THE INTERNATIONAL JOURNAL OF BLOCKCHAIN LAW

Volume 4

December 2022

GBBC
Global Blockchain
Business Council

Geneva | London | New York | Washington, D.C. | Austin | Seattle

TABLE OF CONTENTS

NOTE FROM THE EDITOR-IN-CHIEF

DR. MATTHIAS ARTZT
SENIOR LEGAL COUNSEL
DEUTSCHE BANK

Dr. Matthias Artzt is a certified lawyer and senior legal counsel at Deutsche Bank AG since 1999. He has been practicing data protection law for many years and was particularly involved in the implementation of the GDPR within Deutsche Bank AG. He advises internal clients globally regarding data protection issues as well as complex international outsourcing agreements involving data privacy related matters and regulations.

Welcome to the 4th issue of the IJBL! It is hard to believe we are at our fourth issue, and that the year 2022 is coming to an end! What a year it's been, the Crypto winter, multiple bankruptcies, the Ethereum merge, and the FTX implosion, among many, many other things!

In the immediate aftermath of the collapse of FTX, there has been much focus on FTX's misguided activities and excesses, with many asking how this could have happened and what regulations are required to ensure a fair and secure ecosystem. We have begun to see the contagion from the demise of FTX, and we are nowhere near at the end of this debacle. In this issue, we choose to eschew the FTX drama, at least for now, allowing the facts to unfold and, instead, focus on the novel legal questions related to crypto and blockchain, including investor protections, that continue to propel the crypto dialogue forward. We are proud to offer you our dear reader a variety of compelling content on the most important issues of the day:

Andrea Tinianow´s article, "A Path To Crypto Regelation: New Scholarship Sheds Light During Crypto Winter" provides an overview of the state of play on crypto regulation in the US. Moreover, it spotlights a discussion draft of a scholarly paper by DLx Law LLP called, "The Ineluctable Modality of Securities law".

We bring you a link to our recent (virtual) event, IJBL´s "Hot Topics in Blockchain Law," a lively and unscripted hour-long conversation on pressing legal issues with top blockchain attorneys: David Adlerstein, Sarah Brennan, Jason Gottlieb, Eric Hess, Christine Parker, Stephen Palley, and Andrea Tinianow. We plan to offer this Hot Topics event each quarter. Please keep an eye out for a notice for the next event that will take place in the first quarter of 2023.

For the first time anywhere, a regulatory agency sued a Decentralized Autonomous Organization (DAO) and obtained from the court authorization to circumvent the traditional method for serving the defendant. We bring you the highlights of that case here.

David Adlerstein and Sujay Davé address the issue on how crypto bankruptcies affect the recovery of crypto assets, in their article, "Crypto Bankruptcies Reveal Fault Lines in Asset Recovery". In this article, the authors compare the protections customers are afforded in traditional U.S. financial institutions to those provided by similar institutions in the crypto space. They then discuss how asset recovery protections in the crypto ecosystem may evolve.

Paul Yuen, General Counsel of the Monetary Authority of Singapore (MAS), shares his observations with regards to the digital asset ecosystem in Singapore. MAS has been exploring potential DeFi use cases through DLT, in cooperation with the financial community there. Beyond facilitating experiments involving DLT and new business models, MAS has reviewed and refreshed policies and legislation aiming to adapt them to the evolving financial landscape.

Jake van der Laan´s article on smart contracts offers a response to Michael Jünemann's and Udo Milkau's article which was published in IJBL's 2nd edition, "Can Code be Law? – A Review of Current Developments." Jake expresses the idea of bringing a certain practical realism to our understanding what smart contract platforms may achieve and raises concerns that unabated automation of smart contract enforcement may entail unintended consequences.

And finally, I have added some interesting infographics stemming from the GSMI fact cards with the kind permission of the GBBC.

Happy reading and Happy Holidays!

ABOUT THE CO-EDITORS

You can find the editors' full bios here.

LOCKNIE HSU

PROFESSOR
SINGAPORE MANAGEMENT UNIVERSITY

Locknie Hsu received her legal training at the National University of Singapore and Harvard University, and is a member of the Singapore Bar. Locknie specializes in international trade and investment law, including areas such as paperless trade, FTAs, digital commerce, and business applications of technology.

STEPHEN D. PALLEY

PARTNER
BROWN RUDNICK

Stephen Palley is a litigation partner and co-chair of Brown Rudnick's Digital Commerce group. He has deep technical and U.S. regulatory knowledge, particularly in the digital asset space, and assists clients working on the frontiers of technology, including on deal work for blockchain and other technology enterprises.

THIAGO LUÍS SOMBRA

PARTNER
MATTOS FILHO

Thiago's practice focuses on Technology, Compliance and Public Law, and in particular on anti-corruption investigations handled by public authorities and regulators, data protection, cybersecurity and digital platforms. He was awarded as one of the world's leading young lawyers in anti-corruption investigations by GIR 40 under 40 and technology by GDR 40 under 40.

ANDREA TINIANOW

CHIEF LEGAL OFFICER AND HEAD OF POLICY - AMERICAS
GBBC

Andrea Tinianow, a Delaware attorney, is the Chief Legal Officer and Head of Policy - Americas at GBBC. In 2015, Andrea started the Delaware Blockchain Initiative which gave rise to the "Blockchain Amendments" to Delaware's business entity statutes that authorize corporations (and other business entities) to maintain their corporate records, including stock ledgers, on a blockchain.

JAKE VAN DER LAAN

CHIEF INFORMATION OFFICER & DIRECTOR
FINANCIAL AND CONSUMER SERVICES COMMISSION, NEW BRUNSWICK, CANADA (FCNB)

Jake van der Laan is the Director, Information Technology and Regulatory Informatics and the Chief Information Officer with the New Brunswick Financial and Consumer Services Commission (FCNB) in New Brunswick, Canada. He was previously its Director of Enforcement, a position he held for 12½ years. Prior to joining FCNB he was a trial lawyer for 12 years, acting primarily as plaintiff's counsel.

GARY D. WEINGARDEN

PRIVACY OFFICER AND DIRECTOR OF IT SECURITY COMPLIANCE
TUFTS UNIVERSITY

Gary Weingarden is the Privacy Officer and Director of IT Security Compliance at Tufts University. Gary has multiple certifications in privacy, security, compliance, ethics, and fraud prevention from IAPP, ISC2, ISACA, SCCE, and the ACFE, among others. He is an Observing Member of the Global Blockchain Business Council. Before Joining Tufts, Gary served as Data Protection Officer for Notarize, and Senior Counsel at Rocket Mortgage.

ARTICLE I

A PATH TO CRYPTO REGULATION: NEW SCHOLARSHIP SHEDS LIGHT DURING CRYPTO WINTER

ANDREA TINIANOW
GBBC CHIEF LEGAL OFFICER AND HEAD OF POLICY, AMERICAS

Separate and apart from the unfolding FTX debacle, the last several days marked several pivotal moments in the crypto law world around the heated debate about whether crypto assets are securities.

First was a decision in *SEC v. LBRY*, where a Federal District Court agreed with the SEC that LBRY blockchain had issued its token, LBC, as a security and in doing so violated U.S. securities laws. In contrast, another blockchain project, Web 3 Foundation, announced that the crypto asset, DOT, native to the polkadot blockchain developed by the Web 3 Foundation, had successfully "morphed" from a security to a non-security. These developments are one illustration of the gap between the SEC's position that most cryptoassets are securities and that of the industry.

In these dark days of crypto winter, sometimes the brightest light can come from the least expected of places, like a really long law article with an inscrutable name that considers 276 appellate opinions of *Howey* precedent (which recently made its appearance).

But, before considering each of these items, it is helpful to consider the political and regulatory crypto scrum that is the backdrop for these occurrences.

We begin with what has become a mantra of the Securities and Exchange Commission (SEC) - that most fungible crypto tokens are securities. This maxim didn't start with SEC Chairman Gary Gensler – although he consistently amplifies the message. It began with his predecessor, Jay Clayton, and was supported and expanded upon by Bill Hinman, the former Director of the SEC's Division of Corporation Finance.

Hinman articulated that somehow unlike the oranges that were the subject of the famous *Howey* case, fungible crypto tokens could be securities because they "evidence the investment contract." He also asserted that a token might become a non-security if the "network on which the token or coin is to function is sufficiently decentralized." And thus, since that time, blockchain companies have sought to decentralize their operations in order to satisfy the SEC's guidance on digital assets, so that their tokens might be, or become, non-securities.

Therefore, the question of how one determines whether a token is a security has largely been left to SEC enforcement actions, including prominently the ongoing *SEC v. Ripple*, where amicus briefs have been filed on both sides of the "v."

SEC v. LBRY is just the latest in a line of cases to consider the same question. In that case, the District Court for the District of New Hampshire, this past week, granted the SEC's motion for summary judgment and determined that the LBC tokens issued by the LBRY project were "offered as securities."

According to Jason Gottlieb, Partner, Chair of White Collar and Regulatory Enforcement Group, Morrison Cohen LLP, **"it is important for courts to distinguish between the investment contract which is a security and the token itself which is not. Was that done here? I'm not sure."** (Notably, Gottleib filed an amicus brief in the *Ripple* case on behalf of the Blockchain Association.)

Still others find fault in the fact that the SEC failed to bring in all of the relevant parties as defendants in the LBRY enforcement action.

"In LBRY, the SEC went after a relatively small operation, but failed to go after the exchanges that listed LBRY's native token and allowed it to trade," said Donna Redel, Adjunct Professor, Fordham Law. "This is part of a pattern that means these key cases are rarely fully litigated."

And prior to the *LBRY* decision came a major announcement (albeit one not accompanied by analysis) that a fungible token associated with blockchain project had successfully "morphed," taking it out of the sphere of securities and all that that entails, and into the realm of non-securities. Web3 Foundation asserts in their Medium article, "the PolkadotDOT blockchain's native digital asset (DOT) has morphed and is no longer a security. It is software." This is interesting as a unilateral announcement by the project, and it is not clear whether and if the SEC agrees.

"The SEC's theory on when crypto assets are securities has caused a lot of problems because it has made it hard for the test to be applied repeatedly with consistent results. In that sense, it is no longer a "test," which should have predictable and logical results no matter who applies it.

We are now in a place where the SEC applies the test to say almost all crypto assets are securities, while the industry applies the same test to say that nothing is a security," says Jai Massari, Co-founder and CLO of Lightspark.

How to solve for this disconnect?

Enter Lewis Cohen and his DLx colleagues, Greg Strong, Freeman Lewin, and Sarah Chen, with their discussion draft of a scholarly paper on the nature of crypto assets entitled, "The Ineluctable Modality of Securities Law: Why Fungible Crypto Assets are Not Securities" published last week via Tweet and on the firm's website. It's hefty – 107 pages, not including the many annexes that list, analyze and discuss the 276 federal appellate and Supreme Court opinions that consider the *Howey* question of what constitutes an investment contract.

Cohen, in his tweet thread (which I have condensed here) shared:

"For almost three years, the @DLxLawLLP team has pondered the most consequential of questions in all of crypto law: When and how do the US federal securities laws apply to crypto assets? As lawyers out there will know, the answer to this question turns on a rule set out in a 1946 Supreme Court case, *SEC v. W.J. Howey Co.* — what has become known as the '*Howey* test'. But the *Howey* test is and remains one of the most confusing and misunderstood rules in all of the law. Countless hours of lawyer time, and untold sums of money, have been spent seeking to reveal its secrets. . . . We needed to ingest the whole of the law - every single *Howey* appellate case there ever has been (and many more besides)."

And ingest they did!

The result is scholarship that explains why fungible crypto tokens, generally the object of blockchain fundraising schemes, should not be treated as securities under our current set of laws and precedent.

The theory and discussion which underlie this paper are complex and, at times, difficult. Yet this piece of compelling writing could offer the roadmap to establishing a much needed crypto regulatory framework by our courts and legislatures.

"Balancing the need to provide information and protection to crypto asset purchasers with a regulatory regime that allows this technology to continue to develop in the United States was the starting point for our analysis and thinking," says Strong. **"Requiring disclosure and securities law compliance when crypto assets are sold in investment contract transactions is critical. Just as critical is recognizing that those transactions do not transform such crypto assets themselves into securities under *Howey*."**

Significantly, the article was developed with the input from many well known blockchain attorneys.

"They did the necessary work to look at the appellate case law precedent to see if there is a legal basis for the SEC's morphing theory, that a token can morph from a non-security to a security. They found that the answer is 'no,'" says Massari.

"Lewis and his colleagues have produced a monumental piece of research," says Gottlieb. "It delves into the appellate decisions interpreting *Howey* case law to show why a token itself is not a security, nor does the case law support the notion that it could be."

David Adlerstein, Counsel at Wachtell, Lipton, praises the article as a "thoughtful and timely exegesis of existing *Howey* jurisprudence."

