The new world of meta finance and its yet to be tested efficiencies

Received: 22nd April, 2022

Christopher Edmonds*
Chief Development Officer, ICE, USA

Ashwini Panse**
Chief Risk Officer, North American Clearing, ICE, USA

Christopher Edmonds

Ashwini Panse

ICE, 5660 New Northside Drive NW, 3rd Floor, Atlanta, GA 30328, USA

**Tel: +1 770-857-4700; E-mail: chris.edmonds@ice.com*

***Tel: +1 770-857-4700; E-mail: ashwini.panse@ice.com*

Journal of Securities Operations & Custody
Vol. 15, No. 1, pp. 68–81

1753-1802

Christopher Edmonds *is the Chief Development Officer at Intercontinental Exchange, Inc. (NYSE: ICE). Edmonds oversees all of ICE's clearing house operations and the global risk management team. Additionally, he coordinates the company's marketing and public relations endeavours. He previously served as Global Head of Clearing & Risk and Senior Vice President of Financial Markets, where he oversaw the development of initiatives within ICE's exchanged listed and OTC financial markets. Before being named Global Head of Clearing & Risk, Edmonds was Senior Vice President of Financial Markets with responsibility for all client-facing activities for the fixed income, credit and commodities (including energy, softs and metals) asset classes. Prior to that, Edmonds was President of ICE Clear Credit (formerly known as ICE Trust). ICE Clear Credit was one of the first designated Systemically Important Financial Market Utilities under the Dodd–Frank Act. Under his leadership, the central counterparty transitioned from a limited purpose trust company regulated by the New York State Banking Commission and the New York Federal Reserve to a designated clearing organisation and a securities clearing organisation jointly regulated by the Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC). During Edmonds' tenure as President of ICE Clear Credit, more than US$40tn in credit default swaps were cleared reducing the systemic risk associated with these instruments by more than 90 per cent. Additionally, revenues grew from US$20m per year to more than US$75m. Prior to joining ICE Trust in December 2009, Edmonds was the Chief Executive Officer of the International Derivatives Exchange Group (IDCG). He began with the company as the Chief Operating Officer in July 2008 and was named Chief Executive Officer in September 2008. Under his leadership, IDCG completed its application with the CFTC and launched its designated clearing organisation for currency futures and options in December 2008. IDCG also completed a successful capital raise and executed a line of credit facility in excess of US$120mn during this same time-frame. Previously, Edmonds was the Chief Development Officer for ICAP Energy where he led the company's external growth efforts within the energy and commodities space. He also served as the Chief Executive Officer of ICAP Futures. In this role Edmonds was actively involved with regulatory developments in over-the-counter futures and options, including successful efforts to increase the number of OTC cleared products available in energy and commodities. Edmonds formed an industry coalition to push for cleared OTC products and presented the idea to a number of US-based exchanges in the late 1990s before reaching an agreement with NYMEX that eventually resulted in the launch of ClearPort Clearing in 2002.*

Ashwini Panse *is the Chief Risk Officer for the North American clearing houses at ICE. Panse is also the Head of Risk Oversight for ICE Clear Netherlands and ICE Clear Singapore. Panse oversees the risk management framework at*

the clearing houses and provides expertise, support and challenge to the management of all financial and non-financial risks. Panse joined ICE in 2010, and prior to becoming Chief Risk Officer, Panse served in other leadership roles in risk, compliance and internal audit across ICE's global business units. Panse has served as the Chief Compliance Officer for ICE Trade Vault US, and in her internal audit role, Panse administered the Global Sarbanes Oxley 404 compliance and testing programme and internal audits for ICE's US subsidiaries. Panse is Chair of the World Federation of Exchanges (WFE) CCP Working Group. She is a board member of the FIA Operations America Division, which promotes industry cooperation and exchange of ideas on all topics impacting the US Marketplace. She is also a board member and Treasurer at McKenna Farms Therapy Services Inc., a non-profit organisation that provides therapeutic programmes and resources for children with special needs and their families. Panse began her career at Pricewaterhouse Coopers LLC, holds an MBA in Finance from Xavier University, Williams College of Business and is a certified public accountant and a chartered accountant.

ABSTRACT

Technology has been a long-standing catalyst for change, innovation and the emergence of new business models. As technology evolves and matures, the financial services industry revisits its current processes and capabilities to assess if leveraging more modern technologies can drive additional client and business value. There are some proposed use cases for distributed ledger technology (DLT) that propose disintermediating the entire financial industry. There is no doubt the broader financial industry agrees DLT presents an opportunity to shape the future vision of capital markets and recognises the value inherent in the shared DLT platform that can build security, privacy and auditability into every financial transaction and could potentially eliminate costly reconciliation. However, DLT, like any emerging technology, must be thoroughly vetted through rigorous testing. Moreover, regulators across the globe are promoting responsible innovation and fair competition among markets and market participants. And for innovation to be responsible and competition to be fair, it must comply with regulations. Meta finance aka decentralised finance ('DeFi') that runs on decentralised infrastructure, remains immature and volatile, with several economic, technical, ethical and public policy issues still waiting to be addressed. DeFi enthusiasts claim that meta finance is doing to money what email did to postal services, with a promise to provide a secure financial platform that is open to anyone with access to a computer and an internet connection. It has the potential to transform global finance, but activity to date has focused on the community of digital asset owners. DeFi offers efficiencies driven by automation and disintermediation, powered by blockchains and smart contracts with a vision of a more efficient payment system, with instant transactions and lower costs no matter where on the globe one is located. Its efficiencies and safeguards, however, are yet to be tested and the broader community feels safe and secure with the belts and braces traditional finance offers today. DeFi is not devoid of risks relating to high volatility, market manipulation, fraud, illicit finance and lack of governance, which collectively could severely damage market integrity and investor confidence.

