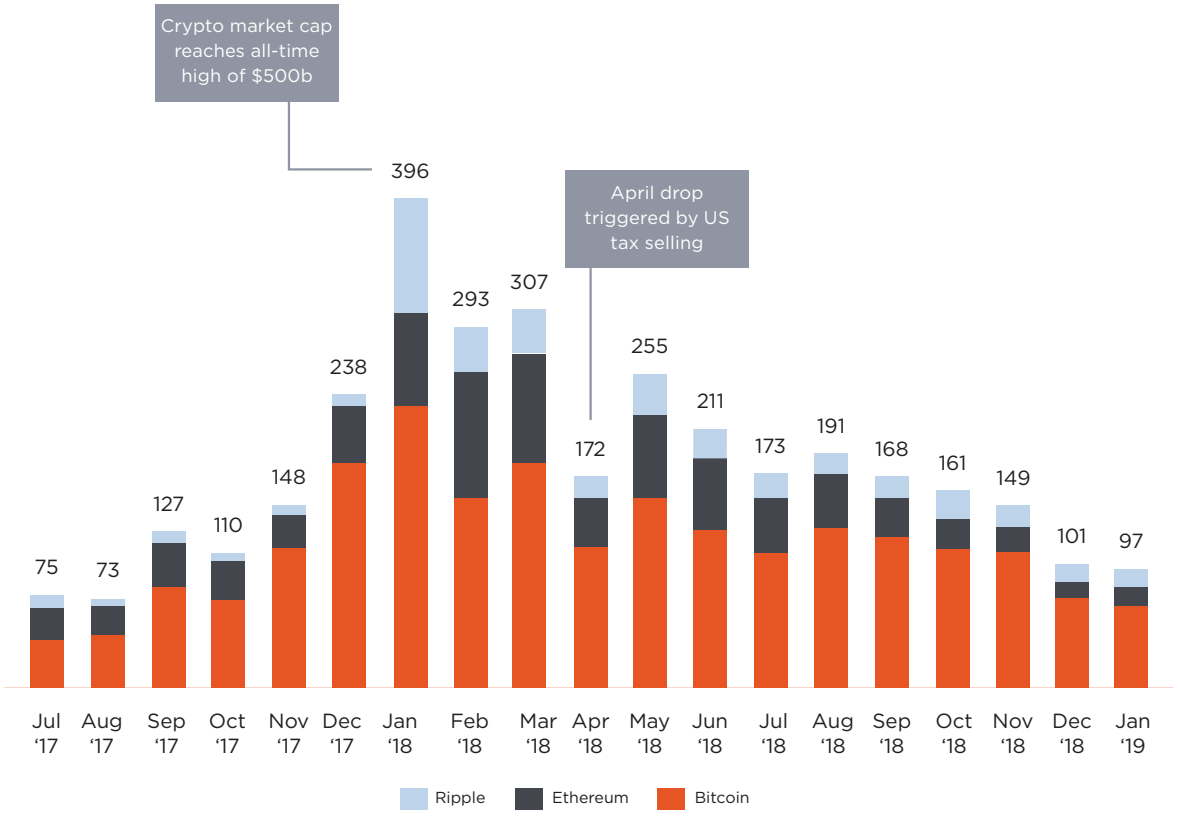
Early thefts and scandals could have precipitated the end of bitcoin and the hundreds of other crypto-assets that sprung up since the Nakamoto paper. But an interesting thing happened; users didn't flee, and while governments ramped up their scrutiny of crypto-assets and the exchanges on which they are traded, most governments didn't try to regulate them out of existence. Big-name venture capitalists began to enter the space, stamping their imprimatur on markets once dominated by hobbyists.

Retail Investors Get Ahead of Institutions

In a historical anomaly, retail investors embraced crypto-assets long before financial institutions. At its peak in January 2018, the total market cap of all crypto-assets equaled a tenth of the value of all gold in the world—an extraordinary statistic for a "currency" conceived less than a decade before. Crypto-assets have created great wealth for early adopters and delivered sweeping losses to many newer holders who purchased assets in the last year.

These market gyrations have challenged senior policymakers, executives, and institutions to understand the reasons for crypto-assets' global traction and the technology that enables decentralized transactions.

Market Cap of the Top Three Crypto-Assets (US $B)



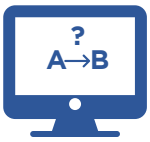
Source: MMC analysis, CoinMarketCap.com

Blockchain—Back Office IT or Trusted Command Center?

Blockchain became known as the technology underpinning bitcoin: a combination of existing peer-to-peer networking, asymmetric cryptography, and cryptographic hashing. While Nakamoto's white paper is replete with diagrams and mathematical formulae explaining the process for securing digital transactions, the concept behind blockchain technology is simple and powerful. The blockchain is a digital platform that records and verifies transactions in a public and secure manner. It allows untrusting parties to reach agreement, or consensus, without relying on a centralized authority.

"Blocks" of transactions, each one time-stamped with a unique code, are built on top of each other. This peer-to-peer structure eliminates the need for, and the vulnerability of, a central administrator. In testimony before the US Senate Banking Committee in October 2018, Coin Center Director of Research Peter Van Valkenburgh argued: "In general, decentralization helps ensure user sovereignty, interoperability, longevity, fidelity, availability, privacy, and political neutrality." Indeed, a banner at the entrance of the headquarters of ConsenSys, a leading blockchain firm, declares: "Welcome to the Decentralized Future."

