Citi GPS

MONEY, TOKENS, AND GAMES

Blockchain's Next Billion Users and Trillions in Value

Citi GPS: Global Perspectives & Solutions

March 2023

Citi is one of the world's largest financial institutions, operating in all major established and emerging markets. Across these world markets, our employees conduct an ongoing multi-disciplinary conversation – accessing information, analyzing data, developing insights, and formulating advice. As our premier thought leadership product, Citi GPS is designed to help our readers navigate the global economy's most demanding challenges and to anticipate future themes and trends in a fast-changing and interconnected world. Citi GPS accesses the best elements of our global conversation and harvests the thought leadership of a wide range of senior professionals across our firm. This is not a research report and does not constitute advice on investments or a solicitations to buy or sell any financial instruments.
For more information on Citi GPS, please visit our website at www.citi.com/citigps.

Ronit Ghose, CFA
Head of Future of Finance
Citi Global Insights

+44-20-7986-4028 |
ronit.ghose@citi.com

Sophia Bantanidis
Future of Finance Analyst
Citi Global Insights

+44-20-7500-9655 |
sophia.bantanidis@citi.com

Nisha Surendran
ICG Lead for Tokenization
ICG Digital Assets, Citi

+44 20-7986-7766 |
nisha.surendran@citi.com

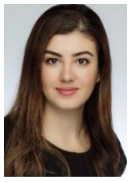
Kaiwan Master
Future of Finance Analyst
Citi Global Insights
+44-20-7986-0247 |
kaiwan.hoshang.master@citi.com

Ronak S Shah
Future of Finance Team
Citi Global Insights

+44-20-7986-3960 |
ronak.sharad.shah@citi.com

Yirou Yu
FinTech & Blockchain
Citi Business Advisory Services

+1-212-723-4131 |
yirou.yu@citi.com



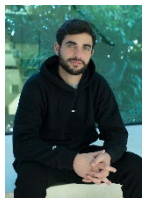
Loubna Regragui
Product Manager
ICG Digital Assets, Citi

+44 20-7986-0490 |
loubna.regragui@citi.com

Henri Arslanian
Co-Founder & Managing Partner
Nine Blocks Capital Mgmt

Bob Blower
CEO
Clarency.com

Nanne Dekking
Founder & CEO
Artory Inc.



Samuel Falic
Co-Founder & President
BlockBar Inc.

Stani Kulechov
Founder & CEO
Aave Companies

Morgan McKenney
CEO
Provenance Blockchain Foundation

Silvio Micali
Professor
MIT

Aaron Powers
Co-Founder & CEO
Hunit

Jessica Renier
Head of Digital Finance Institute of International Finance

Sunil Senapati
Chief Operating Officer
XinFin

Ruth Wandhöfer
Partner
Gauss Ventures

Zooko Wilcox
Founder & CEO
Electric Coin Co.

John Wu
President
Ava Labs

Ryan Wyatt
President
Polygon Labs

With thanks to: Steven Biekens, Shearin Cao, Julien Donnet, Chelsea Lo, Martin Masser, Ciarán McGonagle, Adnan Memon, Ioana Niculcea, Opeyemi Olomo, Puneet Singhvi, Ajit Tripathi, Stephanie Wake, Jack White, and Vasant Viswanathan.

MONEY, TOKENS, AND GAMES

Blockchain's Next Billion Users and Trillions in Value

Kathleen Boyle, CFA
Managing Editor, Citi GPS

Can you always spot disruptive innovation? When we hear the story of how the invention of the automobile hastened the demise of buggy whip companies, we often question why the disruptive potential of gas-powered cars wasn't noticed. In the modern era, most people buying digital cameras in the 1990s would have scoffed at the idea that in a few years' time, we would all be carrying around cameras in our mobile phones.

The potential for tokenization via blockchain has been talked about as being transformative for the past few years but we are not quite at the point of mass adoption. Unlike automobiles or more recent innovations like ChatGPT or the Metaverse, blockchain is a back-end infrastructure technology without a prominent consumer interface, making it harder to visibly see how it could be innovative.

But we believe we are approaching an inflection point, where the promised potential of blockchain will be realized and be measured in billions of users and trillions of dollars in value. Successful adoption will be when blockchain has a billion-plus users who do not even realize they are using the technology. This is likely to be driven by the adoption of central bank digital currencies (CBDCs) by large central banks as well as tokenized assets in gaming and blockchain-based payments on social media. By 2030, up to $5 trillion of CBDCs could be circulating in major economies in the world, half or which could be linked to distributed ledger technology. Tokenization of financial and real-work assets could be the killer use case driving blockchain breakthrough with tokenization expected to grow by a factor of 80x in private markets and reach up to almost $4 trillion in value by 2030.

We first wrote about tokenization in the 2021 Citi GPS report *Future of Money: CBDCs, Crypto, and 21st Century Cash*. At the time, China was starting to pilot test its (CBDC) and other central banks were warming up to the idea of their own digital currencies. In recent months, central banks in multiple large countries have announced plans for CBDCs this decade, giving almost 2 billion people the opportunity to experiment with digital currency.

To be successfully adopted into the mainstream, blockchain needs the help of technology enablers, including (1) decentralized digital identities, (2) zero-knowledge proofs, (3) Oracles, and (4) secure bridges. The legal plumbing also needs to be altered to enable smart legal contracts that will provide a whole new set of rails for global commerce and finance to run on. Regulatory considerations are also necessary to allow adoption and scalability without the hindering innovation.

Although we think mass adoption could still be six to eight years away, momentum on adoption has positively shifted as governments, large institutions, and corporations have moved from investigating the benefits of tokenization to trials and proofs of concept.

© 2023 Citigroup

Blockchain: The Opportunity and the Addressable Need

BILLIONS OF USERS

Blockchain user numbers will be boosted by daily activity. The success of blockchain adoption will be measured by when it is being used by a billion plus end users who do not even realize they are using the technology. Blockchain-based products can make a significant impact in terms of wide consumer adoption in digital currency, especially central bank digital currency (CBDCs), gaming, and social.

CBDCs could be used by **2-4 billion** users globally by 2030, 50% of which could be DLT-linked

With over **3 billion** gamers currently, we expect 50mn-100mn could be Web3 users by 2025, with estimates rising as Web2 hits include tokens

Art and collectibles, NFTs, and digital collectibles could create new paths for content creators and unlock new **monetization opportunities**

TRILLIONS OF VALUE

Almost anything of value can be tokenized and tokenization of financial and real-world assets could be the "killer use-case" blockchain needs to drive a breakthrough. We forecast $4 trillion to $5 trillion of tokenized digital securities and $1 trillion of distributed ledger technology (DLT)-based trade finance volumes by 2030.

Opportunity

Tokenization Total Addressable Market (US$ Trillions)

Source: SIFMA, Preqin, Savills, Finadium, and Valuates

2030E non-financial corporate and quasi sovereign debt

$187 trillion

2030 Estimate
$1.9 trillion Tokenized

2030E real estate funds

$20 trillion

2030 Estimate
$1.5 trillion Tokenized

2030E private equity/ venture capital

$7 trillion

2030 Estimate
$0.7 trillion Tokenized

2030E securities financing and collateral

$42 trillion

2030 Estimate
$0.5-$1.0 trillion Tokenized

2030E trade finance

$12 trillion

2030 Estimate
$1.0 trillion Tokenized

© 2023 Citigroup

TECHNOLOGY ENABLERS

Blockchain promises something that is in parts a replacement of a current functioning system and in parts new capabilities and operating models. From a technology specification perspective, blockchain needs to have transaction scale and throughput, strong guarantees of security, on-chain identity, privacy, Oracles, bridges, and good user experience.

	Technology Drivers	Description	How It Helps Blockchain Adoption
	Decentralized Identity	Leverages blockchain while enabling data privacy and protection for individuals	Drives adoption by providing individuals the ability to access and navigate the digital ecosystem leveraging self-sovereignty and sharing details on a "need-to-know" basis
	Zero Knowledge Proofs	Separate knowledge from verification	Allows for scaling by moving computations off-chain in a verifiable way and privacy by keeping data, transactions, and computations hidden but publicly verifiable
	Oracles	Serve as a bridge between the blockchain ecosystem and external data sources	Allows blockchain applications to access data stored outside the blockchain
	Secure Bridges	Enable users to move assets from one blockchain to another	Drives adopooin by enabling interoperability between different networks and avoiding siloed ecosystems

LEGAL ENABLERS

Contract creation and execution can be a painful process, making it ripe for disruption. Technology-enabled smart legal contracts, are legally binding agreements with obligations performed automatically by a computer. They are dynamic, connect to outside data sources, and allow for human involvement where necessary.

Uses Cases for Smart Legal Contracts

- Real Estate/PropTech
- Escrow Payments
- Insurance
- Supply Chains
- Managing Breaches in Service Level Agreements
- Derivative Agreements

Using distributed ledger technology (DLT) in smart legal contracts can:

- Increase longivity and independence
- Enhance trust and eliminate silos
- Create a tamper proof record
- Increase security
- Create a single source of truth

Contents

© 2023 Citigroup

© 2023 Citigroup

Introduction

Disruptive technologies change the state of doing things: how we live, work, spend, invest, interact, and more. Blockchain — and the associated Web3 concept — are disruptive technologies. They attract controversy and debate, as well as inspire dreams and disillusionment. In this report, we explore some of the key drivers that will take blockchain technology to the next billion users, and potentially trillions of dollars of economic activity.

As classically defined by Clayton Christensen in *The Innovator's Dilemma*:

"*Disruptive technologies bring to a market a very different value proposition than has been available previously. Generally, disruptive technologies underperform established products in mainstream markets. But they have other features that a few fringe (and generally new) customers value. Products based on disruptive technologies are typically cheaper, simpler, smaller and, frequently, more convenient to use.*"[1]

Blockchain fits many of the characteristics set out by Christensen — tokenized, programmable assets with atomic settlement (instant and simultaneous) are a different value proposition than existing fiat money or financial assets. The adoption of public blockchains (e.g., cryptocurrencies), has happened initially in niche communities, such as the technologically savvy, as well as among those living in countries that are peripheral to core financial markets, including Argentina, Nigeria, and Ukraine.

However, blockchain as a disruptive technology is different from many others. As it involves the transfer of financial value, it enters the realm of money — a highly regulated domain in most countries. Hence, while the blockchain revolution began on the periphery, to be powered to mass adoption it needs the support of sovereign institutions, regulated financial institutions, and large companies — as well as the "degens" and the rebels, who are core to innovation, change, and progress.

By 2030, the growth of blockchain will be measured in billions of users and trillions of dollars

Those who have been promised the benefits of blockchain for many years might roll their eyes. But this time may well be different. To be sure, blockchain is not about to have a ChatGPT moment. Blockchain is a back-end infrastructure technology, more akin to cloud computing than artificial intelligence (AI) or the Metaverse, which have a more prominent consumer interface. So, why do we believe the growth of blockchain by 2030 will be measured in: (1) billions of users, and (2) trillions of dollars?

- **Billions of Users:** Blockchain user numbers will be boosted by daily activity — spanning money, games, social, and more. Successful blockchain adoption will be when it has a billion-plus end users who do not even realize they are using the technology.
  - Money**:** Countries with populations totaling approximately 2 billion are likely to experiment with distributed ledger technology-linked (DLT-linked) central bank digital currencies (CBDCs).
  - Games**:** The next generation of gaming will include tokenized assets, initially driven by Asian games and appealing to power users.

[1] Clayton M. Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail* (Harvard Business Review Press, 1997, updated 2016).

© 2023 Citigroup

  - Social: Micropayments, including in Metaverse games, will likely be blockchain-based. Large consumer brands will also help power Web3 adoption.

- **Trillions of Dollars:** We estimate up to $5 trillion could move to newer digital money formats such as CBDCs and stablecoins by 2030, of which roughly half could be DLT- or blockchain-linked. Legal reforms and greater interoperability could drive up to $1 trillion of tokenization in global trade finance by 2030. Securities and funds are the big private-sector, tokenization prize. We estimate up to $5 trillion of non-financial corporate and quasi-sovereign debt; repo, securities financing, and collateral market; and alternative assets, such as real estate, private equity (PE), and venture capital (VC), could be tokenized by 2030. Industry estimates for total tokenization volumes are even higher.

- **Technology and Legal:** Bringing billions of users and trillions of dollars of investments into the blockchain ecosystem requires a change in the technological and legal plumbing that is needed to support, maintain, and operate the system. These changes could include blockchain-based identity solutions, privacy solutions enabled by zero-knowledge proofs, Oracles to connect/feed real-world data on-chain, and of course, a strong regulatory and legal framework that would allow individuals and institutions to embrace this new technology.

How Big Is the Market for Emerging Technologies?

Out of all emerging technologies, blockchain has the highest total addressable market growth forecast

Blockchain and Web3 today are relatively small markets (see Figure 1). When assessing total addressable market (TAM) size and time to impact (i.e., the number of years to reach early majority adoption), we look at several sources. The largest of the emerging technologies today is AI, a general-purpose technology with use cases across nearly every aspect of society and the economy, impacting both consumer-facing and infrastructure layers.

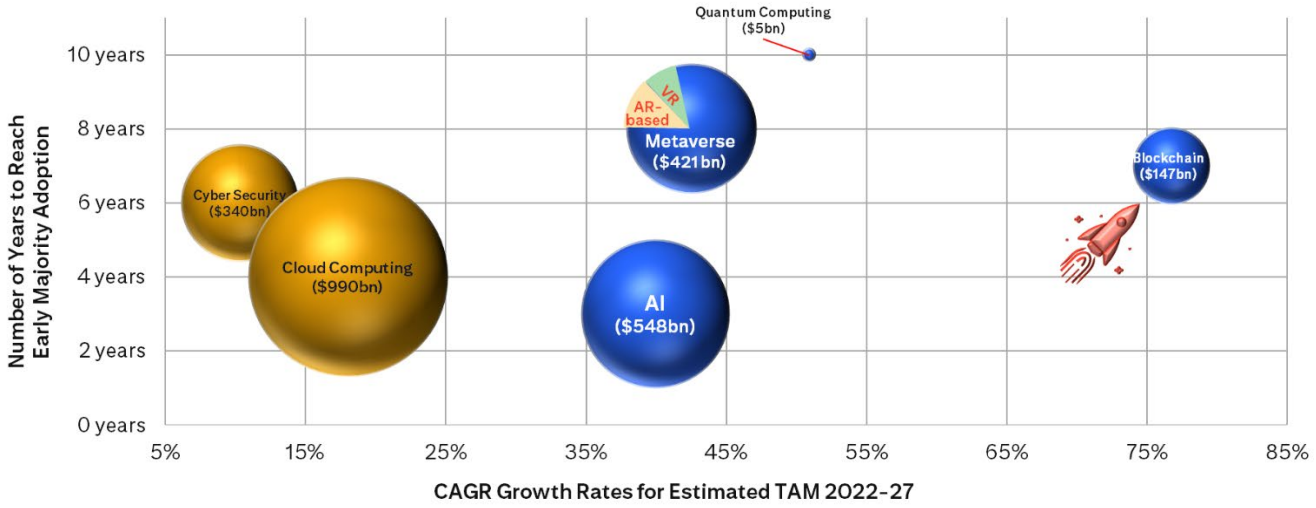
Mass adoption for AI could be as early as 2-4 years driven by the rapid recent increase in data availability and computing power, improved algorithms, and models that have led to products such as ChatGPT, which have caught mass public attention. Blockchain, on the other hand, could take longer for mass adoption (6-8 years perhaps) due to the need for collaboration among participants, standardization of platforms, as well as interoperability, and compatibility with existing systems and software.

However, while challenges exist, including the current, poor consumer user experience and high cost of integration with existing institutional structures, consensus forecasts for TAM growth are the highest for blockchain among emerging technologies. Why? Because large institutions, governments, and corporations are now beginning to adopt it, albeit initially in trials and proofs of concept. As we discuss in the report that follows, we may be at the tipping point for change in this domain.

Notably, in this report we focus on the real-world and tangible use cases of blockchain technology — not the speculative, trading side of the business, which often attracts much media attention due to its color and volatility.

© 2023 Citigroup

Figure 1. Estimating the Impact of Emerging Technologies: Revenue TAM and Time to Impact



Note: Size of bubble represents estimated 2027 Total Addressable Market (TAM) in billions of U.S. dollars.
Source: Citi GPS

Four Key Takeaways From This Report

Blockchain will have a significant impact on digital money, followed by gaming as well as art and collectibles

- **Billions of Users:** A key area where blockchain/DLT will make a significant impact is in digital money. The world of money is being turned on its head with CBDCs of major currencies coming our way towards the second half of this decade, with many CBDC projects being partially DLT-linked. Get ready for CBDC versions of the euro (EUR), British pound (GBP), and Indian rupee (INR). Together, these four jurisdictions constitute more than 25% of the global population and 22% of global bank deposits. Hence, we think CBDCs could have at least 2 billion users and $5 trillion-plus in circulation, and half could be using partly DLT-linked models.

  There are big figures for gaming, with over 3 billion gamers in 2022 — an enormous slice of the population. This means only a relatively small proportion of gamers need to participate in blockchain-based games for them to be a success. Gaming will lead the way in “making blockchain big” from a bottom-up perspective. A small number of the most active gamers from Asia will likely adopt the next generation of Web3 games in the next 1-2 years, triggering an inclusion of tokenization aspects by leading Western and global games studios. The typical gamer does not care about the underlying technology, blockchain, cloud, or otherwise. Web2 or mass market consumer brands will be the key driver of adoption — so Web3 will not replace Web2 but will nestle inside it, Russian doll-like.

  Art and collectibles are also moving onto the blockchain because these industries resonate with one of blockchain’s key features, namely trust and provenance, as well as the ability for a broader range of owners to invest via fractionalization.

© 2023 Citigroup

Similar to the arts, entertainment industries such as music, will use blockchain technology in the form of non-fungible tokens (NFTs). This provides a new path for content creators (be they artists, singers, dancers, or fashion brands) to connect directly with their fans or audiences, affording these creators and brands new revenue streams. Brands from Nike to Uniglo are already embracing NFTs and in-game assets in an attempt to capture younger generations and keep their businesses relevant. In fact, Amazon is planning to launch an NFT marketplace for its 167 million Prime users in the U.S. in 2023. It will be interesting to see how those figures increase if this development goes global.

We estimate tokenized private markets will reach up to $5 trillion by 2030

- **Trillions in Value:** Tokenization of financial and real-world assets is en route. Moreover, almost anything of value can be tokenized — from wine to financial assets to everything in between. Tokenization of financial and real-world assets could be the killer use case blockchain needs for breakthrough, especially for private market assets. Despite currently having a marginal market share (less than 0.1% in annual issuance as of now), we project tokenization to grow by a factor of over 80x in private markets and reach up to around $4 trillion in value by 2030. The significant benefits of tokenization, especially for private funds and securities, will likely drive demand-side uptake, leaving behind expensive reconciliations and settlement failures while embracing operational efficiencies, fractionalization, and accessibility to a wider range of market participants. Beyond private market tokenization, we expect $1 trillion of the repo, securities financing and collateral market could be tokenized by 2030.

  Later in the report, we take a dive deep into tokenization for certain types of financial assets, including digital securities. We examine the main ingredients beyond the blockchain tech need to scale securities tokenization, namely an entirely digitized workflow, support from traditional finance (TradFi) layers, tech-neutral laws, standardized taxonomy, interoperable platforms, and standards, to name just a few. As a standalone, tokenization may offer positives, but the benefits need to offset the integration costs of adding the new disruptive technology to the existing legacy stack — and this is as much a coordination and culture question as a tech one.

The big inflection point for the digitization of trade finance is an upcoming UK legal reform, which will make the acceptance of digital documents acceptable under common law — a solid first step for blockchain deployment

  In the world of financial services, trade finance and blockchain have had an uncomfortable relationship in recent times, with many projects ending up in the graveyard. But change may be underway: Encouraging regulatory developments designed to pave the way for trade documentation to be digitized are solid first steps for blockchain deployment. The big inflection point for the digitization of trade finance is the upcoming UK legal reform that will make the acceptance of digital documents legal under common law — a huge step for the global trade finance industry, as around 80% of global volumes are governed by English law.

- **Technology Enablers:** There is a long shopping list of technological specifications that blockchain must have — ranging from transaction scale to strong user experience (UX) and user interface (UI) — to reach billions of users, combined with four key technology drivers that will drive mainstream blockchain adoption:

  – **Decentralized Digital Identities:** Give users power and control over their personal data, including how and by whom it is used. Digital identities form the backbone of any digital ecosystem and are the core building block to deliver the decentralization promise enshrined in Web3.

© 2023 Citigroup

- **Zero-Knowledge Proofs:** Preserve privacy while still being able to use the underlying data, which has been one of the major stumbling blocks for public blockchain adoption faced by large corporations. Zero-knowledge proofs provide an elegant solution that capitalize on the promise of blockchain without compromising on the confidentiality and privacy of information.
- **Oracles:** Bridge the world of blockchain to real-world data off-chain. They are the mega connector between these two worlds. Blockchain will go nowhere without them.
- **Secure Bridges:** Offers a solution enabling users to move assets from one blockchain to another. As different blockchains are being built for different use cases on different chains, there is a need for these to interoperate and not be working in silos, to avoid fragmentation and limited adoption.

- **Legal Enablers:** The next wave of contracts ("Contracts 2.0) is underway with the development of smart legal contracts (SLCs). A smart legal contract is defined by the UK Law Commission as *"a legally binding contract in which some or all of the contractual obligations are defined in and/or performed automatically by a computer program."*[2] DLT brings unique benefits to the table compared to conventional web platforms, e.g., longevity of decentralized ledgers that fit well with the nature of legal agreements; enhanced levels of security through the use of cryptography and hashing techniques; and the provision of a single source of truth through their consensus mechanism and tamper-proof nature. As such, DLTs would be the most favorable technology to underpin SLCs.

  Regulatory analysis spearheaded by the Law Commission in the UK and emerging regulatory development, which will recognize the digitization of trade documentation, have lowered the barriers to adoption. According to Aaron Powers, co-founder and CEO of Hunit, these contracts will provide a whole new set of rails for global commerce and finance to run on. There are multiple use cases ranging from property to service level agreements. However, we believe that given the nature of these contracts — they are based on conditional logic, meaning that if X happens then Y follows — they will be suited for more basic agreements.

[2] UK Law Commission, *Smart Legal Contracts: Summary*, November 25, 2021.

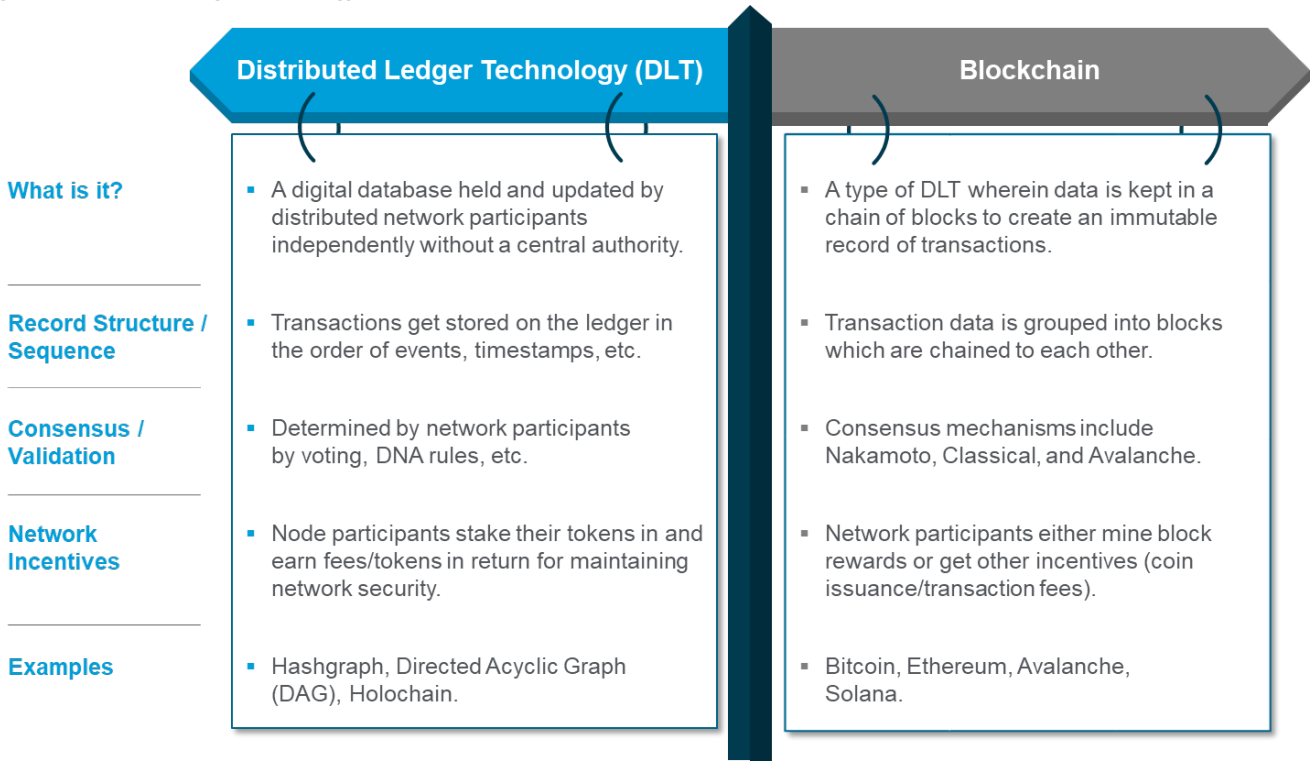
© 2023 Citigroup

Defining Blockchain, DLT, and Web3

Blockchains are a peer-to-peer network based on cryptography that creates a decentralized, immutable ledger that records information and transactions free from any central authority. Blockchains can be either public or private.

Distributed Ledger Technology (DLT) refers to a digital database held and updated by distributed network participants independently, without any central authority. Notably, while all blockchains are distributed ledgers, not all distributed ledgers are blockchains. Below, we summarize key differences between blockchains and DLT:

Figure 2. Distributed Ledger Technology vs. Blockchain



Source: Blockchain Council, 101 Blockchains, Citi GPS

Web3, as it is often called, refers to the third iteration of the internet and is based on ownership and decentralization, which is facilitated via blockchain. Web3 decentralization could result in a more transparent environment and help address issues of ownership and control from the Web2 world.

As we explain in this report, a key driver of Web3 and blockchain adoption will be Web2 consumer companies and established traditional financial institutions. We believe Web3 will run in parallel with Web2 and in some cases will be nested inside it — think of the Russian Matryoshka nesting dolls!

© 2023 Citigroup

Figure 3. A Framework for the Evolution of the Internet: Web1 vs. Web2 vs. Web3

	Web1	Web2	Web3
Time period	1996-2004	2004-2016	2016+
Content	Existing information gathered into a single database	Individuals gained the ability to create information in a global database	Individuals have the potential to monetize their own data
Information	Mostly Read Only	Read and Write	Read, Write & Own
Advertising	Banners	Interactive	Behavioral
Access Medium	Desktop browser access	"Mobile first" always on	Wearable AR/VR, voice, and Internet-of-Things devices
Technologies	HTML, FTP	Flash, Java, XML	RDF, RDFS, OWL

Source: ResearchGate, Wordpress, Citi GPS

Defining Tokenization?

Tokenization refers to the creation of tokens, which are pieces of code on a blockchain, to record information about underlying assets, including their attributes or characteristics, status, transaction history, and ownership

Tokenization refers to the creation of tokens, which are pieces of code on a blockchain, to record information about underlying assets and liabilities including their attributes or characteristics, status, transaction history, and ownership. Tokens enable the trade and transfer of ownership and titles of value directly via a digital ledger. At a high level, tokenized assets can be separated into two categories:

- **Real-World Assets:** These represent highly illiquid, bespoke assets such as real estate, art and collectibles, agriculture, climate assets, and intangible assets like carbon credits and intellectual property. Real-world assets could also include financial assets that are not traded frequently or easily, such as trade invoices, private loans, or mortgages, and are not usually categorized as "securities."
- **Financial Assets:** These refer to the creation of tokens that represent existing financial value such as money, stocks, bonds, commodities, and funds. (See The "Trillions in Value" section for a deep-dive analysis of this important topic.)

In theory, almost anything with monetary value can be tokenized.[3] In this report, we argue that among the best use cases of tokenization will be money (CBDCs) and private financial assets, especially illiquid ones, and over time, in-game assets.

Sizing the Tokenization Opportunity

Tokenization of real-world assets unlocks a new way to monetize illiquid assets

According to a BCG and ADDX study, tokenization of global illiquid assets is estimated to be a $16 trillion business opportunity, or nearly 10% of global GDP by 2030.[4] This includes $3 trillion in home equity, $4 trillion in listed/unlisted and other equity, $1 trillion in bonds and investment funds, $3 trillion in other financial assets, and $5 trillion in other tokenizable assets.

[3] Ravi Chamria, "Comprehensive Guide on Tokenized Real-World Assets," Government Blockchain Association, December 1, 2022.
[4] Sumit Kumar et al., "Relevance of On-Chain Asset Tokenization in Crypto Winter," BCG x ADDX, August 2022.

© 2023 Citigroup

> The total addressable market for tokenization could, at least theoretically, be as high as the total value of global assets, running into the hundreds of trillions of dollars. But do we really need everything to be on the blockchain?
>
> – JOHN WU, PRESIDENT OF AVA LABS[5]

- We believe the private/unlisted market is more suitable for blockchain adoption due to the resulting liquidity, transparency, and fractionalization. For public securities across sectors, tokenization will also provide other benefits in areas such as efficiency, collateral use, golden sources of data, and ESG tracking.
- We are very early in the process of these products growing but, based on conversations with internal and expert domain experts, we forecast $4 trillion to $5 trillion of tokenized digital securities by 2030, assuming 1% of corporate and quasi-sovereign bonds, 7.5% of real estate funds, and 10% of PE/VC funds and 2% of repo, securities financing and collateral markets are tokenized.
- Accompanying securities in tokenization will be the trade finance market, which could see up to $1 trillion of DLT-based volumes, or around 8%-10% of global trade finance volumes, by 2030.
- We will need the support of large financial institutions, which are increasingly focused on tokenization and the support of the law, where notable changes are taking place in areas such as English law, which governs most international trade finance.

Why Tokenize Real-World Assets?

Tokenization of real-world assets unlocks a new way to monetize illiquid assets. For example, a numismatist or philatelist can tokenize their rare collection of coins or stamps by fractionalizing and sharing ownership of assets with buyers across the world and delivering custody of underlying assets to a museum for display and safekeeping. This could help them retain partial ownership and also unlock liquidity.

Artists can also create videos on social media and sell NFTs representing rights to use their videos for marketing and commercial activities, thereby generating yield on their intellectual property (IP) without giving a share to centralized platforms.

Tokenization also unlocks new ways of financing infrastructural assets — roads, heavy machinery, and public goods — and opens new financing avenues for small companies and small and medium enterprises (SMEs) through direct-to-retail decentralized finance (DeFi) channels. Tokenization offers possibilities for blockchain technology to solve traditional problems, such as lack of transparency, liquidity, and democratized access. Tokenization also helps improve the efficiency of holding real-world assets on investor balance sheets, by potentially reducing liquidity capital asks and easing the collateralization process.

[5] Citi Global Insights, "Bridging Banks and Blockchain: Avalanche Deep Dive," webinar, October 19, 2022.

© 2023 Citigroup

- **Real Estate:** Traditional real estate often struggles with poor transparency, illiquidity, and multiple intermediaries. Blockchain could be a good fit as a single, shared source of truth in a market with multiple players, all working with overlapping data and the need for constant reconciliation. Tokenization could also help reduce minimum investment amounts and open up asset discovery.
- **Art and Collectibles (e.g., wine, cars, Pokemon cards, etc.):** Tokenization of art and collectibles can help increase transparency, act as a proof of provenance, increase liquidity, and offer decentralized ownership, including the ability to fractionalize the asset to a group of investors. We discuss this more in detail in the Art and Collectibles section.
- **Unconventional Commodities:** Commodities ranging from gold to agricultural products are increasingly being brought on-chain.
  - **Agriculture:** Platforms like Agrotoken use Oracles and real-world proof of grain reserves to create stablecoins backed by commodities such as soy, corn, and wheat, offering new funding solutions.
  - **Climate-Focused Projects:** Blockchains can help record and transfer carbon credits reliably between suppliers and those with demand while also reducing the entry threshold for carbon trading.

Challenges Bringing Real World Assets On-Chain

A fragmented regulatory landscape and a lack of a unified taxonomy are major scalability hurdles for digital assets

Common scalability hurdles for digital assets include a fragmented legal and regulatory landscape across different jurisdictions and a disunified taxonomy or classification standard at global scale. The tokenization of real-world assets may also encounter additional challenges, which we elaborate on below:

- **Interoperability Issues:** Having multiple blockchains can lead to interoperability problems while interacting with centralized backend systems outside blockchain ecosystems, as well as across new architectures built on different chains.
- **Lack of Experienced Custodians:** There is a limited number of third parties with expertise in safe-keeping tokens and underlying real-world assets.
- **Duplication and Unauthorized Tokenization:** While information on public blockchain is publicly visible, there is a lack of surveillance and standard practice to slash duplicated or unauthorized tokens linked to underlying assets.
- **Real-World Liquidity Risks:** On-chain liquidity tends to be deeper than that in the real world, likely due to fractionalization and democratized market access.
- **Elevated Cyber Risk:** More technological development is needed to enable transparency on blockchain without revealing the actual information of borrowers and asset owners. The most widely used present solution for privacy are zero-knowledge proofs (ZKPs). Tokenization also creates additional risk related to theft and loss of tokens due to cyberattacks on blockchains and digital wallets.
- **Difficulty of Full Disintermediation**: Internet-of-Things (IoT) technology and Oracle networks used for asset appraisal and status reporting of underlying real-world assets are still at a nascent stage and may take time to reach large-scale commercialization. Until then, many crucial steps such as evaluation, accounting, and reporting may still rely on human expertise and manual labor just like traditional finance.