Keywords: decentralised finance, digital assets, innovation, traditional finance, distributed ledger technology, smart contracts, blockchain

DECENTRALISED FINANCE IS GROWING AT A RAPID PACE

With the advancement and huge explosion in the depth and breadth of digital technologies such as machine learning, cloud computing, blockchain and distributed ledger, Web3, smart contracts, cryptocurrency and other emerging technologies over the last few decades, the financial services sector is exponentially evolving. Moreover, decentralised finance (DeFi), is now looking to disrupt how financial organisations operate

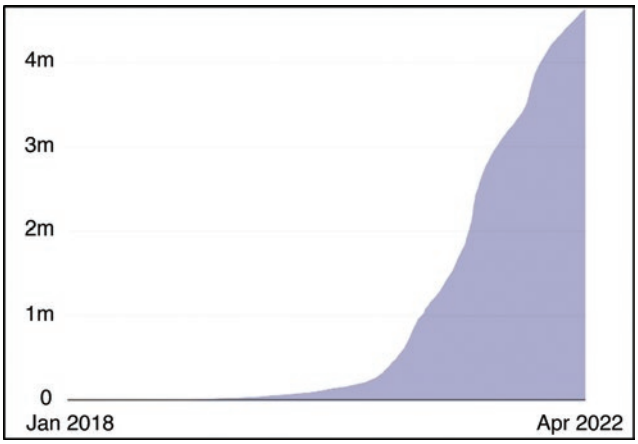

Figure 1 Growth in the number of DeFi users
Source: Dune https://dune.com/rchen8/defi-users-over-time

and how institutional and retail consumers trade, borrow, lend, interact with money and transact business.

DeFi is the latest trend in the crypto asset space which sets out to replicate various activities in the traditional financial system in an open, decentralised, permissionless and autonomous way. DeFi is a collective term for financial products and services that are accessible to *anyone with an internet connection*. With DeFi, the markets are always open and there are no centralised authorities who can block payments or deny access.

Development of the DeFi market relies heavily on smart contracts, which consist of self-executing contracts written as code on blockchain ledgers and are automatically executed upon reaching pre-defined trigger events written in the code. The chart in Figure 1, from an industry source, shows the growth in the number of DeFi users.

TOTAL VALUE OF ASSETS (US$BN) LOCKED IN DEFI TRANSACTIONS

The chart in Figure 2, from an industry source, shows the growth in DeFi across blockchains, as measured in 'total value locked' (TVL).

Blockchain is the backbone for DeFi operations and refers to distributed ledger technologies where data is shared across a network that creates a digital ledger of verified transactions or information among network participants and the data are typically linked using cryptography to maintain the integrity of the ledger and execute other functions, including transfer of ownership or value.

Bitcoin, launched in January 2009, is the world's largest cryptocurrency by market capitalisation. Unlike fiat currency, Bitcoin is created, distributed, traded and stored with the use of a decentralised ledger system, known as a blockchain. Bitcoin's history as a store of value has been turbulent. It has gone through several cycles of boom and bust over its relatively short lifespan. As the earliest virtual currency to meet widespread popularity and success, Bitcoin has inspired a host of other cryptocurrencies in its wake.

Ethereum is an open-source, public, blockchain-based distributed ledger featuring smart contract (scripting) functionality. It enables developers to build blockchain applications with business logic that execute in a trustless environment, where participants do not need to know or trust each other or a third party, while leveraging the high availability of the Ethereum network. This has opened the door to a global financial system where an internet connection is all you need to access applications, products and services that operate in a trustless manner. Anyone can interact with the Ethereum network and participate in this digital economy, without the need for third parties and without the risk of censorship. The scripting language used by Ethereum is Turing-complete, essentially meaning that the types of decentralised applications (dApps) users can design is limited only by their programming skills and creativity.

Smart contracts are pieces of code that run on the blockchain and are guaranteed to produce the same result for everyone

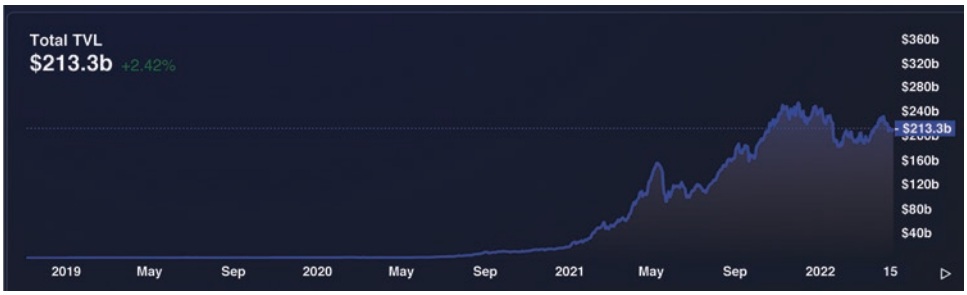

Figure 2 Growth in DeFi across blockchains, as measured in TVL
Source: DeFiLlama https://defillama.com/

who runs them. These can be used to create a wide range of decentralised applications which can include financial products among many others. The term 'smart contract' was coined by Nick Szabo in the 1990s. Vending machines are mentioned as the oldest piece of technology equivalent to smart contract implementation. Everyone who puts the correct amount of coins into the machine can expect to receive a product in exchange. Similarly, on Ethereum, contracts can hold value and unlock it only if specific conditions are met.