How are Blockchain Transactions Executed?



1. CREATE
A transaction is created sending an amount of a crypto-asset to a receiver's address.

2. SIGN
The transaction is signed using the private key of the sender.

3. BROADCAST
The transaction is broadcasted to other nodes on the network.

4. DISTRIBUTE
If the transaction is considered valid by those nodes, it gets forwarded until all nodes in the network have heard about it.

5. APPEND
A miner includes the transaction in a block with other waiting transactions. For this work, the miner is paid a fee.

6. CONFIRM
After the transaction is several blocks deep in the chain, the transaction can be considered finalized.

In an era when data is king, virtually every industry and institution could potentially benefit from blockchain applications. This explains the billions of dollars that have been invested to date by financial institutions, health care conglomerates and scores of other organizations to explore its promise. Moreover, blockchain technology could help to solve intractable societal challenges such as securing the process of voting in elections, improving the distribution of humanitarian aid to refugees, and tracking the provenance of raw materials in complex supply chains.

"**74%** of large organizations see a ***'compelling blockchain use case'***"

Deloitte 2018

"**8%** of CIOs were in ***'short-term planning or active experimentation with blockchain'***"

Gartner 2018

While the promise is vast, the actual uses of blockchain technology in the market are surprisingly few. Many critics argue that there are few applications for blockchain that cannot be accomplished more simply with a traditional database. This is the crucial disconnect between commentators like Nouriel Roubini, who pans digital assets, and innovators who believe that blockchain technology and digital assets will be as important as the internet itself. The disconnect fuels polarizing narratives and begs to be reconciled.

A PRIMER: BLOCKCHAIN BASICS

What is blockchain technology?

A blockchain is a continuously growing list of electronic data records, or blocks that are sequentially linked using cryptography. Blockchain is the underlying technology of most cryptocurrencies. A blockchain is a specific type of distributed ledger technology and a method of organizing data in aggregated, ordered blocks that are chained together and signed by a cryptographic hash function. Distributed ledger technology eliminates the need for a central, trusted counterparty as a means of verification, and blockchain technology adds the support of consensus through various algorithims such as proof of work (POW or mining), proof of stake (POS), and others.

What is on a block?

Most blocks contain a timestamp, a link to the previous block, and transaction data that can include amount, payee, payer, and other types of data.

How does crypto mining occur on the blockchain?

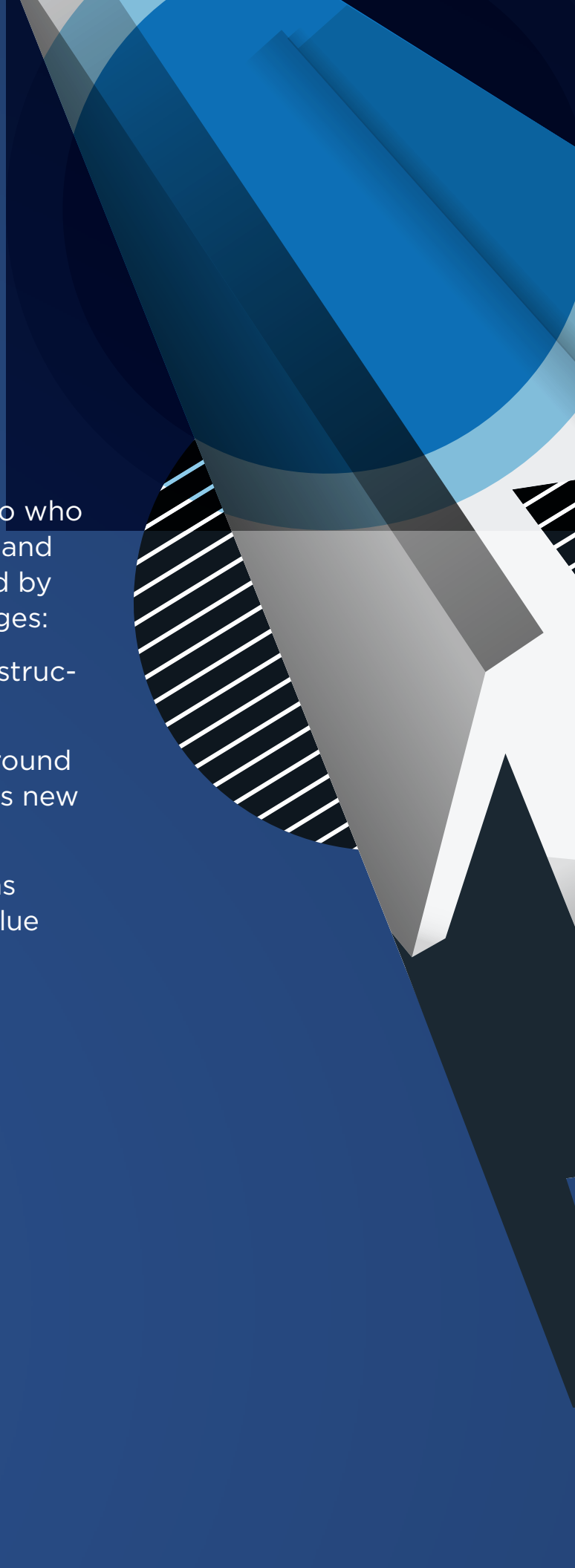
Some nodes of the network, called "miners," perform a specific function in implementing complex consensus algorithims, typically on computationally sophisticated and expensive hardware, and are rewarded for their work in coins or tokens and transaction fees.