"It is a landmark piece of legal scholarship for the industry," says Kayvan Sadeghi, Partner at Jenner & Block. Sadeghi and Cohen recently led a team of attorneys that filed an amicus brief on behalf of Paradigm in the *Ripple* case, borrowing heavily from the *Howey* jurisprudence explored in the DLx article.

The brief argues that "extending *Howey* to classify crypto assets, themselves as 'securities,' would bypass the role of Congress and violate the major questions doctrine." (This was first discussed in a Forbes.com article that I wrote following the U.S. Supreme Court's EPA decision that limited the agency's authority to regulate carbon emissions.)

Moreover, the brief explains that not all applications of securities laws to crypto assets implicates the major questions doctrine, only those that, "attempt to mutate analysis of the transaction into a conclusion about the asset itself." That is, the major questions doctrine is only implicated where the crypto token which is the object of the fundraising transaction is found to be a security, under *Howey* analysis.

The brief continues:

"It is in that leap that the SEC departs from the authority granted by Congress and all appellate precedent. [T]hat novel argument would not only grant authority over the crypto asset secondary market not authorized by Congress, but create the first class of issuer-independent securities – a concept entirely foreign to the laws enacted by Congress."

Heady stuff, but important. Very important. A lot hangs in the balance, namely the future of crypto regulation and innovation in the U.S.

The DLx article can provide the jurisprudential gravitas for U.S. courts, lawmakers, regulatory agencies to get behind a regulatory framework for fungible crypto assets, one that is consistent with U.S. securities law, the *Howey* test and related jurisprudence. So block out the chaos of FTX for a moment, put on the kettle, and give it a read.

Author's Note: This article was first published by Forbes.com and is reprinted here with permission and minor changes. The opinions herein are my own and do not reflect the opinions or position of the Global Blockchain Business Council.

ARTICLE II

‘HOT TOPICS IN BLOCKCHAIN LAW,’ A WEBINAR PRESENTED BY THE IJBL

With shifts in the regulatory landscape across the globe for blockchain and digital assets, it becomes challenging to keep up with the industry and identify the implications from all of the movements within regulation and policy.

To address the need for open discussions around regulation, GBBC’s IJBL hosted the inaugural virtual roundtable, ‘Hot Topics in Blockchain Law,’ to navigate the pressing topics surrounding the blockchain and digital assets regulatory landscape.

Seven blockchain attorneys - David Adlerstein, Sarah Brennan, Jason Gottlieb, Eric Hess, Christine Parker, Stephen Palley, and Andrea Tinianow - unpacked topics including clarity of regulation, the definition of tokens, and more, outlining how these concepts play a significant role in the way blockchain is perceived by policymakers.

IJBL will present ‘Hot Topics in Blockchain Law’ each quarter to engage the blockchain and digital assets community, and encourage open conversations from an array of legal perspectives.

VIEW THE RECORDING ON GBBC’s YOUTUBE

ARTICLE III

GAMECHANGER: THE CFTC SUES A DAO

ANDREA TINIANOW
GBBC CHIEF LEGAL OFFICER AND HEAD OF POLICY, AMERICAS

INTRODUCTION

In late September, the Commodity Futures Trading Commission ("CFTC") made headlines by bringing an enforcement action against a decentralized autonomous organization (DAO). **With its lawsuit against Ooki DAO and a related settlement order against the DAO's predecessor company and its co-founders, the CFTC raised novel legal issues relating to DAO compliance with federal commodities laws and state rules governing service of process.**

Significantly, CFTC Commissioner Summer Mersinger issued a dissenting statement indicating her disapproval with the CFTC's legal bases for the lawsuit, as well as the CFTC's failure to undertake a public notice-and-comment period prior to suing the DAO. In addition, a recent hearing in the federal court lawsuit against DAO suggest that the CFTC may be able to move forward with its suit against the DAO even though no individual natural persons have been served.

Let's unpack that.

THE SETTLEMENT ORDER

On September 22, the CFTC issued a settlement order simultaneously filing and settling charges against bZeroX, LLC, and its co-founders for violating exchange-trading and registration requirements in the Commodity Exchange Act (CEA), and the CFTC's anti-money laundering rules.

The settlement order found the co-founders liable based on dual theories: control person liability based on their control of bZeroX, LLC, the limited liability company that developed the trading protocol, and personal liability related to the Ooki DAO, the successor to bZeroX, LLC. The CFTC based their claim of personal liability on the fact that the co-founders used Ooki tokens to vote on Ooki DAO governance. The settlement order required the respondents to pay a $250,000 civil monetary penalty and to stop engaging in prohibited activities set forth in the order.

THE LAWSUIT

In addition to the settlement order, **the CFTC filed an enforcement action** in the U.S. District Court for the Northern District of California **against Ooki DAO—a decentralized autonomous organization** (and successor to bZeroX, LLC)— for violating the same laws as alleged in the settlement order and seeking injunctive relief.

Significantly, the CFTC seeks remedies with respect to the holders of Ooki tokens who voted in the governance of the Ooki DAO during the relevant time period. **The CFTC argues that Ooki DAO meets the federal definition of an unincorporated association and, as such, its voting members are personally liable for the debts of the DAO, and, by extension, the activities of the DAO.** The CFTC seeks restitution, disgorgement, civil monetary penalties, trading and registration bans, and injunctive relief.

THE ALLEGATIONS

The CFTC order finds and the complaint alleges the following:

From approximately June 1, 2019 to approximately August 23, 2021, the individual defendants designed, deployed, marketed, and made solicitations concerning a blockchain-based software protocol that accepted orders for and facilitated margin and leveraged retail commodity transactions (functioning similarly to a trading platform).

On approximately August 23, 2021, bZeroX, LLC, transferred control of the bZx Protocol to the bZx DAO, which subsequently renamed itself and is currently doing business as the Ooki DAO. As alleged, the Ooki DAO operates the Ooki Protocol in the exact same manner as bZeroX LLC.

The protocol permitted users to contribute margin (collateral) to open leveraged positions whose ultimate value was determined by the price difference between two digital assets, from the time the position was established to the time it was closed. The protocol purported to offer users the ability to engage in these transactions in a decentralized environment—i.e., without third-party intermediaries taking custody of user assets.

As a result, the protocol operated as a futures commission merchant (FCM) in violation of the CEA, and failed to comply with the Bank Secrecy Act compliance program, as required of FCMs.

THE DISSENT

Commissioner Summer Mesinger criticizes the Commission's decision to hold token holders (who participated in DAO governance) liable for the DAO's alleged violations, asserting that the Commission is improperly picking winners and losers and, further, that it has acted without proper legal authority, notice, or public input.

Her dissent largely rests on these four grounds:

- State-law principles of partnership law which provide for joint and several liability do not apply under these set of facts;
- The approach undermines the public interest by disincentivizing good governance;
- The approach constitutes "regulation by enforcement" and is based on a set of rules that were never articulated by the Commission; and
- The Commission could have pursued alternative, traditional bases to find the DAO liable, such as aiding and abetting liability.

SERVICE OF PROCESS HAS BEEN CHALLENGED BY FOUR GROUPS

The CFTC's unorthodox method of serving Ooki DAO raises another novel legal issue in the case. The CFTC sought and was awarded court approval to serve the DAO by posting the summons and complaint in the DAO's chat box on its website and on an online forum.

None of the putative defendants have appeared in the case and, so, none have responded to the complaint. Significantly, **friends of the court have stepped forward to file *amicus curiae* motions in opposition to the court's order granting the CFTC's motion for alternative service.**

To date, crypto legal consortium LeXpunK, the DeFi Education Fund, and venture capital firms Paradigm and Andreessen Horowitz, have all filed amicus briefs opposing the CFTC's motion to serve the token holders via an alternative method.

The briefs cast aspersions on the CFTC's method of services. For example, the LeXpunK brief argues that the CFTC's method of service failed to provide the putative defendants with sufficient notice of the lawsuit and, thus, falls short of what is required under traditional norms of due process under the U.S. Constitution.

The DeFi Fund and Paradigm argue that the CFTC cannot prove a violation has occurred based solely on the ownership of a DAO token. They both also argue that the CFTC has incorrectly characterized Ooki DAO as an "association" under the CEA.

Finally, Paradigm argues that the CFTC failed to satisfy requirements for service of process on Ooki DAO pursuant to California law. In its Consolidated Opposition, the CFTC countered that the CFTC's service method complied with applicable law and resulted in actual notice, that it is not required to serve all members of the Ooki DAO and that it has sufficiently alleged that Ooki Dao is an unincorporated association for purposes of alternative service.

A hearing took place on December 8, 2022. The Court suggested from the bench that he was inclined to accept that the CFTC had in fact properly served "the DAO," showing sympathy to the CFTC's stated concerns about allowing users to avoid regulatory enforcement by using the DAO structure. As of the date that this article was finalized, no ruling had been handed down. If the Court does allow the CFTC to move forward in this manner, lawyers involved in the matter have expressed skepticism that anyone will respond for "the DAO" and believe that the case will be resolved by a default judgment. The CFTC has stated that any judgment will only be enforceable as to "the DAO" but in its briefing left open the possibility that an injunction would apply to people involved in control of the DAO.

FINAL WORDS

- **The CFTC has put front and center the question of whether holders of Ooki DAO governance tokens who participated in DAO governance may be held liable for the (non-compliant) actions of the Ooki DAO.** We may see more of these types of enforcement actions as decentralized organizations continue to proliferate.

- In the unlikely event that the Court finds that the CFTC's service was insufficient, such a ruling could hobble the CFTC's lawsuit against the DAO. On the other hand, the CFTC could refile, but this time go after specific token holders who may be known to the CFTC – which could result in a worse outcome for certain putative defendants.

- **Assuming service is proper, if none of the token holders answer the CFTC's complaint, the court would likely enter a default judgment against the DAO.** It is unclear how the default judgment would be enforced against the Ooki token holders and how this would impact the DAO (and its token holders). Further, such default judgment would likely have a chilling effect on DAOs in the U.S. generally and, specifically, have the less than desired effect of suppressing token holder participation in DAO governance.

- The Ooki DAO's alleged failure to comply with KYC/AML rules could lead to coordinated enforcement action by OFAC and, potentially, other regulators.

ARTICLE IV

CRYPTO BANKRUPTCIES REVEAL FAULT LINES IN ASSET RECOVERY

SUJAY S. DAVÉ
PRINCIPAL
THE BRATTLE GROUP

DAVID ADLERSTEIN
COUNSEL
WACHTELL, LIPTON, ROSEN & KATZ

INTRODUCTION*

The crypto industry contains a wide variety of institutions and business models, including centralized and decentralized exchanges, hedge funds, brokers, decentralized autonomous organizations (DAOs), and bank-like entities.

Some are close analogues of traditional financial institutions, while others are altogether novel. As crypto prices plummeted in the first half of 2022, several centralized crypto institutions experienced financial distress, and their customers faced uncertainty about how asset recovery may occur in the event of bankruptcy.

This issue came into sharp relief as Celsius Network LLC, a company that offered customers interest-bearing crypto accounts, froze customer assets and filed for bankruptcy in July.

Celsius customers quickly discovered that their assets do not have the same level of protection expected of traditional financial institutions despite some similarities in products and services.

More recently, while the precipitating circumstances vary, the customers of crypto exchanges FTX and BlockFi find themselves in a similar predicament as the two entities froze customer assets and filed for bankruptcy in November.

In this article, we compare the protections customers are afforded in traditional U.S. financial institutions to those provided by similar institutions in the crypto space. We then discuss how asset recovery protections in the crypto ecosystem may evolve.

* The views expressed are the authors' and do not necessarily represent the views of their respective firms.

ASSET PROTECTION AT TRADITIONAL FINANCE INSTITUTIONS VERSUS CRYPTO BUSINESSES

Banks in the United States are generally considered safe and well-regulated places to keep savings. The U.S. has a dual banking system, with banks chartered either at the national level by the Office of the Comptroller of the Currency (OCC) or a state regulator. Bank holding companies and state-chartered Federal Reserve member banks are federally regulated by the Federal Reserve, and state-chartered banks that are not Federal Reserve members are federally regulated by the Federal Deposit Insurance Corporation (FDIC).

Banks are subject to comprehensive prudential supervision, including with respect to their capital, asset quality, management, earnings, liquidity, and sensitivity to market risk (the so-called "CAMELS"), as well as how they meet the needs of borrowers in their communities (e.g., under the Community Reinvestment Act).

If a bank fails due to an inability to meet obligations to depositors, the FDIC – established by the Glass-Steagall Act in 1933– steps in to ensure depositors get prompt access to their insured deposits.

Prior to Glass-Steagall, bank failures and bank runs were quite common. These days, in the event of a bank failure (the most recent wave of which came in the wake of the 2008 financial crisis), the FDIC acts in two capacities: as an insurer and a receiver.