Central bank digital currency (CBDC) refers to a form of digital money or monetary value, denominated in the national unit of account, that is a direct liability of the central bank.

Stablecoin refers to a category of cryptocurrencies with mechanisms that are aimed at maintaining a stable value, such as by pegging the value of the coin to a specific currency, asset or pool of assets or by algorithmically controlling supply in response to changes in demand to stabilise value.

BELTS AND BRACES: TRADITIONAL FINANCE

Disintermediation without appropriate substitute mechanisms will only increase the risk for investors and exacerbate market harm.

Traditionally, market intermediaries have acted as gatekeepers to ensure investor protection and market integrity, establishing time tested rule books for operation, and preventing market abuse, imposing capital and liquidity controls, performing anti-money laundering and know your customer checks and monitoring for sanctions. Traditional markets — by design and legally tested regulations — provide for market governance and confidence for all users.

Supporters of DeFi argue that cutting out intermediaries offers consumers more control over their investments. But intermediaries such as exchanges, futures commission merchants, payment clearing facilities and asset managers have developed over the past 200 or 300 years to reliably provide critical financial services to support the financial markets and the investing public. Intermediaries provide information, analyses and advice to the public seeking access to financial markets. Intermediaries often have fiduciary or other legal duties to act in the best interests of their customers. They provide liquidity to the markets and support the stability of the financial system in times of stress. They provide custody of assets and safeguards for investments. They are responsible for preventing money laundering through financial markets. Regulated and licensed intermediaries must meet established standards of conduct and can be held legally responsible for failing to meet those standards of conduct. Intermediaries can be held accountable when things go wrong.

Examples of belts and braces

- Adequate financial, operational and managerial resources;
- appropriate standards for participant and product eligibility;
- adequate and appropriate risk management capabilities;
- ability to complete settlements on a timely basis under varying circumstances;
- standards and procedures to protect member and participant funds;
- efficient and fair default rules and procedures;
- adequate rule enforcement and dispute resolution procedures;
- adequate and appropriate system safeguards, emergency procedures and plans for disaster recovery;
- obligation to provide necessary reports to multiple regulators from different jurisdictions to oversee activities;
- maintenance of all business records for five years in a form acceptable to the regulator;
- publication of rules and operating procedures;
- participation in appropriate domestic and international information-sharing agreements;
- avoidance of actions that are unreasonable restraints of trade or that impose anti-competitive burdens;
- governance arrangements and fitness standards;
- rules to minimise conflicts of interest in the decision-making process, and a process for resolving any conflicts;
- composition of governing boards to include market participants;
- well-founded legal framework.

DEFI: LACK OF APPROPRIATE GUARDRAILS

DeFi applications and markets give rise to several risks, some inherent in DLT based systems, and others stemming from innovations in the architecture and operations of such markets.

Federal Reserve Chairman Jerome Powell said at the Bank of International Settlements (BIS) Innovation Summit on 23rd March, 2022

> In particular, we don't know how some digital products will behave in times of market stress, which could lead to large destabilizing flows, nor do we know how stresses in crypto markets could potentially spill over into the traditional finance system.[1]

REGULATORY NON-CONFORMANCE

The current regulatory framework is designed for a system that drives industry-wide consensus and has financial intermediaries at its core. The existence of intermediaries is contrary to the very essence of decentralised finance, and it is often difficult to even identify parties involved that can be assessed or regulated. Enforcement of existing regulation is also difficult to apply given the absence of a responsible entity. As such, current regulatory frameworks may not be entirely suitable to regulate decentralised networks. The absence of single regulatory and supervisory access points in decentralised DeFi networks is one of the key policy issues that remains to be overcome.

Given the decentralised nature of the networks based on which DeFi applications operate, and their community-driven governance, it is difficult to identify decision-making entities/actors that can ultimately be held accountable for the operation of the network (Figure 3).

Difficult to understand: DeFi faces several early-stage challenges. It uses interfaces which investors are not accustomed to using and which are difficult to fully understand. Blockchain data and smart code are transparent for all to see, but understanding