© 2023 Citigroup

As the infrastructure supporting tokenization continues to develop and mature, we expect to see more blockchain-native assets, with their entire life cycle being managed and completed on-chain.

© 2023 Citigroup

A Conversation With Henri Arslanian on the ChatGPT Moment for Blockchain

Henri Arslanian is the co-founder and managing partner of Nine Blocks Capital Management, an institutional-grade hedge fund manager focused exclusively on digital assets. Henri was previously a partner and global crypto leader at PwC. Henri is also the author of numerous best-selling crypto and fintech books, including *The Book of Crypto* (Palgrave, 2022), which became a global top 10 bestseller in financial services, and *The Future of Finance* (Palgrave, 2019), which became not only a global top 10 best-seller in financial services but was also recognized as one of the "Best FinTech Books of All Time" by BookAuthority.

Q: Blockchain has been talked about for several years. What is holding it back? What is the ChatGPT moment for blockchain/Web3 adoption?

Henri: We have seen a lot of discussions around blockchain and distributed ledger technology since 2015. However, blockchains need to be seamlessly integrated into our daily activities for mass adoption. The technology needs to be easy to use for the common person, such that they do not even know when they are using it.

For example, when we connect to WiFi on our smartphones, we access the internet, without understanding the protocols and infrastructure operating behind the scenes. A similar integration is needed for blockchain and Web3 tools. We are not there yet.

More recently, we are seeing interesting developments. For example, Coinbase launched an Ethereum layer 2 solution, called Base, which is designed to offer a developer-friendly platform for people to build decentralized applications (dApps) by accessing the front-end of the Coinbase interface, without actually knowing if they are dealing with DeFi, NFTs, or other layer 2 solutions.

In my view, blockchain offers tremendous benefits, with potential use cases spanning digital identity, digital proof of address, digital birth certificates, digital academic degrees, and digital land title deeds. Development of blockchain for any of the above use cases could lead to a significant boost in mainstream adoption.

In the near term, I am most excited for the gaming sector. The gaming industry has over 3 billion users already. Today, several games operate in the Metaverse or a Metaverse-like ecosystem, where blockchain can be adopted for in-game purchases of new skins for avatars, weapons, real estate, or other accessories. I see a lot of scope for synergies between the gaming and digital asset industries.

Q: Which industries are likely to be most and least impacted by blockchain in the next 5-10 years?

Henri: In my view, every industry is likely to be impacted by emerging trends in blockchain and digital assets. Industries unable to quickly adapt to change, or ones with several intermediaries, are likely to be most impacted. Humans, by nature, adopt a protectionist approach when faced with radical change. A relatable example could be the early response from traditional taxi operators across major cities following the introduction of Uber services.

Today, we see a similar situation with law societies and legal bodies taking action against LawTech and RegTech startups. In my opinion, traditional legal services are often cumbersome, with large volumes of complicated documents requiring time and money. Startups are exploring the use of AI, machine learning, and blockchain to make these services more accessible and easier to use for the general public.

Embracing blockchain could help remove process inefficiencies. However, industry bodies are often looking to protect their members (e.g., lawyers and notaries) against making access to justice more accessible. This is similar to how the taxi unions tried to ban and take action against Uber in its early days.

© 2023 Citigroup

Looking at other industries, traditional auditing processes rely on a sampling of transactions, as it is very difficult to review all transactions, especially in large companies. Accounting firms and standard setters can explore the use of blockchain, enabling continuous audits by putting transactions on-chain.

Over the next 5-10 years, I see great potential for an autonomous future. We could have self-driving cars transport us from location A to B. The car I own could then self-drive other passengers when I am not using it and thus bring me a return on my investment. This example can be extended to other verticals as well. The car could be connected to the financial ecosystem, where it periodically checks the best refinancing rates in the market. It could also help find the cheapest and most sustainable source of energy for charging. The list goes on.

Most of these examples are of automation or AI, but for transactions to work, the backend systems need to be linked to some form of blockchain or DLT. Blockchain combined with AI can have tremendous synergetic benefits.

Q: Can central bank-issued digital currencies (CBDCs) play a significant role in driving blockchain adoption in the years ahead?

Henri: In my view, we are likely to see mainstream adoption and usage of CBDCs in the next few years, both for retail and wholesale use cases. The unfortunate events around the crypto collapses in 2022 and the ensuing concern and fears in the digital asset market are only likely to accelerate CBDC development.

According to Bank of International Settlement (BIS) data, over 90% of the global central banks are exploring or running pilots and experiments for CBDC use. Countries such as the Bahamas and Nigeria have already launched their CBDCs, known as Sand Dollar and eNaira, respectively. Several other countries, like India, are running pilots. The e-CNY pilot in China has already scaled to several hundred million users.

CBDCs are likely to remain a political and societal debate in the foreseeable future. Proponents of CBDCs cite advantages such as reduction of corruption, which ordinarily occurs in paper-based money that is not easily traceable. Tax evasion prevention could be another benefit, as CBDCs help eliminate the shadow economy. On the flip side, critics cite concerns over user privacy and the potential for excessive government controls. However, CBDCs are a key area to monitor, especially the progress in emerging and developing markets like India, China, and Africa.

Q: How can we protect ourselves in a digital world with deepfakes and skepticism? Can blockchain help build trust?

Henri: Looking ahead, I see deepfakes and frauds continuing to grow in quantity and quality. The use of blockchain can help mitigate some concerns by establishing authenticity and provenance.

Blockchain is also important for the content creator economy. Today, Web2 platforms own user-created content. This poses risks should the platform operator unilaterally decide to restrict or delete it. Web3 can help transfer ownership back to the users. Web3 can also help create a content-vetting mechanism, using the independent users from its community model, to help detect fakes and frauds.

© 2023 Citigroup

Billions of Users

Some of the key areas where blockchain-based products can make a significant impact on consumers will be in money, gaming, and social. In this chapter, we discuss how blockchain is revolutionizing this space, why is it happening now, and how it could reach billions of users.

Nearly 2 billion individuals from India, Europe, and the UK could use CBDCs, which may be partly DLT-linked by 2030

First, let us look at digital programmable money (i.e., central bank digital currencies —CBDCs). There will likely be tokenized versions of major currencies such as the euro (EUR), British pound (GBP), and Indian rupee (INR) in use during the 2020s, in addition to the Chinese renminbi (RMB), which has already been trialed for a couple of years. Together, these four jurisdictions constitute more than 50% of the global population and 35% of global bank deposits.

We discussed CBDCs in detail in a previous Citi GPS report, titled *Future of Money: Crypto, CBDCs, and 21st Century Cash*. Since then, interest in CBDCs has only increased among policy makers. In recent months, we have had large country central banks announcing CBDC plans, including India and the EU.

The technology choices are still being ironed out, but distributed ledger technology (DLT) and blockchain options are being considered. About 20% of deposits are forecast to move to tokenized money formats.[6] Hence, we think CBDCs overall could have 2 billion users and over $5 trillion of value in circulation — of which about half could be on a DLT-linked model.

In the next 1-2 years, we could see 100 million gamers move to blockchain-based games

Gaming could potentially be one of the biggest segments for bottom-up Web3 consumer adoption. In 2022, over 1 million unique active wallets connected to game dApps daily in 2022.[7] With the advent of improved Web3 games, especially from Asian studios in the next 1-2 years, we could see the most active gamers (nearly 100 million “whales”) move over to blockchain-based games. This could trigger a rush by mainstream gaming studios to incorporate blockchain and tokenization elements in their games.

The emergence of Web3 and the growth of the creator economy empowers users to own their content. And Web2 companies are getting in on the action with one social media forum onboarding millions of users into Web3 through their “collectible avatars” (NFTs).

> We believe new technologies like blockchain and NFTs can allow creators to build deeper relationships with their fans…
>
> – NEAL MOHAN, CEO OF YOUTUBE[8]

[6] Bank of England, “New Forms of Digital Money: Discussion Paper,” June 2021.
[7] Sara Gherghelas, “DappRadar x BGA Games Report — 2022 Overview,” DappRadar, January 26, 2023.
[8] Andre Beganski, “New YouTube CEO Is Bullish on Web3 Tech Like NFTs and the Metaverse,” Decrypt, February 20, 2023.

© 2023 Citigroup

Consumer brands and fashion labels like Adidas, Nike, Burberry, and Gucci are embracing NFTs and in-game assets in an attempt to be part of the next big cultural and marketing trend. In April 2023, Amazon plans to launch a NFT marketplace for its 167 million Prime users in the U.S., and this initiative could go global thereafter.[9]

[9] Michael Bodley, "Amazon NFTs Will Be Tied to Real-World Assets, Token Possible," Blockworks, March 6, 2023.

© 2023 Citigroup

Central Bank Digital Currencies (CBDCs)

Key Takeaways on CBDCs

Until now, only smaller CBDC projects have been based on DLT; however, in the coming years, we could see some major central bank CBDC (or parts of it) based on DLT

1. **More Big Countries Catching Up:** Initially, only a few smaller island nations and Nigeria launched CBDCs and China was in advanced stages of researching and piloting a CBDC. Now, major countries in terms of economy, currency, and population size are warming up to the idea of CBDCs. For example, the central banks of India, the UK, and Europe have been making plans to launch CBDCs (potentially DLT-linked) before the end of the decade.
2. **Billions of Users:** Taking into account only Europe, India, and the UK, there are about 2 billion individuals and businesses that could be using some form of CBDC. Businesses in countries with multi-CBDC bridge arrangements would also use DLT-linked CBDCs, although their domestic CBDCs would be non-DLT-linked.
3. **Technology:** Until now, only the smaller CBDC projects have been based on DLT. However, we can envision some major banks issuing DLT-based (or partially DLT-based) CBDCs and India's retail CBDC could have some sort of DLT. China's participation in the mCBDC Bridge is based on a DLT.
4. **Money Mobilized:** Central banks estimate up to 20% of deposits could transition to newer digital money formats.[10] We could have $5 trillion of CBDCs circulating in major economies in the world in this decade, half of which could potentially be DLT-linked.

India, the UK, and Europe are all planning to launch CBDCs — potentially DLT-linked — during the 2020s

CBDCs are increasingly relevant as a financial policy and plumbing question. Collectively, the EUR, GBP, and INR constitute around 15% of the world's monetary base (i.e., M0, which is currency in circulation and money being held by banks in reserves), or $15 trillion, and 22% of the global narrow money (i.e., banknotes and coins, plus overnight deposits), at $71 trillion. Central banks estimate up to 20% of the deposits could transition to newer digital money formats.[11] We could have $5 trillion of CBDCs circulating in major economies in the world in this decade, of which half could be DLT-linked.

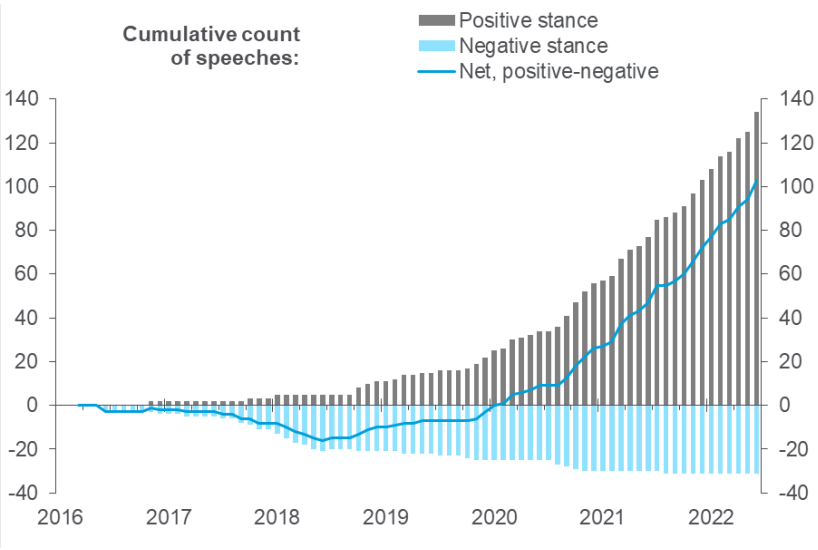
Besides individuals, millions of businesses and importers/exporters will use bilateral or multi-CBDC (mCBDC) arrangements developed between different countries. For example, the mCBDC Bridge between China, Hong Kong, Thailand, and the UAE uses DLT and is piloting different use cases, starting with cross-border foreign exchange (FX) trade settlement (discussed in detail in the "Trade Finance" section).

Interest in CBDCs continues to increase among policymakers. Central banks' accelerating interest has been driven by the announcement of a private sector stablecoin, Libra, led by Meta (then Facebook); China being in advanced stages of work on an e-RMB (or e-CNY); the growth of digital finance in general, and the acceleration of this mega-trend during the COVID-19 pandemic.

[10] Bank of England, "New Forms of Digital Money: Discussion Paper," June 2021.
[11] Ibid.

© 2023 Citigroup

Figure 4. Positive and Negative Stance of Central Banks on CBDCs (Number of Speeches)



Note: Search on "CBDC," "digital currency," and "digital money." Classification based on authors' judgement. Score takes value of -1 if speech stance clearly negative or if explicitly said there was no specific plan at present to issue digital currencies. Value of +1 if speech stance clearly positive or project/pilot launched/in pipeline. Other speeches (not displayed) have been classified as neutral. The material is available on the BIS website free of charge: www.bis.org.

Source: Citi GPS, BIS Working Paper "Rise of the Central Bank Digital Currencies: Drives, Approaches, and Technologies"

Growth of CBDCs during the 2020s will have implications for:

- **Domestic Payment Systems:** CBDCs could be competition for existing payment rails.
- **Digital Wallets:** State-backed digital tokens could spur growth of digital wallets.
- **Bank Balance Sheets:** Partial replacement of deposits, reserve requirements.
- **Cross-Border Flows in CBDCs:** CBDCs could partially replace correspondent banking.
- **Sovereign Competition:** Will currencies with a tokenized version be used more?
- **Technology:** Many of the CBDC projects are partially DLT-linked.

We discuss these points in greater detail in the rest of this chapter.

Why CBDCs?

CBDCs are increasingly important in financial and monetary policy questions and could also work as an efficient tool to mobilize bank reserves

A survey on CBDCs by the Bank for International Settlements (BIS) suggests emerging markets and developing economies (EMDEs) report a higher motivation for issuing CBDCs versus advanced economies. Financial inclusion and domestic payment efficiency remain top motivators for CBDC development amongst EMDEs.[12]

[12] Anneke Kosse and Ilaria Mattei, *BIS Papers No 125: Gaining Momentum — Results of the 2021 BIS Survey on Central Bank Digital Currencies*, Bank for International Settlements, May 2022.

© 2023 Citigroup

Private forms of digital money often create closed loops wherein users are not able to transact with other users or merchants outside of the system. Moreover, convertibility to different forms of money is also restricted. A CBDC accepted nationwide would act as an interoperable payment instrument.

Another use case, not much discussed, is to act as a tool for bank reserves and balance sheet management. UK banks hold around £947 billion ($1.2 trillion) worth of reserves with the Bank of England, while the minimum quantity of reserves needed by UK banks may be around £325 billion to £480 billion.[13] CBDCs could work as a replacement of these reserves.

Bank reserves held at the central bank are not transferable, and hence not fungible. However, central bank-issued money, including a CBDC, is fungible. If CBDCs are treated as high quality liquid assets, banks can use them as collateral to borrow (repo). CBDCs could be seen as a balance sheet and liquidity management tool for central banks and commercial banks.

Work around researching and launching CBDCs has partly accelerated in response to the launch of a private stablecoin. However, ironically, the successful launch and adoption of CBDCs would lead to more stablecoin projects becoming mainstream. This is because the stablecoin protocol is now able to hold reserves in CBDCs, which are more stable and liquid than money market instruments.

What Are CBDCs?

CBDCs are central bank-issued digital money denominated in the national unit of account and representing a liability of the central bank

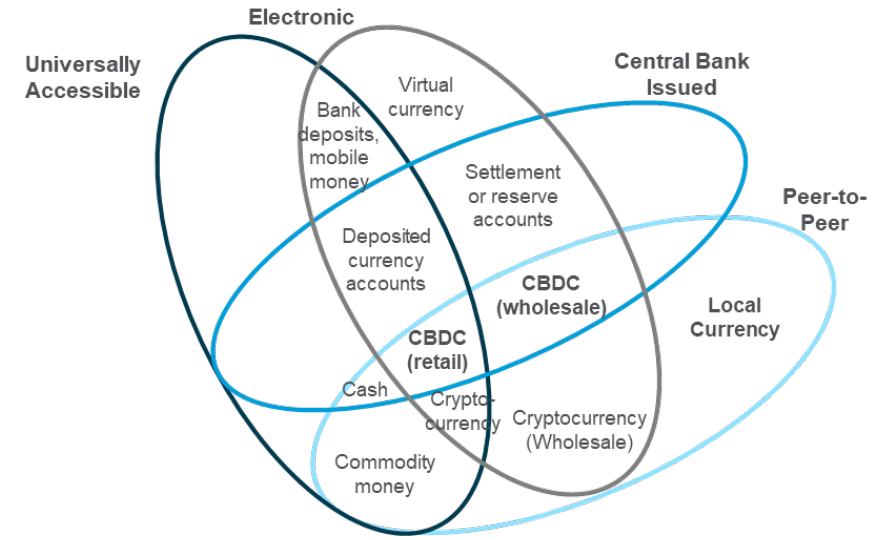
A CBDC is central bank-issued digital money denominated in the national unit of account, and represents a liability of the central bank.[14] It is the liability of a central bank that is the key distinguishing feature between other forms of digital payment instruments (e.g., card payment, e-money, credit transfer) which are liabilities of private institutions.

The money flower (Figure 5) was first published by BIS in 2017, which makes it quite old, but still classic and relevant as it captures examples of money from the past, present, and future.[15] BIS distinguishes between two possible forms of CBDCs: (1) a widely available, consumer-facing payment instrument targeted at retail transactions and (2) a restricted-access, digital settlement token for wholesale payment applications.

[13] Bank of England, "What Do We Know About the Demand for Bank of England Reserves?," February 2023.
[14] Anneke Kosse and Ilaria Mattei, *BIS Papers No 125: Gaining Momentum — Results of the 2021 BIS Survey on Central Bank Digital Currencies*, Bank for International Settlements, May 2022.
[15] Morten Bech and Rodney Garratt, *Central Bank Cryptocurrencies*, BIS Quarterly Review, September 2017.

© 2023 Citigroup

Figure 5. Money Flower: A Taxonomy of Money

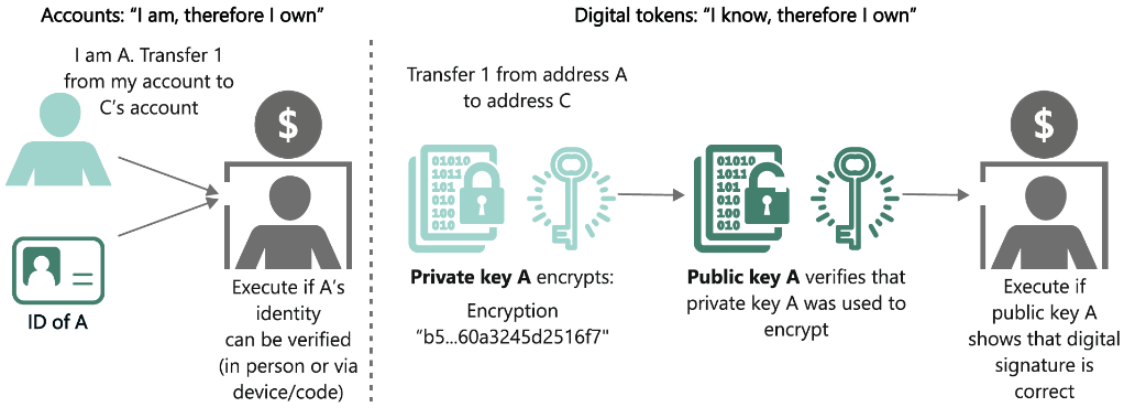


Source: BIS Quarterly Review "Central Bank Cryptocurrencies." Material available freely at www.bis.org

In terms of verification of payment, both token-based CBDCs and account-based CBDCs are possible. In payment economics, the way of verification distinguishes two kinds of payment systems: tokenized and account-based.

- **Token-based CBDC:** Coin, notes, and electronic stored value are examples of the tokenized system. In a token-based CBDC, claims are honored based on demonstrated knowledge, e.g., digital signature. However, KYC-ed wallets, i.e., wallets verified for "know your customer" rules, can also be used. Token-based CBDC are also called value-based CBDC.
- **Account-based CBDC:** An intermediary verifies the account holders' identity for transactions, e.g., banking account and cards. In an account-based CBDC, ownership is tied to an identity and transactions are authorized via identification.

Figure 6. Account-Based Access vs. Token-Based Access



Source: BIS speech titled "Digital Currencies and the Future of the Monetary System." Material available freely at www.bis.org.

© 2023 Citigroup

To DLT or Not to DLT? That Is the CBDC Question

We expect some major CBDCs to be blockchain-based, either in full or in part

Many of the smaller-currency CBDCs are DLT-linked (see Figure 7). We expect some major CBDCs, in full or in part, could also be blockchain-based — although the major sovereigns appear to want to primarily rely on a centralized ledger due to policy preferences (e.g., China). The domestic implementation of many of the major CBDCs is expected to be on a centralized ledger, mainly due to policy preferences and efficiency gains at scale.

We expect cross-border CBDCs could be primarily DLT- or blockchain-based, for the sake of ease and because it could bring down the cost and time of foreign exchange transfers, thereby creating operational efficiencies. It could also disintermediate layers of correspondent banking and lead the race of superior currency technology.

For example, Project Icebreaker is a collaboration between the Bank of Israel, Norges Bank, Sveriges Riksbank, and the BIS Innovation Hub that is testing the technical feasibility of conducting cross-border and cross-currency transactions between different DLT-linked CBDC proofs of concept. The aim is to gain a deeper understanding of the technologies used, as well as to identify the key technical and policy choices and trade-offs that central banks would need to consider in designing CBDC implementations that facilitate cross-border payments.

China is currently well ahead of major peers in developing a CBDC (referred to as e-RMB, e-CNY, or Digital Currency Electronic Payment or DCEP) and is already at the point of extensive pilot testing. Given the country's sprint to becoming a cashless society, we expect fast adoption of DCEP over the next five years relative to other CBDCs.

The e-RMB does not have a fixed path on its technical route. The central bank has initiated a “horse racing” model where several designated operators have adopted different technical routes for developing DCEP. We believe the core ledger will remain a centralized one with DLT options possible at the distribution layer.

© 2023 Citigroup

Figure 7. Select Central Banks' CBDC Projects

Country / Region	Announcement Year	Status	Retail / Wholesale	Technology	DLT / Non-DLT
Australia	2022	Research	Wholesale	Ethereum	DLT
Australia	2021	Research	Retail	Ethereum	DLT
Bahamas	2022	Launched	Retail	NZIA Cortex DLT	DLT
Bhutan	2021	Research	Retail, Wholesale	XRP Ledger	DLT*
Brazil	2022	Proof of concept	Retail		DLT
Canada	2016	Pilot	Wholesale	R3 Corda	DLT
Canada	2017	Research	Wholesale		Non-DLT*
China	2022	Pilot	Retail		Non-DLT
Eswatini	2022	Research	Retail	Filia	Non-DLT
Euro Area	2020	Research	Retail, Wholesale		Non-DLT*
France	2022	Pilot	Wholesale	DL3S	DLT
France	2022	Pilot	Wholesale	DL3S	DLT
Hong Kong	2021	Research	Retail		DLT*
mBridge	2022	Research	Retail		DLT
India	2022	Pilot	Retail		DLT
India	2022	Pilot	Wholesale		Non-DLT*
Jamaica	2022	Launched	Retail	DSC	Non-DLT
Japan	2021	Proof of concept	Retail		Non-DLT*
Japan	2016	Research	Other		DLT
Nigeria	2022	Pilot	Retail	Hyperledger Fabric	DLT
Norway	2022	Proof of concept	Retail	Ethereum, Hyperledger Besu	DLT
Saudi Arabia	2022	Research	CBDC		DLT*
Singapore	2022	Pilot	Wholesale		DLT*
South Africa	2022	Research	Wholesale	Quorum	DLT
South Korea	2022	Proof of concept	Retail		Non-DLT*
Sweden	2017	Proof of concept	Retail		DLT
United Arab Emirates	2022	Research	Retail		DLT*
United Kingdom	2022	Research	Retail		Non-DLT*
U.S. Fed CBDC	2022	Research	Wholesale		Non-DLT*

*Denotes Citi estimates.
Source: Citi GPS, CBDC Tracker

Risks and Implications of a CBDC

Out of the 100+ central banks involved in CBDC research, development, and piloting, only three central banks have officially launched CBDCs: Nigeria, the Bahamas, and Jamaica. Others are in pilot stage, most significantly China, India, Japan, and the UAE.

China was the first large economy to pilot a CBDC in April 2020. However, the results from these live CBDC projects and the pilots are quite unimpressive.

The risks and implications of CBDCs include:

- **Central Banks Competing with Private Players:** CBDCs could potentially increase competition in a country's payments sector — either directly by competing with existing forms of payments, or indirectly by competing with private payment and digital wallet players if the CBDC is designed as a platform open to private payment providers.

© 2023 Citigroup

- **Loss of Privacy:** Risk of excess surveillance and loss of privacy of private citizens' transactions are often cited as a risk and a hindrance for uptake of a central bank digital currency. CBDC transactions will not be anonymous, unlike traditional cash transactions.[16] For example, Nigeria's digital currency faced criticism citing potential surveillance and curbs on freedom.[17] Ways to address such fear could include making data visible only to the financial intermediaries, such as banks and third-party payment companies, and not automatically to the central banks.

- **Loss of Bank Deposits:** The Bank of England (BoE) estimated 20% of household and corporate bank deposits may flee from banks to new forms of money.[18] As a result, banks may replace the lost deposit money with wholesale funding that is costlier than customer deposits. The higher cost will have to be passed on to the borrowers through increased lending rates. Disintermediation of banks could also affect efficient monetary policy transmission. Notably, the European Central Bank (ECB) is considering a cap of €3,000 for holding digital euros, and the Bank of England is considering a cap of £10,000-£20,000 for digital pounds.[19]

- **Limited Uptake:** In the Bahamas, the per capita value of CBDCs is just 86 cents compared with the per capita cash value of $1,365. Less than 0.5% of Nigerians are using the eNaira. Outstanding e-RMB is at only $2 billion or 0.13% of outstanding monetary base, or M0 and 0.005% of M2, as of December 2022. Reasons for the slow update range from inertia and complexity to a lack of digital literacy.

Case Studies

Case Study 1: Digital Euro

The ECB is working with euro area national banks on the subject of introducing a digital euro. The investigation phase started in October 2021 and is expected to take nearly two years. The ECB is exploring how a digital euro can be designed and distributed, as well as its impact on the market. After the third quarter of 2023, it will take another three years of building to go live, so the earliest launch of the digital euro will be 2026 or beyond.

Why is the ECB looking into launching a digital euro? According to the ECB, it is considering launching a CBDC in Europe to respond to the increasing demand for safe and trusted electronic payments. Having digital money issued by the central bank would provide an anchor of stability for the payment and monetary systems. A digital euro would also strengthen the monetary sovereignty of the euro area and foster competition and efficiency in the European payment sector.

[16] Bank of England and HM Treasury, *The Digital Pound: A New Form of Money for Households and Businesses*, February 7, 2023.
[17] Abubakur Nur Khali, "Nigerian Election and Naira Crisis is Fueling Bitcoin Adoption," *Forbes*, March 1, 2023.
[18] Bank of England, "New Forms of Digital Money: Discussion Paper," June 2021.
[19] Lorenzo Burlon et al., *Working Paper Series: The Optimal Quantity of CBDC in a Bank-Based Economy, No. 2689*, European Central Bank (ECB), July 2022; Bank of England and HM Treasury, *The Digital Pound: A New Form of Money for Households and Businesses*, February 7, 2023.

© 2023 Citigroup

A progress report, released in December 2022, outlined a set of design and distribution options and the role of the Eurosystem and intermediaries.[20] The ECB is still in the investigative stages regarding what technology it will use for issuing and settling a digital euro.

Funding and defunding functionalities would enable the end user to top up or withdraw digital euro holdings by transferring money in or out of private money or cash. Furthermore, waterfall and reverse waterfall functionality will be an added feature that can be activated at user discretion — this means pushing funds from the digital euro wallet in excess of the threshold limit to a linked private account at the time of receiving a payment, and vice versa.

Subsequent progress reports will assess further functionalities such as programmable payments, cross-currency payments, and additional distribution models.

Case Study 2: Digital Pound

The Bank of England and HM Treasury published a digital pound consultation paper in February 2023 arguing it is likely that a retail, general purpose digital central bank currency — i.e., a digital pound — will be needed in the UK. This would be a new, digital form of money, issued by the BoE for use by households and businesses for everyday payment.[21]

The central bank's motivation and drivers for a CBDC include geopolitical concerns, a decline in cash usage, developments in the digitization of money from non-bank players, and improving cross-border payments.

The BoE is in the initial exploration stage, and the work over the next 2-3 years will inform its decision and reduce the lead time to launch should the decision at the end of this stage be to implement the digital pound. The digital currency could then be introduced in the second half of the decade.[22]

Over the past decade and half, cash transactions in the UK have fallen from 62% in 2006 to 15% in 2021.[23] The cost of accepting card payments for the smallest merchants is four times higher than for the largest merchants. Innovation in public money, toward a a digital format of cash, can likely reduce payment costs and improve efficiency in payments.

The technological functionalities emerging in money and payments, such as decentralized finance, blockchain, and smart contracts, are outside the traditional financial sector and could be applicable in the design of a digital pound.

A digital pound risks disintermediation of the banking sector and will have an influence on financial intermediaries' balance sheets, income statements, business models, and services. While holding limits can act as a mitigant, there may be additional risks should the limits be higher than anticipated. During the introductory period, an individual limit of £10,000-£20,000 may be imposed.

---

[20] ECB, *Progress on the Investigation Phase of a Digital Euro: Second Report*, December 21, 2022.
[21] Bank of England and HM Treasury, *The Digital Pound: A New Form of Money for Households and Businesses*, February 7, 2023.
[22] Ibid.
[23] UK Finance, *UK Payments Markets Summary 2022*, August 2022.

© 2023 Citigroup

The proposed digital pound is based on a platform model where the central bank would issue the digital pounds recorded on the core ledger. The platform model would be technology-agnostic — meaning the central bank could issue a digital pound on a centralized database or through distributed ledger technology.[24]

UK policymakers say a digital pound could complement and support new forms of private digital money and payment services if designed appropriately, e.g., by acting as the "bridging asset" between different platforms enabling convertibility. The ledger will allow private sector players to connect to the core ledger via Application Programming Interfaces (APIs). The private sector would provide a wallet interface where users can interact.

While the consultation paper is focused primarily on a retail CBDC, for the BoE this is not a question of simply retail or wholesale. They are working extensively on both areas, including through the renewal of Real Time Gross Settlement (RTGS), but they are also investigating other models. This rhetoric shows a shift from the notion that the BoE is not looking at wholesale CBDCs.

Case Study 3: Digital Rupee

The Reserve Bank of India (RBI) has launched CBDC pilots in both wholesale and retail segments. The pilot in the wholesale segment was launched in November 2022, with use cases limited to the settlement of secondary market transactions in government securities. Potentially, some layers of the CBDC tech stack could be on a centralized system with others remaining on distributed networks.

The pilot in the retail segment was launched in December 2022 within a closed user group (CUG) comprised of participating customers and merchants. This pilot has components based on blockchain technology.

Given the success of the United Payments Interface (UPI), India's highly regarded digital payments scheme, why is a CBDC needed?

- **Backing:** A CBDC is backed by India's central bank — the RBI — while UPI is backed by several commercial banks. Moreover, UPI settlements are accomplished through central bank money.
- **Better Settlement and Finality:** Unlike UPI or other digital payments, CBDC will move from the payer's wallet to the receiver's wallet without any intermediation of banks. This reduces settlement risk in the financial system and enables finality. As of January 2023, some major banks had technical decline rates (transaction failures) of around 2%.[25]
- **Anonymity and Privacy:** Digital currency will not leave a digital footprint, and no third party can find transaction details (buyer and sender names, transaction values, etc.) as the information is not available from any bank or intermediary.