As the "insurer" of a bank's deposits, the FDIC will, as a matter of last resort, pay deposit insurance to the depositors up to the insurance limit (although in most bank failures the FDIC usually arranges for a healthier financial institution to assume all of the deposits of the failed bank and frequently its assets as well, albeit subject to FDIC loss-sharing).

FDIC deposit insurance covers the balance of each depositor's account, dollar-for-dollar, up to the insurance limit (the standard amount being $250,000 per depositor), including principal and any accrued interest through the date of the insured bank's closing.

As the "receiver" of the failed bank, the FDIC assumes the task of collecting and selling the failed bank's assets and settling its debts, including claims for deposits in excess of the insured limit.

Meanwhile, assets held by broker-dealers – such as E-Trade, Vanguard, and TD Ameritrade – are covered by the Securities Investor Protection Act (SIPA). Aimed at protecting cash, investor funds, and most types of securities in the event of the failure of their broker, SIPA in 1970 established the Securities Investor Protection Corporation (SIPC), a federally mandated, member-funded nonprofit whose purpose is to expedite the recovery and return of customer assets during the liquidation of a failed broker-dealer.

SIPC provides protection up to $500,000, which includes a $250,000 limit for cash. SIPC only protects the custody function of the broker-dealer, meaning that SIPC works to restore to customers their securities and cash in their accounts with the brokerage when the firm liquidation begins. SIPC does not protect against the decline in value of securities or losses due to a broker's investment advice or recommendations.

These protections afforded to bank deposits and customer accounts at broker-dealers do not currently extend to assets held or custodied with centralized crypto institutions such as Celsius, which as a general matter do not have bank charters and are not operating as broker-dealers. While some centralized cryptoasset exchanges and custodians are subject to prudential supervision under state law (such as New York's "BitLicense" regime), their regulation is often limited to money transmittal licensure with the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN).

Traditionally, money transmitters – also known as money service businesses (MSBs) – are services that help individuals and businesses pay bills, make online purchases, and remit money to friends and family. Any business that issues money orders, traveler's checks, or other types of monetary value can be classified as an MSB; payment services like Square, Venmo, and PayPal are familiar examples.

Unlike banks and broker-dealers, money transmitters are largely regulated at the individual state level, and they operate without insurance protection like that of the FDIC or SIPC (although customer funds may have the benefit of FDIC insurance by virtue of arrangements established by a money transmitter with a bank). Many states require MSBs to post surety bonds – essentially a fixed guaranty amount by a third party – of varying amounts against defaults on an obligation in the event of insolvency, but even where in place, this protection may provide inadequate coverage to retail customers in the event of an insolvency.

FIGURE 1: ASSET PROTECTION WITH TRADITIONAL FINANCIAL INSTITUTIONS

	Banks	Broker-Dealers	Money Transmitters
Protection	Deposit insured by FDIC (federal government)	Brokerage account insured by SIPC	Surety bonds – varying amounts
Level of protection	$250,000	$500,000	Depends on state law
When funds become available after a failure	Usually no disruption	Usually 30 to 60 days	Varies widely by state

Sources: Pew Trusts, SIPC, Federal Reserve Board, SEC

WHAT HAPPENS WHEN A CRYPTO INSTITUTION GOES BANKRUPT?

Because crypto institutions are not protected by insurance like that of the FDIC or SIPC, recovery of customer assets in the event of bankruptcy will in most cases be administered – at least in part – in bankruptcy proceedings, with customers potentially having the status of unsecured creditors.

A look at the business models and recent bankruptcies of centralized cryptoasset lenders illustrates the fragile asset protections for customers of such institutions, and highlights the need for customers to proceed with care before determining to either lend to or use these centralized services to custody their cryptoassets.

Crypto Lenders

Among the many innovations accompanying the growth of "Decentralized Finance" (DeFi) in recent years is the emergence of centralized crypto lenders such as Celsius, which have offered remarkably high interest rates on deposits – in many cases, up to 20% annually.[1]

The business model for these lenders at a surface level resembles that of traditional banking. The provider accepts customers' deposited cryptoassets, offers a return, and rehypothecates the deposited cryptoassets, either lending them to borrowers at a higher rate or themselves participating in DeFi yield strategies.

1 Customer protections, associated with decentralized cryptoasset lending platforms are beyond the scope of this article.

Predictably, when the cryptoasset market crashed, this business model came under tremendous pressure, which was exacerbated by lacking prudential oversight.

As shown in Figure 2, the assets locked up in crypto lending protocols, such as Aave, Maker, and Compound, grew from essentially zero in 2020 to $50 billion by April 2022, at which point the market experienced a pronounced crash.

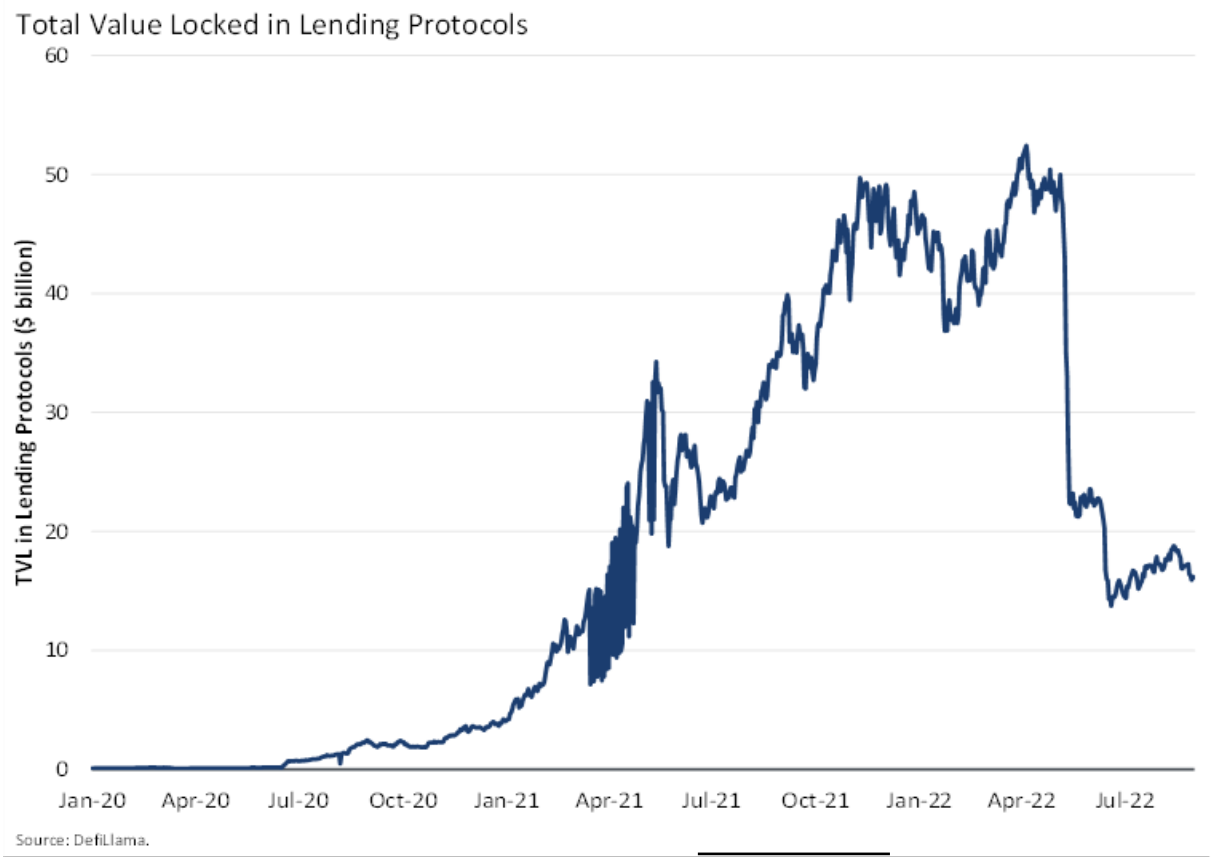
Despite having facial similarities to traditional banking, crypto lending platforms are not regulated like traditional banks and can engage in a variety of return-seeking strategies (such as highly concentrated lending to a small number of counterparties) that are unavailable to traditional brick and mortar banks, including by not having to abide by CAMELS requirements imposed by banking regulation.

Prominent among these is the lending platform Celsius that declared bankruptcy on July 14, 2022, shortly after freezing all customer assets and blocking withdrawals.

Celsius described itself as "a platform of curated services that have been abandoned by big banks – things like fair yield, zero fees, and lightning quick transactions."[2] Essentially, customers would deposit their crypto assets on the platform, and Celsius would deploy those assets to various return strategies, promising yields as high as 17%.

Unlike a bank deposit, however, Celsius described in its terms of service that customer deposits are controlled by Celsius and, in essence, a loan to Celsius.[3] Celsius aimed to generate those returns through institutional lending (to exchanges, hedge funds, and other counterparties), retail lending (allowing customers to borrow stablecoins, which are digital assets pegged to "stable" reference assets, like the U.S. dollar), "yield farming" through which crypto investors earn yield by lending and "staking" (i.e., locking up through a smart contract) crypto for interest and other rewards, deploying crypto in decentralized finance protocols, cryptoasset mining, and proprietary hedge fund-like trading strategies.

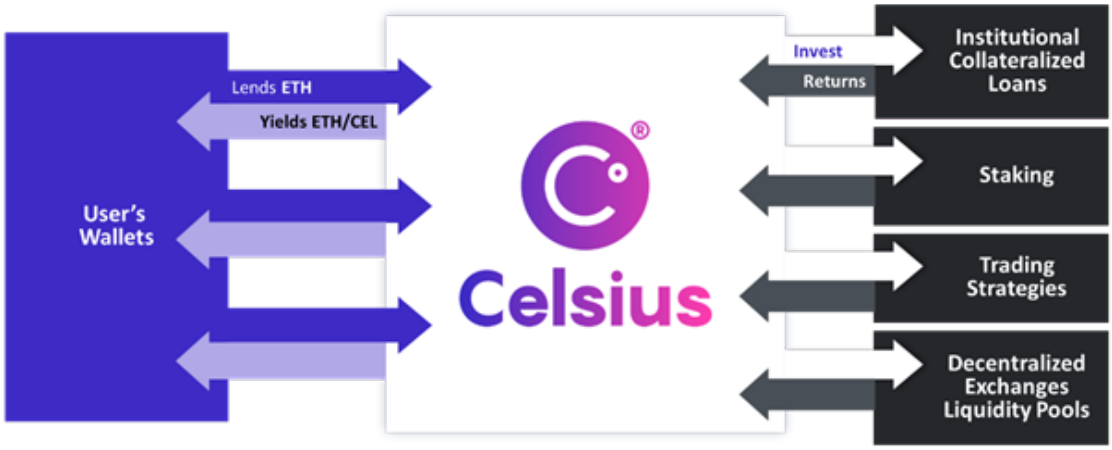
FIGURE 2: DEPOSITS AT CRYPTO LENDERS (2020 – 2022)



2 FT. (2022, June 13). Celsius/cryptos: heat is on. Retrieved from Financial Times: https://www.ft.com/content/98a250fa-bebb-4269-97fe-605be597b2e7

3 Celsius. (2022, April 14). Terms of Use. Retrieved from Celsius: https://celsius.network/terms-of-use

FIGURE 3: CELSIUS BUSINESS MODEL



Celsius also sold a native token, CEL, and promised a higher yield to customers if they accepted the yield in CEL. Celsius also offered a plain vanilla wallet function whereby customers could simply store their digital assets, not receive yield. Unfortunately for these customers, Celsius evidently commingled custodial assets with assets that were lent to them, and apparently did not establish legal arrangements to insulate custodial assets from being reachable by Celsius's general creditors.

This year's sharp decline in the price of crypto assets frankly blew up Celsius's model. As cryptocurrency prices plummeted, Celsius suffered from trading losses, liquidations, major counterparty failures, and losses on under-collateralized loans, among other issues.[4] When it reached the point where it was unable to meet obligations, on June 13 Celsius froze withdrawals. According to its bankruptcy filing, Celsius owes its customers more than $4.7 billion.[5]

As noted, Celsius is neither a bank nor broker-dealer despite having a business model sharing some attributes of both, which means its customers do not have the benefit of FDIC or SIPC insurance or the receiver/trustee role the FDIC and SIPC can play in a liquidation. The treatment of depositors in the Celsius bankruptcy case ultimately depends on the outcome of pending litigation.

If Celsius depositors are treated as unsecured creditors or investors, they will not receive preference treatment in the liquidation, which would prioritize their claims over other Celsius creditors. Among many issues likely to be considered by the court is the extent to which depositors' funds were commingled with those of Celsius and the interpretation of the terms of service agreed to by customers.