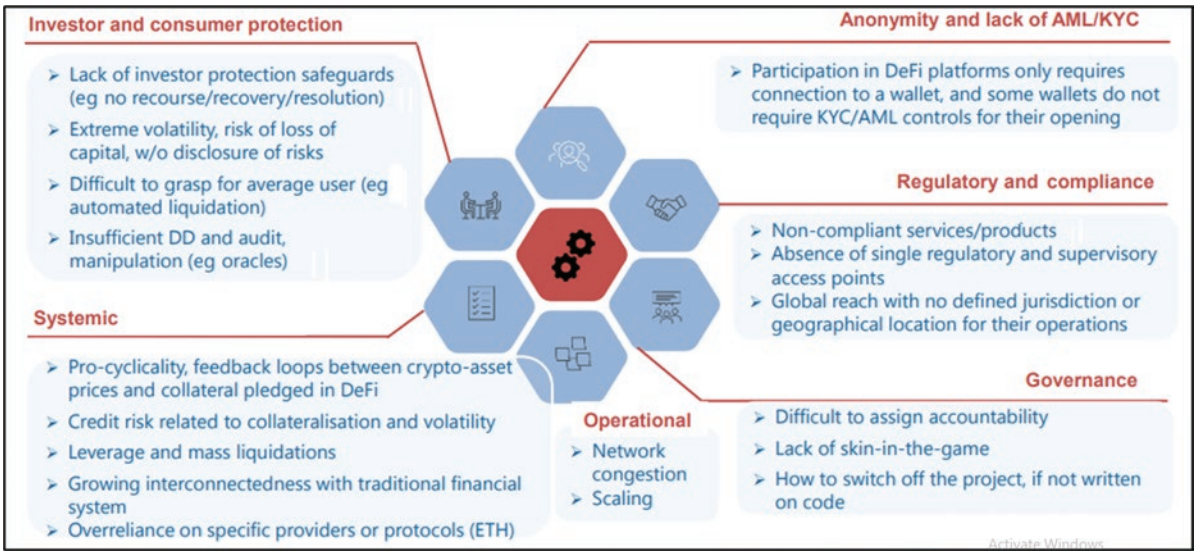

Figure 3 Issues associated with DeFi
Source: Multitude of Potential Risks — OECD (2022), 'Why Decentralised Finance (DeFi) Matters and the Policy', https://t4.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf, p. 42

this data and code requires technical knowledge. This increases the likelihood of, and opportunity for, bad actors to perpetrate fraudulent schemes and engage in illicit activities and other misconduct. Trust is shifted from intermediaries to protocols and code, which can be subject to error, vulnerability and attack and can result in errors in transactions, lack of dispute mechanisms and lack of redress.

Lack of information or misinformation: Digital engagement and social media are being used as prominent tools to gain traction; however, they are not devoid of misinformation. Given the lack of regulatory safeguards, disclosure of material information that could have a substantial impact on the performance of the product or system, such as is necessary to make informed investment decisions, is sometimes missing. Information could be hidden to create an uneven playing field and asymmetries. Potential investors are deprived of information about governance arrangements. There must be a clear path for adjudication, which — by definition — requires a data set(s) all participants can agree is the appropriate data set.

Governance and investor and consumer risks: Appropriate governance of DeFi protocol and smart contracts is essential. However, if only a key set of investors and venture capitalists retain ultimate control, there could be a misalignment of incentives. For instance, if the holder of the administrative key has unilateral control of users' funds held in a smart contract or protocol, there is a risk that the smart contract or protocol could be disabled or altered[2] unexpectedly by the administrator or there could be an insider theft of crypto assets held in the smart contract or protocol. There are plenty of reports of fraudulent schemes and exit scams designed by developers and influencers, who raise capital and escape swiftly, often without leaving any trace. Users seldom have any recourse in case of default or failure of the DeFi protocol, and in most cases, it is difficult to identify a responsible party or central authority to turn to in case of consumer concerns. There are no recovery schemes or resolution mechanisms,

exposing participants to risks of total loss of investment in case of default. DeFi projects can go live with little or no due diligence. Any software developer can launch a new project with zero audit or testing, and there have been numerous cases where the existence of bugs or other technological glitches were identified post-launch. This resulted in the malfunction or even collapse of the systems, with participants incurring significant monetary losses.

Stablecoin: Stablecoins have many of the features of crypto assets but seek to stabilise the price of the 'coin' by linking its value to that of a pool of assets. Therefore, stablecoins might be more capable of serving as a means of payment and store of value, and they could potentially contribute to the development of global payment arrangements that are faster, cheaper and more inclusive than present arrangements. That said, stablecoins are a nascent technology and. as a result, are largely untested and their audited oversight is more limited than is necessary for confidence.

Regardless of size, stablecoins pose legal, regulatory and oversight challenges and risks related to legal certainty; sound governance; money laundering, terrorist financing and other forms of illicit finance; safety, efficiency, and integrity of payment systems; cybersecurity and operational resilience; market integrity; data privacy, protection, and portability; consumer and investor protection; and tax compliance.

Front-running: The Ethereum blockchain, upon which most DeFi apps are built, has been vulnerable to front-running as perpetrators have had sufficient time to reorder transactions in a favourable way. Front-running can result in users with transactions that have been reordered obtaining less favourable transaction terms. If enough front-running occurs on any blockchain, it can result in stale transactions, faulty consensus and an ultimate loss of confidence in the ability of the blockchain to process transactions and achieve settlement finality.

Security breaches: Most crypto service providers have not been able to implement reliable security systems that minimise breaches on their platforms. Moreover, the ubiquitous use of cloud at the foundation of DeFi offerings provides nefarious actors a common access point. Lack of a regulator's ability to test system safeguards and the existence of vulnerabilities means cybercriminals are increasingly taking advantage of security gaps for personal gain, at the expense of their victims.

Cyberattacks increased substantially in mid-2021 and have remained elevated. The attacks are associated mostly with compromised wallet keys, vulnerabilities in computer code and scams by developers. Cyberattacks cause large and often persistent losses. Cyberattacks not only steal assets but also undermine the reputation of a platform, often triggering withdrawals by depositors as they fear not being able to redeem their deposits. An entire platform can collapse in the aftermath of an attack as in the case of the Mt. Gox Scandal.

Cybersecurity and market failures at major digital asset exchanges and trading platforms have resulted in billions of dollars in losses. According to Bitfury Crystal's most recent report,[3] 120 security attacks, 73 attacks on DeFi protocols and 33 fraudulent schemes have so far resulted in the theft of approximately US$12.1bn worth of crypto assets in total.

Figure 4 shows the total amount of crypto assets stolen every year since 2011. The most popular method of crypto-theft has been the infiltration of crypto-exchange security systems. DeFi hacks were the fastest-growing way to steal crypto in 2020–1. Over US$1.7bn was stolen from such protocols. This can be explained by the fact that the technology is new and still has a lot of vulnerabilities. The number of cybercriminal attacks has remained relatively high and overall, the security breaches were still mainly experienced by large-scale exchanges.