[24] Government of India Press Information Bureau, "Central Bank Digital Currency (CBDC) Pilot Launched by RBI in Retail Segment Has Components Based on Blockchain Technology," December 2022.
[25] NPCI, "UPI Ecosystem Statistics: January 2023," accessed March 21, 2023.

© 2023 Citigroup

- **Cost Considerations:** Reserve banks and commercial banks incur costs of INR 210 billion ($2.5 billion) annually in handling physical currency and INR 126 billion for settling UPI transactions (assuming 0.1% blended merchant discount rate, or MDR).[26]
- **Extend Use to Cross-Border Payments:** The initial focus of the digital rupee is on domestic payments, but once scaled it can be used for cross-border payments. This can help with remittances and provide strategic sovereign flexibility.

Case Study 4: Digital Dollar

There are three U.S. CBDC or tokenized dollar projects: (1) the Digital Dollar Project (DDP), (2) Project Hamilton by the Federal Reserve Bank of Boston and MIT's Digital Currency Initiative, and (3) CBDC-related exploration at the Federal Reserve Board (FRB).[27]

The DDP is a non-profit, non-governmental organization devoted to catalyzing the research, exploration, and real-world experimentation of a potential digital dollar. Its initial May 2020 whitepaper proposed a model of a potential digital dollar for public consideration to test and evaluate through a series of pilots and other research initiatives.[28] In November 2022, the DDP completed its first private sector-initiated, simulated, U.S. CBDC pilot in partnership with the Depository Trust and Clearing Corporation (DTCC) and with technical support from Accenture.[29]

The core tenets of DDP's model are: (1) tokenized architecture, (2) being complementary to cash and digital money, (3) distribution via commercial banks, (4) user privacy, (5) monetary policy neutrality, and (6) promotion of private sector participation and innovation.

The two-phased Project Hamilton involved researching the technical aspects of a U.S. dollar CBDC and creating a design for a modular, extensible transaction processing system. In February 2022, the project released some open-source research software, one of which was blockchain-based and the other of which was non-blockchain-based. The project concluded in December 2022.

The FRB has made no decisions on whether to pursue or implement a CBDC. Instead, it is just the exploring potential benefits and risks of CBDCs through technological research and experimentation. [30]

In parallel with the above mentioned CBDC projects, the Regulated Liability Network (RLN) was launched in November 2022 as a 12-week proof of concept with members of the U.S banking and payments community, and the New York Innovation Center, which is part of the Federal Reserve Bank of New York.

---

[26] Tufts University Fletcher School Institute for Business in the Global Context, *The Cost of Cash in India*, June 2020; Reserve Bank of India Department of Payment and Settlement Systems, *Discussion Paper on Charges in Payment Systems*, October 3, 2022. The source cites a 0.25% cost for P2M UPI transaction. We assume blended 0.1% for all transactions.

[27] Digital Dollar Project, *White Paper 2.0: Revisiting the Digital Dollar Project's Exploration of a U.S. Central Bank Digital Currency*, January 2023.

[28] Digital Dollar Project, *Exploring a US CBDC*, May 2020.

[29] DTCC, *Digital Dollar Project and DTCC: Security Settlement Pilot*, November 2022.

[30] Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation*, January 2022.

© 2023 Citigroup

The pilot explores the feasibility of an interoperable network of digital central bank liabilities and commercial bank digital money using distributed ledger technology. The RLN is an important step in the development of an always-on, programmable, multi-asset financial system. As of March 2023, the pilot is being conducted in a test environment using simulated data, and a report summarizing the fIndings will be released in 2023.

In February 2023, Congressman Tom Emmer proposed a bill aimed at limiting the Fed's ability to issue a CBDC. This could slow the progress on a digital dollar.

© 2023 Citigroup

A Conversation With Jessica Renier on CBDCs

Jessica Renier is Managing Director and Head of Digital Finance at the Institute of International Finance. Jessica has an extensive background in financial services and digital finance, with broad exposure to international policy, including positions at the U.S. Department of the Treasury, Deloitte Consulting, Federal Reserve Banks of New York and Dallas, J.P. Morgan Securities and the Hoover Institution. Most recently, Jessica served as Program Associate Director for the Housing, Treasury, and Commerce Departments, as well as the Small Business Administration, within the White House's Office of Management and Budget.

Q: Why are central banks more in action with CBDCs now compared to five years ago?

Jessica: Many central banks around the world are doing research with the primary goal of buying themselves optionality. This is optionality to launch a CBDC — retail or wholesale — should they determine it advantageous to do so, which they have not yet determined. China, which is, and has been ahead here for some years in CBDC development, is quite certain. However, it is more recent activity by a major western economy, specifically Europe, that is motivating greater interest in having the optionality to launch — if enough use cases are met, enough risks can be managed, and enough jurisdictions move forward with them. There are geopolitical implications under consideration, not just economic.

The rise of interest and activity in cryptoassets and stablecoins over the last five years has put more pressure on central banks to innovate and on governments to evaluate national security implications of technological advances in payments technology. In last few years, work on CBDCs has gone from internal conversations and desk research to consultative reports to gather public and private inputs on potential risks and benefits, to examining design features and digital wallet thresholds, to central banks building and testing proofs of concept. We are still far from real due diligence, however, on any of the risks or potential designs in practice.

Agustín Carstens, General Manager of the Bank for International Settlements (BIS) in his speech on February 22, 2023 at the Monetary Authority of Singapore (MAS) stated that CBDCs and tokenized deposits replicate existing forms of money in a technologically superior way, while preserving what he has previously referred to as the "the soul of money." The speech goes on to highlight BIS' forward thinking on wholesale as well as retail CBDCs, again, putting this in the context of tokenized deposits being a critical component of the future of a technologically superior financial system.

Q: Given that some smaller CBDC projects have been blockchain/DLT-linked, what will be the tech stack for major currencies like GBP, EUR, USD, and INR be?

Jessica: Several economies are pursuing sovereign digital currencies, all referred to as CBDCs, and yet they look very different from each other from a technology standpoint. If central banks do proceed, I do not see consensus yet on the best way to build one — and I am not certain a consensus will be reached on the technical level. Different countries have different reasons for pursuing a CBDC, whether they be related to the status of their existing infrastructure, types of payments and volume of funds that flow through their currency, differences in privacy policies, or differences in the ability of a given country to support the maintenance and security of such a system.

There has been and continues to be much excitement and belief that blockchain technology could solve a range of problems or bring efficiencies to processes that would benefit from being made technologically superior. I have no doubt that it will. That said, we are seeing the normal arc of innovation here, too. Investors get excited about a new or emerging technology, they test many hypotheses for its use, and then determine which realize value and which do not.

© 2023 Citigroup

There are many use cases where blockchain will not be a good fit, and that is to be expected. It is very possible that countries find during their CBDC research that the objectives that their jurisdiction may be looking to achieve are not actually served by a blockchain or particular DLT-linked solution.

Q: Is the United States being left behind in the race to CBDCs? What are the implications of wholesale CBDCs on the U.S. dollar?

Jessica: I do not think the U.S. is being left behind on the CBDC front. In the arc of innovation, some people always want to be out of the gate first and others take a bit more time to evaluate the use cases and technology to assess the fit while observing early lessons learned by those who are first out of the gate. There are still others who will take their time, watch it for a little longer, think more about it, evaluate the pros and cons more extensively, and then scale more quickly if and when they decide to proceed. Not everyone is positioned to do this. Some do not have the same capabilities or market dynamics to contend with as others, which typically drive this type of decision.

We often hear the mantra in entrepreneurial circles “innovate fast and fail fast.” By doing this, you avoid dragging out or exacerbating the downside of the failure and get busy implementing important lessons that were learned that may allow you to succeed the next time. However, CBDCs are sovereign currencies. A sovereign currency cannot afford to fail. It is not one of many digital assets or cryptocurrencies whose value can be wiped out without severe systemic impacts. The U.S. dollar is the world’s reserve currency and clearly does not have the option to fail, but it does have the ability to scale quickly.

Being first is less important for some than for others. I do not think the U.S. is ‘behind’ by accident. The U.S. is exactly where it intends to be. That said, it is understandable that other countries may want to develop CBDCs on a faster timeline. There are potentially significant geopolitical implications in the case of new wholesale CBDC systems that may reduce some dependence on the U.S. dollar in the execution of world trade where most invoices are denominated in dollars.

Irrespective of whether the U.S. ultimately launches a CBDC, U.S. entities such as the Digital Dollar Project and MIT’s Digital Currency Initiative, among others, are advancing leading research, conducting pilots, and catalyzing public discussion around appropriate principles for CBDCs — principles that are already and will, no doubt, continue to influence the thinking of both U.S. authorities and other countries pursuing CBDCs.

© 2023 Citigroup

Gaming

Five Key Takeaways on Gaming and Web3

We spoke with Ryan Wyatt, President of Polygon Labs, on the future of gaming in the Web3 world. We feature our full conversation further into the report; below are five key takeaways from our discussion.

1. **Gamers Do Not Care About Technology and Innovation:** Gamers do not typically care about the underlying technology powering their favorite games. For example, how often have you sought to understand the benefits of cloud computing and what it means for gaming? Do you determine which particular multi-player game to play based on whether it is hosted on Amazon Web Services or Google Cloud? The moment gamers have a Web3 equivalent of their existing game(s), they will likely switch as Web3 games can enable earning while playing their (new) favorite game.

2. **Challenges with Play-to-Earn Games:** Ryan expresses his view that the economics in play-to-earn games are often complex, while the gameplay tends to be rudimentary and not much fun. Furthermore, content was missing in the first generation of Web3 games, so gamers did not cling onto a game and make it a big hit. However, a few interesting concepts emerged from the play-to-earn model, such as the idea to reward users for participating in games, which can offer several interesting use cases.

3. **Power of Web3 and Blockchain in Gaming:** Games like *Minecraft* and *Roblox* already offer elements of ownership via mini-games, mods, and cosmetic items. However, one can imagine the power of putting these elements on-chain, improving visibility and portability, and allowing gamers to sell items or trade them with friends inside or outside the game.

4. **East vs. West in Game Development:** New gaming models (e.g., mobile or free-to-play) often originate from countries in the Eastern hemisphere. Countries such as South Korea, followed by Japan, are among the hotbeds of gaming innovation. By contrast, gaming studios in the Western hemisphere tend to be late adopters but help drive mass adoption.

5. **Inflection Point:** With over 3 billion gamers worldwide today, we are likely to see nearly 50 million to 100 million adopt games with some element of Web3 or blockchain by 2025. Gamers in Asia are likely to be the early adopters. However, it is useful to focus on the revenues and not the user numbers — a small fraction of global gamers account for the lion's share of money spent on games. We are likely to see a significant shift in transaction spends from off-chain to on-chain in the coming years. The disproportionate shift by heavy spenders to blockchain-based games is likely to be the inflection point for the entire ecosystem to incorporate token- and blockchain-based games.

© 2023 Citigroup

Gaming is the largest category in the entertainment industry, with revenues exceeding those of the film and music industries.[31] The gaming market is sizeable, with nearly 3.2 billion gamers as of 2022, based on data from Newzoo (see Figure 9).[32] Even if blockchain-based games are adopted by only a fraction of the total gaming community, this could translate to significant adoption numbers in the blockchain and Web3 ecosystem.

The gaming industry is intrinsically well-suited for blockchain, with gamers broadly having a good understanding of digital ownership and virtual assets

In our view, the gaming industry is intrinsically suited for blockchain. Gamers are tech-savvy, with most already having a good understanding of digital ownership and virtual assets. The emergence of Web3 and the rise of new economic models, such as play-to-earn, aim to empower gamers with ownership of their in-game assets. These digital assets can range from cryptocurrencies to in-game resources that are tokenized on the blockchain. But this has not really worked well so far.

Up to now, blockchain-based games are often developed by crypto-native folks with a greater focus on in-game tokens and monetization, versus the need to make games fun and exciting. Hardcore gamers often criticize the shallower and simpler gameplay in blockchain-based games. Some gamers also worry NFTs and in-game tokens could be yet another tool to extract more money from gamers.

> Out of the huge number of people who play games online, only a relatively small number need to participate in blockchain-based games for them to be a success.
>
> – RYAN WYATT, PRESIDENT, POLYGON LABS[33]

The next generation of game developers is already working to incorporate digital asset components into fun games. This should help address the gaming community concerns and drive adoption rates. For example, the recently concluded *Dookey Dash* competition by Yuga Labs delivered a fun gaming experience for the Bored Ape Yacht Club community, attracting participation from all over the world and demonstrating the growing importance of NFTs in gaming.

We believe the next iteration of blockchain-based games will include digital asset elements with other models beyond play-to-earn games. Regular pay-to-play or free-to-play games will include blockchain elements, possibly even without the gamer's explicit awareness.

[31] Ryan Parreno, "Gaming Is Five Times Bigger Than Movies Now," Gameranx, December 13, 2022.
[32] Newzoo, *Global Games Market Report 2022*, July 2022.
[33] Richard Waters et al., "Will the Crypto Crash Derail the Next Web Revolution?," *Financial Times*, July 6, 2022.

© 2023 Citigroup

Figure 8. Different Economic Models for Gaming

Pay to Play	Free-to-Play	Play-to-Earn
■ Games requiring purchase in order to play. ■ This includes full-priced games and games that require monthly subscription.	■ Players can access large portions of the game without requiring them to pay for anything. ■ Some games may require players pay for access to extra content or monetize with ads.	■ Player of the game can earn rewards and money just by playing the game. ■ Helps to bring digital identity, assets, and ownership into the players' hands. In-game assets are often represented as NFTs.
E.g. *Gran Turismo, Grand Theft Auto, Rainbow*	E.g., *CrossFire, Dota 2 League of Legends*	*E.g., Axie Infinity, Decentraland, The Sandbox*

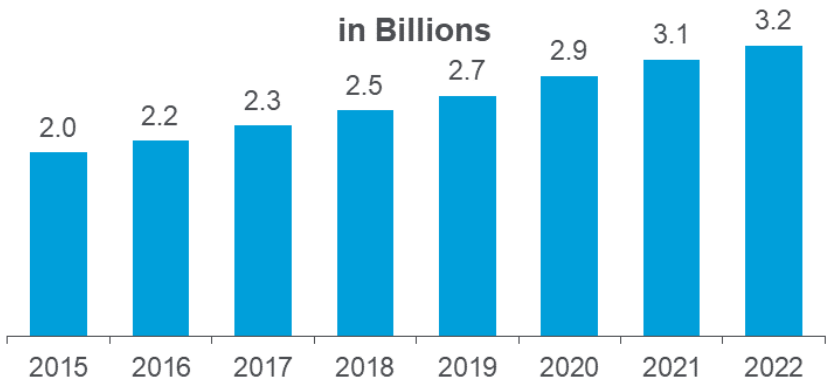
Source: Citi GPS

Increasing Demand for Digital Experiences

There were over 3.2 billion gamers worldwide as of 2022

The number of gamers worldwide grew from 2.7 billion in 2019 to 3.2 billion in 2022 (Figure 9). Two years of pandemic- and lockdown-fueled growth have likely helped 2020 and 2021 see a noticeable jump in number of gamers, including new and lapsed players. [34]

Figure 9. Global Number of Gamers



Source: Newzoo (www.newzoo.com)

According to data from Newzoo, the global games market was forecast to generate $184 billion in 2022. By region, Asia accounts for nearly half of the global revenue pie; followed by North America, with 26%; and Europe, 18%.[35]

Gaming has played a crucial role in shaping the Metaverse and Web3 ecosystem, with games like *Roblox* and *Fortnite* boasting millions of users

The buzz around the metaverse, especially in late 2021 and early 2022, has amplified the transition to the virtual world. The gaming industry has played a fundamental role in shaping the Metaverse, with games like *Roblox* and *Fortnite* boasting hundreds of millions of users and offering users goals and objectives to achieve in a virtual gaming environment.

[34] Newzoo, *Global Games Market Report*, July 2022.
[35] Ibid.

© 2023 Citigroup

A Conversation With Ryan Wyatt on Gaming and Web3

Ryan Wyatt is the President of Polygon Labs, leading the business team working to help advance the Polygon ecosystems across various products. Before serving as President, Ryan was the Chief Executive Officer of the Polygon Studios division, which was the gaming, NFT, and Metaverse vertical. Before Polygon, Ryan spent almost eight years at Google, where he created YouTube's gaming vertical and built it into the video platform's second-biggest business, generating billions in revenue.

Q: Why do we need blockchain-based games? How early are we likely to see new releases?

Ryan: An increasing number of gamers who buy in-game assets and merchandise want the ability to sell or trade it, much like they can with physical items in the real world.

But end-gamers do not care about the underlying technology; they only want to play an exciting game, not understand the benefits of cloud computing for gaming or inquire if the game is hosted on Amazon Web Services or Google Cloud. In my view, having a public distributed ledger that is visible for the entire ecosystem is enough to justify the product-market fit of building an in-game marketplace.

While blockchain-based games are a distinct category today, I expect all games to leverage blockchain as the underlying infrastructure in the coming years. Game development often follows a four- to five-year cycle, and we could see new games leveraging on-chain elements using Unreal Engine as early as the second half of 2023 or the beginning of 2024.

Q: Why have early blockchain-based games and the play-to-earn model not been very successful?

Ryan: I have never been very interested in the play-to-earn gaming model, as the model does not fundamentally work from a tokenomics perspective. The economics of play-to-earn games are often structured in a complex manner. Most games also tend to be very rudimentary and not much fun to play. This has led to pushback from the gaming community.

However, a few interesting concepts emerge from the play-to-earn model. For example, the idea of rewarding users for participating in games can offer several interesting use cases.

Q: Several games today already include elements of ownership. Why do we still need blockchain for ownership?

Ryan: Games such as *Minecraft* or *Roblox* already offer elements of ownership, whereby gamers can spend money to buy different components such as mini-games, mods, and cosmetic items. Gamers are responding positively to this but wait until you give them more power and ownership over their in-game assets. They are likely to be even more engaged. Imagine if you put in-game assets on-chain today; gamers could now start to sell these assets or trade them with friends.

Innovation in game development is seldom driven by customers telling developers what the latter should build. Consumers did not ask developers for cloud gaming, multi-player games, mobile games, or play-to-earn games, and they certainly are not going to ask for blockchain-based games.

In-game assets on-chain is likely to be net positive for everyone in the ecosystem and help create a free-flowing economy. Gamers can have visibility of different in-game assets, who owns them, and how they can be purchased. Developers can also enforce creator royalties, allowing the content creator to receive royalties every time the digital item is resold. This could materially change the business model of game developers.

© 2023 Citigroup

Q: Who is likely to lead new blockchain-based game development in the next one to two years?

Ryan: I see a lot of momentum for blockchain-based games from developers in the Asia-Pacific region. New gaming models, such as mobile games and free-to-play, often originate from countries in the Eastern hemisphere, while studios in the Western hemisphere tend to be late adopters. Gaming studios in the East can be seen as lead indicators for innovation, while studios in the West help drive adoption.

Over the next one to two years, large reputable game developers in Asia are likely to launch blockchain-based games. This is likely to include non-Web3-native and Web3-native cohorts of gaming studios, as well as other developers who have left large established studios to develop their own blockchain-based games.

In my opinion, we could see the release of a big breakout game from the native Web3 developer group initially, which is then likely to be replicated by other developers. I would closely watch game developments in South Korea, followed by Japan. In the long term, game development by studios in the Western countries is likely to drive mass adoption.

Q: We currently have over 3 billion gamers worldwide. Of this, how many are likely to play games with some element of Web3/blockchain by 2025?

Ryan: I should first point out that the statistic of over 3 billion gamers worldwide is a very broad number. It includes the casual gamers who started playing *Candy Crush* two months back while waiting at the LAX airport lounge, as well as the hardcore gamer doing this for several years.

In terms of the number of gamers, I would estimate nearly 50-100 million are likely to adopt games with some element of Web3/blockchain by 2025.

However, I am more fascinated by the potential revenue pie for in-game Web3 and/or blockchain-based assets. In my opinion, this is likely to be the big driving force for blockchain-based games. Even today, a small fraction of global gamers account for the lion's share of money being spent on games (let us refer to them as "whales").

Over time, we are likely to see a significant shift in transaction spends in games from off-chain to on-chain. One hundred million gamers shifting to blockchain-based games, from a total of over 3 billion gamers worldwide, may not seem like much. However, the disproportionate shift in value of wallet (i.e., the shifting of whales to Web3) is likely to be the inflection point for the gaming ecosystem.

© 2023 Citigroup

Social

Imagining Social Media on a New Path

Web3 social media can help authenticate identities, verify accounts, and build trust

Web3 proponents cite the need to build a new system that is decentralized. Blockchain-based social media could help authenticate identities, verify accounts, and infuse transparency in the process. Blockchain's ability to create a shared, immutable digital record of transactions could also help users see where particular information originated in order to judge its credibility. This could help build trust.

Companies such as Aave are building decentralized social media platforms like Lens Protocol, where users have ownership of their cryptographic profiles as opposed to being locked to a specific Web2 platform. Users can mint a profile, follow others, and create and collect publications, completely on-chain. Ownership of content and control over the distribution channels remains with users.

> "I believe that creating more access to blockchain-based technology requires non-financial applications. People will come into the blockchain space not only by the financial play, but from using decentralized social media and playing games. I believe games and social media might be the way that most of the people get their awareness about the blockchain as a technology."
>
> – STANI KULECHOV, FOUNDER AND CEO OF AAVE COMPANIES[36]

Sizing the Creator Economy

In the Citi GPS report *The Creator Economy: Getting Creative and Growing*, we estimate the market for the creator economy is currently about $60 billion per year and will grow nearly 9% through 2024, when it should approach $75 billion. Many segments of this economy are growing in double-digit percentages.

Figure 10. Sizing the Creator Economy Market ($ billion)

	2017	2018	2019	2020	2021	2022E	2023E	2024E	CAGR '17-'21	CAGR '21-'24E
Ad-based video	7.4	9.8	12.8	16.7	25.6	25.9	27.1	30.4	37%	6%
+ eCommerce	3.3	3.9	5.0	10.3	13.5	13.3	13.6	15.7	43%	5%
+ eSports	1.3	1.5	2.2	4.2	5.3	5.8	6.3	6.9	43%	9%
+ Fee-based video	0.3	0.3	0.4	2.4	3.3	3.9	4.3	4.7	85%	12%
+ Education	0.7	1.2	1.6	2.0	2.7	3.3	4.1	5.0	42%	22%
+ Podcasts	0.2	0.4	1.1	1.6	2.1	3.0	3.7	4.2	80%	26%
+ Metaverse	0.1	0.3	0.5	0.9	1.9	2.3	2.8	3.3	109%	20%
+ Donations	0.3	0.4	0.8	1.0	1.3	1.6	1.8	2.0	48%	15%
+ Mobile game creatior	0.1	0.2	0.3	0.4	0.5	0.9	1.1	1.5	53%	39%
+ Publishing	0.0	0.0	0.0	0.0	0.1	0.2	0.2	0.3	211%	50%
= Total	**13.5**	**18.0**	**24.6**	**39.5**	**56.5**	**60.1**	**65.2**	**74.0**	**43%**	**9%**
memo: growth		33%	36%	61%	43%	7%	8%	13%		

Source: Citi GPS

[36] Citi GPS, *Metaverse and Money: Decrypting the Future*, March 2022.

© 2023 Citigroup

Blockchain-based social media platforms aim to take social media on-chain, offering the benefits of enhanced privacy, ownership of personal data, and greater control of user-generated content. Most platforms also offer digitally native tokens for monetization of creator content. However, decentralized social media networks are still nascent, and the user experience is not as rich as in their traditional counterparts.

© 2023 Citigroup

A Conversation With Stani Kulechov on Decentralized Social as a Driver for Blockchain Adoption

Stani Kulechov is the Founder and CEO of the Aave Companies, a software development company that builds open-source, blockchain-based software. Aave Companies are best known for creating the Aave Protocol, a decentralized, open source, and non-custodial liquidity protocol which allows users to supply crypto-assets (i.e., earn interest on them) and borrow crypto-assets. He is a seasoned entrepreneur with extensive experience developing technology in the crypto, blockchain, FinTech, and — most recently — social media spaces. In 2017, Stani released ETHLend, one of the first DeFi dApps and soon after, the Aave Protocol. In 2022, Aave Companies introduced Lens Protocol, the Web3 social layer that allows users to own their social profile and enables developers to build social media applications on top of Lens or integrate Lens features into existing blockchain applications.

Q: What is Aave and your journey to setting up Aave?

Stani: "Aave" means ghost in Finnish. The reason for naming the network Aave is because we build technology that is decentralized. After building the software, we give ownership to the user community, essentially becoming a ghost at this point. The software and protocols operate via smart contracts on the blockchain with community governance.

I started building blockchain-based applications in 2016, while a law student. The first version of the Aave Protocol back in those days was called ETHLend (short for Ethereum lending). It was a proof of concept of how cryptographic assets could be traded on an ongoing basis on the blockchain, as well as used as collateral to borrow liquidity and earn yield.

In 2017, we introduced the Aave Protocol — a peer-to-protocol that allows users to supply and borrow cryptographic assets and earn yield. The protocol is now fully decentralized and operated by the Aave Decentralized Autonomous Organization (DAO).

Over the years, with support from the Aave DAO, we have contributed new updates to the Protocol, with the focus on creating a more capital-efficient and risk-averse protocol. The latest version, currently V3, secures about $5 billion in total value locked (TVL) across multiple networks.

The Aave Protocol has been deployed on the Ethereum main network, Polygon, Avalanche, and on layer 2 networks, such as Optimism and Arbitrum. At Aave Co., our vision is a people-powered internet that benefits all. At the heart of this is broadening access — to finance and other markets. The Aave Protocol helps create globally-accessible markets, offering a liquidity pool where all participants have equal rights to the same yield, irrespective of their location.

Bitcoin and Ethereum gave us the idea of owning our assets without third-party intermediaries such as banks and brokerages.

We are also enabling users to own their social profile and not be beholden to a particular social media platform. Creating this kind of social capital ownership is important, as unlike financial capital, which many people don't have and if they do, it can't be spent, social capital is owned by everyone and can be held for a lifetime. At Aave, we focus on creating technology that increases access and is open, secure, transparent, and governed by users.

Q: What is Lens Protocol? Why do we need decentralized social media?

Stani: Lens Protocol is the blockchain social layer that aims to enable users to own their social capital. It is another use case on the blockchain, such as finance was. On Lens, users create a universal profile. They own their social profile, data, content, and followers. We call this social capital, and it is valuable, as we see large social media companies have garnered huge wealth from owning users, user-generated content, and followers.

© 2023 Citigroup

What is great about social capital is that we all have it. It is the digital version of the connections we make, our personal networks, the time we spend with our friends and in communities and groups or one-on-one, and the ideas we share and consume. In the case of digital social media, we often have greater connections online.

With Lens Protocol, you own your social profile cryptographically as an NFT. It is secured and guaranteed by the blockchain. You are not locked into a specific platform, and if you move between Web3 applications, you take your profile, content, and followers with you. In fact, by making connections with other individuals in Web3, you can effectively create your own social graph, distribution, and monetization.

Creating greater adoption to blockchain-based technology requires new, non-financial, applications. Blockchain adoption will increase with new use cases such as decentralized social media and games.

Later, some of these new blockchain users will become DeFi users as well, but the most important thing is to be able to use blockchain without necessarily having financial assets. The way we build Lens Protocol (and the way other builders are creating applications on top) is to create compelling new experiences, where the technology is in the background and users feel like they're using traditional applications that are easy, compelling, and engaging.

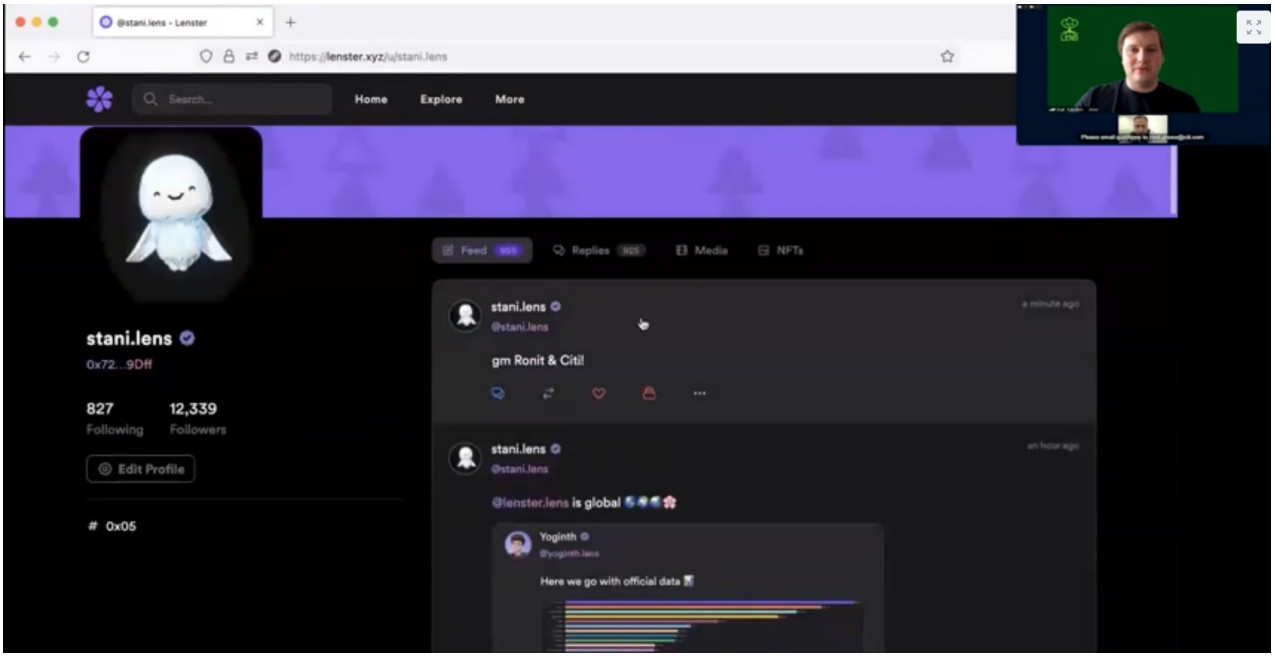
Ideally, user activity happens on the front end or the application layer. When users post, comment, or mirror content, their activity is reflected immediately. There are no gas fees (i.e., transaction costs) and users don't have to sign in with their crypto wallet. The blockchain technology functions on the backend and is seamless. When we make the technology easy to use, more people will come into Web3 and then use the whole Web3 economy.

In Figure 11, you can see Lenster — a desktop, third-party, community-based application built on top of the Lens Protocol. There are also mobile applications, such as Orb, built on top of Lens that are intuitive and fun. I'm writing here “gm, Ronit and Citi.” When I post, the content is reflected right away, like on traditional social media. But my post is indexed on the blockchain.

We are trying to break the concept of having one Ethereum address (i.e., wallet), where you store all your assets and blockchain interactions. There could be a scenario where you have one address that secures your financial assets, and another one that holds other types of activities that are guaranteed and secured on the blockchain too, but also owned by you.

© 2023 Citigroup

Figure 11. Snapshot of Lenster Platform Built on Top of Lens Protocol



Source: Citi GPS

Q: Why does an average user care about blockchain-based social media?

Stani: In my opinion, blockchain allows builders to create new and novel user experiences and applications. It is not easy to compete directly against existing social media giants who have billions of users. That defeats the purpose. The idea is to invent new experiences and monetization models that attract users, brands, and creators.

For example, we see new applications and use cases being built in blockchain finance all the time. Innovation and improvement are happening across products, services, and platforms. The same will occur in Web3-based social media. By creating Lens and a social media layer, we are making it easy for builders to create new experiences, interests, crafts, and applications on top of Lens, with Lens infrastructure in the background.

It is easier to build with Lens Protocol, as it is open and provides tools and infrastructure for builders, and it has a built-in user base of people with a Lens profile.

All applications built on Lens protocol are growth-hacking the user base together. Every application can then choose how they curate content for users from that common pool of users.

Q: How different are Web3 social media's incentives and monetization strategies from Web2?

Stani: In Web2-based social media platforms, users create data and provide it to the platform. Platforms then use this data to know more about their users and sell them services and products they might be interested in, such as via personalized ads and marketing campaigns. One could argue the platform makes money by extracting users' attention from the data they provide.

© 2023 Citigroup

Web3 social and Lens has a different dynamic. Users are not locked into individual platforms. When you own your social graph and your profile, the applications and algorithms have to work for you, because you have the freedom to move to other applications and take your profile, content, and followers with you. For this reason, the application experience and algorithms must keep you engaged.

This change in dynamics means that as a user, you can choose how you monetize yourself and which experiences and applications align with your interests. You are not locked into a specific application at all. I think that's the biggest point of value. Lens also has built-in monetization tools that allow you to monetize your content.

All content posted (i.e., user-generated content) can be collected as NFTs — like an asset class. For example, a song or art piece can become an asset that other users view and collect as an NFT, helping content creators monetize their assets.

Users can also “mirror” this content and earn mirroring fees (think of this as monetizing the Repeat or Share button). Users can build any kind of monetization rules around their content. Importantly, users own and control their social graph without relying on the platform. This also means they do not have to leave behind their profile, content, and followers if they decide to move to another platform.

Q: The Lens Protocol is set up as a DAO. What are the benefits and challenges of operating a DAO? What are DAOs best suited for?