What are private and public keys?

In the case of bitcoin, a private key is a number that can authorize transactions. In asymmetric cryptography, there are two related keys, or a key pair, consisting of a public key, which is made freely available on the internet, and a private key, which is kept secret. Public keys are derived from their corresponding private keys, but cannot be reverse engineered thanks to strong cryptography. Private keys are needed for any transaction to occur.

What is a digital wallet?

Digital wallets are software or hardware devices that enable users to send, receive, and securely store digital assets. All digital wallets have associated private keys, public keys, and corresponding addresses.



On the Brink of Legitimacy?

In our judgment, the ultimate answer as to who is right about the future of crypto-assets and blockchain technology will be determined by the ability to overcome three key challenges:

- Can a credible institutional market infrastructure be created for crypto-assets?
- Can government authorities coalesce around a common regulatory framework for this new asset class?
- Can blockchain technology prove itself as a secure network for the exchange of value at scale?

1 Can a Credible Institutional Market Infrastructure be Created for Crypto-Assets?

From the initial vision articulated by Nakamoto 10 years ago, remarkable progress has been made in legitimizing bitcoin as a digital currency. By the estimates of some experts, more than $1 trillion in bitcoin transactions were cleared in 2018. Crypto exchanges and custodians like Bittrex, Circle, Coinbase, Binance, Xapo, and BitGo have all played important roles in the development of this volatile, fledgling market. And there are early indicators of more mainstream adoption of bitcoin. For example, large multinational companies such as Bloomberg, Dish Network, Expedia, Square, and Tesla have begun to accept bitcoin as a form of payment.

Several types of investors have been instrumental in driving the growth of crypto-assets:

- **Alternative Investors.** Family offices, professional traders, small hedge funds, and venture capital firms pursue a range of trading strategies related to crypto-assets. Investment philosophies include a belief in crypto-assets as a new asset class, a desire for early access, and an appetite for diversification.
- **Government Skeptics.** Many people distrust government-controlled currencies for ideological reasons, especially after the global financial crisis. Some believe conventional currencies controlled by central banks give governments too much control over the fortunes of private citizens or are skeptical of government in general. Others believe governments and central banks will mismanage the economy and particularly fear hyperinflation.
- **Privacy Seekers.** Many individuals place a high value on the privacy possible with crypto-assets. Though most privacy seekers are not criminals, heightened privacy features present law enforcement concerns. At the same time, it is important to note that most blockchain transactions are pseudonymous but not private. Blockchains provide public records of transactions without exposing identities, so while they provide a measure of privacy protection, transactions leave digital fingerprints. Dedicated “privacy coins” such as Zcash and Monero, which provide additional privacy features, can present verification challenges.
- **Speculators.** Speculative traders are attracted to the volatility of crypto-asset prices. This group focuses on maximizing short-term trading gains with minimal interest in the long-term performance of crypto-assets. Online communities of crypto-traders have developed around a range of speculative trading strategies.

The Road Ahead

To attract institutional investors, assure regulatory authorities, and fully achieve the promise of these innovations, a credible institutional market infrastructure is necessary. There is no small irony in the fact that bitcoin, conceived in an era of distrust about financial institutions and governments, now arguably needs traditional structures to cement its status and realize its potential.

To be sure, crypto-assets will likely endure without the involvement of large financial institutions. Sufficient demand exists among dedicated user groups around the world and the underlying technology has proven to be resilient without large financial players.

The support and capabilities of existing financial systems, however, will likely be necessary to convert crypto-assets into a viable, alternative asset class and blockchain into one of the principal platforms for transferring value across the internet.

Traditional financial institutions and international financial organizations, including central banks, are starting to recognize that crypto-assets could be part of the digitization of a wide range of assets and financial instruments.

Recent Investments in Crypto Market Infrastructure

Modern finance relies on a complex web of institutions—including exchanges, clearinghouses, broker-dealers, custodians, transfer agents, and the like—to effect transactions and keep track of ownership. Each is regulated by a government agency or self-regulatory organization (SRO) to promote investor protection, sound markets, good governance, and transparency.

With crypto-assets, consumers may take custody of assets themselves and execute transfers as easily as sending an email or they may use third-party exchanges to store assets and make trades. The fact that all such transfers of value are immutably recorded on a public blockchain could make some functions of traditional financial institutions unnecessary or redundant. The new paradigm shifts or eliminates some of the regulatory touchpoints that government agencies or SROs have in traditional financial transactions.

Investments by Large Financial Institutions

Several global financial institutions are taking the lead. After four years of research and development, Fidelity Investments announced in October 2018 that it was creating a digital-asset brokerage and custody business. Fidelity's announcement came just months after Nomura formed a joint venture with technology company Ledger and investment firm Global Advisors for crypto-asset custody.

Endowments, sovereign wealth funds, and pension plans are taking note. Indeed, the leaders of Yale University's endowment, heralded for their investment prowess, recently announced investments in two crypto-asset funds.