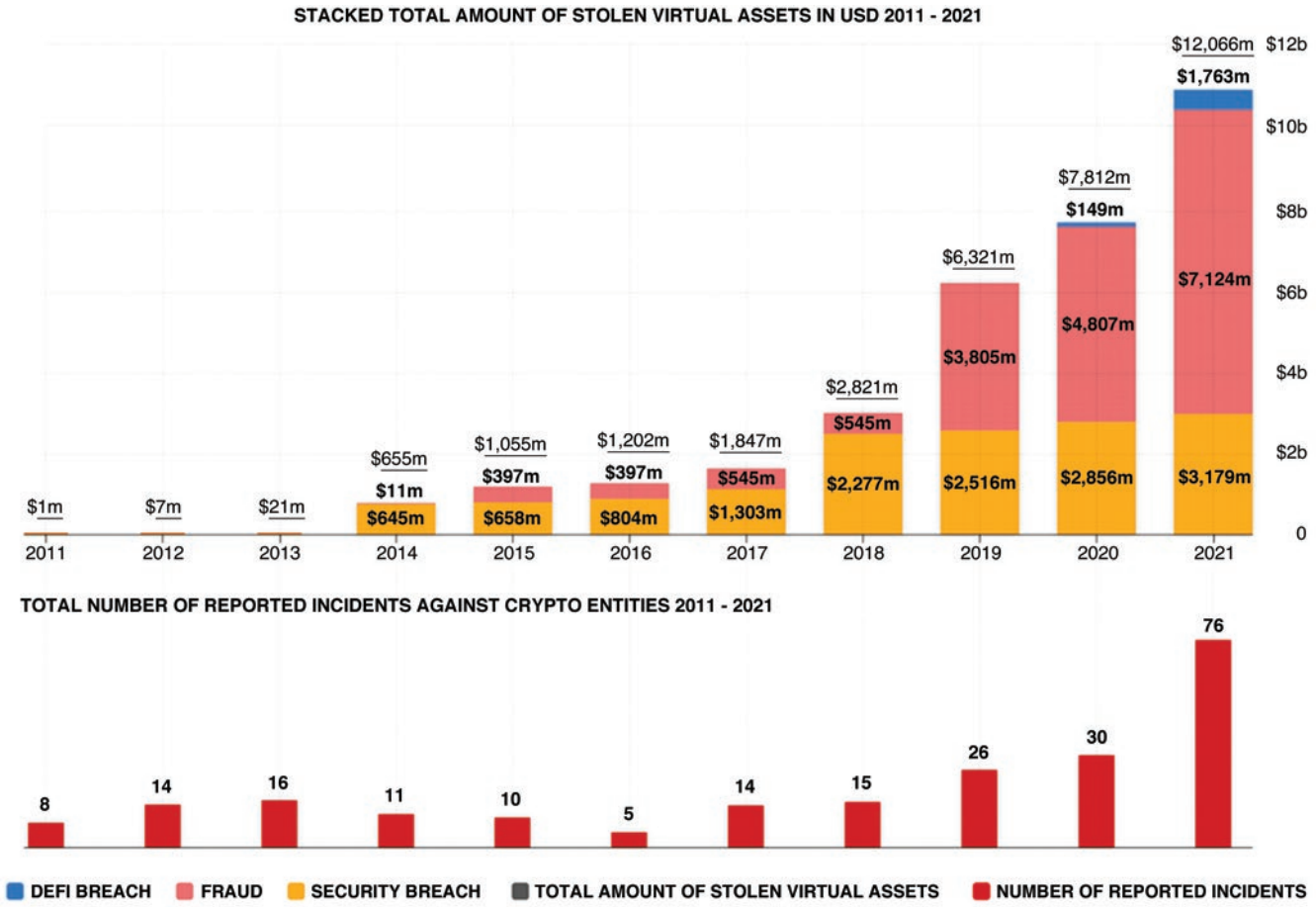

Figure 4 Crypto assets stolen each year 2011–22
Source: Bitfury, 'Crypto and DeFi Hacks and Scams Report 2021'

Smart contracts: Smart contracts are the foundation of DeFi protocols. Currently, smart contracts are in the initial stages of evolution, and we are a long way away from pieces of code sitting entirely independently as a contract, without any reference to a natural language document (Figure 5).

Some believe new legislation is unnecessary as these so-called 'smart contracts' are already covered by existing laws and it would be potentially confusing for companies and their lawyers to consult multiple sources of legislation when conducting business nationwide. They believe that a smart contract may be simply a digital instruction to execute an agreed sequence of events in accordance with pre-defined terms and may or may not be a contract at all.[4]

There is an effort[5] to modernise uniform state laws to accommodate emerging technologies like DLT, virtual currency, and other digital assets by the Uniform Law Commission and American Law Institute. Several very supportive and innovative state legislators in the US are also exploring legislation for this new technology and there is already a patchwork of laws emerging.

The UK Law Commission[6] also published its advice to Government, on 25th November, 2021, concluding that the current legal framework in England and Wales is clearly able to facilitate and support the

Figure 5 Evolution from natural language contracts to smart contracts
Source: ICE

use of smart legal contracts. They however recognised areas of uncertainty and possible difficulties that are unique to smart contracts. For instance,

> Smart legal contracts may present unique challenges when seeking to identify the geographical location of breaches, actions, and enrichments, particularly where the obligations under a smart legal contract concern a digital asset, rather than a physical asset with a clear real-world location.