Stani: This is a very fascinating and philosophical question. In my view, most of what we have built are public goods. Public goods are governed openly, allowing users to make decisions jointly, express opinions, and achieve consensus together via discussion and voting.

Governance of a DAO is slower than operating a company with concentrated decision-making powers. In my view, starting a new project with concentrated decision-making makes sense if you want to make quick progress. However, once the product reaches scale and delivers utility, it does not need extensive changes. Product ownership should be transferred to the community at this stage.

Lastly, it is also important to note that even while operating a DAO, there might be a need for continued updates, features, and other changes to enhance the protocol. This requires good alignment with stakeholders in order to keep the protocol relevant, competitive, and secure.

© 2023 Citigroup

Art, NFTs, and The Metaverse

Traditional Art on the Blockchain

Trust, which blockchain can help enforce, is the most important factor in the art world

Trust is the most important factor in the art world. Blockchain technology can help enforce trust without compelling anyone to trust one single individual or institution. Tokenization of art helps enable the storage of information on-chain by cryptographically "signing" the artwork, embedding due diligence certificates on smart contracts, and thus keeping the information accessible to all.

In November 2018, Christie's raised nearly $318 million in the Barney A. Ebsworth Collection sale.[37] The auction was recorded on Artory's permissioned blockchain and was the most valuable art auction to be recorded on a blockchain.

Five Key Takeaways on Blockchain and Traditional Art

We sat down with Nanne Dekking, Founder and CEO of Artory Inc., New York and Artory GmbH, Berlin, to discuss the future of blockchain technology in the traditional art market. Below are five key takeaways from our discussion.

1. **Establishing Trust in the Art Market Is Complicated:** The art market is plagued with fraud, forgery, and theft. Building a trustworthy registry of digital records without any central authority can be difficult.

2. **More Trust Is Always Good:** The use of blockchain does not signify traditional market players cannot be trusted. On the contrary, it suggests they can be trusted more, as all information is captured on an immutable record. Reassurance in the art market is not new.

3. **Blockchains Help Enhance Provenance:** Blockchains enable the creation of an immutable record with ownership history, independent appraisal comments, certifications, etc., throughout the life cycle of an artwork. These due diligence certificates, also known as asset tokens, are close to being legally bound, digital representations of proof of ownership.

4. **Traditional Players Are Adapting to Change:** Despite their initial reluctance, artwork owners and traditional galleries, such as Sotheby's, Christie's, and Phillips, are now seen collaborating with blockchain-based companies to create digital certificate tokens to capture all information related to the artwork.

5. **New Artwork Investment Opportunities Are Arising:** Digital certification of artwork can also be wrapped in a security token, creating institutional-grade investment opportunities in high-value art and collectibles. Art-focused funds based on the blockchain create a transparent ecosystem for potential investors by offering intricate access to artwork data, individual performances, and diligence updates.

For more thoughts, see our full conversation with Nanne Dekking further in the report, where we discuss the on-chain storage of information related to physical art, the response of traditional art market players to emerging technologies, and the potential for other asset classes to be brought on-chain.

[37] Christie's, "The Barney A. Ebsworth Collection Sale — a Landmark for the American Art Market," December 12, 2018.

© 2023 Citigroup

Case Study: Art Tokenization, Sygnum, and Artemundi

Swiss digital asset bank Sygnum, and art investment company Artemundi, partnered in 2021 to tokenize Picasso's *Fillette au béret* painting, enabling investors to purchase and trade "shares" in the artwork called Art Security Tokens (ASTs).[38]

Art security tokens allow fractional ownership of fine art masterpieces within the Swiss regulatory/legal framework. Here, direct ownership in the artwork — not a fund or investment vehicle holding the painting — was tokenized, with legally binding ownership under Swiss DLT law. While the *Fillette au béret* was priced at CHF4 million, professional/institutional investors of Sygnum could invest in and trade these ASTs, representing fractional ownership in the painting for as low as CHF5,000. This significantly lowers the barrier to art as an asset class to high-net worth investors.

Figure 12. *Fillette au béret* at an Art Event at Kunsthaus

Source: Sygnum and Artemundi

[38] Sygnum, "Sygnum Bank and Artemundi Tokenize a Picasso on the Blockchain," July 15, 2021.

© 2023 Citigroup

A Conversation With Nanne Dekking on the Art of Tokenization

Nanne Dekking is the Founder and CEO of Artory Inc., New York and Artory GmbH, Berlin with 25+ years of global expertise and influence in the art market. Artory connects the art market with the digital-first, financial ecosystem. Combining leading technology, art expertise, digital certification, and tokenization, Artory secures on the blockchain verified artwork information from expert partners. In his former position at Sotheby's New York, Nanne was Vice Chairman and the Worldwide Head of Private Sales. He was the Chairman of the Board of Trustees of The European Fine Art Fair (TEFAF) through June 2020 and is a current advisory board member of the Responsible Art Market Initiative.

Q: Can you describe blockchain and art for us — the discovery, eureka moment, and relevance?

Nanne: It is complicated to build trust in the art market. We often trust someone because they happen to know the right information. However, buying an artwork should never be about an individual; it should be about the best individuals who can make a fair judgment about the artwork. Unfortunately, trust in the art market is hindered by the lack of any centralized repository containing all catalogs and independent appraisals of the artwork. We often ponder how technology can mitigate risks in the art market.

I was lucky to be introduced to the concept of blockchain by renowned art collector and businessman Hasso Plattner when I was Vice Chairman at Sotheby's Auction House. This eventually led to the founding of Artory in 2016, with the aim of connecting the art market with the digital-first financial ecosystem.

In 2019, we made history by registering the Barney A. Ebsworth Collection, one of the largest collections of American Art ever sold at auction, on the blockchain in collaboration with Christie's. We were also the first company to enable living artists to cryptographically sign off on a token to create immutable certificates of authenticity.

Use of blockchain can enable the creation of an immutable record of information, such as provenance and transactions. Information about an artwork can be securely stored on-chain as a static record. These are known as asset tokens and are close to being legally-bound, digital representations of proof of ownership.

It is also valuable to create a record of auditable statements made by individuals throughout the life cycle of an artwork. Customers can check this information on the blockchain, with details of when and by whom the information was verified. These due diligence certificates can be securely stored on-chain using smart contracts. They are also dynamic in nature and can be periodically updated with new information, including annual valuations, condition reports, or insurance updates.

However, one must understand that not everything on the blockchain needs to be public. We work on the model of permission-based access to information. The public part of an artwork's information is stored on-chain, and for the private information, attestations of diligence can be stored on-chain. Underlying data supporting the attestation is stored safely off-chain. Only select individuals can access the private information related to their specific artwork.

We can also take the artwork token with due diligence certificates a step further by wrapping it in a security token. This enables art-focused funds to create a transparent ecosystem for potential investors with intricate access to different artwork pieces the fund has invested in. For example, investors holding portfolio of artwork can get exclusive access to artwork data, individual performances, and diligence updates.

© 2023 Citigroup

Figure 13. Examples of Art Non-Fungible Tokens (NFTs)

Venus Pudica, called the "Venus de' Medici," French school, circa 1700. Formerly in the collection of J. Pierpoint Morgan. Tokenized by Artory in collaboration with Christie's for the 2022 sale: *Galerie Steinitz: Provenance Revealed.*

The Man of Sorrows, Sandro Botticelli, circa 1444/5-1510. The first Old Master painting to be recorded on the blockchain. Tokenized by Artory in collaboration with Sotheby's for the 2022 sale: *Master Paintings and Sculpture.*

Untitled (2004), Kehinde Wiley. First physical artwork to be recorded on the Algorand blockchain. Tokenized by Artory in collaboration with leading art appraisal and advisory firm Winston Art Group.

Source: Artory

Q: As an art investor, why do we need blockchain to establish trust, especially since we already have well-known trusted subject experts?

Nanne: As in all businesses, some subject experts in the art market can be trusted more than others. However, why should an investor or collector depend on any individual or the inconsistent ways they store information? If one can be trusted, why not ensure all gathered information is stored in a centralized, secure platform?

Let me illustrate this with an example. In 2022, we worked on a project with Galerie Steinitz in Paris and Christie's. Galerie Steinitz is an internationally renowned dealership in classic 18th- and 19th-century decorative art. In 2022, Christie's hosted the sale *Provenance Revealed: Galerie Steinitz*, featuring a collection of masterpieces of the decorative arts. It was important for them to highlight the robust and storied provenances of the pieces, as authenticity for these types of pieces is usually confirmed by a validated chain of ownership. A few pieces sold, for example, had stamps from the palace where the French royal family stayed in the 18th century. Information was signed off and validated by both Steinitz and Christie's, and both parties were keen to tokenize this trust information through Artory.

Do you know for sure everything is correct? Of course, you can never be completely certain, but at least you know who created the statement.

For people who buy those 18th-century pieces, they at least see a record of who said what, and at what point in time. In my opinion, this is more important than just trusting any particular individual. Visibility into who is making the statement is extremely important, and Artory secures this information with the blockchain. The statements on the blockchain are as only good as those individuals and institutions making the statements. As the saying goes, garbage in, garbage out. This is why Artory only ever allows trusted experts to record statements on the blockchain.

© 2023 Citigroup

Q: How can one ensure information stored on the blockchain corresponds to a particular physical artwork?

Nanne: Frauds and fakes exist in the art market. Several companies are exploring the use of unique identifier technology to ensure real-world assets have a physical link to the associated blockchain information. Most simply rely on high-resolution images to compare with the originals, but such results vary over time based on the angle of photography, humidity in the environment, or inevitable changes in condition. Companies are also experimenting with use of tags that can be placed discretely on an artwork, alerting individuals if someone tries to remove them. However, I have yet to come across a technology that holds up in litigation.

For now, artworks are best kept in custody, where trust systems and workflows are in place to ensure everything captured on the blockchain corresponds to the physical artwork in storage.

Q: How have traditional players reacted to use of blockchain and NFTs in art?

Nanne: In the early days, as a knee-jerk response, the art market was not very keen on blockchain. Some questioned if there were reasons not to trust traditional and established market players, or if the traditional model was not truthful to clients. In reality, that was not the case. The use of blockchain did not signify traditional players could not be trusted; on the contrary, it suggested they could be trusted more.

Reassurance in the art market is not new. The European Fine Art Fair (TEFAF), one of the biggest art fairs in the world, uses an independent vetting committee for each artwork it shows. This is not to suggest that people do not trust TEFAF's dealers; rather, it adds an additional layer of reassurance. Every artwork in the fair is likely to go through nearly 90-100 independent appraisers.

The use of blockchain in art will create trust and reassurance in the artwork being sold. Blockchain allows for the creation of secure digital certificates for an artwork, containing information related to the artwork, from credible art institutions (e.g., Christie's, Sotheby's, and Winston Art Group). Blockchain can also enable on-chain storage of contractual agreements related to the artwork using programable smart contracts.

Blockchain's uses in art are gaining prominence. Artwork owners and galleries are now collaborating with Artory to create tokens with digital certificates to capture statements made about their artworks. The market has also seized opportunities to sell new forms of art — NFTs. New players like OpenSea created NFT marketplaces, while traditional players like Sotheby's, Christie's, and Phillips are also active in the space.

Q: Can blockchain and NFTs be used for other real-world assets, beyond art?

Nanne: In my view, NFTs like Artory's asset tokens play a crucial role in providing assurance of authenticity and provenance. They reassure users that information stored on-chain, related to the physical asset, is captured in a secure manner and cannot be edited or tampered with. This information can also be linked to the physical asset and securely transferred as ownership changes hands. As a result, tokens can be associated with a number of physical assets, including real estate, classic cars, gemstones, and other collectibles. The tokenization process ultimately prepares real-world assets for the rapidly developing Web3 financial ecosystem.

© 2023 Citigroup

NFTs also support the creator economy by assigning value to, and proving ownership of, digital artworks. NFT marketplaces enable discovery of new collectors, and many marketplaces offer automatic enforcement of resale royalties in a digital artwork secondary market.

© 2023 Citigroup

New Forms of Digital Art (NFTs)

Digital art has come a long way from the first image on the blockchain in 2011 — in Bitcoin block 138725, a tribute to cypherpunk and cryptographer Len Sassaman — an image of Sassaman created with ASCII art.

The use of blockchain for art, via NFTs, exploded into the mainstream in March 2021, with the sale of the digital artwork *Everydays: The First 5000 Days* by digital artist Mike Winkelmann, popularly known as Beeple, for $69 million at Christie's.

A total of 3.8 million sale transactions of art and collectibles, worth $9.5 billion, occurred between March 2022 and February 2023, according to data from nonfungible.com.

Unlike in the physical world, where artists do not get a revenue share from secondary sales, NFTs can be crafted to ensure the artist gets a percentage of subsequent secondary sales after an initial minting.

The shift to digital has led to a stronger focus on diverse artists and genres, and on artists who work outside mainstream platforms. We expect this trend to continue in the foreseeable future, along with new synergies between auction houses, galleries, artists, and collectors, as well as sustained growth in private sales.

The economy and community built around NFTs has dragged prominent influencers, venture capitalists, and business personalities into its fold (some as paid sponsors). Two projects specifically worth noting are:

- **CryptoPunks:** A collection of 10,000 pixelated characters built and generated procedurally from a project in 2017, which exploded into the mainstream in 2021, with the cheapest "punk" ranging anywhere around $30,000 and the rarest fetching close to $10 million.
- **Bored Ape Yacht Club (BAYC):** An NFT collection with a fixed supply of 10,000 unique Bored Ape NFTs on the Ethereum blockchain and a reported all-time trading volume of $1.3 billion by March 2023.[39] The Bored Ape also doubles as the Yacht Club member card and grants users access to members-only benefits.

How Do NFTs Work?

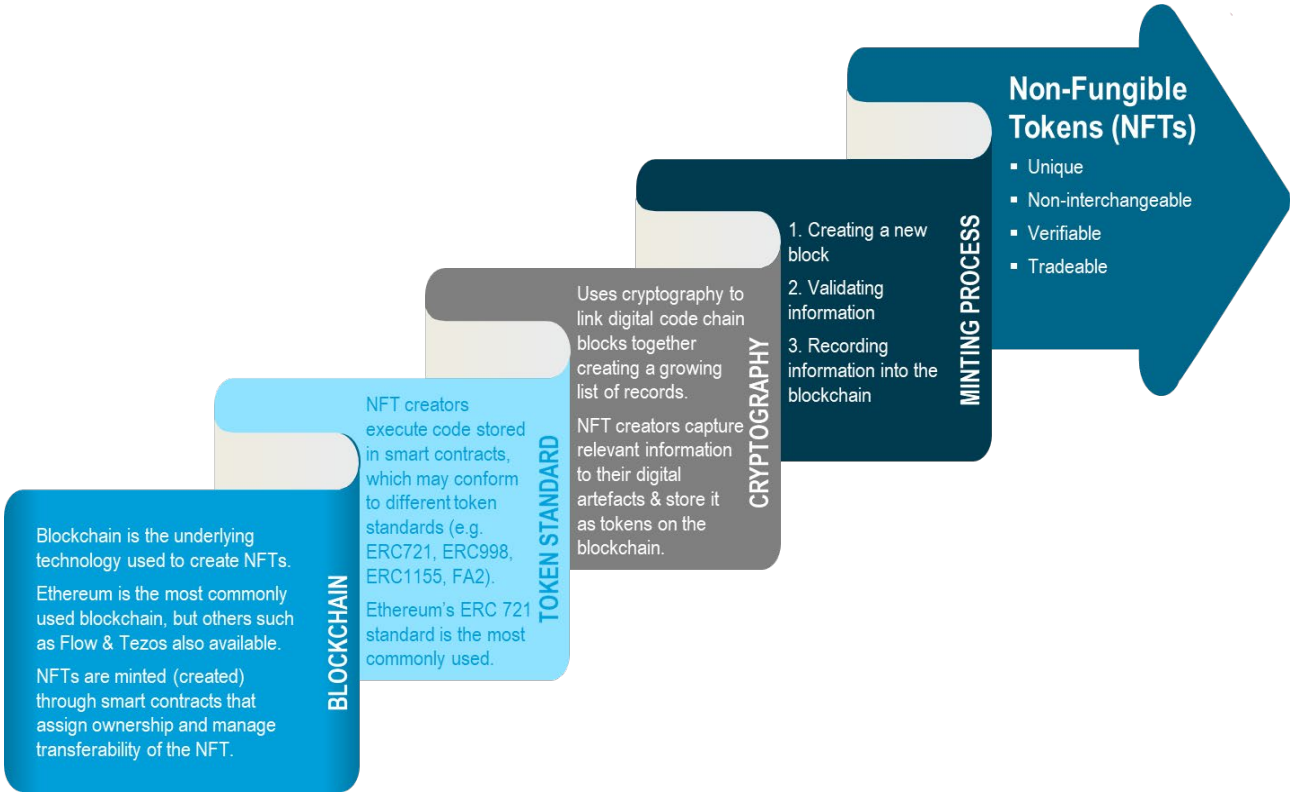
Like all other forms of assets, art and collectibles need the same guarantees of permanence, openness, and "nonfungibility" for them to be counted as intrinsically valuable. As NFTs are recorded on the blockchain, it adds "permanence" to the item that outlives the creator. NFTs are created from within smart contracts on the blockchain, by the process of "minting" — i.e., creating an NFT, typically an ERC-721 token, from a digital asset and recording it on the blockchain.

NFTs usually do not store the digital asset itself on the blockchain (to do so would incur storage costs in the thousands or millions of dollars, as every contract in the Ethereum blockchain must be stored on every full node on the network), but instead contain a URL that points to the metadata, usually stored via decentralized file storage systems such as InterPlanetary File System (IPFS) or Arweave.

[39] Based on data from OpenSea.io as of March 11, 2023.

© 2023 Citigroup

Figure 14. How Do NFTs Work?



Source: Citi GPS

Bringing Collectibles On-Chain

Corporate brands are exploring the use of exclusive digital collectibles in the Web3 ecosystem

Aside from digital art, collectibles are also finding their way on-chain. This includes video clips, digital trading cards, music clips, and more. Corporate brands are exploring the use of exclusive digital collectibles in the Web3 ecosystem. Simply put, collectibles represent digital assets created, encrypted, and stored on a blockchain.

It is now possible for fine wine aficionados to own a piece of their favorite winery or distillery through tokenization. NFTs enable collectors to invest in luxury wine or spirits, with the physical assets held in custody in a temperature-controlled warehouse and allows them to trade these collectibles on a blockchain.

For example, the BlockBar platform enables luxury brands to issue NFTs against their collection of wines and rare spirits. The primary objective is to own exclusive wine and spirit bottles as well as trade them on the secondary marketplace, while the physical bottle remains in a safe, temperature-controlled warehouse.

Adoption of Web3 by Consumer Brands

Corporations are experimenting with NFTs to drive customer loyalty, engagement, and marketing

In the Citi GPS report *Metaverse and Money: Decrypting the Future*, we captured the popular use cases of NFTs, including in digital collectibles, fashion and luxury, gaming, and social tokens to name a few. Corporate adoption of NFTs and other tokens is picking up traction and could potentially be the vector that brings a billion users on board.

© 2023 Citigroup

Corporates across the spectrum, notably Starbucks, Nike, Disney, and others, are experimenting with NFTs to drive customer loyalty, engagement, and marketing. E-commerce platform Shopify is launching a Web3 toolkit to enable merchants to easily create Web3 commerce experiences.

Creating and Engaging with Brand-Centric Communities

Beyond the art world, blockchain can be used as a way of recording the authenticity of other physical goods using NFTs

Consumer brands, fashion labels, and luxury goods are embracing NFTs and the Web3 ecosystem. Below are examples of some brands making early moves:

- **Adidas:** Recently announced an NFT collection titled "Into the Metaverse," comprising virtual wearables for the Metaverse, with physical clothing to match.
- **Balenciaga:** Designed virtual outfits and various accessories for *Fortnite* avatars.
- **Burberry:** Announced a partnership with Mythical Games to launch NFTs in its flagship, player-owned *Blankos Block Party* blockchain game.
- **Gucci:** Attracted headlines when a single virtual bag sold for $4,000 through "Gucci Garden," a pop-up world on the gaming environment *Roblox*.
- **Nike:** Acquired digital sneaker maker RTFKT Studios. Also built an immersive world, Nikeland in *Roblox*, featuring Nike buildings, arenas, and fields where players can compete in mini-games.
- **Uniqlo:** Partnered with Microsoft to sell virtual outfits for *Minecraft* players.

Using blockchain as a way of recording provenance is going beyond art. It extends to the authenticity of other physical goods by uniquely identifying a specific physical object on-chain using NFTs.

This link of the physical object to its NFT could be achieved by using Radio Frequency Identification (RFID), Near-field Communication (NFC) tags, Quick Response (QR) codes, or unique identifier numbers. Veracity Protocol, a Web3 technology company, brings a novel approach to this "linkage" by leveraging micro-structure-based authentication.

The underlying principle here is that an object's surface area has intrinsically random properties, and when this micro-structure of an object is captured optically by even an iPhone, it enables unique identification of that specific object (even in a mass-production scenario). This technology is finding use cases in luxury goods, critical industrial components, and collectibles.

NFT-based digital assets can act as a seal of authenticity for physical assets, creating more trust, especially in the high-end collectible market

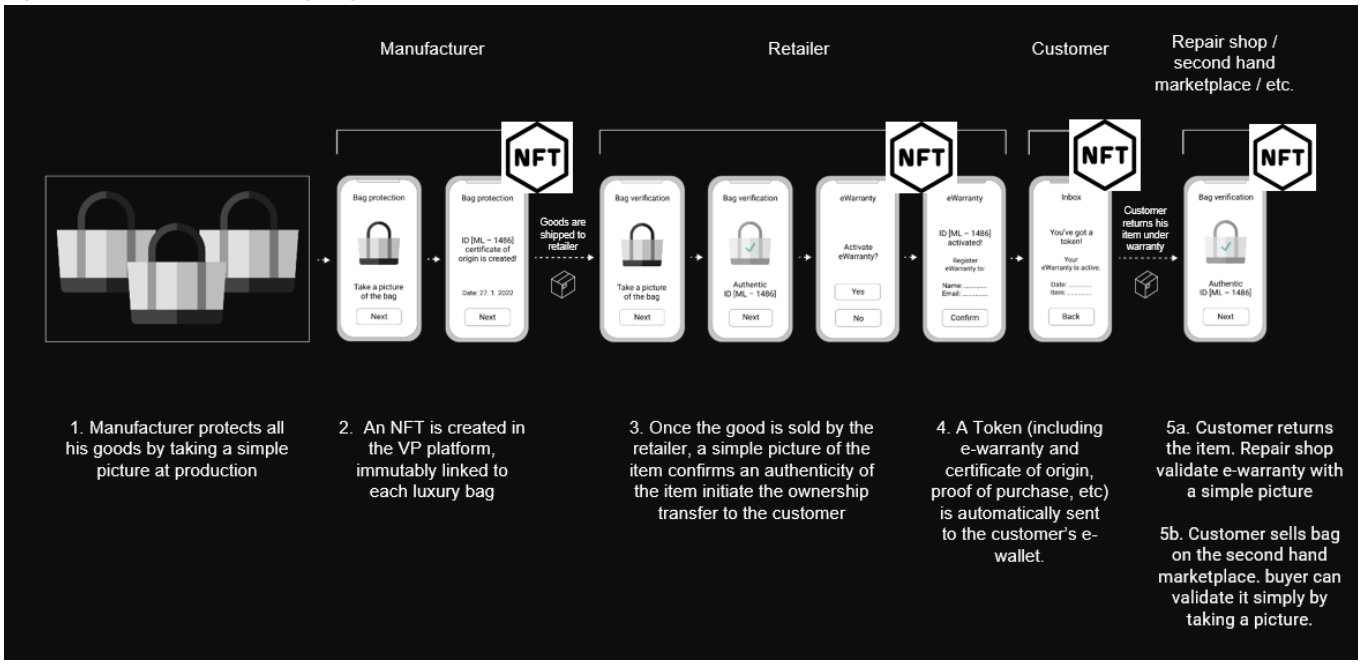
NFT-based digital assets can act as a seal of authenticity for their corresponding physical asset, creating more trust, especially in the high-end collectible market. Specific use cases for corporates and brands include:

© 2023 Citigroup

- **Creating Marketing "Buzz":** A leading brand could collaborate with street artists or digital artists to create unique versions of their products for auction; ownership of the product can then be transferred and evidenced via an NFT token. For example, Amazon is working on offering its customers the ability to purchase NFTs tied to real-world assets, delivered to their doorstep.[40]

- **Event-Ticketing and Driving Loyalty:** NFTs can be used to simplify (or improve the security of) existing processes. For example, a brand could launch a special edition product or an event where an NFT is used to "gatekeep" access. It can double as a ticket that can be used for admittance via a QR code. The ticket might include images or videos, so it becomes a collectible.

Figure 15. Tokenization of Luxury Bags



Source: Veracity Protocol

Super-Charging Customer Loyalty Programs

A Web3 loyalty program could provide brands with direct insights and help incentivize favorable shopping and engagement behavior. Consortiums and interoperability across loyalty tokens of different brands could help make erstwhile siloed programs more attractive, while also helping brands capture a long tail of less-engaged users.

For example, Starbucks launched a Web3-based rewards program, Starbucks Odyssey, allowing Starbucks Rewards members to earn and purchase digital stamps. Members can also buy and sell these collectible stamps in the marketplace. These digital reward stamps are issued as NFTs and can be used to unlock benefits such as access to exclusive events or limited edition merchandise.

[40] Michael Bodley, "Amazon NFTs Will Be Tied to Real-World Assets, Token Possible," Blockworks, March 6, 2023.

© 2023 Citigroup

A Conversation With Samuel Falic on Authenticating Rare Wines and Spirits With NFTs

Samuel Falic is the Co-Founder and President of BlockBar Inc., which sells wine and spirits, authenticated via blockchain, directly from luxury brands. Samuel co-founded the company with his cousin, Dov Falic, in 2021.

Q: What is the role of blockchain in the wine and spirits industry?

Samuel: Counterfeiting in the wine and spirits industry is a real problem. Wine and spirits have been known to be forged, relabeled, or watered down, especially with limited edition and collector pieces. Certifying genuine wine and spirits can be difficult.

Use of blockchain in this space can enable storage of information related to the bottle on-chain, facilitating provenance. Customers can securely and reliably access information on their wine and spirits at any point until the point of consumption. This includes information on the bottle's origin, certifications of sustainable harvest methods, number of units produced, virtual tasting room experiences, and more.

In addition to proving authenticity and provenance, the use of blockchain and new-age digital platforms helps consumers and investors get direct access to the wineries and distilleries of rare collectible bottles worldwide. Ease of access and creation of a marketplace also offer investors an alternative asset class.

Meanwhile, technology helps wineries and distilleries build a database of super-premium customers whom they can target for new releases. The platform also attracts younger demographics to the wine and spirits collectibles market who may not have otherwise been active in the space via the traditional store model.

Q: Can you tell us more about BlockBar?

Samuel: BlockBar.com sells luxury wine and spirits authenticated via blockchain and obtained directly from luxury brands, offering bottle owners access, storage, insurance, global shipping, and a secondary marketplace. Each NFT corresponds to a physical bottle. Bottles released on the BlockBar platform are rare and editioned in batches as small as one.

Customers own the physical bottle, which is safely stored by BlockBar in a centralized warehouse. A digital version of the bottle (i.e., an NFT) serves as a proof of authenticity and verification of ownership. BlockBar proves authenticity via the Ethereum blockchain. The digital NFT is stored in wallets protected by Fireblocks.

Figure 16. How Does BlockBar Work?

Source: BlockBar Inc.

Similar to other NFTs, these digital bottles can be sold, transferred, exchanged, or gifted on the secondary marketplace built by BlockBar. Any sale, transfer, or exchange of the digital NFT also results in the ownership transfer of the physical bottle, although the physical bottle remains intact in BlockBar's centralized storage.

© 2023 Citigroup

Consumers also have the right to receive physical delivery of their bottle, if they are keen to consume it. When a consumer chooses to redeem the NFT and receive physical delivery of the bottle, the associated NFT is permanently burnt.

Q: Any details on customer demographics or prominent markets for your business?

Samuel: BlockBar currently has over 500,000 active users. Over 80% of our customer base are Millennials in the age group of 27-42 years. Further, Gen Z in the age-group of 21-26 years makes up a little over 10%, while the remainder is made up of Boomers and Gen X of over 43 years of age.

In terms of prominent markets for business, most of our users are from the United States, United Kingdom, Singapore, Hong Kong, Germany, and Mexico.

Q: Can blockchains be used for other collectibles as well, beyond wine and spirits?

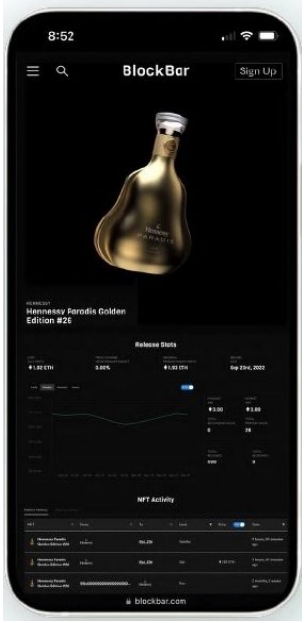
Samuel: In my opinion, there is extensive market potential for wine and spirits, and we anticipate exponential growth in the foreseeable future. We see high-end luxury spirits as a growing asset class for alternative investments.

Additionally, blockchain technology can also be used to democratize access to a range of other high-end luxury goods that necessitate proof of authenticity, provenance, and transparency of ownership records.

In my view, there is scope to explore use of blockchain in the luxury watch or high-end sneaker businesses as well. However, it is crucial to have direct access to the manufacturer in order to establish authenticity and eliminate counterfeits.

Figure 17. Example of BlockBar NFT

1. Proof of authenticity
2. Verification of ownership
3. Right to redeem the physical bottle



Source: BlockBar Inc.

© 2023 Citigroup

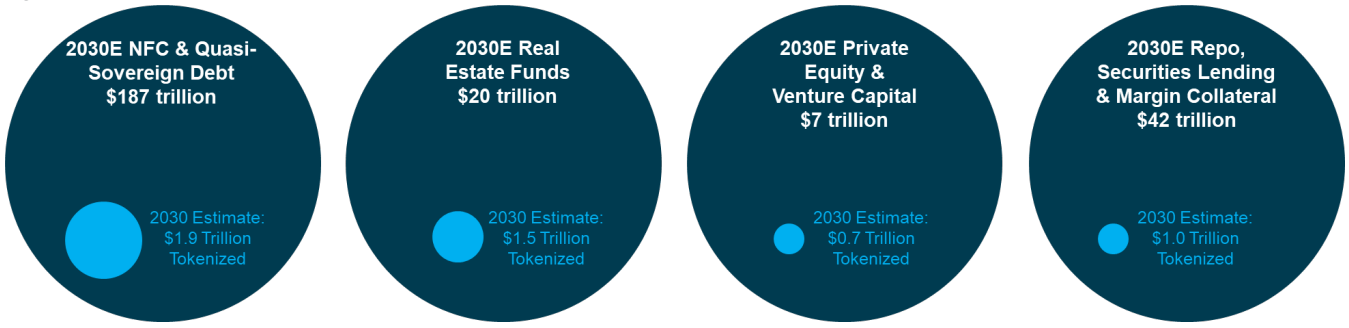
Trillions in Value

Tokenization of Digital Securities

With the global outstanding equity and fixed income market valued at over $250 trillion, traditional securities could represent the biggest use-cases for tokenization

- **Why Important?** The global outstanding equity and fixed income market is valued at over $250 trillion; thus, traditional securities have the potential to represent one of the biggest use cases for tokenization.[41] We believe the private/unlisted market is likely to adopt tokenization faster due to the resulting benefits of liquidity, transparency, and fractionalization.
- **What Is the Total Addressable Market (TAM) Size?** We are very early in the process of these products growing but — based on conversations with internal and expert domain experts — we forecast $4 trillion to $5 trillion of tokenized digital securities, assuming 1% of corporate and quasi-sovereign bonds, 7.5% of real estate funds, 10% of private equity and venture capital funds and $1 trillion of securities financing and collateral activity are tokenized. Accompanying the tokenization of securities will be the trade finance market, which could see up to $1 trillion of volumes based on distributed ledger technology (DLT), or around 8%-10% of global trade finance volumes, by 2030.
- **Why Now?** We will need the support of large financial institutions, who are increasingly focused on tokenization and the support of the law, where notable changes are taking places in areas such as English law, which governs most international trade finance.
- **What Is the End State?** The end state is digitally native infrastructure for financial assets in which DLT and smart contracts open up new capabilities, features, and new delivery mechanisms that are hitherto unimaginable in traditional infrastructure. We discuss this in greater detail through the rest of this chapter.

Figure 18. Tokenization TAM in Trillions of Dollars



Note: We assume 6.5% nominal GDP growth rate for all asset classes. We estimate 1% of NFC & Quasi Sovereign Debt, 7.5% of Real Estate funds, 10% of PE/VC, and 2% of Securities Lending & Borrowing to be tokenized by 2030

Source: SIFMA, Preqin, Savills, Finadium, Valuate, Citi GPS

A security is a tradable financial asset or instrument, but the legal definition might vary by jurisdiction. “Digital Security” can be loosely defined as “a tradable financial asset or instrument that has a digital representation on a DLT through tokenization.” We await exact legal definitions from various jurisdictions, which are just emerging.