Investments by Large Technology Companies

A turn in a wholly different direction may also be on the horizon. Building on the lessons from online payments, large technology players could reshape financial services by using crypto-assets or digital assets more broadly. Just before year end, Samsung announced that it is developing a crypto-asset wallet app for the Galaxy S10 phone. Microsoft has had a blockchain as a service business for the last three years and Amazon Web Services unveiled blockchain services late last year.

A fascinating question is how and when native startups and trading platforms that have brought bitcoin and blockchain technology to this point will partner with large financial institutions, tech companies, and traditional exchanges.

The Beginnings of Institutional-Grade Financial Instruments

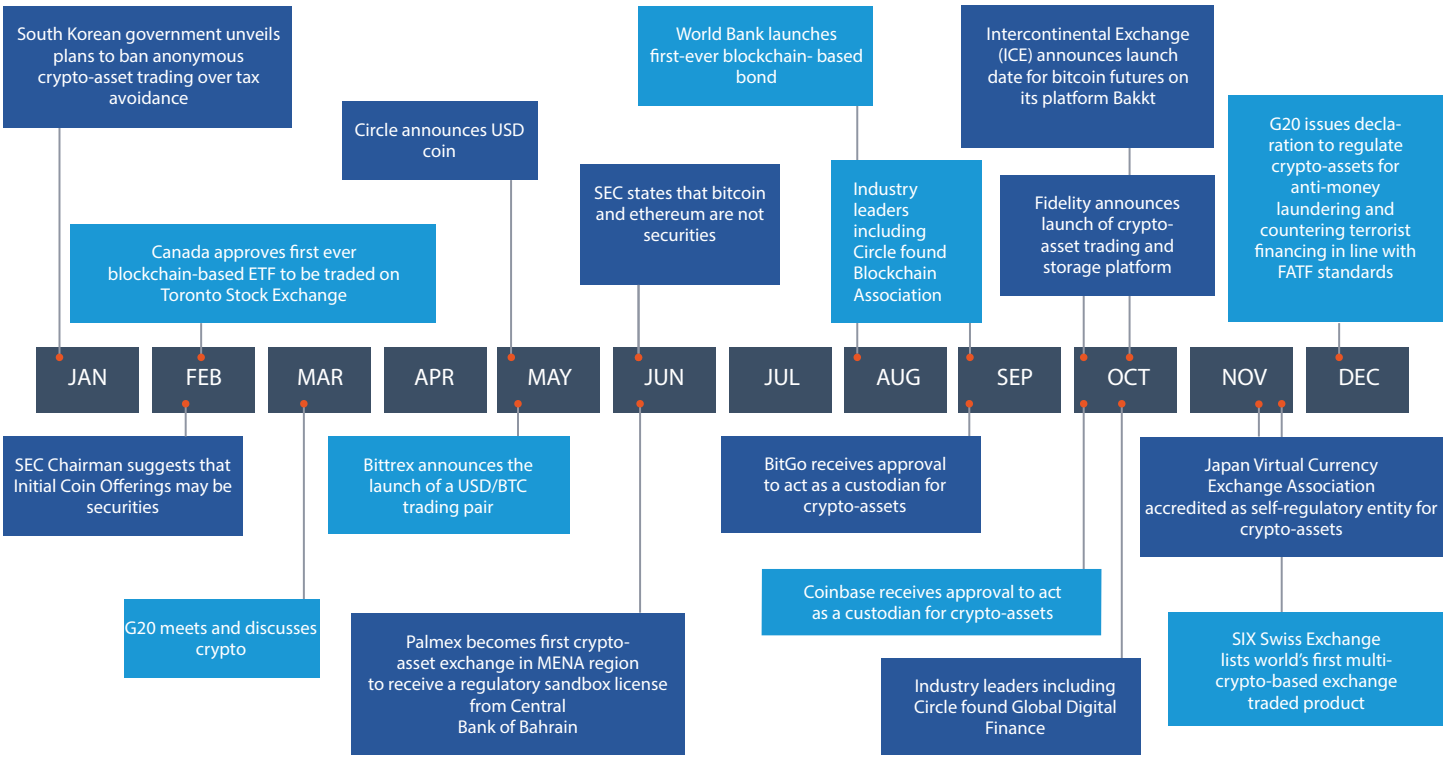
Institutional financial instruments for crypto-assets are beginning to take shape. Back in November 2017, the Chicago Mercantile Exchange (CME) announced that it was creating the first-ever futures contract for trading crypto-assets. The price of bitcoin surged on the news. The CME and the Chicago Board Option Exchanges began to trade derivative contracts in crypto assets that, importantly, could be settled in cash—meaning that investors would receive cash rather than bitcoin when the futures contract ends.

In late 2018, the Intercontinental Exchange (ICE), the owner of the New York Stock Exchange, announced that it was in active discussions with the Commodity and Futures Trading Commission (CFTC) regarding the launch of physically settled bitcoin futures. Trades on this platform, dubbed Bakkt ("backed"), would be cleared and settled with physically-delivered bitcoin in an ICE "warehouse." In other words, ICE would take physical possession of bitcoins. This potential game changer requires an exemption or waiver from the CFTC. Although current CFTC regulations allow ICE to hold collateral only in the form of cash, securities, or commodities—not crypto-assets—partners and investors have poured $182 million into Bakkt.