EVOLUTION OF REGULATORY APPROACH

Crypto and DeFi have become decidedly more mainstream in the last couple years, with a ramp-up in regulatory scrutiny by financial authorities. They are not, however, without their unique challenges. DeFi's elevated market, liquidity and cyber risks may need adjustment to the regulatory perimeter, but DeFi's anonymity, lack of a centralised governance body and legal uncertainties render the traditional approach to regulation ineffective. The rapid emergence and development of the digital asset market has, by design, largely taken place on the outskirts of the traditional financial market structures and the existing regulatory regime covering the digital asset industry is in its early stages and very incomplete.

Digital asset trading platforms and service providers have grown rapidly in size and complexity and while it cannot be said that the industry is completely *unregulated*, there are important principles missing from the regulatory framework that we see in other regulated markets.

Since the first cryptocurrency (Bitcoin) launched in 2009, the question of how exactly to fit the components of this new, decentralised financial ecosystem into traditional categories has been widely debated. *Is Bitcoin a security or a commodity? Who should regulate it?*

SEC Chair Gary Gensler, during his nine-month reign as Chairman of the SEC, has maintained his stance that most crypto tokens are akin to securities and are therefore within the remit of the regulator. He reiterated to CNBC in August 2021 that the SEC considers many cryptocurrency coins and tokens to be securities under the Howey Test,[7] saying, 'If somebody is raising money selling a token and the buyer is anticipating profits based on the efforts of that group to sponsor the seller, that fits into something that's a security.'[8] Also in August 2021, he said, in his speech to the Aspen Security forum: 'In my view, the legislative priority should center on crypto trading, lending and DeFi platforms. Regulators would benefit from additional plenary authority to write rules for and attach guardrails to crypto trading and lending.'[9]

In a recent address, the former Commodity Futures Trading Commission (CFTC) Commissioner Dan M. Berkovitz stated: 'In a pure "peer-to-peer" DeFi system, there is no intermediary to monitor markets for fraud and manipulation, prevent money laundering, safeguard deposited funds, ensure counterparty performance, or make customers whole when processes fail. A system without intermediaries is a Hobbesian marketplace with each person looking out for themselves. Caveat emptor

"*let the buyer beware*".'[10] Berkovitz further argues that DeFi derivative instruments are likely to be illegal under the Commodity Exchange Act.[11] Apart from the legality issue, it is untenable to allow an unregulated, unlicensed derivatives market to compete, side-by-side, with a fully regulated and licensed derivatives market. In addition to the absence of market safeguards and customer protections in the unregulated market, it is unfair to impose the obligations, restrictions and costs of regulation upon some market participants while permitting their unregulated competitors to operate wholly free of such obligations, restrictions and costs.

We are past the stage where digital assets and decentralised financial technologies are a research project — they represent a market capitalisation in excess of US$3tn. The issues are at the front and centre for regulators and the unique and varied features of digital assets can pose significant financial risks to consumers, investors and businesses if appropriate protections are not put in place quickly.

The new and unique uses and functions that DeFi can facilitate may create additional economic and financial risks requiring an evolution to a regulatory approach that adequately addresses those risks. Regulators and supervisors today are exposed to reputational risks if consumers lose money on crypto activity and DeFi. '*Investors deserve regulatory consistency, not confusion*.'[12]

The digital sector now demands more and more regulatory attention and time.

The volatility spikes observed in the main crypto asset prices intensify the fragility of the DeFi market when such assets are pledged as collateral for borrowing and leverage or provided as liquidity for yield farming. This can induce massive automatic liquidations in DeFi protocols. Such liquidations can have a domino effect on investor holdings across the board and may even have spillover effects in traditional markets.

Digital asset issuers, exchanges and trading platforms, and intermediaries whose activities may increase risks to financial stability, should, as appropriate, be subject to and in compliance with regulatory and supervisory standards that govern traditional market infrastructures and financial firms, in line with the general principle of *'same business, same risks, same rules.'*

President Biden's Executive Order[13] acknowledged an increase in the combined market capitalisation of non-state issued digital assets from approximately US$14bn in early November 2016 to US$3tn in November 2021. President Biden called on the Financial Stability Oversight Council to identify specific financial stability risks and regulatory gaps posed by various types of digital assets and make recommendations to address them.

Following this, CFTC Chairman Rostin Behnam released the following statement:

> The Executive Order signed by President Biden today marks a significant step. The EO will ensure greater cooperation and coordination between various cabinet-level agencies, the independent market regulators, and prudential regulatory bodies. With increased adoption and growth in the digital asset market comes the need for increased education and outreach to protect against new and emerging risks. President Biden is right to emphasize the need for increased customer education and consumer protection, while combating illicit activity and safeguarding financial stability.[14]

Several international organisations (G7, G20, the Financial Action Task Force [FATF], the Financial Stability Board [FSB] and the International Organization of Securities Commissions [IOSCO]) are actively working on a variety of issues relating to crypto assets, with a particular focus on investor and consumer protection, market integrity, bank exposures, payment systems, financial stability monitoring, anti-money laundering and countering the financing of terrorism.

Ongoing international work should drive development and implementation of holistic standards, cooperation and coordination, and information sharing. The G7 report[15] outlining a set of policy principles for central bank digital currency (CBDCs) is an important contribution to establishing guidelines for jurisdictions for the exploration and potential development of CBDCs. The G7 report highlighted that any CBDC should be grounded in the G7's long-standing public commitments to transparency, the rule of law and sound economic governance, as well as the promotion of competition and innovation.