Crypto exchanges

Centralized cryptocurrency exchanges – probably the most widely familiar type of crypto institution – are platforms for custodying and trading cryptocurrency that operate 24 hours a day, seven days a week. There are hundreds of exchanges globally, with some of the more well-known in the U.S. including Coinbase, Kraken, and Gemini. These exchanges offer a simple custodial wallet function allowing customers to trade one cryptocurrency for another – e.g., Bitcoin for Ether – or to buy crypto using U.S. dollars.

Customers can also maintain dollar-denominated or stablecoin-denominated balances. Customers deposit their fiat and crypto assets directly with crypto exchanges, which take custodial control of the assets.

Crypto exchanges operating in the U.S. are commonly registered as money transmitters. This means that, in order to operate, they have registered individually with each of the states in which they have customers. Crypto exchanges are not registered as broker-dealers at present, despite some similarities in function, and they are not registered as banks.

4 Arkham, "Report on the Celsius Network" (July 7, 2022), https://www.arkhamintelligence.com/reports/celsius-report

5 Atkins, J. (2022, July 19). Celsius owes $4.7B to customers as the first bankruptcy hearing takes place. Retrieved from Coingeek: https://coingeek.com/celsius-owes-4-7b-to-customers-as-first-bankruptcy-hearing-takes-place/

Thus, customer assets are not protected by SIPC or FDIC insurance (although, as noted earlier, some cryptoasset exchanges are subject to state-level prudential supervision; for instance, Coinbase and Gemini each have a New York "BitLicense").

Coinbase created a stir when, pursuant to a Staff Accounting Bulletin promulgated by the Securities and Exchange Commission (SEC),[6] it noted in its Q1 2022 Form 10-Q that customers with assets on the exchange would be given similar treatment as general unsecured creditors in the event of a bankruptcy:

Moreover, because custodially held crypto assets may be considered to be the property of a bankruptcy estate, in the event of a bankruptcy, the crypto assets we hold in custody on behalf of our customers could be subject to bankruptcy proceedings and such customers could be treated as our general unsecured creditors.[7]

If the past is any indication, customers of bankrupt crypto exchanges are likely to face a frustrating and lengthy process for customers seeking asset recovery. Mt. Gox, once the largest crypto exchange in the world, filed for bankruptcy after a hack in 2014 resulted in the theft of 850,000 Bitcoins – now worth billions of dollars. Eight years later, Mt. Gox's creditors have yet to receive any recovery of the lost funds. The bankruptcy process is still ongoing, and there are signs that creditors may receive some form of recovery, but the timing remains unclear, as does the amount or form of any recovery (i.e., U.S. dollars or Bitcoin).[8]

HOW ASSET RECOVERY IN THE CRYPTO ECOSYSTEM MAY EVOLVE

In its Staff Accounting Bulletin No. 121, released on April 11, 2022, the SEC noted that the lack of legal precedent and regulatory protections means that the treatment of arrangements between customers and crypto platforms will be decided in court proceedings. SEC Chief Gary Gensler echoed this at the 2022 Annual FINRA Conference in May, saying of crypto lending platforms, "The investing public is not that well protected. If the platform goes down, guess what? You just have a counterparty relationship with the platform. Get in line in bankruptcy court."[9]

After years of inaction from regulators, legislators, and litigators alike, the crypto landscape appears to be at an inflection point, with numerous items of proposed Federal legislation and intensified focus at the most senior levels of the U.S. government in the wake of President Biden's Executive Order of March 9, 2022 on "Ensuring Responsible Development of Digital Assets."

Based on the bitter experience of Celsius and its ilk, it seems clear that customers would greatly benefit from companies that hold cryptoassets for customers clearly stating the capacity in which it holds the assets — whether as principal (meaning the customer is an unsecured creditor); as regulated custodian (whereby the assets are held by a regulated financial institution responsible for safekeeping); or in an unregulated intermediary capacity, as governed by contract law.

In the first scenario, the customer is fully exposed to default risk—which poses consumer protection concerns, and depending on the facts, could require a cryptoasset lender to register its offerings as securities with the SEC—but at least the customers understand the risk at the outset.

6 https://www.sec.gov/oca/staff-accounting-bulletin-121

7 Coinbase Global, Inc., SEC Form 10-Q, March 31, 2022, p. 83

8 Kharif, O. (2022, July 7). Mt. Gox Creditors Inch Closer to Repayment as Bitcoin Dump Looms. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2022-07-07/mt-gox-creditors-inch-closer-to-repayment-as-bitcoin-dump-looms

9 Stein, Philip R. (2022, May 27). Crypto Companies, Investors Await Looming Regulations and Litigation Resolutions. Retrieved from JD Supra: https://www.jdsupra.com/legalnews/crypto-companies-investors-await-1522030/

In the second scenario, the custodied assets belong to the customer under existing regulations, and the custodian must comply with rigorous requirements for regulated custodians, such as the Investment Advisers Act of 1940 or applicable banking laws and regulations.

The third scenario presents a current gap in the law. One means of closing it would be the adoption of proposed amendments to the Uniform Commercial Code (UCC) related to digital assets to separate retail investor assets from bankruptcy estate assets, thereby preventing the commingling of assets deposited for purely custodial purposes with assets deposited through a yield-bearing product. The proposed amendments clarify that a customer retains ownership of cryptoassets held by a securities intermediary, such as an unregulated custodian (subject to satisfaction of certain requirements), even in the event of the intermediary's insolvency.

***

The mantra "not your keys, not your coins" is often heard in cryptoasset space, meaning that irrespective of beneficial ownership, whoever holds the cryptographic keys that control the digital assets actually have control of the assets. However, self-custody remains a challenging task for many rank and file users. As a matter of public benefit, as well as preserving the integrity of markets and avoiding contagion in a downturn scenario, customers should be able to custody their cryptoassets with third party professionals with a clear understanding of their legal rights in a scenario of counterparty distress. Industry and customers alike must internalize the lessons of recent experience if crypto markets are to thrive going forward.

The authors would like to thank Shubham Dubey, Milo Levine, Paula Jaramillo and Andrea Tinianow for their input on this article.

ARTICLE V

DEVELOPING AN INNOVATIVE AND RESPONSIBLE DIGITAL ASSET ECOSYSTEM: PERSPECTIVES FROM SINGAPORE

PAUL YUEN
GENERAL COUNSEL
MONETARY AUTHORITY OF
SINGAPOORE (MAS)

ABSTRACT

The rapid pace of digital developments has fuelled innovation and the emergence of new business models in the financial sector. Conventional models of financial services are now exploring the potential benefits of decentralised finance (DeFi) through distributed ledger technology (DLT).

DLT can enable more efficient transactions and robust records, with greater opportunities for digital assets ecosystem. MAS has been exploring potential DLT use cases with the financial community, providing appropriate enablers along with suitable safeguards.

Beyond facilitating experiments involving new technology and business models, policies and legislation have been reviewed and refreshed over the past few years to adapt to the evolving financial landscape. Measures have been taken to address the potential risks, including those seen in the cryptocurrency markets.

INTRODUCTION

Over the past 2 decades, the global financial system has undergone significant changes. Beyond global regulatory reforms implemented in response to the global financial crisis, innovations in technology and business models presented many new opportunities as well as challenges and risks. For instance, the emergence of crowdfunding or peer-to-peer lending platforms has enabled non-bank entities to intermediate the funding needs of businesses and social enterprises through the crowd[1].

There is potential to streamline these business models further through automated applications built on DLT, enabling settling and recording of transactions on a real-time basis.

The developments in DLT coupled with cryptography and the ability to tokenise different forms of assets[2], claims and instruments will underpin the growing digital asset[3] ecosystem.

1 Traditionally, business enterprises often obtain financing directly from banks. Some may engage banks (or other financial institutions) to raise funds from private or public markets.

2 This enables assets to be fractionalised and monetised.

3 Digital assets represent anything of value the ownership of which is represented in digital form through a process of tokenisation. The potential use cases of tokenisation include cash, securities, carbon credits, and even physical assets such as property and art work.

The process of tokenisation in a distributed ledger provides opportunity for transformation in existing processes and arrangements in the financial sector – facilitating more efficient transactions, enhancing financial inclusion and potentially unlocking economic value.

These innovations, which are rapidly gathering momentum, can profoundly re-shape the current financial landscape.

They can improve the public's access to financial services and enhance the robustness and efficiency of financial services and transactions. At the same time, these innovations present issues in private law that need to be better understood and discussed. There is also a growing and urgent need to address the risks that are amplified through these new architectures.

MAS' ROLE IN REGULATION AND INNOVATION

As central bank and integrated supervisor of the financial services sector in Singapore with a mandate to foster a sound, reputable and competitive financial centre[4], the Monetary Authority of Singapore (MAS) cultivates high standards of governance and practice among financial institutions through ongoing supervisory engagements and regular reviews and adaptation of rules, policies and guidance to respond to emerging risks and trends. At the same time, **MAS collaborates with industry stakeholders to harness the innovative and productive use of financial technology (FinTech) as part of its broader effort to transform the financial services industry**.

This balance is evident from industry collaborations and regulatory reviews undertaken within the past few years, such as (i) Project Ubin, (ii) Project Guardian, (iii) Regulatory Sandbox, (iv) Review of payments legislation; and (v) Engagements and Regulatory guidance on crypto-related developments.

(I) Project Ubin – Exploring more efficient alternative systems built on DLT

MAS launched a multi-year and multi-phase industry collaboration in 2016 to explore the use of DLT for clearing and settlement of payments and securities transactions, producing reports on lessons learnt at the conclusion of each phase[5]:

a. Phase 1: Tokenised Singapore Dollar (SGD) (2016-2017) – Participants evaluated the business, technology and economic factors involved in developing a proof-of-concept to conduct inter-bank payments facilitated by DLT.

b. Phase 2: Re-imagining Real-time Gross Settlement (RTGS) System using DLT (2017) – A consortium of financial institutions and technology partners led by MAS and the Association of Banks in Singapore (ABS) successfully developed a prototype comprising 3 different models[6] for decentralised inter-bank payment and settlements with liquidity savings mechanisms. The consortium considered ways to address the need for transactional privacy and deterministic finality in performing multilateral netting in a decentralised manner.

4 Section 4 of the Monetary Authority of Singapore Act 1970 (MAS Act) sets out the principal objects and functions of MAS.

5 The summary and reports are accessible at https://www.mas.gov.sg/schemes-and-initiatives/Project-Ubin.

6 Prototypes were developed on 3 leading DLT platforms: Corda, Hyperledger Fabric and Quorum to explore the different models.

c. Phase 3: Delivery versus Payment (DvP) on DLT (2018) – Together with MAS, Singapore Exchange (SGX) developed DvP for settlement of tokenised assets using DLT, seeking to achieve interledger connectivity and settlement finality for Singapore Government Securities (SGS) and cash depository receipts (CDRs) on separate DLTs. Besides compressing the settlement cycle, smart contracts for DvP can enable consistent and coherent implementation of rights and obligations.

d. Phase 4: Cross-border Payment versus Payment (PvP) (2018-2019) – This industry collaboration between Canada, United Kingdom and Singapore examined the challenges and frictions in cross-border payments and explored alternatives for new and more efficient models to process cross-border transactions.

e. Phase 5: Enabling Broad Ecosystem Opportunities (2020) – This final phase of Project Ubin saw the successful development of a domestic multi-currency payments network prototype that addressed immediate business needs for cross-currency exchange and foreign currency transactions[7]. It demonstrated the clear value for using DLT and the potential for adapting it as an international settlement model that could lead to cheaper, faster and safer cross-border payments.

Some industry participants have built on their experiences from Project Ubin. Partior, for instance, provides a blockchain-based platform that enables participants around the world to transact with one another in real time using digitised commercial bank money[8].

MAS' digital currency connectivity progressed, with MAS collaborating with the Bank for International Settlements Innovation Hub Singapore Centre (BIS Hub)and a few central banks in Project Dunbar[9].

Building on these experiences, MAS launched Ubin+ on 3 November 2022 to expand its collaboration with international partners on cross-border foreign exchange (FX) settlement using wholesale central bank digital currency (CBDC). This will encompass various projects that explore the exchange and settlement of participating countries' wholesale CBDCs with an automated market maker arrangement; the interoperability of DLT and non-DLT payment systems[10]; and connectivity across heterogenous digital currency networks.

MAS has also announced a joint experiment with the Federal Reserve Bank of New York's New York Innovation Centre to investigate how wholesale CBDCs could improve efficiency of cross-border wholesale payments involving multiple currencies[11].

While MAS does not see a compelling need for a retail CBDC in Singapore at this juncture[12], MAS has embarked on Project Orchid – a partnership with the financial industry to develop the infrastructure and technical competencies necessary to issue a digital Singapore dollar, should the need arise in future[13].