Meanwhile in Europe, Germany's second-largest stock exchange, Boerse Stuttgart Group, announced plans to launch an end-to-end crypto-asset platform in the first half of 2019 that will serve as a trading venue, ICO platform and custody service. The SIX Swiss Exchange also decided in November 2018 to approve the first-ever crypto-asset Exchange-Traded Product (ETP).

Looking at traditional trading infrastructure, in October, the Depository Trust & Clearing Corporation (DTCC) completed a study showing that distributed ledger technology is capable of supporting average daily trading volumes in the US equity markets of more than 100 million trades per day. HSBC announced that they used blockchain technology to settle $250B in forex trades in 2018.

2018: Notable Developments



2 Can Government Authorities Coalesce Around a Common Regulatory Framework for this New Asset Class?

It is not easy for crypto-asset regulators. The market is dynamic and cross-border. The technology is novel and rapidly evolving. The potential for fraud is all too real.

Globally, regulators are struggling to address the fact that crypto-assets cross the traditional boundaries of currencies, commodities, and securities.

Inconsistent Messages in the US?

Within the US, the approaches taken by the two principal federal regulators—the CFTC and the Securities and Exchange Commission (SEC)—in regulating crypto-assets have been markedly different. At a recent speech to the Crypto Valley Summit in Switzerland, one SEC Commissioner, Hester Peirce, stated that the United States was "sending mixed messages":

> "Our sister regulator, the Commodity and Futures Trading Commission, has allowed the development of crypto-derivatives markets, but the SEC so far has not approved any application to list an exchange-traded product based on cryptocurrencies or crypto-derivatives trade on US exchanges."
>
> **Hester Peirce**
> SEC Commissioner

If that was not complicated enough, the SEC determined that bitcoin and ether are not securities, but suggested that initial coin offerings (ICOs) of other crypto-assets may be considered securities. In June 2018, the Director of the Division of Corporate Finance at the SEC, William Hinman, stated: "within the Ethereum network, and its decentralized structure, current offers and sales of Ether are not securities transactions." His principal justification was that the two largest platforms for crypto-assets—bitcoin and ether—are sufficiently decentralized as to be outside the realm of traditional securities exchanges. Meanwhile, the SEC has brought securities enforcement actions against multiple crypto-asset firms involved in initial coin offerings.

Mixed Messages Elsewhere in the World

If the messages sometimes seem confusing within the US, it gets even more complicated internationally. In September 2017, the Chinese government announced a comprehensive ban on the purchase or sale of any crypto-asset in China. The Chinese even banned hotels from hosting events on cryptocurrencies. Yet, even there, the message is mixed. For example, the Chinese allow the mining of bitcoin, described by experts as the backbone of the bitcoin network. Indeed, half of all bitcoin mining in the world occurs in China.

By contrast, Australia has recognized crypto-assets as a means of payment and as an asset class. In Japan, the government recently authorized a self-regulatory body for crypto exchanges—the Japanese Virtual Currency Exchange Association—to create and enforce rules for trading platforms. The French government has introduced policies to support initial coin offerings, and the Swiss Federal Council released a report outlining changes to existing law "so that Switzerland can establish itself and evolve as a leading, innovative, and sustainable location for fintech and blockchain technology companies."

Finding a Place on Global Agendas

Recognizing the need for joint solutions, G20 leaders have convened a work stream on crypto-assets, as have other global bodies such as the Financial Stability Board, the International Organization of Securities Commissions, the Financial Action Task Force (FATF), and the Organization for Economic Cooperation and Development (OECD).

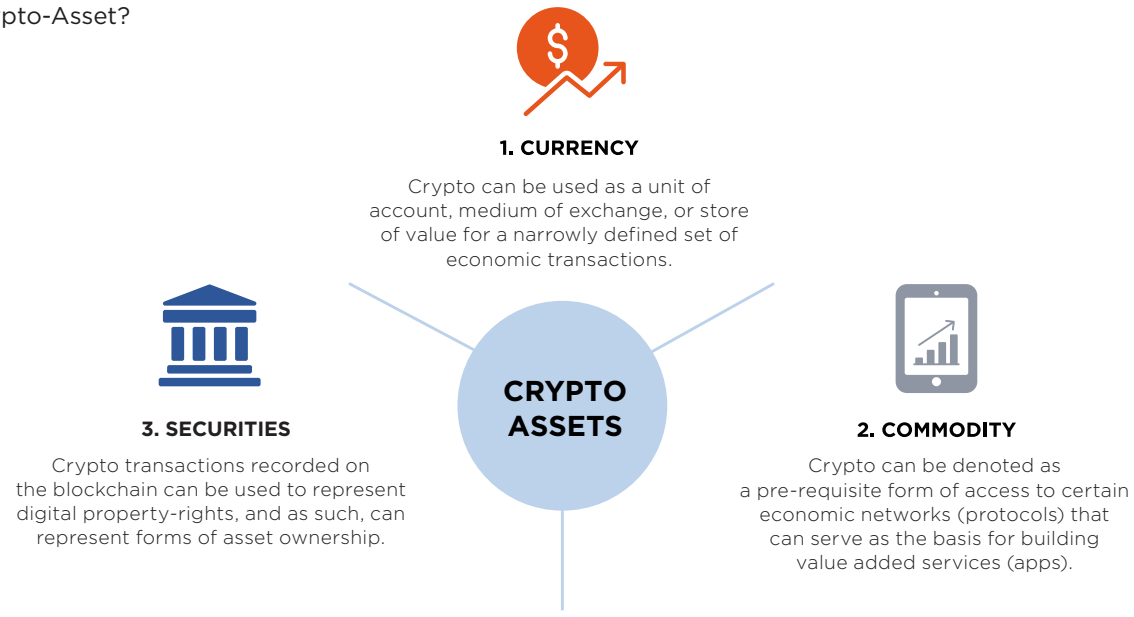
Regulatory "Sandboxes"