The International Monetary Fund (IMF) considers DeFi a risk to global financial stability, especially as it grows more interconnected with the traditional financial system. It suggests that stablecoins and centralised exchange be the focus of supervision. It has published a new report[16] on global financial stability, which covers the DeFi market, among other things. Additionally, it suggests that authorities should 'encourage DeFi platforms to be subject to robust governance schemes, including industry codes and self-regulatory organizations. These entities could provide an effective conduit for regulatory oversight.'

The Organisation for Economic Co-operation and Development (OECD)[17] sees a role for supervisory authorities and international standard-setters in assessing the risks of DeFi, exploring how existing rules may be enforced in DeFi applications and addressing regulatory gaps. The OECD concedes that the regulation and oversight of DeFi applications may be challenged by their global reach and operation, given that their activities often have no defined jurisdiction or geographical location and may be accessed virtually anywhere in the world.

RESPONSIBLE INNOVATION

With new and transformative technologies, come disparate views and opinions. In her remarks[18] on 7th April, 2022, US Secretary of the Treasury, Janet L. Yellen, encouraged policymakers, business people, advocates, scholars, inventors, engineering and software development communities and citizens to come together for a constructive public–private dialogue to ensure any ground-breaking innovation reflects lessons learned throughout our financial history and is consistent with values and laws; promotes economic competitiveness and growth; protects consumers, investors and businesses; avoids regulatory arbitrage; safeguards financial stability from systemic risks; and provides equitable access to safe and affordable financial services.

Digital asset technologies and the digital payments ecosystem should be developed, designed and implemented in a responsible manner consistent with the rules governing traditional finance. System features should include privacy and security in its architecture, integrate features and controls that defend against illicit exploitation, and reduce negative climate impacts and environmental pollution, as may result from some cryptocurrency mining.

Development of CBDCs have the potential to support efficient and low-cost transactions, particularly for cross-border funds transfers and payments, and to foster greater access to the financial system, with fewer of the risks posed by private sector-administered digital assets. There are also, however, potential risks and downsides to consider. Timely assessments of potential benefits and risks under various designs should be prioritised.

Any technology driven financial innovation is inherently cross-border and requires international cooperation and collaboration to ensure that new technology does not lead to further fragmentation.

CONCLUSION

In conclusion, there is a lot more work that needs to be done to create a new system

that can adequately provide the governance and regulatory framework suitable for DeFi. Enhanced regulatory surveillance and robust and comprehensive national regulatory frameworks delivered through common global standards by standard-setting bodies will be necessary.

References and notes

(1) Powell, J. (2022) 'In Conversation: Emerging Challenges for Central Bank Governors in a Digital World', BIS Innovation Summit, available at https://www.bis.org/events/bis_innovation_summit_2022/overview.htm (accessed 1st April, 2022).

(2) Mt. Gox Scandal: Mt. Gox was a cryptocurrency exchange that operated between 2010 and 2014. Mt. Gox was considered the world's largest Bitcoin exchange at its peak. It handled 70 to 80 per cent of the total Bitcoin trading volume. In early February 2014, the exchange suspended withdrawals after claiming to have found suspicious activity in its digital wallets. The company discovered that it had 'lost' in the range of 650,000 to 800,000 Bitcoins between 2011 and 2014. The company filed for bankruptcy shortly thereafter. This issue was claimed to be the result of a bug in the Bitcoin software that allowed users to alter transaction IDs, sometimes referred to as 'transaction malleability'. More than 24,000 customers around the world lost access to hundreds of millions of dollars' worth of cryptocurrency and cash. Mark Karpelès, former CEO of Mt. Gox was accused of embezzling money from Mt. Gox and manipulating its data, as well as breach of trust. On 14th March, 2019, the Tokyo District Court found Mark Karpelès guilty of falsifying data to inflate Mt. Gox's holdings by $33.5m, for which he was sentenced to 30 months in prison, suspended for four years, meaning he will serve no time unless he commits additional offences over the next four years. The court acquitted Karpelès on several other charges, including embezzlement and aggravated breach of trust, based on its belief that Karpelès had acted without ill intent. Nonetheless, the verdict said Karpelès had inflicted 'massive harm to the trust of his users' and there was 'no excuse' for him to 'abuse his status and authority to perform clever criminal acts'. Equity Guru (2019) 'Deciphering Cryptocurrency: Crypto 101 — Exchanges', Equity Guru, available at https://bpb.opendns.com/b/https/equity.guru/2019/06/07/deciphering-cryptocurrency-crypto-101-exchanges/ (accessed 1st April, 2022).

(3) Khaustova, M. (2021) 'Crystal Blockchain's Year in Review 2021', Crystal BlockChain.com, available at https://crystalblockchain.com/articles/crystal-blockchains-year-in-review-2021/ (accessed 1st April, 2022).

(4) Chamber of Digital Commerce (2016) 'Smart Contracts: 12 Use Cases for Business & Beyond, A Technology, Legal & Regulatory Introduction — Foreword by Nick Szabo', available at https://d3h0qzni6h08fz.cloudfront.net/Smart-Contracts-12-Use-Cases-for-Business-and-Beyond_Chamber-of-Digital-Commerce.pdf (1st April, 2022).