7 Various use cases were discussed with relevant industry experts and partner organisations to identify the benefits of integrating use cases with a DLT-based payments network. These use cases are broadly categorized into 4 areas: (a) capital markets; (b) trade and supply chain finance; (c) insurance; and (d) beyond financial services.

8 A new blockchain-based payments platform backed by a few banks, Partior is achieving end-to-end settlements in Singapore dollars and US dollars of less than 120 seconds through an "atomic" clearing and settlement model that replaces the sequential operational approach to payments settlements. This enables it to provide a better alternative for wholesale settlements by banks, which takes an average of 2 days to complete.

9 These comprise Reserve Bank of Australia, Bank Negara Malaysia and the South African Reserve Bank. The project demonstrates that financial institutions across different countries can transact directly with one another on a common multi-CBDC platform using CBDCs issued by participating central banks, enabling cheaper and faster cross-border payment transactions. A copy of the report for Project Dunbar is accessible at https://www.mas.gov.sg/-/media/MAS-Media-Library/development/fintech/Dunbar/Project_Dunbar_Report_2022.pdf.

10 MAS is participating in SWIFT's CBDC Sandbox together with 17 central banks and global commercial banks. SWIFT is the Society for Worldwide Interbank Financial Telecommunication, a Belgian cooperative society that facilitates the execution of financial transactions and payments between banks.

11 The media release can be accessed at https://www.mas.gov.sg/news/media-releases/2022/new-york-fed-and-monetary-authority-of-singapore-collaborate-to-explore-potential-enhancements-to-cross-border-payments-using-wholesale-cbdcs.

12 Link to "A Retail Central Bank Digital Currency: Economic Considerations in the Singapore Context" (November 2021): https://www.mas.gov.sg/-/media/MAS/EPG/Monographs-or-Information-Paper/A-retail-CBDC---Economic-Considerations-in-the-Singapore-Context.pdf.

13 Information on the report detailing potential uses of digital SGD and Project Orchid is accessible at https://www.mas.gov.sg/news/media-releases/2022/mas-report-on-potential-uses-of-a-purpose-bound-digital-singapore-dollar.

(II) Project Guardian – Piloting use cases in Digital Assets

With the useful insights and experiences from Project Ubin, MAS announced the commencement of Project Guardian in May 2022. This is a collaborative initiative with the financial sector that explores the economic potential and feasibility of use cases involving asset tokenisation and DeFi – the process of digitally representing assets or items of value through a smart contract on a blockchain.

This enables financial and real economy assets to be fractionalised and exchanged over the internet on a peer-to-peer basis. Use cases are being developed in 4 main areas, comprising (i) open, interoperable networks; (b) trust anchors; (iii) asset tokenisation; and (iv) institutional grade DeFi protocols[14]. The first industry pilot saw live trades executed on FX and government bond transactions against liquidity pools comprising tokenised Singapore Government securities bonds, Japanese Government bonds, Japanese Yen and Singapore dollar[15].

More industry pilots have been launched to explore a wider range of use cases.

(III) FinTech Regulatory Sandbox – Facilitating Experimentation in Live Environment

The FinTech Regulatory Sandbox[16] serves as an important enabler for financial institutions and FinTech players to experiment with innovative technology in a live environment within a well-defined space and duration. MAS launched this framework in 2016, recognising that some industry players seeking to introduce innovative models or solutions may not be able to adhere to all applicable rules from the start.

The perimeters and conditions imposed by MAS for the sandbox period are customised according to the objectives and needs of the relevant sandbox entity.

This framework was enhanced with Sandbox Express in 2019 to provide a faster option for market testing under pre-defined conditions. MAS announced further refinements in November 2021 through the Sandbox Plus, incorporating expanded eligibility criteria to include early adopters of technology innovation, streamlined application with financial grant[17], and participation in Deal Fridays[18].

(IV) Review of Payments Legislation

During this period, the legislative and regulatory framework for payments has been subject to regular reviews. These reviews proceeded in tandem with efforts to harness the benefits of innovation continue.

Following a review of the payments landscape and public consultations between 2016 and 2018, MAS proposed a new Payment Services Bill in November 2018 with the objective of providing a more conducive environment for innovation in payment services whilst ensuring that risks across the payments value chain are mitigated.

The Bill sought to streamline existing payment-related legislation[19] and expand the scope of regulated payment services to include digital payment token (DPT)[20] service. This would cover dealing in or facilitating the exchange of DPTs. This Bill was passed in Parliament in January 2019 and came into force in January 2020.

14 These include potential DeFi applications in wholesale funding markets through the creation of permissioned liquidity pool comprising tokenised bonds and deposits.

15 The media release can be accessed at https://www.mas.gov.sg/news/media-releases/2022/first-industry-pilot-for-digital-asset-and-decentralised-finance-goes-live.

16 Link to "Overview of Regulatory Sandbox" at https://www.mas.gov.sg/development/fintech/regulatory-sandbox.

17 This facilitated faster time-to-market, enabling applicants to be more market-ready when they graduate from the regulatory sandbox.

18 A platform for deal-making opportunities, giving sandbox entities access to external investor community to enable them to benefit from the network, mentorship and funding.

19 By combining the Payment Systems (Oversight) Act and the Money-changing and Remittance Businesses Act.

20 Cryptocurrencies fall within the definition of DPT.

This also marked the introduction of rules relating to digital payment token services, including requirements to address ML/TF risks in cryptocurrency-related activities[21].

Further amendments were passed in Parliament in January 2021 to implement enhanced international standards adopted by the Financial Action Task Force (FATF)[22]. This strengthens MAS' levers to address ML/TF risks by expanding the scope of DPT services to include (i) facilitating the transmission of DPTs from one account to another, (ii) custodial services for DPTs, and (iii) facilitating the use of DPTs for payment even where the service provider does not come into possession of the moneys or DPTs involved.

In addition, the amendments enable MAS to impose user protection measures on DPT service providers when necessary. This includes requiring service providers to segregate customer assets from their own assets. MAS would also be empowered to impose additional measures on service providers to maintain stability in Singapore's financial system, safeguard the efficacy of the monetary policy or where it is in the public interest to do so.

MAS recognises that with the borderless operating environment, service providers can engage in regulatory arbitrage by structuring their businesses to evade regulation.

For instance, service providers established in Singapore may structure their businesses such that services are provided in another market where such activities are not regulated, thereby evading regulation. A new Bill[23] was passed in Parliament in March 2022 providing, inter alia, that digital token service providers created in Singapore will be regulated by MAS even if they provide such services outside Singapore[24].

(V) Engagements and Regulatory Guidance on crypto-related developments

While cryptocurrencies are not legal tender and have no fundamental value, they are an accepted medium of exchange in distributed networks. The growing popularity of cryptocurrencies in recent years has triggered a proliferation of initial coin offerings (ICOs). The increase in such fund raisings without sufficient disclosures to, and understanding by, the general public raised consumer risks.

ICOs are also susceptible to money laundering and terrorist financing risks. Against this backdrop, MAS provided guidance on 1 August 2017, clarifying the regulatory treatment of digital tokens[25]. MAS highlighted the potential regulatory implications if the digital token constitute digital payment tokens under the Payment Services Act 2019 or capital markets products under the Securities and Futures Act 2001.

21 This includes the "travel rule" for cryptocurrencies which is set out in MAS Notice PSN02, accessible at https://www.mas.gov.sg/-/media/MAS-Media-Library/regulation/notices/AMLD/psn02-aml-cft-notice---digital-payment-token-service/Notice-PSN02-last-revised-on-1-March-2022.pdf.

22 FATF adopted enhanced standards for virtual asset service providers (VASPs) in 2019. FATF has defined a virtual asset as a digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes. VASPs are defined by FATF to include persons carrying on a business of conducting one or more of activities that involve (i) exchange between VA and fiat currencies; (ii) exchange between one or more forms of VA; (iii) transfer of VA; (iv) safekeeping and/or administration of VA or instruments enabling control over VA; and (v) participation in and provision of financial services related to an issuer's offer and/or sale of VA.

23 The Financial Services and Markets Bill 2022 provides for a financial sector-wide approach in specific areas that are pertinent across the financial sector (e.g. technology risk management), complementing MAS' existing entity and activity based regulation.

24 The FSM Bill aligns the scope of "digital token services" (DTS) to the enhanced FATF standards.

25 "MAS clarifies regulatory position on the offer of digital tokens in Singapore" [http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx].

While prices of cryptocurrencies have increased over the past few years, they have not performed well as a medium of exchange or a store of value due to the significant volatility in their prices.

Cryptocurrencies have taken a life of their own outside the blockchain and been subject to heavy speculation. MAS has consistently warned the public about the risks of trading in cryptocurrencies since 2017, highlighting that cryptocurrencies are highly risky and not suitable investment for retail public, as the prices are subject to sharp speculative swings. Following MAS' observation that some DPT service providers were actively promoting their services through various channels, MAS issued guidelines on 17 January 2022 setting out its expectations that DPT service providers should not promote their DPT services to the general public in Singapore[26].

The events leading to the "crypto winter" in the first half of 2022[27] have resulted in losses to many investors and uncovered weaknesses and abuses in existing market practices, validating MAS' concerns and reinforcing the need for standards and practices in the cryptocurrency market to be tightened. Globally, international standards bodies[28] and a number of financial regulators in major jurisdictions are reviewing the necessity of legislative interventions to address the risks involved in such activities, including concerns from market integrity and potentially financial stability perspectives.

The Financial Stability Board (FSB) on 11 October 2022 published a consultation paper setting out proposals for the international regulation of crypto-asset activities. These comprise recommendations to:

(a) promote the consistency and comprehensiveness of regulatory, supervisory and oversight approaches to crypto-asset activities and markets and strengthen international cooperation, coordination and information sharing; and

(b) revise high-level recommendations for the regulation, supervision and oversight of "global stablecoin" arrangements to address associated financial stability risks more effectively.

These recommendations are grounded in the principle of "same activity, same risk, same regulation". Regulation should also take account of novel features and specific risks of crypto-assets and address potential financial stability risks that could arise from the growing interlinkages between the crypto-asset ecosystem and the traditional financial system.

PROPOSED MEASURES TO REDUCE RISKS TO CONSUMERS FROM CRYPTOCURRENCY TRADING ACTIVITIES

MAS has similarly been reviewing these issues taking into account (i) money laundering risks, (ii) technology risks, (iii) consumer protection risks, (iv) market integrity risks and (v) financial stability risks emanating from cryptocurrency trading activities. Steps have been taken, through earlier legislative reforms, to address the first 2 risks.

26 https://www.mas.gov.sg/news/media-releases/2022/mas-issues-guidelines-to-discourage-cryptocurrency-trading-by-general-public. DPT service providers cannot engage in marketing or advertising activities in public or through engagement of third parties (e.g. influencers). They may only market or advertise on their own corporate websites, mobile applications or official social media accounts.

27 The collapse of TerraUSD and LUNA result in significant investor losses, triggering the bankruptcies of a number of crypto firms and precipitating domino effects through the crypto industry.

28 These include the International Organisation of Securities Commissions and Financial Stability Board.

As for the other risks, besides repeated warnings to the public and financial education programmes, the recent amendment to the Payment Services Act 2019 empowers MAS to impose user protection measures to protect consumers and additional measures to maintain stability of Singapore's financial system, if needed[29].

To address the risks arising from the speculative activities relating to cryptocurrencies, MAS issued a consultation paper on 26 October 2022 proposing measures to reduce risks to consumers from cryptocurrency trading.

These are broadly grouped into consumer access measures[30], business conduct measures[31], technology and cyber measures[32] and market integrity measures[33]. The consultation will remain open till 21 December 2022. MAS intends to issue Guidelines as a first step to implementing the proposals.

29 The Amendment Bill was passed in January 2021.

30 MAS intends to apply the measures to retail investors. Comments are sought on the value of DPT holdings that should count towards the status of an investor (as a retail or accredited investor), and the proposal to assess an investor's knowledge of the risks of DPT services. MAS also proposes to restrict DPT service providers from offering of incentives as well as retail investors' use of credit or leverage in DPT transactions.

31 MAS proposes to introduce business conduct standards for DPT service providers in key areas of concern. These include segregation of customers' assets, risk management controls for customers' DPTs, restrictions on lending out retail customers' DPTs, and measures to identify and mitigate conflicts of interest. MAS also invites comments on a proposal for DPT trading platform operators to publish their policies and procedures for selecting, listing and reviewing DPTs, and the proposed complaints handling policies and procedures.

32 Among other requirements, MAS proposes to require DPT service providers to maintain high availability and recoverability of critical IT systems that they use to support their services.

33 While DPTs are represented on a blockchain, most DPT transactions are in fact conducted through providers that facilitate trade matching. Noting that DPT markets have been susceptible to unfair trading practices, which distort price discovery and undermine customers' trust and confidence in the functioning and integrity of DPT markets, MAS invites comments on effective systems, procedures and arrangements that should be implemented by DPT trading platform operators to promote fair, orderly and transparent trading of DPTs. These include measures to detect and deter unfair trading practices.