A number of regulators are experimenting with an interim step dubbed a "regulatory sandbox." A "sandbox" lets industry participants test new technologies in a limited live environment without a full-scale roll-out subject to the full litany of regulatory requirements.

The United Kingdom's Financial Conduct Authority (FCA), in collaboration with 11 financial regulators and related organizations, announced the creation of the Global Financial Innovation Network (GFIN). This formal collaboration grew out of the FCA's earlier proposal to form a global sandbox. Hong Kong, Abu Dhabi, Kuwait, Kenya, and Bermuda, along with Arizona and Ohio and the US Consumer Financial Protection Bureau, each have sandbox initiatives, but they vary in size, scope, and objectives.

While this approach can provide short-term solutions, market participants are naturally looking for longer-term regulatory clarity and predictability.

What is a Crypto-Asset?



A Call for Regulatory Clarity

We identify four ways to promote clarity and foster legitimacy amidst the complexity of crypto-asset and blockchain operating environments. We make two recommendations for regulatory authorities and two for market participants.

For Regulators

- ***Flex existing regulatory regimes while recognizing that some new rules may be needed for crypto-assets.*** Debates are underway over the extent that existing regulations apply to this new technology. We recommend a flexible, principles-based approach to regulation that promotes innovation, protects investors, safeguards market integrity, and penalizes any illicit use of crypto-asset infrastructure. Regulating by function will likely work better than treating crypto-assets as a single category. Early in 2019, the European Securities and Markets Authority (ESMA) acknowledged that some aspects of the Financial Instruments Directive (MiFID II) apply to crypto-assets but that areas of the regulation may require additional interpretation or reconsideration specific to crypto-assets.
- ***Pursue multi-jurisdictional consensus around a set of best practices.*** The decentralized nature of crypto-assets can make it hard to point to a single responsible party to be regulated, or even identify a primary regulator. Rather than seeking to enforce artificial territorial rules in a largely borderless market, regulators should explore the feasibility of establishing protocols and standards for best practices across jurisdictions. For example, the International Organization for Standards (ISO) is currently working on standards related to governance; security, privacy and identity, interoperability of blockchain systems, and smart contracts.

For Industry Participants

- ***Engage with regulators to help them understand the underlying technology and to dispel myths.*** Regulators and industry participants should routinely interact to improve the overall understanding of the technology and respond to legitimate concerns related to investor protections and market integrity. In the US, the Blockchain Association—founded by Circle, Coinbase, and others—is the blockchain industry's first association dedicated to engaging with the US government.
- ***Prioritize adoption and enforcement of Know Your Customer and Anti-Money Laundering Protections.*** Industry participants must rigorously ensure compliance with "know your customer" (KYC), anti-money laundering (AML), and combating the financing of terrorism (CFT) rules that apply to traditional financial institutions. With the potential for fraud, money laundering, and terrorist financing, confidence in crypto-assets can grow only if industry participants make robust investments in compliance. There is no substitute for compliance.

3 Can Blockchain Technology Prove Itself as a Secure Network for the Exchange of Value at Scale?

Security remains one of the most widely misunderstood aspects of crypto-asset risks and blockchain technology. The confusion occurs because blockchain is a protocol that seeks to elevate the security and assurance of data, but multiple users have lost their crypto-assets from breaches and intrusions. For blockchain technology to expand to multiple uses, and secure the transmission of value at scale, users must practice sound cyber risk management.

To date, most blockchain cyber-attacks have not breached the blockchain technologies themselves. The high-profile breaches, particularly at crypto-asset exchanges, have occurred in large part due to poor operational controls relating to the storage of private keys. The rapid global growth of crypto-assets caught a number of early exchanges by surprise, and security controls fell behind.

TOP FIVE EXCHANGE HACKS

Exchange	Date	Amount	Token stolen
Mt. Gox	March 2014	$450,000,000	BTC
Bitfinex	August 2016	$72,000,000	BTC
Nicehash	December 2017	$60,000,000	BTC
Coincheck	January 2018	$534,800,000	NEM
BitGrail	March 2018	$195,000,000	NANO

Source: Circle Research, available at: https://www.circle.com/en/research/decentralized-exchanges

Nascent Standards and Historic Security Breaches

Notwithstanding some of the security advantages of blockchain technology, cyber criminals and other adversaries have exploited poor cyber risk management practices across the decentralized system. Attacks have focused largely on cryptocurrency exchanges, wallet providers, and poorly-written smart contracts. In many cases, perpetrators have taken advantage of human weaknesses ranging from coding errors to poor cyber hygiene as weak points in the system.