[41] Securities Industry and Financial Markets Association (SIFMA), *2022 Capital Markets Fact Book*, July 2022.

© 2023 Citigroup

What are the motivations for the traditional financial industry looking toward tokenization? Traditional assets like stocks, bonds, and funds are for the most part a solved problem in terms of access, trading, and transparency.

So why does BlackRock CEO Larry Fink believe "the next generation for markets, the next generation for securities, will be tokenization of securities"?[42]

Why does WisdomTree founder Jonathan Steinberg ponder, "What could (tokenization) do to ETFs? What ETFs did to mutual funds? And that's a question about the wrapper. So that's about tokenization…"?[43]

What is the driving factor behind the likes of private equity giants like KKR, Apollo, and Hamilton Lane setting up tokenized versions of their funds on digital exchanges and venues like Securitize, Provenance Blockchain, and ADDX? And why are some of the largest asset managers such as Franklin Templeton and WisdomTree experimenting with tokenizing mutual funds on public blockchains such as Ethereum or Stellar?

Why Tokenize Traditional Financial Assets?

Distributed ledger technology (DLT) and tokenization offer an entirely new tech stack that lets stakeholders perform all activities on the same shared infrastructure operating as one "golden source" of data

Traditional financial assets are not broken, but sub-optimal as they are limited by traditional systems and processes. Certain financial assets — such as fixed income, private equity, and other alternatives — have been relatively constrained while other markets — such as public equities — are more efficient. Given the difficulty in investing in and trading certain financial assets versus public equities, current allocations into these assets may be subdued.

The financial industry may have lapsed into accepting the sub-optimality and accounted for it in the way they invest in these assets by under-allocating such assets in their portfolios while paying a premium for assets with operational access. Assumptions that investors do not want certain asset classes might have been made on those assets just being harder to access, or more expensive and cumbersome to manage.

Today, different parts of the financial market infrastructure run on different rails, some built in the days of COBOL and Telex. Payment runs on its own tech stack, as does asset discovery and pre-trade matching, while clearing and settlement is on yet another stack.

The financial industry has multiple layers of intermediaries working on the same data, but they do so in their own silos and require a lot of back-and-forth reconciliation. Cross-border payments go through multiple hoops on the correspondent banking infrastructure. Post-trade settlement on funds and bonds goes through a sequential process flow of Central Security Depositories (CSDs) and Central Counterparty Clearing Houses (CCPs), all introduced to reduce counterparty risk and settlement failures in traditional workflows.

[42] New York Times Events, "BlackRock CEO Larry Fink on ESG Investing," YouTube, November 30, 2022.
[43] VettaFi, "Jonathan Steinberg on The Blockchain Interviews," July 29, 2022.

© 2023 Citigroup

What DLT and tokenization offer is an entirely new tech stack that lets all stakeholders do all activities on the same shared infrastructure as one golden source of data — no more expensive reconciliation, settlement failures, waiting for the faxed documents or "originals to follow" by post, or investment choices being restricted by operational difficulty in access. But these are just operational efficiencies — this is not the promised end-state.

What Is the End State?

The tokenization end state includes a digitally native financial infrastructure, accessible globally, operating 24x7x365 with DLT-powered smart contracts

The end state is a vision of a digitally native financial asset infrastructure, globally accessible, operating 24x7x365 and optimized with smart contract and DLT-enabled automation capabilities, which enable use cases impractical with traditional infrastructure.

New product features could range from debt instruments paying daily, hourly, or even by the minute cash flows to embedded live ESG (environmental, social, and governance) tracking in any security, to flexible tailor-made funds based on each client's investment profile or philosophy. Fund tokens could do accreditation checks at the level of the instrument. The digital infrastructure could also expand market access of these instruments to targeted accredited and high-net worth investors, matching products better to risk profile, and enabling smarter and simper distribution.

Apart from different ecosystem players potentially using a shared "golden-source" infrastructure, different asset classes could be represented on the same ledger, unlike today. A cash token can be handled in a similar way to a bond token, although they are conceptually and functionally different. The nuances of each asset can be captured at a smart-contract level (for instance, restricted holding periods for a fund token and sanctions screening for a cash token). A smart contract can then be programmed to auto-trigger cash token payouts for corporate actions or dividend payouts. The possibilities with token-level control and automation are endless. But this needs an entirely new "smart" infrastructure that supports programmability, verifiability, and trustless integrity. Enter DLT and tokenization.

But There Is Skepticism…

Despite the promised benefits, several traditional players are skeptical. The challenge with the mainstream narrative on tokenization is if each benefit is looked at in isolation, it probably does not offer a lot of delta. It does not answer the question of "So what?" Do investors really want 24x7 bond trading? Settlement failures in U.S. equities are not a particular problem. For private funds, use of emails with an excel template works well given infrequent trades. We do not really think investors care about secondary liquidity, as they have not asked for it. Alternative assets are hard and expensive to access, so we are not likely to include them in our models. The list goes on.

But putting all benefits together, there is critical mass. For example, there is value in 24x7 seamless liquidity, for use case such as collateral, atomic and instant settlement, easy asset discoverability, conditional payments and corporate actions controlled by smart contracts, completely new product features, and compliance enforced at the token level.

© 2023 Citigroup

Why Is Adoption So Slow? Gradual, Then Sudden?

Anecdotally, we are referring to changing an aircraft's engine while it is still flying at 30,000 feet. Further, the new engine requires complete rewiring, while still being "backward compatible" with the old systems.

- **Legal and Regulatory Framework:** A key factor holding back tokenization initiatives is the lack of an established legal and regulatory framework to support tokenized instruments. A few European jurisdictions, such as Switzerland, Luxembourg, France, Germany and now the UK, as well as Asian jurisdictions such as Singapore and the Philippines, have begun to create these models, resulting in early transactions being based in these areas.

- **Building New Rails:** Tech entrepreneur Andreas Antonopoulos refers to "infrastructural inversion" when new technology infrastructure is laid on top of the old, creating conflict.[44] There is initially a lot of resistance — the new technology feels slow and sub-optimal compared to the old one it is replacing, as it must interoperate with the existing technology. This adds layers and costs — the antithesis of what the new technology set out to solve. Similarly, we are talking about building out entire new rails of financial market infrastructure, replacing the functioning rails handling trillions of dollars daily.

- **Potential Disintermediation:** To make matters worse, some of the players who are required to invest and drive change could likely see their existing roles centered on intermediation disappear, or at the very least morph into new roles, involving a lot of investment. Workflows and behaviors need change and new mindsets. Process flows need to upgrade from sequential, synchronous processing based on each intermediary doing one task in the flow and then handing over to the next, to asynchronously and simultaneously accessing and working on the shared data in parallel.

- **Lack of Standards and Interoperability:** The industry needs standards and interoperability. Different financial market infrastructures (FMIs) and consortiums are working on the same problem in parallel, but with no clear interoperability or standardization. This leads to silos in initiatives today. As DLT adoption gains critical mass, there will be more drive to standardization and interoperability.

- **Fractured Liquidity:** Scenarios that include fully digital infrastructure with native digital issuance of tokens also face challenges, but of a different kind. The operational process might be supercharged, but liquidity is fractured in different venues and pools, delaying triggering of the network effects needed to drive more adoption.

- **Public Blockchain Infrastructure Not a Straightforward Fit:** To complicate things further, a lot of the connotation around public blockchain has been sullied by the narrative around cryptocurrencies, price volatility, and scams, but the technology underlying these is based on strong fundamentals that should deliver a better experience, new products and capabilities, and increased digitization.

[44] Andreas Antonopoulos, "Bitcoin and the Coming 'Infrastructure Inversion' - Zurich Meetup March 2016," YouTube, April 2016.

© 2023 Citigroup

However, retrofitting public blockchain infrastructure to traditional FMIs makes the problem worse rather than better. Trustlessness, one of the main problems solved by public blockchains, is not a problem today in the traditional world. Banks trust each other and there are all sorts of controls built in place to penalize errant behavior by regulated entities. However, reconciliation, settlement failure, and traceability are problems. In the context of applying public blockchain to FMI, transaction speed and throughput, liveness and data availability, and transaction-level privacy are important for institutions.

These are, however, only growing pains and will pass as the ecosystem matures, the technology develops, and adoption grows. Once this intermediate, skeuomorphic "straddle" state is crossed, the new disruptive technology breaks free from the old and ideally directionally trends towards the envisioned end-state. We have seen this play out historically time and time again — with electrification, with the internet, with SWIFT (Society for Worldwide Interbank Financial Telecommunications) electronic messaging — new DLT-based financial infrastructure needs critical mass before Metcalfe's Law takes over with its network effects. We still have a long way to go before DLT-based FMIs and tokenization get there.

Tokenization initiatives have grown considerably in the last few years, but it is equally key to focus on the challenges from current initiatives and potential learnings from it. One such example is the Australian Securities Exchange (ASX). In 2015, ASX embarked on re-platforming its Clearing House Electronic Sub-register System (CHESS) with a DLT-linked alternate to provided enhanced clearing, settlement, asset registration, and post-trade issuer services. Arguably, the initiative aimed to change the tech stack without related changes in the business process. Several issues led to repeated delays and the eventual pausing of the project, with the team going back to the drawing board for a new approach. ASX wrote off $165 million in investment, despite having a very high-quality technology that promised considerable efficiencies. Potential learnings from the program, which may be applicable to other ongoing distributed ledger implementations include:

- Need for a comprehensive change in the management governance program for all stakeholders, given the complexity of switching from a centralized legacy system, built decades ago, to a distributed infrastructure.
- Need to take a phased approach in tackling complex transformations with bite-sized delivery plans.
- Need to rework business workflows for distributed environments that have higher latency than centralized systems, and also capitalize on new functionalities enabled by DLT/smart contracts.
- Need to carefully optimize on- and off-ledger processing to get the best out of centralized and distributed models.

Regardless, Leading Ecosystem Players Are Bullish on Tokenization

The benefits of tokenization outweigh its complexity and will likely lead to adoption, albeit in a phased manner

Regardless of complexity, the benefits of tokenization could be significant and will likely lead to adoption, albeit in a more phased manner. Capital markets players are evaluating the potential opportunities offered by tokenization of traditional assets, but the biggest focus is on traditional FMIs.

© 2023 Citigroup

- Traditional FMIs have a large existing user-base, trade volumes, and assets under management: With the real estate market standing at over $300 trillion, securities at over $250 trillion, regulated open-end funds over $60 trillion, and with private markets growing rapidly, even 1% of the total market share is in the trillions.[45] Early mover advantage could be massive.
- In certain jurisdictions, there is relatively clearer regulatory and legal basis for financial assets, even as crypto assets face regulatory headwinds.
- Holding real-world assets and financial assets in tokenized formats will drive new portfolio alpha/structuring opportunities and more flows in the market.
- Market structures could change fundamentally due to digitization and tokenization, and the winners would likely be entities that adapt and change to the new operating model.
- Traditional FMIs might be one of the first ones impacted by the use of DLT and face a threat of disintermediation if they do not act quickly

Benefits of Tokenization

While the immediate benefits for traditional liquid financial assets are focused on clearing, settlement, custody, and asset servicing, illiquid assets have a much broader scope for upside and scalability from tokenization.

- **Liquidity:** High-value illiquid assets may benefit from tokenization as it allows fractionalization which makes it easier to trade in them, transfer ownership, and update records. Fractionalization may significantly improve liquidity for high-value illiquid assets by lowering investment minimums, and catering to personalized liquidity or collateral needs (by being able sell or collateralize only a fraction of a high-value asset and enjoy appreciation/yield on the rest of it).
- **Distribution**: Tokenization would likely provide operational efficiencies, which would take out costs that can be passed on to investors, facilitating broader access. The entire distribution process — from creating tokens to transferring ownership — can be completed on-chain without rent-seeking intermediaries, and theoretically anyone connected to the internet can open a wallet to own tokens.[46]
- **Enable Access**: Although still subject to regulatory constraints, tokenization can help individuals access certain assets traditionally only available to institutional clients or a niche group of investors.[47] Besides, people in less developed regions of the world, with limited access to banking and brokerage firms, can also potentially gain exposure to securities and other real-world assets to benefit from asset appreciation.[48]

---

[45] Paul Tostevin, "The Total Value of Global Real Estate", Savills, September 2021; SIFMA, "2022 Capital Markets Fact Book," July 2022; ICI Global, "Worldwide Regulated Open-End Fund Assets and Flows," March 22, 2023

[46] Kristin N. Johnson, "Disintermediation and Decentralization in Financial Markets," *The Regulatory Review*, May 4, 2021; McKinsey & Company, "What Is Blockchain?", December 5, 2022.

[47] SEC Small Business Capital Formation Advisory Committee, *Expanding Retail Access to Private Markets*, November 2019.

[48] Rajeev Tummala, Rachel Roch, and Xin Yi Tan, "The 10x Potential of Tokenisation," HSBC Insights, August 20, 2020.

© 2023 Citigroup

- **Wider Appeal:** The idea of tokenization appeals to a younger, technologically-advanced demographic and investors with different backgrounds compared to players that prefer traditional securities and platforms. Therefore, established corporates and traditional finance (TradFi) players may use tokenization to expand target audience.

- **Opportunities in Smaller Companies:** Many real-world assets face significant friction to accessing financing in TradFi. Tokenization of certain assets, such as crops, account receivables, and equity shares of small and mid-size enterprises (SMEs), can open more possibilities for financing, capital raising, and investment opportunities for asset owners and those who invest in them. [49]

- **Operational Efficiency:** Smart contracts enable smoother, faster, and potentially cheaper issuance, trading, and post-trade processes, affording improved communication between issuers, investors, dealers, and market infrastructures. This could, in theory, also reduce trade errors and transaction costs. The combination of smart contracts and other interoperable protocols can carry out crucial functions together, which may be applied to processes like know your customer/anti-money laundering, margin calculations, and the application of corporate actions.[50] They also increase servicing efficiency through automated calculations and conditional payments, increased flexibility in corporate voting, and smarter investor communications. Finally, blockchain-based infrastructures have the potential to offer shorter and more flexible netting, clearing, and settlement cycles.

- **Composability:** Tokenization of real-world assets and financial assets may enable innovation by allowing them to be exchanged, mixed, and combined with crypto assets. It enables the financial industry to create new products.[51] Asset managers and wealth managers can create more diversified and flexible portfolios consist of real-world, financial, and crypto assets accessible through a single digital wallet. The composable nature of tokenized models may also enable streaming cash flows, alternative data-driven covenants, and varying investor treatment in traditional financial assets.

- **Trust Minimization and Transparency:** Trading of real-world assets, and of financial and intangible assets such as securities, art, and real estate, and intellectual property, is often dependent on trust among buyers, sellers and sometimes brokers and other third parties with expertise on law, valuation, and transaction. Smart contract-enabled tokenized assets can automatically execute and record transactions and transfer ownerships when pre-set conditions are met, eliminating counterparty risk.[52] Use of Internet-of-Things (IoT) and Oracle networks may also further reduce need for human reporting and the evaluation of certain data and information of assets under custody.

---

[49] AlphaWallet, "How to Empower Small Businesses with Tokenization, the True Killer App for Ethereum," March 25, 2020; Abdulla Bin Touq and Mirek Dusek, "Digital Tokens Could Transform the Economies of the Middle East and North Africa - if the Governance Keeps Up," World Economic Forum, March 24, 2021; LCX, "How Tokenization Can Bring Every Asset to the Digital World," August 18, 2020.

[50] Citi Business Advisory Services, *Industry Revolution Volume IV – The Convergence of the Crypto and Traditional Economies: How Investment Managers Can Deliver Value in a Decentralized "NewFi" World*, June 2021.

[51] Citi Business Advisory Services, *Industry Revolution Volume V*, June 2022.

[52] Ashish Sinha et al., "Smart Contracts Could Improve Efficiency and Transparency in Financial Transactions," S&P Global, October 2022

© 2023 Citigroup

Blockchain's immutable and transparent nature also makes it harder to commit fraud, and even when fraud happens, blockchains can act as a comprehensive audit trail to help auditors more easily prove the fraud compared to manually parsing through documents.

Tokenization of real-world assets, especially real estate, art, and collectibles, brings much-needed transparency and traceability to provenance and appraisals. Blockchain can automatically update the historical record of ownership with each transaction and record time-stamped signatures of appraisals, offering clear proofs of the quality and authenticity of the real-world assets.[53] The historical accuracy of the appraisers can become visible on-chain, providing a more transparent view of their expertise, and price discovery becomes easier with visibility into real-time prices at which assets were traded. [54]

The above benefits of tokenization may apply to all types real-world and financial assets, yet certain types are riper and more suited for disruption than others, and the next section demonstrates how current use cases are challenging traditional business models.

Deep Dive Into Traditional Securities Tokenization

The use of blockchain can yield benefits across the life cycle of digital securities, the most immediate being operational efficiencies unlocked in clearing, settlement, custody, and asset servicing

The use of blockchain and DLT can unlock benefits along the full life cycle of digital securities, with the most immediate opportunities being operational efficiencies unlocked in clearing, settlement, custody, and asset servicing. Long-term impact is likely to come from new DLT-enabled product capabilities and primary and secondary liquidity for illiquid asset classes.

When we refer to digital securities, there are two broad approaches to tokenization:

- **Tokenized Outstanding Securities:** Refers to the immobilization of an underlying traditional security in a digital infrastructure and reissuance in a tokenized format. This is currently the most common and widespread approach. The use of DLT to record transfer of securities can improve the efficiency of existing processes as paperwork and manual processes are eliminated (subject to local regulatory requirements), while also allowing for fractionalization and use as collateral. Before these benefits are unlocked however, the operating model could temporarily look more complex as now there are two infrastructures being run and maintained — the off-chain and on-chain versions, and the tokenized securities need to interoperate with the off-chain infrastructure. Valuable benefits include instant settlement, broader distribution across the full accredited investors pool, and use for collateral or repo.
- **Native Digital Security Tokens:** Refers to the process of issuing fresh securities directly onto DLT infrastructures and holding them in DLT-linked wallets. While outstanding examples remain limited for now due to regulatory constraints, this is where the largest impact is expected in the long-term.

[53] Citi Global Insights, "The Art of Tokenization: An Overlap of Blockchain & Art," November 23, 2022.
[54] The CLG Podcast, "Tokenizing Real-World Assets with MakerDAO's Teej Ragsdale," podcast, accessed March 21, 2023; Andrei Larion, "Real Estate Tokenization," University of Florida Warrington College of Business, August 26, 2022.

© 2023 Citigroup

Native issuance allows us to not only unlock the operational efficiencies listed earlier, but is unfettered from having to sync or be backward compatible with traditional operating model. This opens the door for new and innovative product features like flexible coupons, ESG tracking, and dynamic portfolio reallocation. Until native issuance hits critical mass, however, there would be fractured liquidity given clear demarcation between off-chain and on-chain liquidity in assets that have a non-tokenized form and a digital form on-chain.

Figure 19. Tokenization of Off-Chain Assets vs. Digital Native Issuance

Tokenization of Off-chain Assets	Digital Native Issuance
Re-birth of existing assets	Birth of new assets
Digital representations exist on-chain	
Underlying assets also exist off-chain[55]	Underlying assets exist only on-chain[55]
Akin to securitization drawing an analogy from traditional finance	A step towards dematerialization where digital forms replace physical forms entirely
Usually pool together assets and issue digital tokens that act as "stores of value" and carry the rights associated with these underlying assets	Powered by public key cryptography that boosts functionalities like atomic and instant transferability, token-level compliance, and conditional settlement
Real World Assets: real estate, collectibles like art and wine agriculture, and non-conventional commodities **Financial Assets:** stocks, bonds, commodities, and funds issued, traded, and managed both on-chain and off-chain	**Real World Assets:** intangible assets like intellectual property (IP) **Financial Assets:** stocks, bonds, and funds issued, traded, and managed solely on-chain **Private Assets:** loans

Source: Citi GPS

Notably, tokenization of real-world and financial assets may facilitate a phased glidepath to DLT adoption under a more well-managed and compliant environment given the existing financial infrastructure and regulations of the underlying assets. Tokenization can act as an on-ramp for legacy assets into the digital ecosystem, which may enable an organic transition of capital into new digital structures, thus avoiding a disruptive migration or drawn-out existence of parallel infrastructures.

Appendix 2 contains a summary of digital financial market scaling infrastructure and ecosystem players supporting digital securities, between new digital disruptors and traditional FMIs scaling to adapt to the new technology.

While the tokenization of outstanding securities is under exploration, recent activity in the native issuance of digital securities has focused on bonds. Bonds are a good fit for tokenization given current market challenges with existing friction points, as well as a supportive and innovative issuer community, primarily among supranationals, who have been some of the biggest drivers of innovation historically.

[55] Marcelina Fryszka, "Two Types of Asset Tokenization on Ethereum," Medium, August 10, 2021.

© 2023 Citigroup

Figure 20. Examples of Major Native Digital Securities Pilots

Issuer	KfW	UBS Group	European Investment Bank (EIB)		
Currency	EUR	CHF	EUR		GBP
Size	EUR20 million	CHF375 million	EUR100 million		GBP50 million
Legal Regime	German Law	Swiss Law	French Law	Luxembourg	Luxembourg
Exchange Listing	Not listed	SIX / SDX	Not listed	SOL (Securities Official List section in the LuxSE)	SOL (Securities Official List section in the LuxSE)
Issue Date	Dec 2022	Nov 2022	Apr 2021	Nov 2022	Jan 2023
Tenor	2 years	3 years	2 years	2 years	2 years
Pricing	2.381%	2.330%	0.000%	2.507%	FRN
Infrastructure	Clearstream, on D7 digital post-trade platform	SDX	Forge	DAP by GS	Orion by HSBC
Settlement	T+0	T+0 on SDX T+2 on SIX	T+1 Using CBDC (BdF)	T+0 Using CBDC (BdF)	T+2
Custody	Traditional	SDX/SIX	Wallets by bookrunners	Wallets by bookrunners	Wallets by bookrunners
Key Innovation	▪ Digital bond in the form of central register security based on the German Electronic Securities Ac(eWpG)	▪ Can be held in both CSDs of SDX and SIX and tradable on both	▪ Public permissioned blockchain issuance using ETH	▪ Private permissioned blockchain ▪ Prospectus was filed with a regulator	▪ Combination of private and public blockchains ▪ Deal record on public blockchain mirror that provides increased transparency on an anonymised basis

Source: Company Websites, Citi GPS

Sample Use Case: Digital Securities as Collateral

A key securities market segment that faces significant operational friction and could derive immediate benefits from tokenization is the collateral/securities borrowing and lending market, or as it is colloquially called, the repo market.

Existing trade and post-trade processes remain largely manual and inefficient, but new DLT-based solutions to these are emerging

Although it transacts over $2 trillion in monthly volumes, the market's existing trade and post-trade processes remain largely manual and inefficient, consuming significant risk capital.

Several new DLT-based digitization and tokenization initiatives have emerged to target this large and inefficient market by creating digital collateral records on DLT infrastructure. Once digitized, these can be part of a single, seamless collateral pool enabling faster collateral flows (this is useful for rapidly growing flows such as variation margin postings in the over-the-counter derivatives market) by tapping into smart contract features like atomic and conditional settlements.

Platforms such as HQLA^X, JPMorgan's Onyx repo platform, and Broadridge's DLT Repo have begun to process billions in securities lending volumes already and have potential to scale up further. This would bring significant operational and capital savings to the industry.

Given current industry momentum, it seems feasible that digital collateral markets could become the first scaled use cases for digital tokenized securities flows.

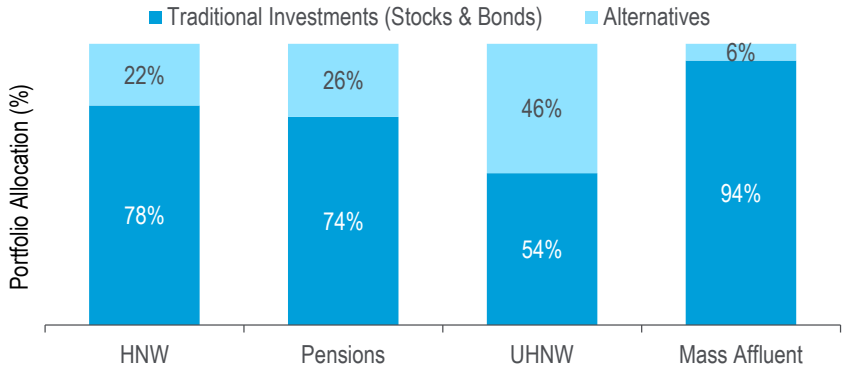
© 2023 Citigroup

Sample Use Case: Private Fund Tokenization

Historically, investment in private market funds has been a challenge for retail investors, and the space has been largely restricted to large institutional investors and ultra-high net worth individuals.

A stated objective of the alternative-assets ecosystem is to increase allocation to retail investors, such as accredited investors and the mass-affluent segment. The mass-affluent segment currently allocates around 6% to alternative assets, while institutions allocate 30%-50%.

Figure 21. Investor Portfolio Allocations (%)



Source: Citi GPS

Tokenization could solve private-market investment challenges related to high minimum investment amounts, long holding periods, limited liquidity, underdeveloped secondary markets, fractured asset discovery, complex investment processes, and lack of investor awareness

Challenges underpinning this continued under-allocation are high minimum amounts for investment; long holding periods; limited liquidity, including the lack of a well-developed secondary market; fractured asset discovery options; complex and manual investment processes; and a lack of investor awareness and education, among others.

Tokenization, along with wider digitization of the end-to-end workflow, promises to solve a number of these challenges. Although we are in the early days, asset managers are testing the waters by launching digitized versions of popular funds.

Private-market investment firm Hamilton Lane partnered with digital securities exchange ADDX to tokenize a share class of its popular global private asset fund, leading to a decrease in the minimum ticket size to $10,000 from $125,000 or more, through traditional, non-tokenized distribution channels.[56] This also opens up investors to the option of being able to trade these funds on the digital exchange.

Late in 2022, alternative asset manager KKR also tokenized its healthcare fund on Avalanche, a public blockchain, using digital assets firm Securitize.[57] Meanwhile, private equity firm Apollo launched investment management operations with fintech Figure on the Provenance blockchain to launch new tokenized funds.[58]

[56] Hamilton Lane, "Private Markets Leader Hamilton Lane Partners With ADDX To Offer Tokenized Access To Its Global Private Assets Fund, In Major Foray Into Asia," March 29, 2022.
[57] KKR Press Release, "Securitize Launches Fund Providing Tokenized Exposure to KKR Fund for the First Time in the U.S.," September 13, 2022.
[58] Apollo, "Apollo and Figure to Collaborate on Blockchain-Enabled Initiatives," July 14, 2021.

© 2023 Citigroup

Beyond Tech: What Is Needed to Scale Securities Tokenization?

Multiple things still need to be put in place to scale securities tokenization

- **Digitization Before Tokenization:** Before tokenization can have a meaningful impact on the workflow, the entire workflow must be digitized. To the extent that legal documentation is captured in a digitally native way (rather than by scans and PDFs), it enables composability with smart functionalities. Different jurisdictions are prioritizing laws and regulations that enable digital documents to be legally valid, and this would pave the way for more adoption (covered further in the "Trade Finance" section). Later in this report, we also cover in-depth smart legal contracts, which have promising potential to assist automated execution, including using real-world data captured through Oracles.

- **Support from Traditional Finance Players:** If established financial service providers could widen their approach to adopting the emerging and fragmented DLT network, they may help normalize adoption of tokenization for investors. TradFi players' involvement could standardize processes and enable consumer acceptance around tokenization.

- **Technology-Neutral Laws**: As issuance momentum builds, pilots and proofs of concept have explored the boundaries of innovation within current financial services legislation and tested associated legal and regulatory frameworks.

  These have led to prioritization of a clear need to have flexible technology-neutral laws around clearing and settlement, and new digital-native infrastructures for trading and settlement of tokenized assets. The European Union's new pilot regime for market infrastructures based on distributed ledger technology (the DLT Pilot Regime), which recently went live in March 2023, is one such effort to spur innovation by providing a clear regulatory and legislative sandbox.

- **Interoperable Platforms and Standards:** Further, existing pilot transactions point to the need for interoperable platforms and standards; failing both, liquidity will get fragmented and siloed, and the DLT initiatives will struggle to hit critical mass. User experience has a long way to go, especially for the majority of traditional investors unfamiliar with the concepts of tokens and wallets.

- **Digital Cash Infrastructure:** Digital securities also require digital cash infrastructure to enable delivery versus payment (DVP), a key tenet of settlement automation. New digital cash infrastructures are emerging, such as Regulated Liability Network, Partior, and Fnality, which could help automate the cash leg of the transactions. Central Bank Digital Currencies (CBDCs) could also play a pivotal role, as discussed earlier in this report.

- **Industry and Governmental Collaboration:** Scaling would require industry and government collaborations in creating supportive regimes that incentivize and encourage innovation. As noted earlier, only a few jurisdictions have begun to create these models, resulting in early transactions being based in these jurisdictions.

- **Standardized Taxonomy:** Common scalability hurdles for digital assets include the fragmented legal and regulatory landscape across different regions and the lack of a global unified taxonomy and classification standard.

© 2023 Citigroup

Open Question: What Is the ChatGPT Moment of Tokenization?

What will be the use case, product, or enabling regulation that propels the gradual cautious experimentation with tokenization to mainstream attention? This remains an open question.

Will it possibly be the multi-trillion-dollar repo market tapping out new efficiencies and balance sheet optimization, saving millions — if not more — for participating institutions? Could it be the average investor on the street getting access to esoteric private funds in a highly liquid format? Could it be a new regulatory framework that enables traditional financial assets crossing the threshold into DeFi-like use cases and on public blockchain?

The ChatGPT moment for the tokenization of financial assets remains to be seen.

© 2023 Citigroup

A Conversation With John Wu on Tokenization

John Wu is President of Ava Labs. In this role, he leverages his expertise from over 20 years as a fintech executive and technology investor to create a blockchain-enabled solution for originating, issuing, and trading financial assets. John was previously CEO of the SharesPost Digital Assets Group, enabling compliant token trading of private shares and funds. Prior to that, he was a technology investor and founder of Sureview Capital, a global hedge fund backed by the Blackstone Group.

Q: How can blockchain help financial services and other industries?

John: Blockchains benefit not just companies in the financial services space, but all enterprises, through operational efficiencies in exchanging value. While Software as a Service (SaaS) firms also try to make things more efficient, they often achieve this by connecting siloed, monolithic servers and optimizing workflows with automation.

When you start with a single source of truth, instead of creating APIs (Application Programming Interfaces) or reconciliations across servers, you instantly start with a more efficient construct. This is the promise of blockchain. Blockchains enable workflow automation and database management with everyone having the shared source of truth.

The other use of blockchain is for tokenization of an asset. When you tokenize an asset, it transfers the right of ownership into a digital form on a blockchain. This offers ease of use for owning and transferring assets, as the rules around ownership and transfer are embedded into the code. As a result, one does not need as many lawyers, auditors, and other intermediaries.

These are the two major benefits of blockchain for institutions, not just financial services — efficiency of the database structure and tokenization. Blockchains offer a more eloquent solution for ownership rights and transfer of assets.

KKR, a private equity firm, partnered with the Avalanche platform and Securitize, an alternative trading system, to tokenize a part of one of their private equity funds on-chain. It enables the qualified purchasers to gain access to those private equity funds in a more direct way with lower investment minimums. After a year's time, the idea would be to introduce secondary-market liquidity into traditionally illiquid assets.

Q: For what asset classes do you see the most value in tokenization? Why?

John: The more complicated the asset class, the more value tokenization can add. In structured products, you have so many different participants all trying to figure out the transparency of the data and then get a pricing on the data. If you're a smaller entity, you have limited access and transparency to the complicated and illiquid assets.

Historically, illiquid assets tend to have more intermediaries and are more suited for disruption by blockchain and tokenization. Intain, an asset-backed securities administration platform for institutional borrowers and investors, is moving its tokenized marketplace to Avalanche and is starting to realize the benefits.

On the other end of the spectrum, tokenization can enable emerging market participants to have access to public market assets in developed markets.

Q: Will tokenization of private securities be a game changer for blockchain?

John: I personally am very excited. Moreover, I was also previously the CEO of a company that tokenized private securities. Hence, my excitement is multi-fold.

In my opinion, it is very hard to get access to private securities today, unless you are an institution. Blockchains can help tokenize these securities and widen access.

© 2023 Citigroup

From a technology perspective, one can easily fractionize the concept of broker-dealer custody legally. One broker-dealer can be on the company's cap table, but they can fractionalize and let smaller investors own smaller portions of the shares and are allowed to trade that private security.

I believe this is a great opportunity. Until recently, individual investors did not have many opportunities to invest in private companies before they went public. Hence, I am very passionate about enabling access to illiquid private securities for individuals and smaller investors.

Q: Where are we in the context of financial institution and enterprise interest in blockchain adoption?

John: There are still a lot of tools and infrastructure that need to be put in place to totally obfuscate away all the infrastructure continually being built in this space.