PROPOSED MEASURES TO ENHANCE STANDARDS OF STABLECOIN-RELATED ACTIVITIES

Globally, regulators (including in US) have started conversations on the need and possible forms of regulation for stablecoins, including those built on existing banking and e-money frameworks. While cryptocurrencies may not be suitable as a medium of exchange for transactions in a digital asset ecosystem, MAS sees potential in stablecoins performing this role if they are well-regulated and backed by arrangements that provide a high degree of assurance of value stability. To this end, MAS has issued a consultation paper on 26 October 2022 setting out the proposed regulatory approach for stablecoin-related issuance and intermediation activities[34].

MAS proposes to regulate the issuance of stablecoins which are pegged to a single currency (SCS), where the value of SCS in circulation exceeds S$5 million. The key proposals[35] relate to:

- Value stability – SCS issuers are to hold reserve assets (in cash, cash equivalents or short-dated sovereign debt securities) of at least 100% of the value of the outstanding SCS in circulation, to facilitate redemption at par on a timely basis following any redemption request;
- Reference currency – These could take the form of Singapore dollar or any Group of Ten (G10) currencies;
- Disclosures – SCS issuers are to publish a white paper disclosing the details of the SCS, including the redemption rights of stablecoin holders;
- Prudential standards – SCS issuers are to comply with base capital and solvency requirements as well as restrictions on undertaking other businesses.

34 Besides such stablecoins issued by non-banks, MAS considers that banks may also issue stablecoins as a liability against their balance sheet to perform a similar function. This consultation will similarly close on 21 December 2022.

35 Further details are set out in the consultation paper which is accessible at: https://www.mas.gov.sg/publications/consultations/2022/consultation-paper-on-proposed-regulatory-approach-for-stablecoin-related-activities.

MAS proposes not to impose additional reserve backing and prudential requirements on banks that issue SCS by tokenizing liabilities of the bank since banks are already subject to stringent risk-based capital and liquidity requirements.

MAS' proposed regulatory approach to stablecoins is guided by MAS' support for the development of value-adding payment use cases for stablecoins, the adoption of a progressive regulatory approach that is fit for purpose and facilitates stepping up (if needed), and MAS' desire to maintain an open regime to accommodate different forms of stablecoins, including those issued by banks.

CHARTING THE PATH AHEAD

These public consultations are part of MAS' ongoing effort to develop an innovative and responsible digital asset ecosystem in Singapore. Technology will continue to re-define, re-shape and transform the delivery of financial services and products. Globally, the international community[36] is starting to consider how to regulate DeFi. DeFi raises novel questions that need to be addressed. MAS is on the same journey of inquiry.

Beyond the risks that regulators, including MAS, seek to address, there are undoubtedly opportunities that can be harnessed through various possible use cases that leverage on distributed ledger technology. MAS will continue to collaborate with industry partners and the global community to develop a vibrant digital asset ecosystem.

36 This includes international standards setting bodies (e.g. FSB, IOSCO, OECD) and financial regulators across developed jurisdictions.

ARTICLE VI

SMART CONTRACTS AND "CODE IS LAW" - SOME ADDITIONAL CONSIDERATIONS

JAKE VAN DER LAAN
CHIEF INFORMATION OFFICER & DIRECTOR
FINANCIAL AND CONSUMER SERVICES COMMISSION
NEW BRUNSWICK, CANADA (FCNB)

INTRODUCTION

I read with interest the article entitled "Can Code be Law? A Review of Current Developments", published in the second edition of this Journal [JM22]. The authors set out a few differing perspectives on the question of how to go about understanding what a smart contract is and then discuss a number of issues which are surely to arise should some form of contract formation automation become more widely adopted.

As part of their discussion, the authors postulate a potential future computer based system which automates the intermediation of the creation of a "meeting of the minds" between two contracting parties. In this envisioned system parties would start the contract creation process by entering their respective proposed contractual terms into a portal (a computer front end interface). [1]

These terms would then be reviewed and confirmed by the respective parties in some way[2], and upon the completion of such confirmation a (smart) contract would be computationally generated[3] and immutably committed to a blockchain.

The authors point out a number of practical and legal obstacles to the actual creation and implementation of such a "contract synthesizer", including the inherent inflexibility of an automated contract creation process to fully include all the various potential dimensions of a contract, the potential (if not the likelihood) of software bugs, the inability of the parties to understand, and thus properly accept, how the software which creates the digital contract actually works[4], and last but not least, the inability to readily change, update, renew or cancel a contract immutably committed to a blockchain.

All of these are valid points.

I wish to make two, what I believe to be important, additional comments with respect to the proposed creation of these types of systems on the blockchain.

First, although there is no question that how we form and execute contracts will continue to evolve [Kla22], and that we may very well see the automation of various aspects of the contract creation and execution processes in the future, we need to bring a certain practical realism to our sense of the capacity of decentralized smart contract platforms being able to support these types of complex synthetic contracting systems.

This realism also requires we articulate more precisely and objectively what is meant by a "smart contract" insofar as that term is used in the context of decentralized blockchain based implementations.

Secondly, as we explore the creation of these types of mechanisms, we need to more fully appreciate the role that our existing broader contract law framework plays in the maintenance of the rule of law in our society generally, and that the unabated automation of contract enforcement may bring unintended consequences.

Let's start with "rightsizing" the smart contract.

DEFINING THE SMART CONTRACT

The term "smart contract" was first coined by Nick Szabo, a computer scientist and lawyer, in 1997 [Sza97]:

"A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart-contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimise exceptions both malicious and accidental, and minimise the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs."

Since this initial limited "executive" definition, the idea of what constitutes a smart contract has expanded to a host of differing meanings now employed within the blockchain technology ecosystem and its various observers. Regrettably, it appears that some of these definitions have been fueled by ideologically driven statements like the one found on the website of the Ethereum Classic platform (see also the introductory comments in [WC17]):

Unlike the legal jurisdictions that exist today that are regularly manipulated by the whims of the powerful, future virtual jurisdictions will be governed by the principle of Code is Law, meaning that for the first time, humanity can operate under actual, as opposed to the guise of, Rule of Law, codified not in esoteric and misinterpretable legal texts, but in pure mathematics. Code is Law is made possible by blockchain technology, and is a straightforward concept that keeps these virtual jurisdictions sovereign. It means that the code of a Smart Contract is the ultimate arbiter of the outcome of an onchain interaction, as opposed to some overriding force from outside the network. As a result, applications are unstoppable, and run exactly as programmed without downtime, censorship or third party interference.[5]

Other more ideologically tepid, but nonetheless enthusiastic articulations of what constitutes a smart contract in the context of blockchain technology, include:

- "... self-executing electronic instructions made in computer code that lead to a contractual agreement between two parties." [Per19]

- "... agreements wherein execution is automated, usually by computers. Such contracts are designed to ensure performance without recourse to the courts. Automation ensures performance, for better or worse, by excising human discretion from contract execution." [Ras16]

- "... legally binding agreements with the impossibility of breach." [Sav17]

- "... an agreement among multiple parties written at least in part in computer code." [Vig21]

- "... the computational encoding of a contract's terms into the ledger's operations, which are then automatically executed on the occurrence of predefined triggers without reliance on third parties to enforce the bargain." [Yeu17]

- "... aim at removing the human factor from decision making. The human factor is often proven to be the most error-prone and unreliable element of the standard, traditional contracts." [Rub20]

• ”A major difference between a traditional contract and a so-called smart contract, is that contracts create enforceable obligations, whereas smart contract automatically enforce obligations … They are self-enforcing meaning the court will not need to enforce them by ordering damages or specific performance.” [Lue19]

• ”… contracts whose terms are encoded in computer language instead of legal language. Smart contracts can be executed … so that the terms of the contracts are automatically enforced by a protocol that all nodes in the network follow. A smart contract can be fully autonomous if all the objects referred (such as currency, payments, obligations, property titles, assets, licenses) have a digital representation in the platform.” [Upd18]

• ”software, perhaps run on blockchain, and designed to execute future exchanges or other coordinated actions between persons who might otherwise not trust one another to perform.” [Kla22]

• ”A collection of code and data (sometimes referred to as functions and state) that is deployed using cryptographically signed transactions on the blockchain network.” [Yag+18]

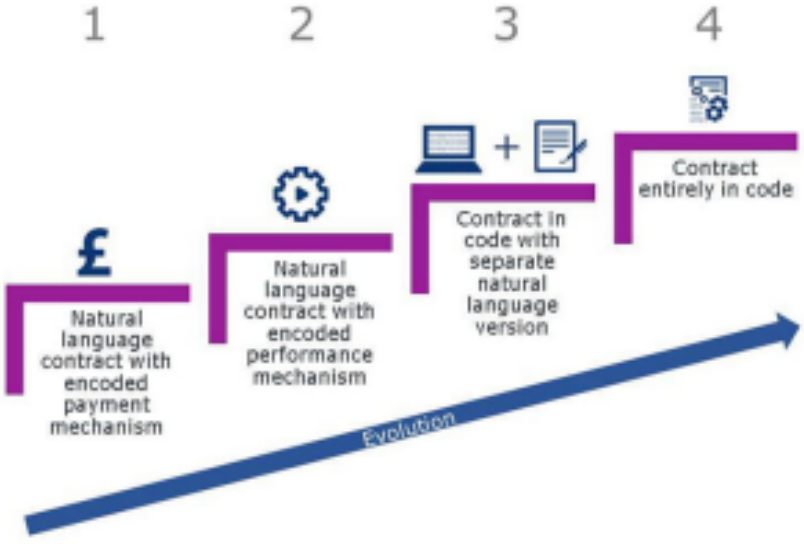
In addition, some observers prognosticate a gradual evolution of smart contracts towards a state where contracts are completely embodied in code through steadily more advanced natural language processing functionalities [Upd18]. **See Figure 1:**

Many in the legal community do not have a deep knowledge of the technical make up of the various blockchain related technologies. In turn, most computer scientists and information technology creators lack a good understanding of how the legal system works [LM20].

Add to this the fact that humans tend to overestimate their own competence - the Dunning Kruger effect [Dun11] - and that computer users are generally prone to overestimating the capabilities of computer systems, particularly where the interfaces interact with the user in a humanlike manner [FK92] [KW16].

It is easy to see how a degree of ”wishful thinking” may creep in, particularly in an already hype permeated space such as the blockchain ecosystem [Gre16]. The more sober reality is that a smart contract is nothing more than a small piece of code that is stored on a blockchain, triggered by blockchain transactions and which reads and writes data to that blockchain.

FIGURE 1: FOUR STAGES OF SMART CONTRACT EVOLUTION, FROM [UPD18].



It is not imbued with any magical properties which enable it to do things other software cannot do. In fact its capabilities are much more limited than traditional software **precisely because** it is stored and only runs on a blockchain. This is for a number of reasons.

First, blockchains suffer from the "Scalability Trilemma" which states that a blockchain can only achieve two of the three properties of decentralization, security and scalability. Any form of decentralization (the hallmark of a blockchain) has a direct and degrading effect on the scalability of that system, given that the now required consensus mechanism consumes resources and imposes limits on the speed with which the system can update itself, i.e. process transactions [HHS20]

Second, smart contracts must be executed sequentially, in the same order, one after the other. This "predictable repeatability" is necessary in order to maintain the integrity of the blockchain. They can thus not meaningfully[6] exploit strategies for im proved performance such as parallel processing [SH19].

Third, smart contracts must execute deterministically, that is generate the same outputs given the same inputs, each and every time. This is achievable if all input data is stored within its blockchain, but gets problematic if off-chain data is required to enable the smart contract's functionality.

More complex computational systems like the one postulated in [JM22] will most certainly require some form of off chain data to properly function. There are some options to bring off-chain data into a blockchain via "Oracles", but these in turn bring negative performance and storage implications for the blockchain network [Gre16]. They also have cost consequences. Computation on the blockchain can get expensive very quickly as the complexity of a smart contract ramps up [JD20].

Fourth, the type of software required to create more complex functionality in a smart contract is severely limited by the overall computational capacity of the "virtual machine" architecture of blockchain smart contract platforms. For example, the Ethereum Virtual Machine, currently the most popular platform for smart contracts, has roughly 1/5,000th of the compute power of a Raspberry Pi 4, a $45 utility computer [Wea21].

Although Solidity (the programming language used to create smart contracts on the Ethereum platform) may be Turing Complete[7], and thus theoretically capable of encoding any logic we may see fit to create, the practical reality is that the computational limitations of a distributed computer such as the Ethereum Virtual Machine, simply prohibit the actual implementation of any code which does anything more than perform basic input driven transactional logic.