One of the earliest and most damaging security incidents involved Mt. Gox—a bitcoin exchange set up in Tokyo in 2010. By 2013, Mt. Gox was handling 70 percent of all bitcoin trades worldwide. In February 2014, however, Mt. Gox announced that 850,000 bitcoins, valued at the time at $450 million, were missing. Though 200,000 bitcoins were subsequently "found," the exchange was forced to file for bankruptcy and halt operations. A bug in the exchange's system, that went unidentified for years, allegedly enabled this compromise.

In the wake of the well-publicized compromise of the Decentralized Autonomous Organization (DAO) smart contract, the targeting of a South Korean cryptocurrency exchange by North Korean actors, and other successful attacks, regulators, and industry participants have naturally begun to scrutinize the control environments at exchanges and wallet providers. Earlier this month, the SEC announced that a key priority for its Office of Compliance Inspections and Examination (OCIE) in 2019 will be inspections of the control environment and storage practices at crypto-asset firms.

Private Access Keys

Perhaps the single most important risk to blockchain security is private key management. Access keys, also known as private keys, are long numbers that grant access to specific digital assets. In addition to providing trading services, diversified trading enterprises like Circle, Coinbase, Bittrex, and BitGo can manage private keys for their customers. This shifts the burden of securing the private keys from users to the exchange or wallet provider, though institutions and individuals can elect to self-custody crypto-assets. As crypto-asset market infrastructure grows, regulators could require dedicated third-party custodians to store private keys for asset amounts above a certain threshold. At companies like KN0X, private keys are separated into "shards" and placed in physical security boxes to minimize the chances of a breach.

An array of digital wallet offerings, involving both software and hardware, enable users to send, receive, and securely store digital assets. Maintaining the confidentiality, integrity, and availability of private keys requires fairly robust controls. A number of user-controlled software wallet solutions store the access keys in a wallet file on a user's hard drive. If located in a well-known directory, these files can be an ideal target for crypto-asset malware.

FireEye has observed myriad malware families—traditionally aimed at stealing banking credentials—that incorporate the ability to target cryptocurrency wallets and online services. Developers have identified 30 common vulnerabilities and exposures (CVEs) since at least 2010, many of which could have caused denial of service attacks on the network, exposure of user information, degradation of transaction integrity, or theft of funds.

Example of Ethereum Public and Private Keys

Private key:
`99228c09a1320a7c7e43c290bla8e032b4c4c2f4b91c97ee3a2cb99308943059`

Public key:
`e736055153ae191a7a782e07cd3389bbfe154621fb79bbe3eb5ab72ddc491299`
`2f87d629a4d10510a37e1ddd02d6918bbd00b0f0de2f7bd0cda280e4f15471e9`

EVOLVING CYBER-ATTACKS

Ransomware, "Cryptojacking," and "51% Attacks"

Along with the theft of crypto-assets, the authors have observed multiple types of cyber-attacks involving the blockchain and crypto-assets including ransomware, "cryptojacking," and 51% attacks.

A long-standing security issue, ransomware infects and encrypts a target system, preventing its usage until a ransom, typically paid in a cryptocurrency like bitcoin, is paid by the victim.

A stealthier security risk is "crypto-jacking" or deploying mining software that silently utilizes a company's system processing power in the background, often unbeknownst to the user.

A 51% attack occurs when a miner or group of miners is able to amass a majority of a blockchain's hashing power, thereby allowing the perpetrator to rearrange transactions and "double spend" coins. Once a theoretical concept, this type of attack has led to the theft of crypto-assets.

While blockchain technology offers the promise of enhanced security, it also presents its own challenges. Greater responsibility for security is put into the hands of users to properly secure and store their keys, particularly if they are holding assets on behalf of others. With appropriate security practices that are audited and then validated by experts, institutional-grade security can be achieved for crypto-assets and future digital versions of financial instruments.

Decentralized Security Paradigms

While most blockchain security challenges can be addressed through existing best practices in cyber-security, linking distinct institutions and parties across complex financial systems through distributed networks creates several new cyber-security challenges.

To maintain strong network security, the roles and responsibilities of each type of participant in a blockchain network or exchange must be clearly defined and enforced, and the cybersecurity risks posed by each type of participant must be identified and managed. This is a tall order.

Blockchain development teams need to understand the full range of potential threats that arise from participating institutions interoperating with third parties, and better architect secure platforms that interface with these protocols.

Executive management teams working with blockchain development teams should institute the following controls:

- Assess and anticipate threats resulting from interoperability.
- Utilize threat intelligence to anticipate changes in risk.
- Conduct penetration testing using various attack scenarios and vectors.
- Document the development process.
- Obtain independent audits of the design and development process.

Developers should also incorporate the principles of the Systems Development Life Cycle (SDLC) or security-by-design practices and internalize those principles into the institutional or corporate culture.

Digital Banking Evolutions

Around the world, both financial institutions and central banks are searching for the most secure and efficient ways to transact online. Blockchain technology has the potential to automate and replace paper-based transaction verification in complex, multi-party networks at scale. Hundreds of use case evaluations are underway.