(5) In 2019, the Uniform Law Commission (ULC) and American Law Institute (ALI) appointed a drafting committee to consider whether amendments to the Uniform Commercial Code (UCC) were advisable to accommodate emerging technologies like artificial intelligence, distributed ledger technology and virtual currency. The committee has drafted uniform model amendments to the UCC to deal with digital assets among other items and will present the draft to the ULC and ALI for approval, after which the amendments will be presented for consideration and enactment by the stateside legislatures in autumn 2022. Several states have already started to enact legislation containing portions of this draft, particularly as it applies to virtual currencies. A high-level summary of the committee's work has been prepared by the law firm DLA Piper. Tank, M. H. K., Whitaker, D., Grant, A. and Caires, E. S. M. (2022) 'ULC Approves Important New

Amendments to the Uniform Commercial Code for State Adoption', DLA Piper, available at https://www.dlapiper.com/en/us/insights/publications/2022/08/ulc-approves-important-new-amendments-to-the-uniform-commercial-code-for-state-adoption/ (accessed 2nd August, 2022).

(6) The UK Law Commission published its advice on smart legal contracts on 25th November, 2021. It was informed by the detailed responses received to the call for evidence, published in December 2020. The UK Law Commission (2021) 'Smart Projects', available at https://www.lawcom.gov.uk/project/smart-contracts/ (accessed 1st April, 2022).

(7) When determining whether a digital asset is a security, the SEC considers whether the asset constitutes an 'investment contract'. For an asset to be considered an investment contract, it must meet the three criteria of the Howey Test which was developed and named after the Supreme Court case SEC v. W. J. Howey Co., 328U.S. 293 (1946). The Howey Test requires that there must be (1) the investment of money (2) in a common enterprise (3) with a reasonable expectation of profits to be derived from the efforts of others.

(8) Gensler, G. (2021) 'SEC Chair Gary Gensler Speaks with CNBC's "Squawk Box" Today', CNBC, available at https://www.cnbc.com/2021/08/04/cnbc-exclusive-cnbc-transcript-sec-chair-gary-gensler-speaks-with-cnbcs-squawk-box-today.html (accessed 1st April, 2022).

(9) Gensler, G. (2021) 'Remarks Before the Aspen Security Forum', US Securities and Exchange Commission, available at https://www.sec.gov/news/speech/gensler-aspen-security-forum-2021-08-03 (accessed 1st April, 2022).

(10) Berkovitz, D. M. (2021) 'Keynote Address of Commissioner Dan M. Berkovitz Before FIA and SIFMA-AMG, Asset Management Derivatives Forum 2021', CFTC, available at https://www.cftc.gov/PressRoom/SpeechesTestimony/opaberkovitz7 (accessed 1st April, 2022), (emphasis added).

(11) The CEA requires futures contracts to be traded on a designated contract market (DCM) licensed and regulated by the CFTC. The CEA also provides that it is unlawful for any person other than an eligible contract participant to enter a swap unless the swap is entered into on, or subject to, the rules of a DCM. The CEA requires any facility that provides for the trading or processing of swaps to be registered as a DCM or a swap execution facility (SEF). DeFi markets, platforms, or websites are not registered as DCMs or SEFs. The CEA does not contain any exception from registration for digital currencies, blockchains, or 'smart contracts'.

(12) Berkovitz, D. M. (2021) 'Keynote Address of Commissioner Dan M. Berkovitz Before FIA and SIFMA-AMG, Asset Management Derivatives Forum 2021', CFTC, available at https://www.cftc.gov/PressRoom/SpeechesTestimony/opaberkovitz7 (accessed 1st April, 2022).

(13) On 9th March, 2022, President Biden issued an Executive Order on ensuring responsible development of Digital Assets. Biden, J. (2022) 'Executive Order on Ensuring Responsible Development of Digital Assets', The White House, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/ (accessed 1st April, 2022).

(14) Behnam, R. (2022) 'Keynote of Chairman Rostin Behnam at the FIA Boca 2022 International Futures Industry Conference, Boca Raton, Florida', CFTC, available at https://www.cftc.gov/PressRoom/SpeechesTestimony/opabehnam21 (accessed 1st April, 2022).

(15) At their meeting in Chantilly in July 2019, G7 Finance Ministers, and central bank Governors agreed that stablecoins raise serious regulatory and systemic concerns and stablecoin initiatives and their operators must meet the highest standards and be subject to prudent supervision and oversight, and that possible regulatory gaps should, as a matter of priority, be assessed and addressed. The G7 Finance Ministers and central bank Governors asked for

a report from the Working Group on Stablecoins, including its recommendations. Coeure, B. (2019) 'Update from the Chair of the G7 Working Group on Stablecoins', BIS, available at https://www.bis.org/cpmi/speeches/sp190718.htm (accessed 1st April, 2022).

(16) The International Monetary Fund (IMF) issued its Global Financial Stability Report. The most recent release is Chapter 3: 'The Rapid Growth of Fintech: Vulnerabilities and Challenges for Financial Stability'. International Monetary Fund (2022) 'Global Financial Stability Report', IMF, available at https://www.imf.org/en/Publications/GFSR/Issues/2022/04/19/global-financial-stability-report-april-2022 (accessed 1st April, 2022).

(17) Organisation for Economic Co-operation and Development (2022) 'Why Decentralised Finance (DeFi) Matters and the Policy Implications', OECD, Paris.

(18) US Secretary of the Treasury Janet L. Yellen delivered remarks on digital assets policy, innovation and regulation at American University's Kogod School of Business Center for Innovation. Yellen, J. (2022) 'Remarks from Secretary of the Treasury Janet L. Yellen on Digital Assets', US Department of the Treasury, available at https://home.treasury.gov/news/press-releases/jy0706 (accessed 1st April, 2022).