All of this to say that a reality check is necessary in our understanding of what a smart contract is. Regrettably the term smart contract is now well engrained in our discussions around blockchain mediated contract automation. Perhaps the best option is to convert the word "smart" into a more descriptive acronym: a "Simple Machine Automated Repeatable Transaction".

THE RULE OF LAW

Legal scholars have expressed concern about the automation of contract law on the grounds that, among others, it may have negative impacts on our legal system's ability to ensure fairness and flexibility in contracting [Hil21] [Ver18], the maintenance of human rights online [Coh19], as well as the public's ability to effectively contest unjust contractual arrangements [Wal11]. Others have expressed legitimate concerns about how well legal norms are capable of actually being translated into computer code [Hil18].

All of these concerns exemplify that contract law is more than the mere committal of respective obligations to paper:

Contract law also addresses deception at the time of formation, prevents opportunism, fills gaps in the parties' agreement, and gives parties the flexibility they need to address unforeseen circumstances or future disagreements. And contract law serves broader social functions, such as marking breach as a moral wrong, enforcing obligations of corrective justice, denying public support to agreements society deems unfair or otherwise problematic, and providing a form of civic participation through the courts. It is not obvious that a smart contract could be designed to serve any of those other purposes, and highly unlikely that a smart contract could ever serve all of them. [Kla22]

With respect to that aspect of contract law at which smart contracts are effective - providing automated enforcement of contractual terms in a trustless manner - the lack of opportunity for an affected party to meaningfully (fairly and publicly) dispute such enforcement may have the unintended consequence of degrading acceptance of such systems over time.

The value of having a meaningful ability to dispute is significant: it reinforces that we are all moral agents entitled to dignity and respect, it provides the community with an opportunity to reaffirm its commitment to the law's demands, and provides an important source of information and feedback to those who make the law [Yeu17].

Broader adoption of automated enforcement may also have knock on effects on the delicate social, political and cultural foundations of the rule of law:

... although conventional legal enforcement is underpinned by the coercive power on the state to compel compliance (or to order financial compensation in lieu), ultimately the effectiveness of the legal guarantee rests on the uncoerced acceptance of legal subjects to respect its commands.

Thus, as transacting parties come to rely on technological coercion to guarantee the security of their transactions, property and perhaps in future even of persons, over time this may weaken our commitment to the mutual self restraint upon which the modern rule of law depends since security is no longer critically dependent upon our willingness to exercise such self-restraint. [Yeu17]

See also [Lev17] for a broader discussion in the same vein.

The broader effects of automating the contractual life cycle need to be more fully understood, lest we engage collateral effects which I suspect (and hope) no one wants.

ENDNOTES

1 Consider further the respective challenges and limitations of implementing this. Could the terms be entered as text, necessitating some sort of natural language processing functionality to convert them to code? Or would terms be selected from a set of pre-defined options, which would limit the parties' ability to express their respective positions?

2 The devil is also in the details for this step. How would disputes over specific terms be resolved? How would the traditional "language tweaking" process be automated?

3 Again, the devil is in the details here as well.

4 Which also poses a challenge to any court subsequently seeking to interpret a software based encoding of contractual terms [Kla22].

5 https://ethereumclassic.org/why-classic/code-is-law

6 There are some blockchains which have explored novel ways of introducing a limited form of parallelization, but none have been able to surmount the Scalability Trilemma.

7 A computational device is Turing Complete if, in principle (although not necessarily in practice) it could be used to solve any computational problem.

REFERENCES

[Coh19] Julie E Cohen. "Internet Utopianism and the Practical Inevitability of Law". In: Duke Law & Technology Review 18.1 (2019). https://scholarship. law.duke.edu/cgi/viewcontent. cgi?article=1343&context=dltr.

[Dun11] David Dunning. "The Dunning–Kruger effect: On being ignorant of one's own ignorance". In: Advances in experimental social psychology. Vol. 44. https : / / casualpsych . com / wp - content / uploads / 2021 / 10 / The-Dunning-Kruger-Effect.pdf. Elsevier, 2011, pp. 247–296.

[FK92] Batya Friedman and Peter H Kahn Jr. "Human agency and responsible computing: Implications for computer system design". In: Journal of Systems and Software 17.1 (1992). https : / / faculty . washington . edu/pkahn /articles/Human_Agency_Responsible_Computing.pdf, pp. 7–14.

[Gre16] Gideon Greenspan. "Why Many Smart Contract Use Cases Are Simply Impossible". In: Coindesk Opinion (2016). https://www.coindesk.com/markets / 2016 / 04 / 17 / why - many - smart-contract-use-cases-are -simply-impossible/.

[HHS20] Abdelatif Hafid, Abdelhakim Senhaji Hafid, and Mustapha Samih. "Scaling blockchains: A comprehensive survey". In: IEEE Access 8 (2020). https://ieeexplore.ieee.org/stamp /stamp. jsp?tp=&arnumber=9133427, pp. 125244–125262.

[Hill8] Mireille Hildebrandt. "Algorithmic Regulation and the Rule of Law". In: Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 376.2128 (2018). https:// royalsocietypublishing.org/doi/epdf/10.1098/rsta.2017.0355, p. 20170355.

[Hil21] Mireille Hildebrandt."Understanding Law and the Rule of Law: A Plea to Augment CS Curricula". In: Commun. ACM 64.5 (Apr. 2021), pp. 28–31. issn: 0001-0782. doi: 10.1145/3425779. url: https://doi. org/10.1145/3425779.

[JD20] Abdul Jabbar and Samir Dani. "Investigating the link between transaction and computational costs in a blockchain environment". In: International Journal of Production Research 58.11 (2020). https://www. tandfonline. com/doi/epdf/10.1080/00207543.2020.1754487?needAccess=true&role=button, pp. 3423–3436.

[JM22] Michael Juenemann and Udo Milkau. "Can Code be Law? A Review of Current Developments". In: International Journal of Blockchain Law 2 (2022). https://gbbcouncil.org/wp-content/uploads/2022/03/IJBL-VolumeII.pdf, p. 36.

[Kla22] Gregory Klass. "How to Interpret a Vending Machine: Smart Contracts and Contract Law". In: Available at SSRN 4045711 (2022). https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi ?article =3451&context=facpub.

[KW16] Bart P Knijnenburg and Martijn C Willemsen. "Inferring capabilities of intelligent agents from their external traits". In: ACM Transactions on Interactive Intelligent Systems (TiiS) 6.4 (2016). https://www. usabart.nl/portfolio/agentsdraft.pdf, pp. 1–25.

[Lev17] Karen EC Levy. "Book-smart, not street-smart: blockchain-based smart contracts and the social workings of law". In: Engaging Science, Technology, and Society 3 (2017). https://estsjournal.org/index.php/ ests/article/download/107/61/, pp. 1–15.

[LM20] Kelvin FK Low and Eliza Mik. "Pause the blockchain legal revolution". In: International & Comparative Law Quarterly 69.1 (2020). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3439918, pp. 135–175.

[Lue19] Andrew Luesley. “Unravelling Smart Contracts: Smart Contracts and the Law of Rescission in Canada”. In: Asper Rev. Int’l Bus. & Trade L. 19 (2019). https://journals.library.ualberta.ca/asperreview/index.php/asperreview/article/download/223/222, p. 155.

[Per19] Jose Carlos Pereira. “The Genesis of the Revolution in Contract Law: Smart Legal Contracts”. In: Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance. ICEGOV2019. Melbourne, VIC, Australia: Association for Computing Machinery, 2019, pp. 374–377. isbn: 9781450366441. url: https://doi.org/10.1145/3326365.3326414.

[Ras16] Max Raskin. “The law and Legality of Smart Contracts”. In: Geo. L. Tech.Rev. 1 (2016). https://moodle.epfl.ch/pluginfile.php/2861851/mod_ resource/content/1/Raskin-1-GEO.-L.-TECH.-REV.-305-.pdf, p. 305.

[Rub20] Jakub Ruby. “Code is Law? Smart Contracts Explained”. In: Finematics, Decentralized Finance Education (2020). https://finematics.com/smart-contracts-explained/.

[Sav17] Alexander Savelyev. “Contract Law 2.0: ‘Smart’ Contracts as the Beginning of the End of Classic Contract Law”. In: Information & Communications Technology Law 26.2 (2017). https://publications.hse.ru/pubs/share/folder/8uijw5g6qm/199179205.pdf, pp. 116–134.

[SH19] Vikram Saraph and Maurice Herlihy. “An empirical study of speculative concurrency in ethereum smart contracts”. In: arXiv preprint arXiv:1901.01376(2019). https://drops.dagstuhl.de/opus/volltexte/2020/11968/pdf/ OASIcs-Tokenomics-2019-4.pdf.

[Sza97] Nick Szabo. “The Idea of Smart Contracts”. In: Nick Szabo’s papers and concise tutorials 6.1 (1997).

[Upd18] Kelvin Ashurst Digital Economy Update. “Smart contracts - can code ever be law?” In: Ashurst website, visited 10 December 2022 (2018). https://www.ashurst.com/en/ news-and-insights/legal-updates/smart-contracts---can-code-ever-be-law.

[Ver18] Mark Verstraete. “The stakes of smart contracts”. In: Loy. U. Chi. LJ 50(2018). https://lawecommons.luc.edu/cgi/viewcontent.cgi?article=2692&context=luclj, p. 743.

[Vig21] Maria G Vigliotti. “What Do We Mean by Smart Contracts? Open Challenges in Smart Contracts”. In: Frontiers in Blockchain 3 (2021). https://www.frontiersin.org/articles/10.3389/fbloc.2020.553671/full\#B17, p. 553671.

[Wal11] Jeremy Waldron. “The Rule of Law and the Importance of Procedure”. In:NOMOS: Am. Soc’y Pol. Legal Phil. 50 (2011). https://philarchive.org/archive/WALTRO-67, p. 3

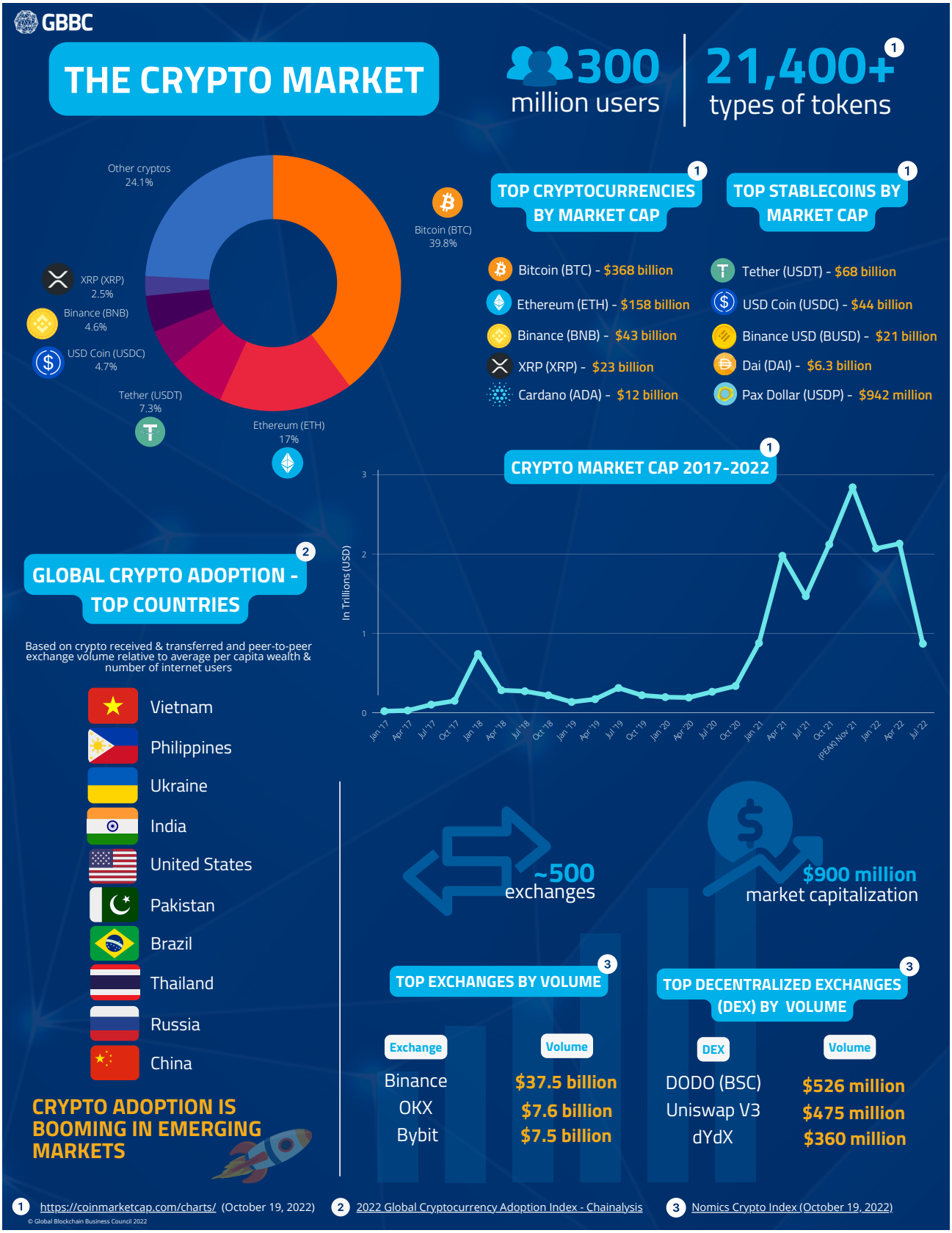
[WC17] Kevin Werbach and Nicolas Cornell. “Contracts Ex Machina”. In: Duke LJ67 (2017). https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2936&context=articles, p. 313.