Over the past two years, we have seen a lot of institutional-grade infrastructure being built and integrated across chains, enabling institutions to directly participate in services such as custody, staking, and wallets. We have come a long way to enable greater institutional participation, but we have not yet hit lift-off velocity, as people are experimenting in a slow manner.

On a scale of 1 to 100, where 100 represents full adoption, in my view, we are still in the early stages, probably near 20 or 25 on the scale. However, just twelve months ago, we were near 5 or 10 on the scale, and just 24 months ago, we were at 1 or 2.

We have come a long way in the last 1-2 years, but we have an equally long way to go for mass adoption. In my view, we will be close to mass adoption when we reach a level of 50 on the above scale. Presently, we are still at the lower end. For reference, reaching a level of 100 would signify we do not even talk about blockchain anymore and use it seamlessly in our daily lives.

© 2023 Citigroup

A Conversation With Morgan McKenney on the Future of Finance and Blockchain

Morgan McKenney is the CEO of Provenance Blockchain Foundation. Previously, Morgan spent nearly 20 years at Citi in a range of senior executive operating roles, including Chief Operating Officer for the Global Consumer Banking business and leading large payment businesses.

Provenance Blockchain is an open-source, public blockchain designed for financial services and leveraged by 60+ financial institutions that have transacted in digital assets across lending, marketplace/exchange and payments. USDF, bank-minted tokenized deposits, will also leverage Provenance Blockchain post regulatory approval.

Q: Why is blockchain important? Why do we need it in financial services?

Morgan: Blockchain in finance enables participants to bilaterally transact and instantaneously settle with any counterparty — known or unknown. This is transformational, and significantly different from the way traditional finance operates. Today, we typically rely on intermediaries to deliver financial services on assets we own, but do not control — we rely on our banks to make payments, move financial assets, and purchase and sell stock on our behalf.

Several innovations in financial systems across jurisdictions have led to real-time settlements, but much of this still operates only domestically and in silos (this is not applicable for cross-border transactions) and is often restricted to the payments space. While there is a growing focus on digitalization of banking services, much of this tends to be at the consumer app layer, while the middle and back office continue to run on existing systems that require extensive reconciliation across participating intermediaries.

Most other financial assets, such as foreign exchange transactions and mortgages, still do not settle in real time. This leads to costliness and time-inefficiency, while also locking up capital for potential operational and counterparty risk.

Blockchain opens up the possibility for two parties to directly enter into a transaction and exchange digital assets in real time, irrespective of their location and without any intermediaries, such as banks. Use of blockchain could also help improve process efficiency, saving time and reducing costs.

Blockchain is finance's internet moment. This is the first time we can re-architect how finance is done today at the infrastructure level, and in doing so, create significant business benefits that also benefit end-consumers.

Blockchain will transform the assembly line of the finance factory by enabling deep-rooted innovation, particularly in the middle- and back-end layers of the ecosystem. An asset created to be digitally native can then be serviced, financed, and securitized on the blockchain, offering substantial downstream benefits.

Q: What business opportunities does blockchain offer beyond efficiency?

Morgan: First, blockchain allows for fractionalization (i.e., miniaturization) and tokenization of various asset classes. High-value assets can be sliced up into smaller affordable pieces. For instance, why get a mortgage for $1 million to make investments in housing properties? This may be out of reach for most people. Instead, customers can get a mortgage for just one-fifth of the property (i.e., $200,000).

Second, blockchain allows for broader access, especially in the case of private assets. When assets are put on-chain, more users can gain access to private assets, as price discovery becomes much easier. Investors also do not need to lock in their capital for several years and can exit more easily, if desired, with the help of secondary liquidity opportunities. As these assets can now be valued, owners can also receive lending on the assets for liquidity. The tokenization of private assets is likely to help drive investor participation in previously illiquid asset classes.

© 2023 Citigroup

Lastly, blockchain can help reduce the cost to serve, thereby driving financial inclusion. Traditional banks would love to broaden their customer footprint if they could, but the cost to serve is just too expensive. This boils down to the infrastructure constraints and high cost of serving customers using old legacy technology. What if you could lower your marginal cost of adding a new customer by using blockchain? Lower costs to serve customers combined with fractionalization could help banks drive financial access to a previously unserved customer segment.

Q: What are the blockchain use cases in financial services?

Morgan: In my view, one of the killer use cases for blockchain technology is in the private asset space, for example: private market securities, alternative assets, real estate, and private funds. These assets typically lack easy price discoverability and are not readily transferable. Thus, acquiring privately-issued assets can be time-consuming and cumbersome. Blockchain can enable issuance of equity interest on-chain.

Moving issuance on-chain can also facilitate secondary offerings to investors. For example, employees of a private company can sell their shares to prospective investors. The companies can also control who can and cannot subscribe to their shares. All these records can be updated on the blockchain in real time.

By contrast, public equity markets tend to be very large and highly liquid. They are therefore not the best use case for blockchain technology.

Q: If blockchain is a game changer, why has adoption been very slow?

Morgan: When we think about traditional financial institutions, we often think of legacy infrastructure. A typical large bank processes between $5 trillion and $6 trillion of payments daily on behalf of its customers. Given the risks, traditional financial institutions prefer to rely on tried, tested, and proven technologies and processes. While we have seen experimentation with blockchain technology for several years, 2022 marked the first year of true adoption by financial institutions in their core businesses.

However, there are some challenges that need to be overcome for large-scale adoption.

Firstly, institutional adoption typically tends to be slower due to large business volumes and the potential for risk.

Secondly, blockchain is not a plug-and-play technology. You have to do a complete business re-engineering to create an amazing customer experience. So, institutions need to re-architect their processes, deploy new digital solutions, and re-think governance procedures throughout their ecosystems. This can prove very challenging, especially for adopting a technology still at a nascent stage. FinTechs such as Figure, showcase how blockchain can be leveraged in the lending and private asset space, as well as with firms working to build capabilities that make adoption easier for institutions. But this will take time to evolve and be embedded.

Blockchains are also known for their transparency, as each is a shared ledger. This is definitely a cause of concern for financial institutions, especially in the context of privacy — how do you restrict others from knowing what the institution is doing on behalf of its customers? Financial institutions also need to ensure their services are only provided to customers with full know-your-customer (KYC), necessitating the need to develop for new KYC/anti-money laundering (AML) solutions on-chain.

© 2023 Citigroup

Lastly, in order to buy financial assets on-chain and to receive sale proceeds thereof, one needs digital money with atomic settlement. Regulatory clarity on the use of digital money is of paramount importance. In our view, banks should be leading in the representation of deposits and money in bank accounts on blockchain, given their regulatory frameworks and risk management strengths.

Blockchain technology is complicated, and several building blocks still need to mature. If we draw an analogy to baseball, we are still in the first or second inning. For mass adoption, the technology needs to be extensively pressure-tested. However, there is growing global attention on blockchain and Web3 technologies with strong capital flows, and a lot of work is being done in this space.

In my opinion, we are unlikely to see widespread adoption of blockchains tomorrow — it is a marathon, and we are sprinting. We are likely 5-10 years away from mass adoption of blockchain globally. However, the benefits of blockchain are significant, and will catalyze adoption in the longer term, particularly in financial services. Increased regulatory clarity, as well as improved capabilities on digital identity and the authentication of user credentials, is only likely to boost adoption.

Q: Why do we need a permissionless blockchain? How do you manage risks?

Morgan: There is an ongoing debate on permissioned versus permissionless blockchains. The most valuable platform companies today — for example, Apple, Google, and Amazon — help bring buyers and sellers together with the help of an innovative platform. For instance, Apple offers an open innovation platform wherein a developer can build an app and publish it on the app store in order to monetize it.

Permissioned blockchains are too similar to the very permissioned intermediated financial services of today. They do not provide enough incremental benefits, given the challenges of adoption.

Permissionless, on the other hand, takes open innovation and harnesses the power of human creativity to build the future. “Permissionless” means something is open for anyone to build, join, and participate in. This is consistent with the use of digital technology to democratize access to financial services globally. In my opinion, internet platforms of the future will be on open, permissionless blockchains that leverage the power of open innovation and encourage access.

Public and permissionless does not mean you need to compromise on standards and governance. The risks of a public open system are and can be managed in a number of ways. For example, we require governance by the community for any code changes or new smart contracts. Asset issuers can embed restrictions into their tokens in terms of where those assets can go. KYC credentialing can be embedded at the protocol layer. We also have technology to help monitor and mitigate risks by scanning the entire network for any compliance gaps. For example, several companies today scan all wallet addresses for sanctioned behavior with the aim to identify how many steps away a wallet holder is from illicit funds. This technology can then restrict any transactions from a sanctioned wallet.

© 2023 Citigroup

Trade Finance

Trade Finance and the Opportunity

Legal reforms and greater interoperability could drive up to $1 trillion of tokenization in global trade finance by 2030

Trade finance is a set of techniques or financial instruments used to mitigate the risks inherent in international trade, ensuring both payment to exporters and the delivery of goods and services to importers.[59] Trade finance is a large market, worth about $8 trillion in 2022 and likely to grow to $12 trillion by 2030 (assuming the same compound annual growth rate of 5.4% on the 2029 forecast of $11.6 trillion).[60] The World Trade Organization (WTO) estimates trade finance plays a key role in facilitating and supporting as much as 80%-90% of international trade. Legal reforms and greater interoperability could drive up to $1 trillion of tokenization in global trade finance by 2030.

Trade finance was one of the earliest discussed enterprise use cases for blockchain, and for many years, it has been a graveyard of grand announcements and dashed expectations. However, just possibly, this may all be about to change. We are not going to see all of trade move to a blockchain-based solution, or even a majority, but interesting change is underway. This time may well be different.

> For businesses, being early adopters and willing participants in an electronic trade document transfer network will immensely help their operations. Besides freeing them from holding onto paper documents, it greatly enhances transaction speeds by cutting document delivery times from days to minutes.
>
> – STEFAN KUKMAN, CEO OF CARGOX, A BLOCKCHAIN-BASED DOCUMENT TRANSFER COMPANY

Almost 80% of global trade has English law as its governing law, and soon English law is likely to start accepting electronic transferable records

One driver of change is upcoming legal reform. Almost 80% of global trade has English law as its governing law, and soon English law is likely to start accepting electronic transferable records.[61] This is a potentially material change with far-reaching consequences for the digitization of trade finance. It should also help reduce the almost 30 billion paper documents printed and flown daily.[62]

The Model Law on Electronic Transferable Records (MLETR) was first introduced in 2017 by the UN Commission on International Trade Law (UNCITRAL) and adopted by Bahrain, Singapore, Abu Dhabi, and others by 2021. MLETR applies to electronic transferable records — bills of lading, bills of exchange, international guarantees, letters of credit, other receipts, and similar.

Why is it relevant? Up to now, only paper documents were legally binding under common law in most countries. Making the electronic form of documents legally binding will be greatly beneficial by improving the speed and security of transmission, permitting the reuse of data, and automating certain transactions through smart contracts. Digitizing trade documents is the first step to the use of digital assets in trade finance.

---

[59] U.S. Department of Commerce International Trade Administration, "Trade Finance," 2022.
[60] Valuates, "Global Trade Finance Market Research Report," January 2023.
[61] London Court of International Arbitration, *2021 Annual Casework Report*, June 2021; UK Parliament, "HL Bill 57," PDF, accessed March 21, 2023.
[62] UK Government, "Paperless Trade for UK Businesses to Boost Growth," October 12, 2022.

© 2023 Citigroup

Digital transformation is projected to offer cost reductions in global international trade and increased trade volumes of up to $9 trillion, or around 10% of global GDP.[63] Legal reform could bring total benefits from paperless trade to $1 trillion across the commonwealth countries by 2026, and similar benefits are also expected in Asia.[64]

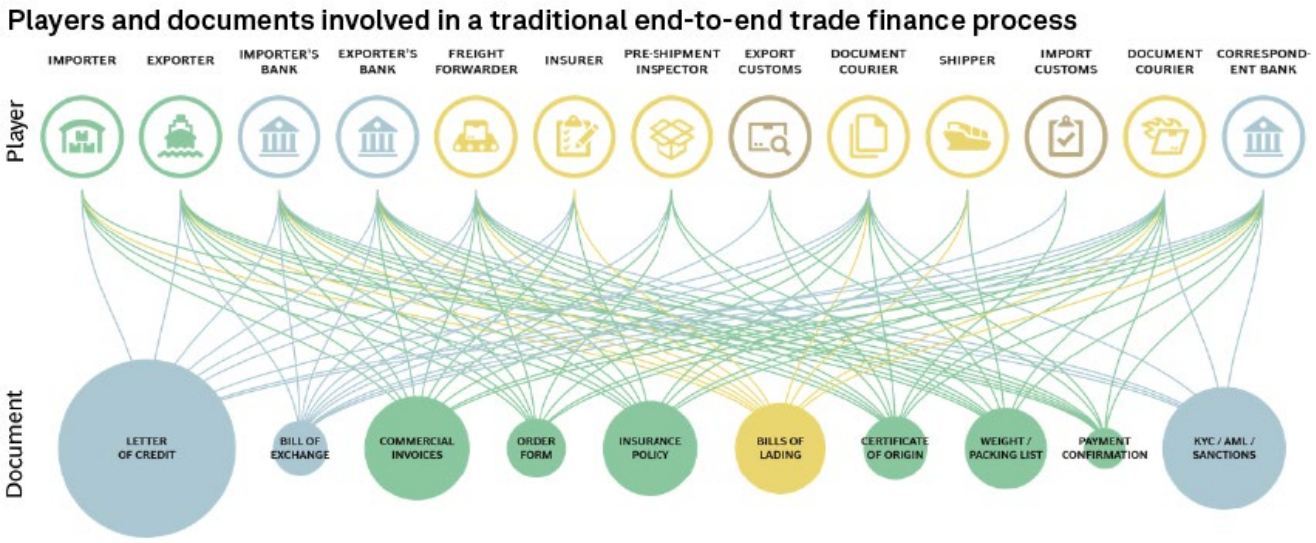
A second driver of change is a greater focus on interoperability. Previously, banks and companies deployed private networks and closed group consortiums — this was the equivalent of some people using SMS messages, others on WhatsApp, and another group on Telegram. But now, there is a greater awareness of the need for communication between networks — to have a network of networks.

Inefficiencies in Trade Finance: The Old and The New

Blockchain has the potential to transform global trade and supply chains by reducing intermediation costs, fraud, effort duplication, and information asymmetry

Several industries have made revolutionary changes, primarily by bringing down barriers to information availability and exchange. Trade — and as a result, trade finance — remains highly paper-based and is one of the least digitized parts of the global financial system. Emerging technologies, including AI, blockchain, and others, have the potential to transform global trade and supply chains by reducing the high intermediation costs, frauds, duplication of efforts, and informational asymmetries.

Figure 22. An Illustration of Different Players and Documents Typically Involved in the Traditional Trade Finance Process



Source: The Boston Consulting Group, "Digital Innovation in Trade Finance: Have We Reached a Tipping Point?" October 2017

[63] Loughborough University and Tech NGI, "The Digital Transformation of International Trade," September 13, 2022.
[64] The Commonwealth, *Quantitative Analysis of the Move to Paperless Trade*, April 2022; Yann Duval, Chorthip Utoktham, and Alexey Kravchenko, "Impact of Implementation of Digital Trade Facilitation on Trade Costs," UN ESCAP ARTNeT Working Paper No. 174, January 2018.

© 2023 Citigroup

- **Authenticity and Access to Documentation:** Typical shipments can involve up to 20 different documents, printed out at varying shipment stages for a host of players. The process involves significant manual input of the same data by different parties, leaving room for errors and fraud due to fragmented and non-interoperable interfaces or technology systems.[65] Lack of knowledge of electronic trade document transfer is a major barrier to global adoption.[66] According to Bain & Company, 50% of a bank's cost for a letter of credit arises from the manual handling and checking of documents, potentially leading to delays and errors.[67]

- **Legal and Regulatory Landscape:** International trade still relies to a large extent on a special category of trade document, which is dependent on being physically possessed, transferred, and delivered. Digital copies of trade documents were not accepted under law. Although UNCITRAL passed new rules in 2017, they were not initially adopted by any major jurisdictional law, but some countries now follow them.[68] Limited regulations around blockchain have led to a lack of common process standards and information disclosure, hampering wider adoption. Data localization laws also pose constraints for blockchain networks with entities from multiple nations.

- **Close-Looped Blockchain Network:** Several private technology players, logistics companies, and financial intermediaries have built bespoke networks to put trade finance processes on-chain, but most have been close-looped. Thus, they failed to build a sufficient critical mass of players. Supply chain blockchains need adoption not just at the distributor/producer level, but across the entire chain, including suppliers, logistics partners, banks, and financiers.

- **Interoperability and Lack of Standards:** Incompatibility between disparate digital platforms has slowed technology adoption.[69] As supply chains become more data-driven and interact with multiple ecosystems, interoperability across all systems interacting with the blockchain will be crucial. A lack of common standards often hinders the seamless flow of data throughout the supply chain.

- **The Old and The New:** Blockchain development is in its early days, and its implementation in trade and supply chains faces several challenges, including an inability to integrate with existing infrastructure. Legacy systems and manual operational processes still need to be updated and automated to a certain extent to be plugged into blockchain, and before that happens, blockchains may not be able to substantially transform the trade finance industry. Before digital assets adoption, you need digitization, but the trade ecosystem is very paper-based.

---

[65] Kati Suominen, *Revolutionizing World Trade: How Disruptive Technologies Open Opportunities for All* (Redwood City: Stanford University Press, 2019); IMDA Singapore "International Trade and Logistics," last updated November 30, 2022.
[66] CargoX, "Market Report: Industry Blindspots Blocking Adoption of Digital Trade Documents Transfer," September 1, 2022.
[67] Glen Williams et al., "Distributed Ledgers in Payments: Beyond the Bitcoin Hype," Bain & Company, June 12, 2016.
[68] United Nations Commission on International Trade Law, "UNCITRAL Model Law on Electronic Transferable Records," July 13, 2017.
[69] CargoX, "Market Report: Industry Blindspots Blocking Adoption of Digital Trade Documents Transfer," September 1, 2022.

© 2023 Citigroup

Blockchain for Trade Finance

In an increasingly digital world, the acceptance of electronic/digital versions of documents for trade finance will drive blockchain adoption.

- **Digital Identity, Document Digitization:** Digital ID and the full digitization of documents using blockchain can help improve supply chain visibility, build mutual trust, and improve authentication of ownership. Digital ID may be used for the verification of individual identities (buyers, suppliers, or inspection agencies) or the identification of assets for inventory and shipment tracking.

- **Operational Efficiency:** Blockchain creates and upholds a single version of documentation that each party can access and edit in real time, eliminating the need for duplicative manual processes and the potential for forgery, resulting in time and cost savings. Digital documents could enable atomic settlement — as soon as the goods or services are delivered, payments using digital money 2.0 could ensure instant settlement and finality. Later in this section, we discuss the use case of a multi-central bank digital currency (mCBDC) for trade settlement across different countries.

  According to Jerry Foster, Chief Technology Officer and co-founder of Plex Systems:

  "*Blockchain technology ensures that, as contracts are altered, each party has a copy of the contract that is updated in real time. If two parties don't have a way of ensuring they are continuously operating on the same contractual obligations by leveraging a shared and immutable contract document, they risk operating under outdated contractual requirements as the document changes.*"

  "Multiple departments within an enterprise are responsible for maintaining, tracking and executing different parts of a contract. Often, separate departments are also storing contracts in different ways, leading to siloed information. This means contract updates and operations may not be shared with the entire team, including legal departments."[70]

- **Cost Reduction and Smaller Clients:** Traditional trade finance involves a lot of manual paperwork and cumbersome legacy systems that can be labor-intensive and expensive. Banks do not have enough monetary incentive to service smaller clients in trade finance, leaving a $1.6 trillion gap.[71]

- **Goods Syncing and Fund Flow:** Today, trade financing, settlement, and goods movement are not connected to each other, so each party has to keep a track of details such as financing, logistics, and ports. Blockchain, with the help of smart contracts, digital documents, and digital currencies, could be an opportunity to address this disconnect.

[70] Jerry Foster, "Emerging Blockchain Uses for Supply Chain: Overcoming Labor and Time Shortages With Smart Contracts," *Forbes*, February 23, 2023.
[71] Asian Development Bank, "2016 Trade Finance Gaps, Growth, and Jobs Survey," September 2016.

© 2023 Citigroup

- **Risk Reduction:** Businesses may feel more comfortable transacting through blockchain knowing that smart contracts can disenable unilateral changes. DLT makes it easier to examine the reputation of buyers and sellers through publicly visible transactions and potentially eliminate dishonest actors. It also can help reduce commercial risk, defined as "the risk of non- and delayed payment caused by the importer's insolvency or cash-flow problems."[72]
- **User Experience:** User Interface (UI) and user experience (UX) may be more friendly with the vendor-researching, negotiation, and end contract process all happening on chain, potentially with a single API.

Furthermore, additional benefits can be realized by syncing alternate data, such as ESG, business key performance indicators (KPIs), KYC analyses, risk assessment results, and insurance appraisals, which can be easily bundled on single platform using blockchain. Also, existing networks like SWIFT can be a data/messaging contributor to an open blockchain ecosystem in trade finance to accelerate adoption and interoperability.

Digital Money 2.0 for Trade Settlement

The People's Bank of China, the Central Bank of the UAE, and the BIS Innovation Hub (by the Bank for International Settlements) joined the mCBDC bridge with the Bank of Thailand and the Hong Kong Monetary Authority (HKMA) to facilitate real-time, cross-border foreign exchange payments on the distributed ledger technology. International trade settlement was chosen as the first business use case to be piloted on mBridge.

Local currencies play limited roles in international trade. Depending on sources, 50%-60% of global trade is denominated in U.S. dollars.[73] This is due to the relatively high transaction costs associated with most regional currencies compared with those of major currencies.[74] In 2020, the correspondent banking model costs (excluding foreign exchange costs) were nearly $120 billion for $23.5 trillion worth of cross-border transfers.[75]

The mCBDC pilot consisted of the four participating jurisdictions directly on the mBridge. The pilot differs from other multi-CBDC projects and pilots in two ways: (1) the settlement of international payments happened directly on the common platform and not on each country's domestic payment systems, and (2) paying and receiving banks carried out transactions directly with each other.

The mCBDC pilot aims to demonstrate the ability of DLT network- and central bank-issued digital currency to improve cross-border payment speed and efficiency, as well as to reduce costs and settlement risk.

---

[72] U.S. Department of Commerce International Trade Administration, *Trade Finance Guide: A Quick Reference for U.S. Exporters*, July 2022.
[73] BIS, "Revisiting the International Role of the U.S. Dollar," December 5, 2022; Carol Bertaut, Bastian von Beschwitz, and Stephanie Curcuru, "The International Role of the U.S. Dollar," Federal Reserve, October 2021.
[74] Junko Shimizu, "Exploring Local Currency Usage to Reduce Exchange Rate Risks in Asia," ASEAN+3 Macroeconomic Research Office (AMRO), January 30, 2019.
[75] Oliver Wyman and J.P. Morgan, *Unlocking $120 Billion Value in Cross-Border Payments: How Banks Can Leverage Central Bank Digital Currencies for Corporates*, November 2021.

© 2023 Citigroup

Technical Details: mBridge Ledger (mBL)

After experimenting with different technology architectures in earlier phases, the project team developed a new native blockchain for mBridge, the mBridge ledger (mBL). In this approach, different modules such as payment, foreign exchange, capital management, and compliance are decoupled and modularised to accommodate the evolving needs from different jurisdictions.

The multi-central bank digital currency (mCBDC) pilot project aims to demonstrate the ability of DLT networks and CBDCs to improve cross-border payment speed and efficiency, lower settlement risks, and reduce costs

At the core of the mBL are the central banks, which each run a validating node that operates the mBL consensus protocol. Each central bank can onboard its domestic commercial banks onto the platform, and the commercial banks of each jurisdiction are all connected to the onboarding central bank and hence to the validating core of the mBL. Once onboarded, commercial banks can transact on behalf of their clients, extending the reach of the platform.

The mBL consensus protocol is a private, permissioned, and distributed system. The mBL uses a consensus mechanism named HotStuff+. However, the platform is considering a new consensus mechanism named Dashing, which is being tested. It uses triple-certificate security, a process in which three certificates with different thresholds are used under different network circumstances. Hence, higher efficiency and robustness are achievable relative to current consensus protocol.

© 2023 Citigroup

A Conversation With Bob Blower on the History and Future of Trade Finance

Bob Blower is the CEO of Clarency.com, a B2B payments platform, and the founder of Jindau.com, an innovative token-based working capital platform. Bob has held senior roles in trade finance for HSBC, National Bank of Abu Dhabi, Standard Bank, and others. He began his career in finance over four decades ago at HM Treasury, working on fiscal, monetary, and regulatory topics.

Q: What is the history of trade finance? When was the last innovation in trade finance?

Bob: The whole principle behind trade finance is to provide a guarantee of payments to an exporter based on the flow of documents between the buyer and seller. It also gets involved in the contractual relationship of the underlying commercial transaction. This process requires a lot of documents evidencing ownership of goods, bill of lading, and more. The bank manually reviews them to ensure all documents are valid and in accordance with terms of the letter of credit before approving payment.

Trade finance involves multiple parties — the shipping company, logistics company, insurers, and various other individuals and agencies who want to see and review the documents.

The letter of credit or bill of exchange has been used in Europe since the Renaissance period. In fact, the 90-day windows on letters of credit are based on the duration of time required to travel from Italy to London. Funnily enough, we still use that same time duration for some financial commitments, even today.

Letters of credit were traditionally governed by internationally recognized rules in English law, rather than national law. The International Chamber of Commerce created a voluntary framework for commercial banks to apply to transactions worldwide; the framework is updated regularly to reflect changing legal conditions.

The fundamental process has not changed for almost 300 years. Letters of credit existed only as paper documents; they were regularly issued by telegraph in the late 19th century. Only in 1973, with the creation of SWIFT, did banks began to migrate to electronic messages, initially telex-based, to convey the terms of credit.

Q: Why did blockchain consortiums in supply chain and trade finance fail? Why will it work this time around?

Bob: In my view, the people who experimented with blockchain consortiums so far predominantly tried to do it from a technology point of view.

However, the recognition in law that the electronic obligation is the same as paper-based obligation was never achieved. So how will companies adopt such technology and not get into legal or regulatory trouble?

Presently, if I receive a bundle of physical documents, my obligation is to check and verify those documents. But I could generate the same documents electronically in seconds and digitally review and check them in microseconds.

English law is changing right now, and it is going to be a game-changer for trade finance. Acceptance of electronic documents will legitimize a lot of blockchain initiatives, which have been trying to bring efficiencies to trade finance since 2015-16.

I am positive about blockchain solving serious pain points in trade finance, but not until it addresses the rule of law and the rules under which it has functioned until now.

I also see a coordination problem.

© 2023 Citigroup

The blockchain initiatives in trade finance have been closed loop until now, so they worked well for collaboration in a controlled environment. However, peers struggled when it came to dealing, transacting, or interacting with peers out of the network. To work smoothly, peers needed to be in existing platforms to prevent the need for reconciliation between on-chain and off-chain interactions, data, and transactions.

In my view, participants need to be connected at the roots. For example, if two banks agree on common blockchain standards, transactions can be processed successfully. Computers at both banks can verify the documents are confirmed and conform with the credit I have received through the bank — this is harmonization of standards and platforms.

If one could get the five largest banks in each market to agree on a network and platform, the rest of the industry would soon follow. Changes in law will further institutionalize the space, and coordination among supply chain participants will drive the adoption of blockchain technology in trade finance.

Q: What are the economic benefits of this legislation in terms of cost savings or value add in trade? What does the adoption look like in the near- to medium-term?

Bob: The Centre for Information Management at Loughborough University held a workshop on the Digital Transformation of International Trade in September 2022 and concluded that digital transformation could result in an 80% cost reduction in global trade while increasing trade volumes by over 40%.

In my view, trade finance has seen very little innovation in the last 300 years, but digitization on the back of changes in legislation could result in a massive economic benefit. A single change in law is likely to reduce the time it takes to send and clear documents, also resulting in economic benefit.

However, I do not anticipate rapid blockchain adoption anytime soon. We are first likely to see greater digitization, which could lead to greater institutional coordination in this area. By 2030, we could see 8%-10% of trade finance on the blockchain.

© 2023 Citigroup

A Conversation With Sunil Senapati on Blockchain Use in Trade Finance

Sunil Senapati is Chief Operating Officer – Trade and Payments at XinFin, an open-source hybrid blockchain protocol. He has 25+ years of experience in Technology, Consulting, and Trade. He has held various positions and worked closely with CXO-level executives providing business transformation using technology. Previously, he has worked with Maersk, Oracle, Bolero, and MonetaGo.

Q: Why have previous blockchain initiatives and pilots in trade finance failed?

Sunil: Blockchain is an ideal technology for trade finance and meets its primary needs of real-time tracking of cargo and documents, increasing transparency, reducing counterparty risk, enabling automation and swift settlements, and reducing transaction costs. The trade finance process involves verification of documents, authentication, transfer of titles from party to party, and multiple parties operating in different jurisdictions and on different platforms, and it is a mammoth coordination task.

Until now, some consortiums have created bespoke blockchain and non-blockchain platforms. For example, in 2018, IBM and Maersk founded TradeLens, a blockchain-enabled trade platform. TradeLens provided every entity involved in global trade with the digital tools to share information and collaborate securely. However, in November 2022, the platform and the offerings were discontinued, as global industry collaboration could not be achieved.

TradeLens could not reach the level of commercial viability necessary. This was a collaboration and adoption problem. A platform led by a shipping major is not seen as a neutral party. TradeLens was the brainchild of a shipping company and a technology company, but they had trouble onboarding banks. One reason: no legal framework that accepted digital documents.

Q: What is changing on the legal front?

Sunil: No major jurisdiction or regulator accepted digital documents in supply chain and trade finance up until recently. This led to limited uptake of any digitization solution in trade. There are billions of paper documents transferred and flown around daily. This process needed to be digitized.

While many companies used digital documents on a bilateral basis, the industry needed mass adoption, and for mass adoption we need regulatory and legal clarity. The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Transferable Records (MLETR) in 2017.

MLETR aims to enable the legal use of electronic transferable records both domestically and across borders. Some jurisdictions, such as Bahrain, Singapore, and Abu Dhabi, adopted the rules between 2018-21, which is a start but not enough, as more countries need to legally recognize the use of electronic documents in trade.

On October 12, 2022, The Electronic Trade Documents Bill (HL Bill 57) was introduced in the House of Lords in the UK Parliament to provide digital trade documents the same legal footing as their paper-based equivalents and to give UK businesses more choice and flexibility in how they trade.

If passed, this bill will modernize old legislation such as the Bills of Exchange Act 1882 and the Carriage of Goods by Sea Act 1992 and will make the UK one of the biggest global trading countries in the world to legalize electronic trade documents. Presently, around 80% of world trade is based on English law.

Q: Will it work this time? Why will we see blockchain adoption in trade finance?

© 2023 Citigroup

Sunil: One of the drivers for adoption of blockchain in trade finance is that the UK is going to start accepting digital documents as part of international trade. This is groundbreaking because given that most of global trade follows English law, it makes digital documents in most of international trade acceptable in a court of law.

This grants much-needed legal and regulatory clarity to trade participants, and even banks, to start their digitization processes. Electronic transferable records may be particularly relevant for certain business areas, such as transport and logistics and finance.

English law accepting electronic documents will be a game-changer for trade finance and blockchain's adoption.

Moreover, the blockchain networks are becoming friendly because they have realized that if they operate in silos, they are not going to get critical mass to carry on operations, let alone see mass adoption. The industry is also experiencing a "network of networks," which essentially connects the individual blockchain networks so they are interoperable.

The learnings from the blockchain and supply chain industry, as well as the openness of legal and regulatory bodies, will help the flow of information in the supply chain and trade finance sector get faster.

Q: What percentage of global trade flows will involve digitized flows and use the blockchain for part of their process by 2025? By 2030?

Sunil: Tough to give a number, but with more countries accepting electronic trade documents, I feel we should see this percentage moving to two digits by 2025.

By 2030 and beyond, we are likely to see greater adoption, with interoperability taking the digitized flows to higher percentages. Wider adoption will require simpler applications, low or no costs to use the basic functionalities, and new liquidity providers to support the trades.

© 2023 Citigroup

[C.] Technology Enablers

Four core components will drive mainstream adoption of blockchain

In this section of the report, we address the big question: What key components of technology are needed to drive mainstream adoption of blockchain? We then delve into four core technology drivers:

- Blockchains enable pseudonymous or anonymous identities. How do we tie these new features to real-world identity and/or authentication? We outline the solution stack around **decentralized identities** and recent developments in this space.
- **Zero-knowledge (zk) proofs** are key for driving blockchain adoption through two impactful applications: scaling and privacy. ZK proofs could be the game-changing technology that allows institutions and large enterprises to use public blockchain without comprising the confidentiality of proprietary data.
- Blockchains can only work on data that is available on-chain and cannot access real-world data or information. **Oracles** are central to connecting blockchains to real world data and information. We map out how Oracles work and highlight important applications where Oracles are used.
- The future is likely to be inherently multi-chain. Interoperability between chains is fundamental to ensuring we do not end up in a siloed infrastructure. We explore why **secure bridges** are fundamental to interoperability and scaling.