After conducting 44 proof of concept initiatives, the Dutch banking group ING declared in late 2018 that blockchain pilots and their expanded decentralized networks are outperforming traditional, centralized models. One of the many pilots run by ING is Vakt, a consortium of large energy companies, multi-national banks, and traders, formed to provide physical post-trade processing for commodities. Vakt is based on Quorum, JPMorgan's enterprise-focused blockchain, and intends to be linked to the Ethereum-based komgo platform for commodity trade finance.

If the security environment can be tightened across crypto-asset networks and exchanges, the potential use cases for blockchain technology might ultimately extend far beyond what is imagined today.

The Bottom Line

It has been an incredible first decade for Satoshi Nakamoto's ambitious vision. The rapid development of crypto-assets and blockchain technology, and successful use cases in financial services, suggest that the building blocks for the next digital transformation of financial marketplaces are starting to form.

With a credible market infrastructure, rational regulatory framework, and enhanced security, the bold promise of these innovations may well be achieved.

And in the interim, fortunes, and massive investments, will be made and lost.

ABOUT MARSH & MCLENNAN. Marsh & McLennan (NYSE: MMC) is the world's leading professional services firm in the areas of risk, strategy and people. The company's approximately 65,000 colleagues advise clients in over 130 countries. With annual revenue over $14 billion, Marsh & McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading firms. Marsh advises individual and commercial clients of all sizes on insurance broking and innovative risk management solutions. Guy Carpenter develops advanced risk, reinsurance and capital strategies that help clients grow profitably and pursue emerging opportunities. Mercer delivers advice and technology-driven solutions that help organizations meet the health, wealth and career needs of a changing workforce. Oliver Wyman serves as a critical strategic, economic and brand advisor to private sector and governmental clients. For more information, visit mmc.com, follow us on LinkedIn and Twitter @mmc_global, or subscribe to BRINK.

ABOUT FIREEYE. FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyberattacks. FireEye has over 7,300 customers across 67 countries, including more than 50 percent of the Forbes Global 2000.

ABOUT CIRCLE. Circle is a global crypto finance company, built on blockchain, powered by crypto assets, and dedicated to helping people and institutions create and share value globally. With our suite of products, we enable our customers to send and receive money around the world easily, as well as invest in and trade crypto assets. Learn more at circle.com.

Contributors

Marsh & McLennan Companies

Marsh & McLennan has formed a task force to focus on the strategic, economic, and risk implications of crypto-assets and blockchain technology. Its mandate is to provide regulatory, capital markets, risk and insurance advice on the emerging risks associated with digital assets.

Please send any inquiries to DigitalAssetRisks@marsh.com.

Marsh

Jennifer Hustwitt, Emerging Risks–Digital, Tech & Innovation
+1 213 399 3471
Jennifer.Hustwitt@marsh.com

Stephen Vina, Cyber Center of Excellence
+1 212 345 0399
Stephen.Vina@marsh.com

Oliver Wyman

Doug Elliott, Partner
+1 646 364 8444
Douglas.Elliott@oliverwyman.com

Chris Allchin, Partner
+44 0 20 7852 7501
Chris.Allchin@oliverwyman.com

Circle

Gus Coldebella, EVP & Chief Legal Officer
gcoldebella@circle.com
Twitter: @g_co

Anders Brownworth, Chief Evangelist
abrownworth@circle.com
Twitter: @anders94

Josh Hawkins, Global Corporate Communications
jhawkins@circle.com
Twitter: @josh_hawkins

FireEye

Grady Summers, EVP & Chief Technology Officer

Randi Eitzman, Senior Threat Pursuit Analyst

Luke McNamara, Principal Analyst

Tony Sapienza

Lynn Thorne

Jeff Lennon

Thank You

Marsh & McLennan, FireEye, and Circle would like to thank Microsoft for their valuable contributions on this paper related to cybersecurity and blockchain.

North America

John Plaisted, Marsh Risk Consulting
+1 212 345 0376
John.Plaisted@marsh.com

Alex deLaricheliere, Head of Banking & Capital Markets
+1 212 345 6740
Alex.deLaricheliere@marsh.com

Tripp Sheehan, Head of Financial Institutions
+1 617 385 0329
Eugene.Sheehan@marsh.com

Matt McCabe, Cyber Center of Excellence
+1 212 345 9642
Matthew.P.McCabe@marsh.com

Devin Beresheim, Head of FINPRO
+1 212 345 5062
Devin.Beresheim@marsh.com

Asia

James Addington-Smith, Head of Asia Specialty
+65 6922 8068
James.Addington-Smith@marsh.com

Naureen Rasul, Head of Cyber–Asia
+852 2301 7206
Naureen.Z.Rasul@marsh.com

Sharon Kerr, Head of FINPRO–Asia
+65 6922 8069
Sharon.Kerr@marsh.com

Europe

David Nayler, Head of Financial Institutions
+44 0 20 7357 2404
David.Nayler@marsh.com

Paul Denny, Head of FINPRO
+44 0 20 7357 2369
Paul.Denny@marsh.com

Additional Contributors

Rob Hunter, Oliver Wyman

Julia McGillis, Marsh & McLennan Companies

Leslie Chacko, Marsh & McLennan Companies

Asha Vellaikal, Marsh Digital Labs

Dave Fuhrman, Marsh

Erin English, Microsoft

Marley Gray, Microsoft

Craig Hajduk , Microsoft

To learn more about FireEye, visit: **www.FireEye.com/services**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

FireEye®