[Wea21] Nicholas Weaver. The Web3 Fraud. https://www.usenix.org/publications/loginonline/web3-fraud. 2021.

[Yag+18] Dylan Yaga et al. “NISTIR 8202 - Blockchain Technology Overview”. In: NIST publications (2018). https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf. url: https://doi.org/10.6028/NIST.IR.8202.

[Yeu17] Karen Yeung. “Blockchain, Transactional Security and the Promise of Automated Law Enforcement: The Withering of Freedom Under Law?” In: TLI Think (2017). https://www.researchgate.net/profile/Karen-Yeung3/publication/314286132_Blockchain_Transactional_Security_and_the _ Promise _ of _ Automated _ Law _ Enforcement _ The _ Withering _ of _Freedom _ Under _ Law / links / 58bfdb8e92851c7b72760db8 / Blockchain -Transactional -Security-and-the-Promise-of-Automated-Law -Enforcement-The-Withering-of-Freedom-Under-Law.pdf.

GBBC'S FACT CARD SERIES ON CRYPTO AND DIGITAL ASSETS*



* GBBC's Fact Card Series highlight key subjects within the blockchain and digital assets space in visual and meaningful ways. These Fact Cards are relevant in the legal and regulatory space as the industry continues to search for clarity among policies when it comes to digital assets, central bank digital currencies (CBDCs), stablecoins, and the green economy. Visit the GBBC website for more information.

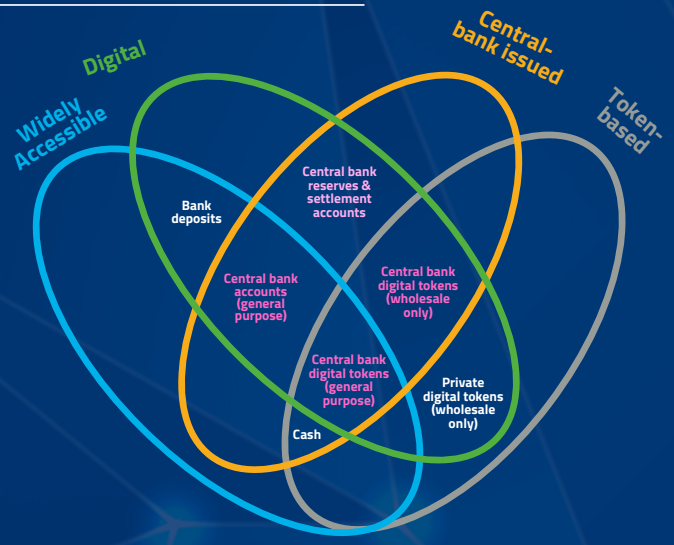
GBBC

CENTRAL BANK DIGITAL CURRENCIES (CBDCs)

Digital form of central bank money

THE MONEY FLOWER [1]

= CBDC Characteristics



Attributes of CBDCs

- Complement current forms of money and methods for providing financial services
- Enable greater efficiency of fund flows at lower cost
- Protect consumer privacy with the right public policy and design choices
- May increase security and reduce fraud or other illicit activities through greater transparency (e.g., ensuring funds reach the right recipients, are used for the designated purposes, and that stolen funds can be canceled)

Types of CBDCs

Retail
Issued by a central bank to individual users, enabling fund transfers directly into their digital wallets

Wholesale
Only available to financial institutions for interbank transfers & wholesale transactions

Global Status of CBDCs [2]

105 countries exploring use cases of CBDCs

50 countries are in an advanced phase of digital currency exploration

81 countries representing 90% of global GDP are exploring CBDCs

60% of central banks are conducting experiments on CBDCs

14% are moving forward with development and pilot arrangement

The share of central banks actively engaging in CBDC work grew to 86% in the last 4 years

1 https://www.bis.org/cpmi/publ/d174.pdf (pg 7)

2 Central Bank Digital Currency Tracker - Atlantic Council

GBBC

STABLECOINS

Stablecoins are digital assets designed to maintain a stable price and reduce volatility, typically by being pegged to external assets with a stable value or by regulating supply through an algorithm [1]

TYPES [2]

FIAT-BACKED
Pegged to fiat currency, holding fiat reserves equivalent to stablecoins in circulation

COMMODITY-BACKED
Pegged to physical assets including metals, oil, and real-estate

CRYPTO-BACKED
Pegged to crypto, generally as a collateralized debt position (CDP)

ALGORITHMIC
Some crypto-backed stablecoins use algorithms and smart contracts to manage supply of tokens with monetary incentives and fees to keep price stable

USES FOR STABLECOINS

REMITTANCES [3]
Enable sending money abroad at minimal cost. Remittances to low and middle income countries were estimated at $589 billion for 2021

DECENTRALIZED FINANCE (DeFi)
Currency with which DeFi applications are built, spanning across a range of alternative financial services

COMMERCIAL TRANSACTIONS
Enable low-cost, cross-border, and direct payments with immediate settlement and currency conversions

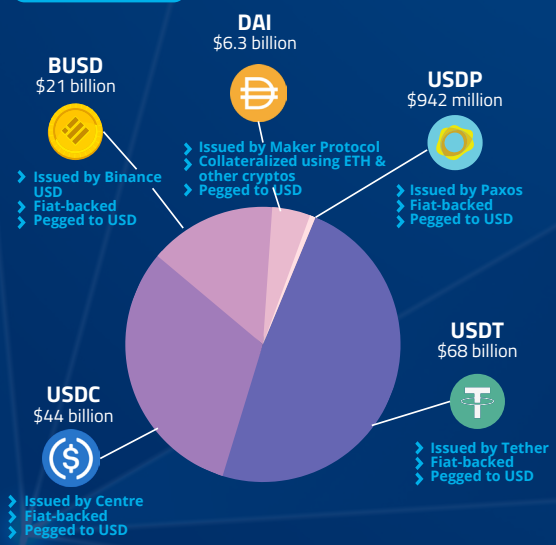
TRADING
A tool to access crypto trading platforms without having to hold fiat directly or incur fees and frictions from the traditional banking system

FINANCIAL INSTITUTIONS
Increase efficiencies and decrease costs with instant fund transfers between in-house accounts

CORPORATE TREASURIES
Improve liquidity management with efficient and transparent fund flows

Stablecoins enable the internet of value, where sending money becomes as easy as sending an email

TOP 5 STABLECOINS [2]
by Market Cap



~200 DIFFERENT STABLECOINS

TOTAL MARKET CAP
$152.9 BILLION

FOCUSES FOR REGULATION

OTHER ISSUES -
- Applicability of Howey Test to treat stablecoins as securities
- How to treat centralized vs. decentralized models
- Where reserves are held
- Insurance

- **RESERVES -** Ensuring adequate quality and amount of reserves to back stablecoins in circulation, including third party attestations
- **REDEMPTION POLICY -** Timeframe, cost, and ease (e.g., what platform to use and any fees to redeem funds)
- **FINANCIAL STABILITY -** Preventing disruptions to the current banking system (e.g., bank runs)
- **CONSUMER & INVESTOR PROTECTIONS -** Ensuring redeemabilty of stablecoins and limiting losses
- **RISKS OF ALGORITHMIC STABLECOIN STRUCTURES -** Given that there may be no collateral

MAJOR GLOBAL REGULATIONS

Markets in Crypto Assets (MiCA) [4]
Crypto regulation in the EU, covering stablecoins

Financial Stability Board (FSB) [5]
Recommendations for Global Stablecoin Arrangements

Principles for Financial Market Infrastructures (PFMIs) [6]
Application of PFMIs to systemically important stablecoin arrangements and relevant entities

New York Department of Financial Services (NYDFS) [7]
Guidance on Issuance of US Dollar-Backed Stablecoins

There is legislation in the works to prohibit algorithmic stablecoins and highlight their risks

1 https://www.gemini.com/cryptopedia/what-are-stablecoins-how-do-they-work#section-algorithmic-stablecoins 2 https://coinmarketcap.com/charts/ (October 19, 2022)
3 https://www.knomad.org/sites/default/files/2021-11/Migration_Brief%2035_1.pdf 4 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593 5 https://www.fsb.org/wp-content/uploads/P131020-3.pdf
6 https://www.bis.org/cpmi/publ/d206.pdf 7 https://www.dfs.ny.gov/industry_guidance/industry_letters/il20220608_issuance_stablecoins

GBBC

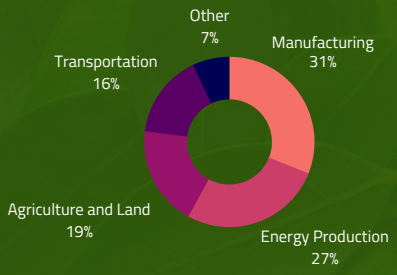
InterWork Alliance

THE GREEN ECONOMY

Read GBBC's Global Standards Mapping Initative 2.0 for Additional Information about The Green Economy

Problem [1]

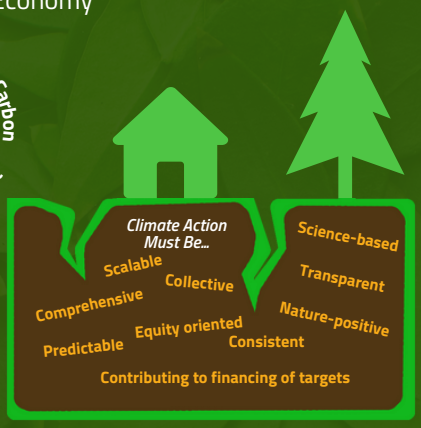
The world generates roughly 51 billion tons of greenhouse gas (GHG) emissions per year



Solution [2]

URGENT CLIMATE ACTION

Reduce emissions & offset carbon



Key Players [2]

- Retailers
- Registries
- Producers
- Supranational organizations
- Governments
- Consumers
- Standards organizations

Types of Carbon Markets [2]

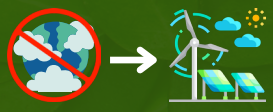
Voluntary

Need global standards for marketplaces of measurable & verifiable carbon reductions

Regulated

Governmental agency (nation-state or treaty) enforces mandate to offset emissions

A Green Economy is a Global Effort [1]



- Decarbonization costs are rising
- Emission reductions are hard
- Demand is outpacing supply for verified offsets
- No alternative technologies

GOALS [3]

1. **Address** climate change and its negative impacts
2. **Aim** to reduce global greenhouse gas emissions to less than 2° C above preindustrial levels
3. **Limit** global temperature increase to 1.5° C

The Role of Blockchain [1]

Decarbonizing the global economy by developing...

- Global interoperable marketplaces for carbon offsets
- Price discovery for offset quality based on additionality, permanence, efficiency, and verifiability
- Emissions tracking across supply chains

CRYPTOCURRENCIES
enable participation in ecosystem management

PROOF-OF-STAKE (POS) CONSENSUS
is fast & energy efficient

DECENTRALIZED AUTONOMOUS ORGANIZATIONS (DAOs)
enable community ownership & governance while bringing together supply & demand

NON-FUNGIBLE TOKENS (NFTs)
allow traceability of emissions, address quality variance, and provide programmatic liability management

1 https://www.morganstanley.com/im/publication/insights/articles/article_cryptoandcarbon_us.pdf
2 https://gbbcouncil.org/wp-content/uploads/2021/11/GBBC-GSMI-2.0-Report-1.pdf
3 https://unfccc.int/process-and-meetings/the-paris-agreement/the-paris-agreement

HOW CAN I GET INVOLVED?

Interested in submitting new work or becoming an editor for the International Journal of Blockchain Law (IJBL)? Review the below submission guidelines and then email us at IJBL@gbbcouncil.org!

Length	3-4 print pages including footnotes
Target Audience for Submission	Broader business community aiming to better understand the technology and the legal issues associated with it
Content	All legal areas related to blockchain technology and digital assets
Structure	Introduction - Description of legal matter - Proposed solution - Conclusion/key takeaways
Writing Style	Not too academic; lucid and clear-cut language
Content is Key	The editors will take care of final product
What can I Submit?	Previously published work is welcome for submission to the IJBL