Blockchain Adoption Is Much Slower Than Internet Adoption:

The internet was available for commercial use starting 1995, and by 2005, it had hit its first 1 billion users. While this was a remarkable journey of exponential growth marked by booms and busts, the internet had found its product-market fit with over 15% of the global population in just about 10 years of being available commercially.[76]

Blockchain, in contrast, has a much slower adoption cycle. Fourteen years since the launch of the first bitcoin blockchain, we are estimated to be at 420 million crypto users globally in 2023, well under the 1.8 billion internet users accumulated over the comparable period.[77]

Slow Adoption — It Is Not Just the Technology:

The internet enabled a "net-new" capability — the information superhighway. Blockchain, by contrast, will create change in part by replacing a current functioning system (the value-transfer layer), but also by advancing a new ideology (self-sovereignty and decentralization), and offering new capabilities and operating models (digital tokens and on-chain functionalities) — all with a layer of speculative price action and volatility thrown in. To complicate things further, the technology brushes up against the core of the monetary system and regulations and needs to interoperate with existing infrastructure. So, when is blockchain *not* a good fit?

We do not envisage DLT-based financial infrastructure fully replacing traditional financial market infrastructure

Notably, blockchain has a number of use cases for which it may not be appropriate and throwing blockchain at a problem could actually degrade user experience, such as in the cases shown below:

[76] Max Roser, Hannah Ritchie, and Esteban Ortiz-Ospina, "Internet," Our World in Data, accessed March 20, 2023.
[77] TripleA, "Cryptocurrency Ownership Data", accessed March 20, 2023.

© 2023 Citigroup

- Systems run by centralized entities (where trust is not an issue) and infrastructure operated and maintained by one party (where a shared golden source of data is not relevant) may not be suited to blockchain. The infrastructure components in several financial markets rely on high-frequency, millisecond-level, low-latency trading data and execution, and fundamentally, present-day blockchains and DLT might not be appropriate in these situations, as they introduce significant latency for transaction confirmation.
- Systems reliant on serialized workflows may also not be a good fit, unless business processes are re-engineered to fit a distributed system.

Blockchain will find product-market fit where distributed infrastructure exists with a shared source of data, cryptographic verifiability, and decentralized control

We do not envisage DLT-based financial infrastructure fully replacing traditional financial market infrastructure (FMI). Instead, blockchain will find product-market fit doing what it does best — operating where a distributed infrastructure with a shared source of data, cryptographic verifiability, and decentralized control is material, leaving other areas in the domain of traditional FMIs.

From a technology specification perspective, we believe blockchain needs to have the items listed below in order to scale to billions of users:

- Transaction scale and throughput (how many transactions a system can process over a period of time) matching traditional finance.
- Strong guarantees of security: safety, liveness, and data availability.
- On-chain identity and a way to map to real-world identity (which can be disclosed selectively).
- Privacy of user identity and transaction data.
- Connectivity between real-world data and information and blockchain.
- Interoperability, i.e., the ability to transfer data and assets across different chains.
- User experience (UX) and user interface (UI) including native mobile support.

Transaction scalability and throughput improvement are focus areas of the public blockchain ecosystem, with different layer 1 (L1) chains — the base-level chain in a network — having their own approach to these problem areas. At a fundamental level, scalability, security, and decentralization have trade-offs, and it is hard to achieve all three at once — as captured by Ethereum co-founder Vitalik Buterin's "blockchain trilemma" concept. There is a lot of ongoing work on scaling with layer 2 (L2) chains, rollups (which gather transactions onto the main chain), sharding (which horizontally splits a database into smaller data sets, or shards), and modular blockchain features. With technology improving, there is an expectation that blockchains will reach throughput levels comparable to traditional applications, although the jury is still out on how long this could take.

© 2023 Citigroup

For blockchains to instill confidence in handling mainstream high-value transactions, they must consistently provide strong guarantees of security: safety, liveness, and data availability. "Safety" means assurance that nothing bad will happen (i.e., that the blockchain will not reach an invalid state — a "state" can be thought of as a snapshot of blockchain transactions at a point in time). "Liveliness" implies the correct thing will happen (i.e., that the blockchain eventually reaches a valid state given some time, even if there are temporary delays). Data availability (i.e., ensuring nodes have full access to block data) is also a key requirement, especially in the context of rollups, which enable the scaling of blockchain by executing transactions off the main chain.

Improvements in blockchain UX/UI are needed, and there are several ongoing projects in this space

Switching gears to the end-user: As covered in earlier sections of the report, UX and UI in the blockchain/Web3 space have a long way to go to drive mass consumer adoption. So far, users have needed to get used to new concepts, including custody of cryptographic keys, hot and cold wallets, remembering an arbitrary list of 12 key words, and "signing" transactions that look cryptic and unreadable.

"Being your own bank," or being personally responsible for your asset and activities, is a lot harder in practice than in theory, with even experienced developers or long-time players losing access to their cryptographic keys or being hacked. There is a lot of ongoing work in this space, including human-readable accounts like Ethereum Name Service (ENS) and the latest news from ETHDenver in early 2023 regarding Ethereum upgrading to "Account Abstraction," which could make Ethereum accounts more user-friendly by enabling customizable features.

A recent *Cointelegraph Magazine* article captures the features of account abstraction below:[78]

"Benefits include two-factor authentication, signing transactions on your phone, the setting of monthly spending limits on an account, the use of session keys to play blockchain games without constantly having to approve transactions, decentralized recovery of wallets; smart accounts can be configured to autopay bills and subscriptions — the list goes on."

In addition, there is pioneering work on making Web3 suitable for native use on mobile phones. In June 2022, Solana Labs announced the launch of its Web3 Saga mobile phone. The company describes the phones as "a premium mobile experience that enables you to trade tokens while waiting in line for coffee, mint non-fungible tokens (NFTs) on your morning commute, and have instant access to the dApps you love most, anywhere, anytime — all powered by Android," according to its website.[79] An integrated secure element microchip on the phone enables securing cryptographic private keys at a hardware level, while the wallets on the phone never directly interact with the keys. With the phones slated for launch in 2023, it remains to be seen if mobile UX can do to Web3 adoption what it did to scaling the internet.

In the next few sections of the report, we dive deeper into technologies driving identity, privacy, Oracles, and bridges.

[78] Andrew Fenton, "'Account Abstraction' Supercharges Ethereum Wallets: Dummies Guide," *Cointelegraph Magazine*, March 1, 2023.
[79] Solana Mobile, "Saga: Web3 in Your Pocket," accessed March 5, 2023.

© 2023 Citigroup

Decentralized Identity

- Decentralized identity is a core technology component that will enable regulatorily compliant uses of blockchain while still preserving anonymous/pseudonymous access.
- Decentralized identifiers can potentially flip the model from big technology platforms owning our identity data to self-sovereignty.
- Decentralized identity introduces a new paradigm of sharing identity information on a "need-to-know" basis for different use cases. It is likely to minimize the "digital footprint" users leave with Personal Identifiable Information (PII) data on the internet.

When it comes to identity, the role of any form of identification is the ability to confirm that "I am who I say I am." In short, it is all about authentication.

We use various forms of identity to authenticate ourselves in our daily lives, such as for unlocking our phones (e.g., face ID, fingerprint), entering offices (e.g., access cards), and traveling (e.g., passports, national IDs).

These different authentication types vary with the nature of the access request and are often specific to certain systems — i.e., you need a password, SMS, or One-Time-Password to access your email account, but to cross the border with another country, you need a legal form authenticating your identity (e.g., a passport).

Identity is about authentication

However, the internet does not have a built-in user authentication system or identity layer. This has led to a host of authentication solutions and logins, individually managed by different applications.

These identities are mostly centralized and siloed, come with limited rights, and come with the condition that we act in a certain prescribed way. Centralized identities are also prone to theft and censorship.

Digitization has changed the way we do most things — transact, interact, and trust. We see development of decentralized versions of everything (e.g., money, finance, and social media), though we are yet to see mass adoption.

Decentralized identity is an essential component in enabling the growth and widespread adoption of decentralized applications and services in the Web3 ecosystem

Decentralized identity is an important building block to deliver the decentralization promise of Web3 or blockchain. This does not imply a lack of centralized parties in identity issuance or verification, but that the mechanism of owning, sharing, and verifying identity is done in a permissionless, decentralized manner. However, the advent of decentralized self-sovereign identity will help us: (1) drive Web3 adoption, and (2) address the shortcomings of centralized identity, including portability and censorship.

However, decentralized identity solutions are in a nascent stage of development and pose risks, including: (1) software and security challenges, (2) loss or theft of private keys, (3) malicious nodes intercepting and cloning personal information, and (4) surveillance capitalism or the commodification of personal data.

© 2023 Citigroup

> Digital identity is our access key to the digital ecosystem, and blockchain is the future of finance and can help make digital identity more secure.
>
> – DR. RUTH WANDHÖFER, INDUSTRY EXPERT, NED, CHAIR OF THE PAYMENT SYSTEMS REGULATOR PANEL, VC PARTNER

Identity: From Beads to Biometrics

About 100,000 years ago, individuals used jewelry and beads to communicate wealth, family ties, and personal identity. Tattoos and body art were also used to convey a person's status, ancestry, and membership in a particular group as early as 4000 B.C. [80] Around 3800 B.C., the Babylonian empire and later the Roman empire made a common practice to collect citizens' data and issue identity documents.[81]

Fast-forward to the 15th century, King Henry V created a document (i.e., a modern-day passport) for English citizens to prove their identity in foreign countries. Throughout the 20th century, countries developed various national identification methods, and in 1977, we have the first record ever of the computerization of personal identification.

Following on, the 21st century has been all about biometrics. In 2004, the U.S. deployed statewide automated fingerprint databases. In 2010, India introduced Aadhar, the world's largest biometric digital ID system, which captures citizens' fingerprints and iris scans and assigns them a unique 12-digit number. Belgium issued electronics ID cards (eIDs) as part of the Belgian Personal identity Card Project (BeIPIC), initiated in 2003. The eID enabled citizens and residents to avail themselves of government services and saw 100% adoption by 2011.[82]

Need for Decentralized Identity

A passport functions as a legal identity, which provides certain rights — from crossing borders to opening bank accounts — whereas a digital identity provides various rights in the borderless world of the internet. Like every technology, we have seen digital identity transform over the years.

We evolved from our simple email example of digital identity in Web1 to the only slightly more secure and further siloed forms of digital identity in the Web2 era that allowed users to rent digital space (which we explain below). Today, we are at the cusp of an emerging concept of decentralized on-chain self-sovereign identity in the Web3 era. This may permit users to own their identity and help them authenticate their digital content and digital assets.

We need to enable decentralized digital identity to enable Web3

As internet use cases grew in the Web2 world, we saw the emergence of various authentication solutions and logins issued by different platforms (e.g., Google, Apple, Facebook) that allowed users to "read and write," i.e., Web2-enabled interaction.

[80] Katina Michael and M.G. Michael, "The Proliferation of Identification Techniques for Citizens Throughout Ages," University of Wollongong, 2006.
[81] Veriff, "The History of ID," May 10, 2022.
[82] Thales Group "Electronic ID Cards in Belgium: The Keystone of eGovernment," accessed March 20, 2023.

© 2023 Citigroup

Large platforms may have become the gatekeepers and controllers of the respective types of digital identity, enabling the right to access, while users became "renters" of the digital space with limited rights. Web3, as the next iteration of the internet, enables "read-write-own" capabilities along with the promise of decentralization, censorship-resistance, and sovereign ownership.

> Decentralized identity and verifiable credentials technology will become a game changer resulting in a metamorphosis of the identity space.
>
> – SUBHA TATAVARTI, CHIEF TECHNOLOGY OFFICER, WIPRO LIMITED

Decentralized identities are generated from a completely neutral protocol, using pure math

Decentralized identities are digital identities generated by a completely neutral protocol, from pure math. Web3 enables users to be identity owners, different from their earlier roles of being renters. Web3-based decentralized identity is not mainstream yet, but it could help us address the shortcomings of Web2-based identities.

Why do we need decentralized identity? Why does decentralized identity matter for the adoption of blockchain and Web3?

- **Centralization**: In a centralized system, the user is completely dependent on the platform issuing the digital identity (e.g., Google, Facebook). This creates a single point of failure. For example, if one uses Google login credentials to sign up to an audio or video streaming platform and the login credentials are stolen or blocked, one could lose access to all accounts and websites that use this identity for authentication.
- **Silos vs. Interoperability:** Web2-based digital identity is siloed in the sense that it can only be used for access, identification, and authentication on a single platform. Admittedly, federatedID allows users to use their digital identities from BigTech platforms, such as login with Google, login with Apple ID, and login with Facebook, to access other sites. However, if a user loses their Apple, Google, or Facebook ID, they will lose also access to other platforms. With international technical standardization, Web3-based identity could be developed such that it is interoperable. This would allow users to carry their Web3-based ID across platforms and services.
- **Censorship-Resistance:** Web2-based digital identity is issued and controlled by companies, leaving users with very little choice or control. We have seen multiple examples of the deplatforming of users by BigTech platforms. This means all user data, content, and contributions can be lost any second at the discretion of a single company or a person. Web3-based identity is not issued by BigTech, but is cryptographically signed and owned by the user, meaning nobody can take it away. Components of Web3-based identity can be issued by centralized parties, but control and presentation of these identifiers are solely in the hands of the user.
- **Data Privacy:** Today, centralized platforms control a user's identity and personal data. Digital identity solutions offer privacy and control over users' personal data. This requires implementation of privacy-preserving mechanisms, like zero-knowledge proofs, to protect personal information from unauthorized access or misuse.

© 2023 Citigroup

- **Security**: In centralized systems, identity security is ensured by the security of central servers and databases, but these "central honeypots" are open to attack by malicious actors. For example, LastPass, an online password management service, revealed in December 2022 that hackers obtained user information such as billing and email addresses, usernames, telephone numbers, and IP addresses.[83]

  Digital identity on a distributed network is harder to penetrate and compromise as robust cryptographic mechanisms, as well as consensus and distribution protocols, can protect against wrongful access, thefts, and misuse. The different digital identity attributes (e.g., age, university degree, work history, car registration) are distributed across the network and thus, there is no central honeypot with all identity attributes that can be hacked.

Figure 23. Evolution of Users and Identity in Various Iterations of the Internet

	Web1	Web2	Web3
Time Period	1996-2004	2004-2016	2016+
Content	Existing information gathered into a single database	Individuals gained the ability to create information in a global database	Individuals have the potential to monetize their own data
Information	Mostly Read Only	Read and Write	Portable and Personal
User Profiles	Tourists	Renters	Owners
Forms of Identity	N/A	Email ID, Usernames, Biometrics	Naming Services, Verified Credentials, Badge, Soulbound NFTs, Proof of Humanity

Source: ResearchGate, WordPress, Citi GPS

Identity in the Web3 World

Digital identity in the Web3 world refers to a unique, verifiable, and decentralized representation of an individual or entity on the blockchain

Digital identity in the Web3 world refers to a unique, verifiable, and decentralized representation of an individual or entity on the blockchain. It typically includes personal information, such as names, addresses, social media accounts, and other identifying characteristics, that is stored in a secure and decentralized manner.

Web3 digital identity solutions aim to provide individuals and entities more control over their personal data and the ability to use it in a secure and trusted manner in online transactions and interactions.

[83] Ben Demers, "Struggling LastPass Suffers New Data Breach. Is Your Account at Risk?" Kiplinger, accessed March 20, 2023.

© 2023 Citigroup

> Self-sovereign identity puts users in control. In accordance with the principle of data minimization, users consent to specific datapoints to be shared as opposed to sharing everything. User data is not stored in one centralized place. They can either store their data themselves or avail of third-party trust providers to do so.
>
> – DR. RUTH WANDHÖFER, INDUSTRY EXPERT, NED, CHAIR OF THE PAYMENT SYSTEMS REGULATOR PANEL, VC PARTNER

Digital identity solutions also make it possible to integrate blockchain technology into various existing systems and applications, which makes it more accessible to a wider audience.

A digital wallet will hold a user's social credentials, digital assets, personal accounts, biometrics, etc. Protected by private keys, the user can decide to selectively expose their identity credentials for different use cases as they deem fit.

Polygon ID

In March 2023, Polygon released a self-sovereign identity infrastructure stack built on zero-knowledge proofs. The new infrastructure offers users a way to verify their identities while safeguarding the privacy of their personal data.

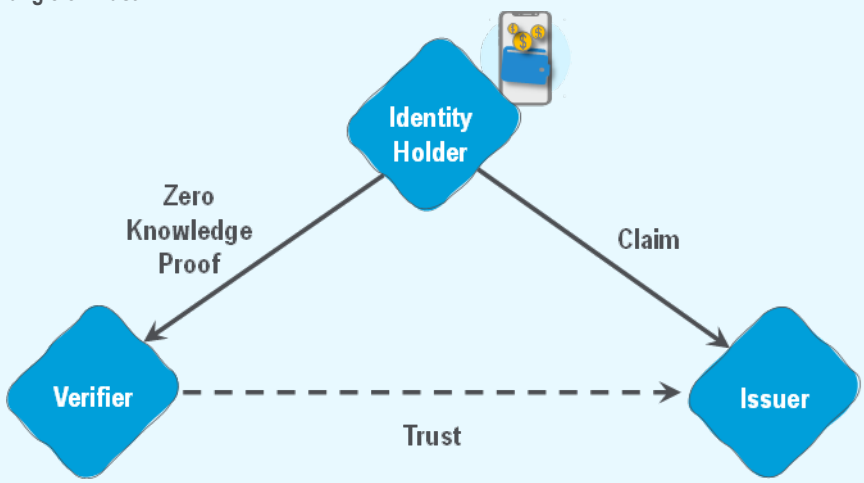
Polygon ID can be used to build off-chain credentials such as diplomas, driver's licenses, or national IDs. Polygon ID can enable users to store and update digital assets (including avatars and objects), achievements, and progress to be used across different games and within the metaverse.

The Polygon ID stack is an open-source license, allowing developers to leverage zero-knowledge technology within their existing compliance processes without sacrificing user privacy.

The Polygon ID is based on three main modules: identity holder, issuer, and verifier. These three entities form what is commonly referred to as the triangle of trust, where trust must exist between a verifier and an issuer.

Every identity is identified by a unique identifier called a DID (Decentralized Identifier), and every identity-based information is represented via a Verifiable Credential (VC). VCs are issued by an issuer to an identity holder, who generates zero-knowledge proofs of the VCs issued and presents these proofs to the verifier for verification.

Figure 24. Polygon ID's Triangle of Trust



Source: Polyton Technologies, Citi GPS

© 2023 Citigroup

How Does Decentralized Identity Work?

Decentralized identity is based on public key cryptography. Users are assigned public-private key pairs, with the public key generating a unique address and the private key functioning like a password that is used for authentication. It is worth noting, however, that the public key encryption is not quantum-proof.

The private key, housed in a Web3 wallet, can then be used to connect to Web3 websites and decentralized applications, bringing one's digital wallet into different apps for seamless interoperability.

According to the World Wide Web Consortium (W3C), the international standards organization that lays out specifications for decentralized identity, a decentralized identifier has the following necessary characteristics:[84]

- **Decentralized:** There should be no central issuing agency.
- **Persistent:** The identifier should be inherently persistent, not requiring the continued operation of an underling organization.
- **Cryptographically Verifiable:** It should be possible to prove control of the identifier cryptographically.
- **Resolvable:** It should be possible to discover metadata about the identifier.

A good example of a decentralized identity stack is Ethereum Name Service (ENS) — an open-source, blockchain-based identity protocol. ENS enables users to create a unique username NFT that resolves to a wallet and eventually allows them to carry a unique ID across Web3 applications.

ENS is a protocol for human-readable crypto addresses and decentralized domain names. It is similar to DNS (Domain Name System), i.e., a system that assigns human-readable domain names to internet protocol (IP) addresses in Web2.

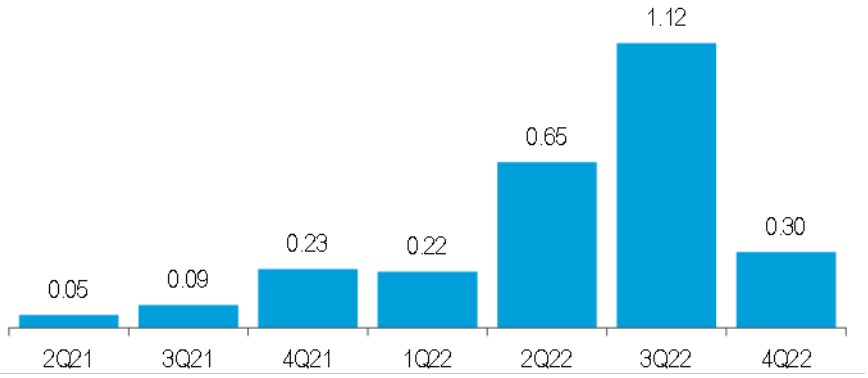
For example, one can send ERC-20 tokens (fungible or non-fungible) to ronitghose.eth instead of a long cryptographic address. It is much easier to remember and easier to do business with (transact) in the Web3 world when identification is simplified.

ENS registrations rose in 2022, driven by crypto users rushing to secure the ".eth" namespace. We expect other identity or decentralized social protocols may launch their own native namespaces such as .crypto or .lens.

[84] W3C Working Group, "Use Cases and Requirements for Decentralized Identifiers," W3C Working Group Note, March 17, 2021.

© 2023 Citigroup

Figure 25. Ethereum Name Service (ENS) Registrations (in millions)



Note: Data as of February 9, 2023.
Source: Dune Analytics, Citi GPS

Sign-In with Ethereum, launched in 2021, enables users to use their Ethereum account and associated ENS name as identifiers across multiple services, including off-chain applications. Users can use their Web3 wallet of choice to connect to the underlying Ethereum accounts and their ENS names to log into applications.

Verified credentials are core building blocks of the decentralized identity technology stack

In the context of decentralized identity, "verified credentials" are core building blocks of the technology stack. Verifiable credentials are a digital, cryptographically secured version of physical and digital credentials, which people can present to organizations that need them for verification. Employee experience certificates, digital passports, and digital driver's licenses are some examples of identity documents that can be issued as verifiable credentials.

Where are decentralized identities stored? A Web3 identity wallet is an application that can be used to store data about an individual's identity. Unlike traditional digital wallets, which are controlled by central authorities, Web3 identity wallets are decentralized and can be controlled by the individual.

Decentralized identity and verifiable credentials in a Web3 wallet can be used to connect to decentralized apps (e.g., decentralized social and gaming), which we believe are in early stages of development but could be drivers of blockchain mass adoption.

Self-Sovereign Identity: Applications and Use Cases

Self-Sovereign Identity (SSI), or Decentralized Identity (DID), is a method of identity that gives control of information back to the user. It eliminates the need to store personal information on a central database and enables individuals greater control over what information they would like to share. SSI, or DID, is a user-centric, user-controlled approach to exchanging authentic and digitally signed information.

© 2023 Citigroup

We think self-sovereign identity could be the passkey to interact in the Web3 world of decentralized finance, decentralized social, and an open Metaverse, among others. A 2022 report by the company cheqd estimates self-sovereign identity's total addressable market at around $550 billion.[85] McKinsey estimates full digital identity coverage in just the seven focus countries they analyzed could add 3%-13% to GDP in 2030.[86]

- **Wipro:** In February 2023, Wipro Lab45 launched the Decentralized Identity and Credential Exchange (DICE) ID. DICE ID is blockchain based and enables the issuance and verification of tamper-proof, self-verifiable digital credentials. DICE ID securely stores authorized personal information issued by verified issuers directly in the user's identity wallet. All data is encrypted and embedded, and the user only receives it into their own identity wallet. This digital wallet can be used to share identity credentials with current or potential employers, healthcare or financial services providers, or educational institutions, among others.[87]

- **Microsoft:** In 2021, Microsoft's digital identity team launched a digital identity network called ION, a new framework for users to authenticate themselves. The decentralized identity network has been live on the Bitcoin network and functions as a layer 2. In the same way that Lightning Network uses Bitcoin's network for payments, Ion uses Bitcoin's blockchain to create digital IDs for authenticating identity online. A public key and its associated private key are used to verify if a user owns an ID.

- **AID:Tech:** AID:Tech provides enterprise-level solutions to international NGOs, governments, and corporates. Through the delivery of digital entitlements through blockchain technology and digital identity, AID:Tech addresses some of the largest obstacles in global development, including legal identity, financial inclusion, and corruption. Its Self-Sovereign Decentralized Digital Identity, which acts as a gateway to digital services, is built on W3C standards and is compatible with AID:Tech's interoperable digital identity protocol.[88]

- **European Citizens and Businesses:** The European Digital Identity Wallet will be available to EU citizens, residents, and businesses who want to identify themselves or provide confirmation of certain personal information. It can be used for both online and offline public and private services across the EU. It gives full control to users to choose which aspects of their identity, data, and certificates they share with third parties, and keeps track of such sharing. The digital identity wallet is expected to go live by 2024.[89]

---

[85] cheqd, *Self-Sovereign Identity: How Big Is the Market Opportunity?* 2022.
[86] Olivia White et al., *Digital Identification: A Key to Inclusive Growth*, McKinsey Global Institute, April 2019.
[87] Wipro, "Wipro Lab45 Taps Into the Power of Blockchain Technology to Change the Paradigm in Digital Identification and Verification," Press Release, February 22, 2023.
[88] *Irish Times*, "Aid:Tech's Technology Will Put People In Charge Of Their Own Data," November 28, 2019.
[89] Alessandro Mascellino, "EU Says It Can Have a Digital ID Wallet By '24 Regardless of Challenges," Biometrics Research Group, November 14, 2022.

© 2023 Citigroup

Identity Enables Access

Self-sovereign identity is the passkey to decentralized finance

What is the impact of not having an identity?

Globally, just under 850 million people do not have a legal identity.[90] Without an ID, they cannot open a bank account, get a loan, receive government benefits, or even access basic healthcare.

In today's age, not having a digital identity is as detrimental as lacking a legal identity, as one cannot access basic benefits of the internet such as education, news updates, and work opportunities, among others. Having an on-chain decentralized identity enables users to directly interact with different protocols and platforms without needing BigTech corporates as guardians.

Self-sovereign identity could be the passkey to decentralized finance. As we saw in previous chapters, blockchain could bring efficiencies to finance and could be the future of finance; similarly, blockchain-based identity (on-chain identity) could be a crucial element to engage with decentralized finance.

Digital identity solutions might be necessary for scaling blockchain to billions of users, as they provide a secure and reliable way to identify individuals and entities on the blockchain network. We may need to enable decentralized digital identity to enable Web3.

While centralized platforms have access to all information linked to the account (i.e., facial features, location, sign-ins, interactions, and payments), a key advantage of decentralized identity is that the user should be able to decide which pieces of information to share with individual applications depending on the use case and specific requirements. This limits potential risk of credential theft or loss.

Globally, firms and platforms are exploring Web3 applications and how they can embed a certain degree of decentralization. Whatever the platform might be — public or private, centralized or decentralized, permissioned or permissionless — user identity is of utmost importance. We might just need to look for solutions that are future proof, interoperable, and censorship free.

Risks of Digital Identity

Risks include bugs or vulnerabilities in code, loss of private keys, malware-infected devices, potential for state or personal surveillance, and concerns around blockchains not being decentralized enough

There are always risks involved in emerging technologies and their applications. The industry and the ecosystem learn key lessons as they deploy these technologies for various use cases. There are risks involved with the use of decentralized identity, and we discuss some of these below:

- **Code Vulnerabilities:** Decentralized identity can leverage blockchain and interacts with various applications. Networks and applications are based on computer code, which could have bugs or other vulnerabilities. If a bugged code fails to authenticate a valid identity or authenticates a stolen identity and allows access on that basis, it could lead to losses (e.g., financial or brand loss).
- **Loss of Private Keys:** Distributed networks are secured on the assumption that private keys are stored safely by their owners. However, humans are capable of making mistakes, and the loss of private keys to malicious actors could bring serious financial loss to the identity owner.

[90] World Bank, "Identification for Development (ID4D) Global Dataset," 2022.

© 2023 Citigroup

- **Compromised Cookies/Access Tokens:** In a standard internet browsing experience, a user typically gets a cookie or an access token that will identify their session. Today, if a user authenticates to a service using a decentralized identity, the identity could for some time depend on a single cookie and not on the decentralized system. If malware infects the user's phone or laptop, it could potentially steal that cookie or access token after identity authentication.
- **Surveillance Capital:** Digital identity, unlike legal or paper-based identity, leaves behind a massive digital footprint that could serve as an arena for state or private surveillance. There could be systematic recording of all personal, financial, and geographical data from the online activity and interactions in order to predict future behavior of the users.
- **Insufficient Decentralization:** One of the common critiques of blockchain networks is that they are not decentralized enough. Arguably, some nodes could be malicious and try to intercept someone attempting to use their decentralized ID with the aim of stealing or modifying it, or even piggybacking into the system using the same credentials.

The rise of identity theft highlights the need for stronger and more secure ways for people to authenticate themselves. Decentralized identity offers some exciting possibilities, but it also presents novel cybersecurity challenges and new attack vectors.

© 2023 Citigroup

A Conversation With Dr. Ruth Wandhöfer on Why Digital Identity Matters to Web3

Dr. Ruth Wandhöfer is a Partner at Gauss Ventures, an early stage FinTech VC firm. Prior to that, Ruth was the Global Head of Regulatory and Market Strategy with Citi's Treasury and Trade Solutions business for over a decade. Ruth is also an independent Non-Executive Director at various firms including a bank, an exchange, a technology firm, and a Fintech and previously at a digital identity firm. She advises governments, financial institutions, FinTechs, and industry associations, as well as provides training and coaching.

Q: Describe digital identity — is it just authentication in a digital environment?

Ruth: Digital identity is about proving who I say I am in a digital way.

If we look at the evolution of the internet, Web1 had static webpages, where users read content, and access to websites and applications was basic. Think about the traditional email applications, which we accessed using an email address and an alpha-numeric password.

Moving to Web2, the internet became more interactive. People could create, upload, and exchange content. Security and authentication evolved from simple static passwords to dynamic passwords (e.g., one-time passwords sent via SMS).

In the current Web2.5 world, authentication procedures are still a mix of old and new technologies. For example, enrolling for a new account at most banks still requires uploading a copy of a passport. Albeit some neobanks have adopted technologies like video call-based onboarding and fingerprint/iris scan authentication.

In my view, biometrics could offer a seamless solution for authentication. Multi-nodal biometrics, combining different biometric credentials for authentication, is likely to gain prominence. Biometric authentication is also more tamper proof, as it relies on elements within us and thus a combination of multiple biometric credentials makes hacking difficult to impossible. Web3 could further adapt these technologies, making the authentication process even more secure.

Q: How will digital identity work for Web3?

Ruth: Web3 is built on the promise of decentralization and aims to give control back to individual users by eliminating centralized platforms that often store tons of personal user information. Web3 aims to provide individual users with more options, including the choice to have their own trusted third-party provider that will act as an intermediary between them and the desired application. Web3 is built on the ideology of user control, user consent, and data minimization. Think of it as having your own secret vault to store all your identity information securely either yourself via an app or with the help of trusted third parties. And when accessing services, you only share the necessary information.

Contrast this with what we find most prevalent today. Most of us are aware of HTTP cookies on websites — we see them every day while browsing on the internet. Unfortunately, many websites are designed in such a manner that users cannot access a particular service until they consent to all the terms and conditions, which often involves a blanket agreement to share their personal information. Such consent journeys are manipulative, inevitably forcing you to share data in order to obtain access. It shows you how nothing is for free as you pay with your data. Web3 aims to reverse this power dynamic.

Q: Please elaborate on a few use-cases of digital ID in the Web3 ecosystem.

Ruth: Web3 is not there yet, rather it is in evolution and development. However, we can still discuss this from a conceptual standpoint.

© 2023 Citigroup

If a user wants to access a gaming platform in the Web3 world — most platforms often restrict entry to only those above the age of 16 or 18 years — digital identity plays a crucial role here to prove their age to the platform.

Looking at the payments space, most transactions in today's Web2/2.5 world are executed using debit or credit cards; but as we gradually move to Web3, we could see a greater role for cryptocurrencies and stablecoins. While transacting in cryptocurrencies does not need users to share identity credentials (as they are mostly pseudonymous), users still need to initiate transactions with their private key.

The Metaverse of the future is likely to offer a range of services from banking, social, gaming, and commercial shopping. All of these are likely to require the user to share credentials in order to gain access and participate. However, we should be in a position of greater control over our data to only share the necessary information with different service providers in order to enable authentication.

Q: Are we ready to take back control of our data as a society? Are we adequately informed to take personal accountability?

Ruth: That is the crux of the matter. The Web3 ecosystem has to be developed with those safeguards built in. Web systems need to be designed in a manner such that users do not just casually consent to cookies for convenience. Users need to be well-informed and moved away from the mindset of "I do not care what I am giving up for it." While users should ideally read the small print, Web3 systems should be designed to be more intuitive with data minimization and consent built at the core. This enables users to consent specifically to data points being shared with the option to enlist the support of trusted third-party providers, who securely store and share the user's data on their behalf. Note that users could decide to store their credentials with different trusted third-party providers to ensure more data security through distribution.

Admittedly, this approach may not fix today's social media platforms, where people, especially the younger generation, share everything with everyone, without properly evaluating the potential dangers.

The dark web is flooded with volumes of personal data/identities, including email addresses, passwords, and bank cards. This has led to the commercialization of data, resulting in significant data risks including identity theft. Social media in the Web3 world is likely to need a complete re-engineering.

Users need to be informed and educated on the potential dangers of misuse of their information in order to move away from sharing all their data with everyone. Tools using cryptography or zero-knowledge proofs can be implemented to curtail sharing of unnecessary data. Web3 systems need to bring more personal agency and control, while also protecting individual user rights.

Q: Describe the regulatory developments in Europe in context of users accessing Web2/Web3 platforms?

Ruth: Europe has commenced work on a digital identity framework. Across Europe, an EU regulation covering electronics identification and trust services (eIDAS) for electronic transactions within the single market has been in place for some time. In parallel, we have seen a number of national developments on electronification of national identity, such as in Belgium. Markets such as the Nordics have established a form of bank ID, allowing citizens access to a host of bank and non-bank services.

© 2023 Citigroup

More recently, the European Union has announced the rollout of a European e-identity wallet starting from April 2023. Member states are expected to provide this on demand to eligible users by 2024. The identity wallet is aimed at citizens, residents, and businesses located in the EU with a broad set of use cases, which include holding digital versions of one's passport, driving license, other travel documents, health records and even banking relationships.

The use of this type of e-identity wallet has the potential to offer limitless possibilities. Imagine, I live in France and notice cheaper mobile plans in Belgium. I could use my European e-identity wallet to enter into a contract with a Belgium network provider and buy my mobile plan from them (not from a firm in France). I could also open a bank account in Germany or rent a bicycle during my holidays in Amsterdam using my e-identity wallet. The e-identity wallet can even be used to log into social media or email platforms, rather than being forced into their proprietary sign-on mechanism.

Q: What is self-sovereign identity?

Ruth: Self-sovereign identity is about bringing back control over your digital identity by leveraging new technologies and processes such as distributed ledgers and decentralization. This can help a user create an identity and self-certify it.

In a self-sovereign identity system, the user is able to both create and control decentralized identifiers. Identity credentials can range from e-commerce transaction histories to social media accounts or data from any issuer. For instance, I may have a university degree certified by my university, which is the issuer of the degree. If I want to apply for a job, I may need to prove that I have a degree. The roles of issuers and validators are still relevant in self-sovereign identity. The verifier in this case will be the prospective employer, who would ask my university to authenticate the degree. The validator is my university, which validates my credential (the degree) so I can share this information directly with my prospective employer through the self-sovereign identity using a digital wallet.

Self-sovereign identities give users greater control over data and privacy with built-in principles of consent and data minimization.

Q: What are the key ingredients to using digital ID across different technologies such as decentralized and centralized ledgers?

Ruth: In my opinion, the success of digital identity hinges on the principles of standardization, recognition, and interoperability. From a standardization viewpoint, the W3C Consortium is working on technical standards for use in digital identity across the web, albeit this is likely to take time.

For any form of identity, it is important for it to be mutually recognized. For example, a digital identity should be recognized across digital and physical borders, enabling the users to access services and products seamlessly. There is also a need for regulators to build a global consensus around the principles of data minimization and consent.

© 2023 Citigroup

Achieving interoperability could prove to be a challenge across different platforms, especially as we bridge Web2 and Web3 worlds. The Web2 world is mostly built around public key infrastructure, while the new Web3 world is likely to be based on distributed ledgers, blockchain, and zero-knowledge proofs where alternatives to public key infrastructures (PKIs) will have to be considered, in particular in light of the emergence of quantum computing. Admittedly though, Web3 is still in its infancy, and we will likely see more innovation across data, hardware, and network solutions in the future.

For further reading, please refer to Ruth's book titled *Redecentralisation: Building the Digital Financial Ecosystem*, published by Palgrave Macmillan and launched in March 2023 (ISBN is 978-3-031-21590-2).

© 2023 Citigroup

Zero-Knowledge Proofs

Zero-knowledge proofs drive blockchain adoption through scaling and privacy

Why are zero-knowledge proofs important to scaling blockchains? How can institutions use public blockchains for transactions when a large majority of transactions — between suppliers, customers, employees, and other counterparties — are proprietary or confidential?

Zero-knowledge proofs are key for driving blockchain adoption through two impactful applications:

- Scaling, by moving computations off-chain in a verifiable way.
- Privacy, by keeping data, transactions, and computations hidden, but still enabling their correctness to be publicly verifiable.

Zero-knowledge proofs have powerful applications in privacy solutions beyond blockchains but are especially relevant in the context of public blockchains, as they provide a solution to a fundamental problem with using them for large institutions (where all participants can see data and easily trace wallet identity to real world entities).

What Is a Zero-Knowledge Proof?

A zero-knowledge proof (zk proof or ZKP) is, in simple terms, a proof that separates knowledge from verification. We use terms such as “succinct” and “argument” below as a way to help ease understanding, but these terms are not rigorously defined.

From high-school mathematics, most of us are familiar with the concept that, in order to prove something, we need to disclose the statement we are trying to prove and walk through the steps of the proof in sequence. But when a statement is proven in “zero-knowledge,” the prover proves a secret statement to the verifier without leaking any information about the statement. We can loosely consider these as “blind-proofs.”

In cryptography, this “proving” process is usually accomplished interactively, with the verifier asking a sequence of questions to the prover, and the prover answering them. These questions could involve, for instance, “opening up” the solution at specific locations to prove that the solution is correct, but this “proving” is done in a way that does not leak information about the whole, secret solution. Repeated enough number of times at different points, there is high probabilistic assurance that the prover knows the solution, although no information about the solution itself leaks during this interchange. This proof can also occur in a non-interactive way, but that would likely require a pre-processing step at both the prover and the verifier.

This abstract concept of proving in zero knowledge is best explained by a simple example, as laid out in the note “Applied Kid Cryptography or How to Convince Your Children You Are Not Cheating.”[91]

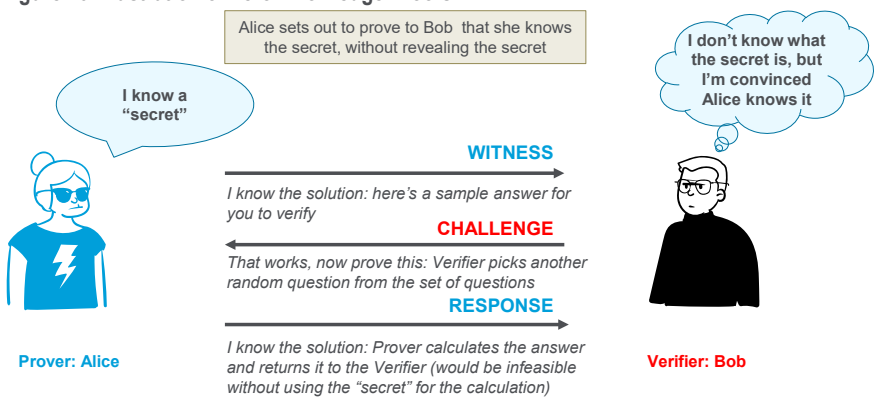
[91] Moni Naor, Yael Naor, and Omer Reingold, “Applied Kid Cryptography or How to Convince Your Children You are Not Cheating,” PDF, March 1999.

© 2023 Citigroup

Consider two characters, Alice and Bob, who are playing the children's game "Where's Waldo?" In this game, the goal is to find Waldo in a book, a character usually in a red hat and a striped red shirt, page after page, in a sea of colorful people. In the example, Alice knows where Waldo is on a page of the book but wants to prove to Bob that she knows this, without revealing the exact location on the page to Bob.

According to the authors of the note, a low-tech solution for this problem could involve Alice using a large piece of cardboard (larger than the book) with a small rectangle cut in the middle. Alice could then put the rectangle on top of the book while Bob is not looking to position Waldo to be visible through the cut-out. Bob now has proof that Alice knows where Waldo is but learns nothing beyond that.

Figure 26. Illustration of Zero-Knowledge Proofs



Source: Citi GPS

This immensely powerful concept — separating knowledge from verification — was first introduced by Shafi Goldwasser, Silvio Micali, and Charles Rackoff in their seminal 1989 paper "The Knowledge Complexity of Interactive Proof Systems." Their work won Micali and Goldwasser the Turing Award in 2013, widely referred to as the "Nobel Prize in Computing."

ZKPs are critical for enabling privacy on public blockchains to drive institutional adoption

As noted earlier, zero-knowledge proofs have powerful applications in privacy solutions beyond blockchain but are critical for enabling privacy on public blockchains to drive institutional adoption. They provide us an elegant solution to "have our cake and eat it too" by capitalizing on the transparency and public verifiability of a blockchain, without diluting the confidentiality and privacy of the information being written to it.

What Is a zk-SNARK?

The most popular zero-knowledge technique for blockchain applications is zk-SNARKS, a kind of zero-knowledge proof that is much easier to verify than it is to compute (e.g., to prove). Verification of this type of proof is usually in the order of a few milliseconds and with small proof sizes (in hundreds of bytes), even for large statements being proved.[92]

[92] Zcash, "What Are zk-SNARKs?" accessed March 20, 2023.

© 2023 Citigroup

> Perhaps the most powerful cryptographic technology to come out of the last decade is general-purpose succinct zero-knowledge proofs, usually called zk-SNARKs.
>
> – VITALIK BUTERIN, CO-FOUNDER OF ETHEREUM[93]

So, what is a "SNARK"? It is not "mocking irreverence" or an "imaginary animal" as a simple web search tells us; within the context of our discussion, a SNARK stands for Succinct Non-Interactive Argument of Knowledge.

An "argument" is similar to a proof, but it is computationally rather than statistically sound (i.e., it is impossible to break in practice with limited computational power). Typically, proofs are interactive and require the prover and verifier to exchange messages, as the prover works to convince the verifier of the proof of a statement. A "non-interactive" proof flips this model and attempts to prove the statement in one shot with no interaction between the prover and verifier. It may, however, need a "trusted setup" phase to enable proving in a non-interactive way. "Succinct" here implies the proof is short and quick to verify. The last keyword, "Knowledge," relates to the concept of sharing information about the statement the prover is trying to prove to the verifier. The default-mode is for knowledge to be shared; a zk-SNARK, however, is a SNARK that enables proving statements in a zero-knowledge way.

As renowned cryptographer and Stanford professor Dan Boneh explains, the way zk-SNARKS solve the privacy problem on a blockchain while retaining public verifiability is by users posting "commitments" to the blockchain, rather than posting transaction data to the blockchain.[94] A commitment is a cryptographically encrypted proof that keeps the data secret (like a sealed bid in an auction — once committed, these cannot be modified) but can later be opened to reveal what is inside. One can now attach a zk-proof to the commitment that the transactions in it are valid, and anyone can check the zk- proofs to convince themselves that the committed data is valid without learning any information about the data contained within. This notion can be generalized to proving a statement that any specific set of "rules" was followed in the commitment posted, by attaching a proof that proves rule-conforming behavior in a zero-knowledge way.

There are applications of zk-proofs beyond blockchain, especially in establishing identity or authentication, without divulging the underlying data. The succinctness property of a zk-SNARK enables us to verify transactions or data in a fraction of the time it takes to do the underlying computation.

[93] Vitalik Buterin, "An Approximate Introduction to How zk-SNARKs Are Possible", January 26, 2021.
[94] Dan Boneh, "Episode 100, Dan Boneh on the Past, Present and Future of Cryptography," *Zero Knowledge*, podcast, October 23, 2019.

© 2023 Citigroup

> SNARKS…are such an important tool because they help resolve this fundamental conflict in blockchains: they help us move from a totally public blockchain to a private blockchain while preserving all the properties of transparency and public verifiability.
>
> – DAN BONEH, CRYPTOGRAPHER AND HEAD OF APPLIED CRYPTOGRAPHY GROUP AT STANFORD UNIVERSITY[95]

Specific Zero-Knowledge Proof Use Cases

Zk-SNARKS enable privacy and scalability

Zk-SNARKS enable two main properties relevant for blockchains: privacy and scalability. Privacy comes from the zero-knowledge property of zk-proofs, where the prover is able to prove a statement to the verifier without revealing the secret. Scalability comes from the succinctness property, where verifying a statement is orders of magnitude faster than running the computations needed to prove a statement.

- **Privacy-Enabled Public Blockchain Transactions**: Zcash, the first widespread application of zk-SNARKs, was developed by cryptographer and cypherpunk Zooko Wilcox, along with other researchers, and is a fork of bitcoin blockchain enabling privacy-protecting transactions. Zcash is based on the peer-reviewed Zerocash protocol, which was published at the IEEE Security and Privacy conference in 2014.

  Zcash offers three parameters of privacy protection — one can encrypt the sender's address, recipient's address, and amount — or a combination of these using "shielding." At the highest level of protection, a fully shielded Zcash transaction has all three parameters fully encrypted and private.

  According to the company, ZCash is fully compliant with anti-money laundering and counter-terrorist financing (AML/CFT) requirements set up by the Financial Action Task Force (FATF) and is designed to comply with the Travel Rule.[96]

  While there is a need for privacy-enabled public blockchain transactions, it is especially critical that this privacy infrastructure is built in a way that is compliant with regulations to ensure these do not become a conduit for breaching regulatory controls on transaction monitoring and recordkeeping.

- **Cryptographic Attestation of Personhood:** The web-performance and security company Cloudflare introduced "Cryptographic Attestation of Personhood" to enable browsers to authenticate "proof of humanness" to servers without divulging device or user identity details.

[95] Ibid.

[96] Zcash, "Zcash Regulatory & Compliance Brief," PDF, June 2020.

© 2023 Citigroup

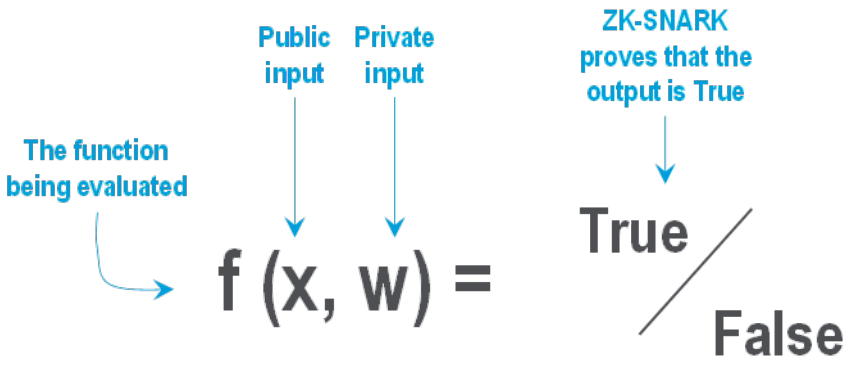
Cloudflare estimated that humanity spends about 500 human years each day on solving CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart), the challenge-response setup that forces us to click on buses, bicycles, and boats to prove that we are human, and not bots.[97] Although this is one slightly trivial first use-case, the concept of using zk-proofs for authentication extends wider than CAPTCHA, and Cloudflare has designed a zk-proof that enables browsers to authenticate users to servers without sending across identifying information. The solution built by Cloudflare is not based on zk-SNARKs (as these were deemed computationally expensive to prove[98]) but based on elliptic curve cryptography, with some modifications.

- **Proof of Membership:** The above example from Cloudflare is a specific use-case of attestation of personhood as implemented for hardware devices, but zk-SNARKS can be used for more general "proof of membership" use-cases.

  Vitalik Buterin, the founder of Ethereum, explains this elegantly in his blogpost, summarized below in non-technical terms:[99]

  Consider a simple function *f(x,w)* that evaluates to True or False depending on public and private inputs as illustrated in Figure 27. Barring private input *w*, which is a secret known only to the prover, the rest of the left-hand side of the equation — the function itself and public input *x* — are not secret. With a zk-SNARK, one can prove that one has a secret *w* that enables this function *f* to evaluate to True, and this can be verified by the verifier without knowing the secret *w*. In non-rigorous terms, the function only evaluates to true if there is a valid secret input, so the verifier can be assured that if the function returned True, there has to be a valid secret.

Figure 27. Illustration: What Does a Zk-SNARK Do?



Source: Vitalik Buterin, "Some Ways to Use Zk-SNARKS for Privacy," June 15, 2022.

[97] Thibault Meunier, "Humanity Wastes About 500 Years Per Day on Captchas. It's Time to End This Madness," The Cloudflare Blog, Cloudflare, May 13, 2021; Watson Ladd, "Introducing Zero-Knowledge Proofs for Private Web Attestations with Cross/Multi-Vendor Hardware", The Cloudflare Blog, Cloudflare, August 12, 2021.
[98] Proving a zk-proof is usually much more computationally demanding than verifying in this scenario. The browser is doing the proving to the server that is doing the verifying.
[99] Vitalik Buterin, "Some Ways to Use ZK-SNARKs for Privacy," June 15, 2022.

© 2023 Citigroup

In the case of a "proof of membership" use case, one wants to prove that an Ethereum wallet *w* is a part of a group of white-listed or verified wallets, listed in *x*. The verification function *f(x,w)* evaluates to True only if the user is able to demonstrate they own the private keys for wallet *w* and that wallet *w* is part of the list of white-listed wallets (i.e., the key works for the wallet and it is part of the white-list — together making the secret valid). Using these inputs, the prover runs the zk-SNARK proving algorithm, which generates the proof that evaluates to true, if and only if the above function evaluates to true.

- **Verification in Cloud Computing:** Zk-SNARKS are part of a wider universe of "verifiable computations," which is the concept of outsourcing computations with an assurance that the validity and correctness of the computations can be ascertained.

> In this setup, a single reliable PC can monitor the operation of a herd of supercomputers working with possibly extremely powerful but unreliable software and untested hardware.
>
> – LÁSZLÓ BABAI ET AL., "CHECKING COMPUTATIONS IN POLYLOGARITHMIC TIME," 1991[100]

The above claim, published in 1991, is highly relevant to today's cloud-centric world. While cloud computing lowered the setup infrastructure costs and made computational investment "elastic" (i.e., growing or shrinking with demand), it also brought with it challenges regarding the reliability, correctness, and integrity of the data stored as well as the computations undertaken by the remote cloud infrastructure.

One solution to the above problem, without making any trust assumptions on the third party making the computations, is to have the remote third-party return a cryptographic "proof" along with its results. The proof proves the computations were done correctly and can be verified without re-executing all the computations. Given all the developments in cryptography in the last decade and half, the time taken to verify the proof is orders of magnitude shorter than the time taken to run the computations.

- **Scaling Blockchains via Roll-Ups:** As Stanford professor and cryptographer Dan Boneh puts it on the Zero Knowledge Podcast with host Anna Rose:

  "So because a Layer 1 blockchain is so expensive, and, you know, not particularly a fast computer, it actually now makes a lot of sense to outsource computation to a GPU and have the GPU prove to the blockchain that what it did is correct. And that's literally the kind of the reason why zk-rollups and zk-bridges and all that have taken off."[101]

  This is the core concept behind different roll-ups — outsourcing computations — that are now scaling Ethereum, a slow and expensive computer.

[100] László Babai et al., "Checking Computations in Polylogarithmic Time," Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, January 1991.
[101] Dan Boneh, "Episode 256: New ZK Use Cases with Dan Boneh," *Zero Knowledge* podcast, November 30, 2022.

© 2023 Citigroup

Sharding has been adopted by Ethereum to scale its capacity

- **Ethereum Danksharding Scaling Solutions:** Apart from the use of zk-rollups for scaling Ethereum, polynomial commitment schemes —the core building blocks used in zk-proofs — are also used in Ethereum's new danksharding scaling solution. Sharding is the technique of horizontally splitting a database to increase its data handling. It is one of the techniques adopted by Ethereum to scale its capacity — by splitting the Ethereum ledgers into chunks or "shards."

  Danksharding is a new sharding design introduced in Ethereum that builds in Ethereum's rollup-centric roadmap to scaling. Instead of increasing space for transactions themselves on the Ethereum layer 1, danksharding provides more space for "blobs" (Binary Large Objects) of data, without the Ethereum protocol attempting to interpret what these blobs of data mean. These data blobs are then used by roll-ups that do the computations on their own chains and submit proofs on the Ethereum layer 1. This essentially changes Ethereum from a single-threaded, slow computer to a multi-threaded, faster one.

Trusted Setups in Zk-SNARKS

Some examples of zero-knowledge construction need trusted setups, i.e., their initial parameters need an element of trust to set up the system. But once set up, the system does not need any trust to operate. This small window of trust needed at inception has led to many interesting "ceremonies," or one-time procedures, to orchestrate the setup in a trust-minimization way, including the esoteric-sounding "Powers of Tau" ceremony.

In this ceremony, participating entities generate Powers of Tau, where tau is a random secret value that the entities destroy after the initial phase is created. It is critical that once the trusted setup is finished, the secret data that led to its creation needs to be destroyed to ensure there is no iota of doubt about a potential backdoor on the protocol. This is done in interesting ceremonies where people break the computers that generated these passphrases or destroy them in other ways.

Of Secret Ceremonies, Radioactive Waste, and Propane Torches

The first public instance of a trusted setup ceremony was the one that birthed the privacy-enabling cryptocurrency Zcash.

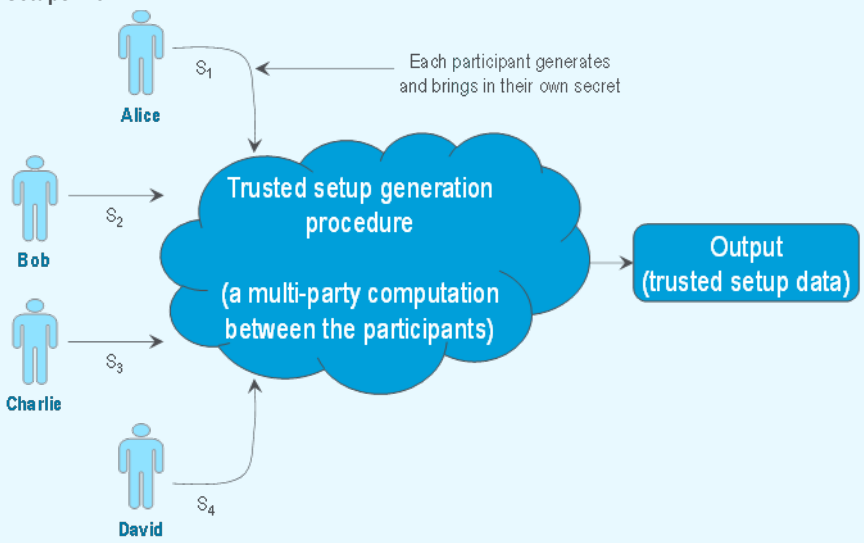
In a riveting article titled "The Crazy Security Behind the Birth of Zcash, the Inside Story," technology writer Morgen Peck covers the secret birthing ceremony of the cryptocurrency, in what she calls a "cloak-and-dagger cocoon of digital secrecy."

The project, a fork of the Bitcoin blockchain, introduces a layer of encryption enabling the masking of the identity of the sender and the receiver and the value of the transaction. Prior to launching the zk-SNARK setup needed for the protocol to run, developers used certain highly secretive private keys, one by one in a multi-party computation setup (with each key being known to only one developer) to make the mathematical parameters for the zk-SNARK circuit work. It was extremely critical that these original secret keys were destroyed once created. If there was even an ounce of doubt that those keys could be accessed by any individual after the launch of the protocol, a potential backdoor could exist, completely invalidating the entire proposition of the currency (i.e., the key holder can mint themselves incremental supply of the coin at their will).

In the case of Zcash, the generation of keys was split between five developers, each in a different part of the world, using an air-gapped computer (not connected to the internet) that was a last-minute purchase from a random computer store to prevent hackers pre-installing the devices with tracking software). The computer was destroyed right after it had fulfilled its role in key generation.

© 2023 Citigroup

Figure 28. How Do Trusted Setups Work?



Source: Vitalik Buterin, "How Do Trusted Setups Work?" March 14, 2022.

Morgen Peck explains it very well in her analogy below:[102]

"I'll hazard an analogy in order to explain more generally how this works: Let's say you have a recipe, and you want to use it to make a single cake that is going to feed everyone in the world and that's the only cake that anyone is allowed to eat, ever. You have to have a recipe to bake the cake, but you also have to make sure no one can ever make it again. So, you split the recipe up into six parts and you design a baking process that allows each participant to add their ingredients and mix them into the batter without the others (or anyone else) seeing what they're up to. After pulling the cake out of the oven, you burn all the pieces of the recipe."

In this analogy, the recipe is the bad key, the cake is the zk-SNARK parameters, and the person hiding the ingredients and doing all of the mixing is a cryptographic algorithm.

Each of the five developers, who were called "station operators" as they each operated their station on how to generate a piece of the parameters needed, then destroyed their secret keys. One of the ceremony participants boxed his laptop within aluminum foil lined cardboard and did his computations when driving across Canada and burned his computer with a propane torch when he was done.

The follow-on 2018 Powers of Tau ceremony of Zcash (for an upgrade of the protocol) used nuclear waste from Chernobyl to generate random numbers for the secret key generation. A portion of the 2018 event also took place in a private plane flying at 3,000 feet over Illinois and Wisconsin to ensure privacy.[103]

[102] Morgen E. Peck, "The Crazy Security Behind the Birth of Zcash, the Inside Story," IEEE Spectrum, December 2, 2016.
[103] Nikhilesh De, "Latest Zcash Ceremony Used Chernobyl Waste," CoinDesk, January 28, 2018.

© 2023 Citigroup

A Conversation With Prof. Silvio Micali on Zero-Knowledge Proofs and Scalability

Silvio Micali is a computer scientist, professor at the Massachusetts Institute of Technology (MIT) and the founder of Algorand, a proof-of-stake blockchain protocol. Micali's research at the MIT Computer Science and Artificial Intelligence Laboratory include cryptography, zero-knowledge technologies, pseudorandom generation, secure protocols, and economic mechanism designs.

One of the preeminent cryptographers of our time, Micali's transformative work on complexity theory led to him being the father of key core components of modern blockchain, including Zero-Knowledge Proofs, Verifiable Random Functions, and Probabilistic Encryption.

Micali is a recipient of the Turing Award in computer science, often referred to as the Nobel Prize of computing, in addition to numerous other accolades such as the Gödel Prize (in theoretical computer science) and the RSA prize (in cryptography).

Q: What are zero-knowledge proofs (ZKPs)?

Silvio: People want secure ways of interacting and transacting on the internet with people they don't know or trust. The world has transitioned from using encryption to digital signatures to secure protocols and now to an emerging technology known as zero-knowledge proofs (ZKPs).

ZKPs allow you to guarantee that the information is true without disclosing any of the information. ZKPs enable separation of knowledge of data from the proof that the knowledge exists. In other words, ZKPs enable authenticating the existence of facts (identity, asset weights, payment proofs, etc.) without disclosing the fact itself.

ZKPs can be leveraged to provide data authenticity and privacy in a variety of commercial and non-commercial applications.

Q: Why are ZKPs relevant for blockchain?

Silvio: Privacy is a fundamental right and a necessity for individuals, businesses, and corporations alike. Blockchain has the potential to be very useful to companies and financial institutions, but you don't want it to compromise on the privacy of users and their transactions.

Banks and financial institutions might want to use blockchain for trading, payments, and a variety of finance processes, leveraging the technology for the mid-office and back-office efficiencies it can bring. However, on-chain data is available to anyone and everyone. Anybody can see the private transactions between two clients of a bank.

ZKPs can mask this information and just confirm that the payment is made or received and the nodes on the blockchain will believe that information. No information such as payment amount, goods or services delivered, or payment terms will be disclosed publicly.

ZKPs can be thought of as a driver of mass adoption for enterprise, institutional blockchain.

Q: What excites you most about blockchain?

Silvio: Blockchain technology is a distributed ledger that satisfies three crucial properties. First, everybody can read the ledger. Second, everybody can write his or her own legitimate transactions on the ledger. And third, nobody can alter not only the content of the transaction in the ledger, but also the order of the transaction in the ledger.

These properties generate added trust and transparency that was previously unavailable. Communication of information and the entire network having a common knowledge of the transaction are two different things. Blockchain promotes common knowledge of all transactions and the network state across all nodes.

Blockchain is an unmediated transactional platform. I have nothing against mediators when they add value, but if the job of a mediator is to enable the very transaction that is being mediated, then we might be better off replacing that mediator with technology. It also enables tokenization and fractionalization of any assets — securities, commodities, currencies, and real estate, among others.

© 2023 Citigroup

Q: According to the "blockchain trilemma" a blockchain network cannot have enough of all three — security, scalability, and decentralization. How does Algorand's consensus mechanism get around the blockchain trilemma?

Silvio: Blockchain trilemma is where any distributed network can't have all three attributes at the same time — scalability, decentralization, and security. How do we solve it?

There are different technologies. For example, proof-of-work, which underlies Bitcoin, simply says to create the next page of a ledger, let's have a computational game. The first one in the world to solve a very complex cryptographic riddle, and present the solution, has the right to append the next page of a ledger.

That is a good solution, but there are problems. It needs thousands of super specialized computers to solve the cryptographic riddle to have even a chance to append a page of a ledger. When expenses go up to create a new page of ledgers, fewer and fewer people can afford these expenses and the network becomes very centralized.

In another technology, called delegated proof-of-stake, it's very simple. You create a group of say 10 people, and it's their business to append pages to the ledger on behalf of the users. By not involving many people as decision makers, you scale the network, but it doesn't solve for decentralization.

Algorand, on the other hand, can achieve all three attributes. The way we solved the trilemma is a little bit counterintuitive. We have 10 billion consensus tokens. Then you select 1,000 tokens. These 1,000 tokens belong to members of the network, and these members form a committee, which approves the next block.

The network is distributed as we have 10 billion tokens, and everybody having a token has a chance to participate. To summarize, the trilemma issue applies to most blockchains, but not to Algorand, as the consensus mechanism is structured like a cryptographic lottery — anyone with a token has a chance of being selected as a validator. Algorand also offers speed, low cost, scalability, and distribution.

Q: Can you describe different types of proof-of-stake mechanisms — e.g., pure proof-of-stake and delegated proof-of-stake?

Silvio: Proof-of-stake is not a single technology but a portfolio of technologies. Delegated proof-of-stake is like a club. If you are invited to the club, good for you. If you are not part of the club, bad for you, because only those invited into the club can decide every transaction in the distributed network.

In delegated proof-of-stake, the security of the entire economy depends on the honesty of a small delegate group within the economy. In Bitcoin, that group is the miners. In Algorand, anybody can participate. Technically, in Algorand, you can have hundreds of millions of people participating in consensus.

Another difference is that a pure proof-of-stake blockchain, which Algorand is based on, doesn't fork. A fork is a chain that splits away from the main chain and forms a separate chain of ledger, creating uncertainty for everyone involved. An unforkable blockchain like Algorand guarantees that all transactions are final and ensures asset ownership is not lost.

© 2023 Citigroup

A third key difference is that there is transaction finality in less than 3.7 seconds. The technical ability of supporting hundreds of millions of entities participating in consensus translates into censorship resistance. In Bitcoin or in delegated proof-of-stake blockchains, you can't propose a new block unless you have enormous computation capacity or are part of the club, respectively. In Algorand, even if you hold a very small stake, such as 1/10,000 of the total stake, and even if you participate in consensus with only a laptop, you have the mathematical guarantee of proposing a block, and to post transactions on the blockchain that others may otherwise censor, at least twice a day!

Q: What are your views on new developments that affects blockchain and Web3 security (e.g., post-quantum cryptography)?

Silvio: It is important that the chain is secure against quantum computers that do not yet exist, because whenever they become available, you don't want to hack the chain backwards. We are going to make our blockchain quantum secure.

In my view, something that is not capable of evolving over time is not going to last very long or remain relevant for very long. We must have a blockchain which incorporates the best and the latest technologies. To do this, you must be able to put capabilities in the blockchain similar to what Algorand has done from the very beginning.

We have embedded in the mechanism the ability to evolve in a consensual manner. Any time there is an upgrade of the protocol, the majority of the participants to consensus must agree, and then that upgrade is used from that point onwards. You want a mechanism that upgrades consensually.

© 2023 Citigroup

A Conversation With Zooko Wilcox on Application of zk-SNARKS

Zooko Wilcox is the Founder / CEO of Electric Coin Co., that launched privacy-focused cryptocurrency Zcash in 2016. Zooko is an original cypherpunk, long-standing technologist and entrepreneur. His work spans decentralized systems, cryptography, and information security. He has contributed to an array of projects, many of which champion privacy implementations, including DigiCash, Mojo Nation, ZRTP, "Zooko's Triangle," Tahoe-LAFS, BLAKE2, and SPHINCS, to name a few.

Zcash is the first widespread commercial application of zk-SNARKs. The cryptocurrency was built to empower economic freedom and was created from the original Bitcoin code base with several key improvements, namely privacy-preserving shielded addresses and a community development fund.

Q: Where are zk-proofs as a technology, today? What will drive their adoption?

Zooko: Zero-knowledge proofs are highly customized for each use case and they have not yet hit general-purpose technology adoption. We can think of this like an "application-specific integrated circuit" mode of semiconductor chips, where each integrated circuit is designed for a specific use case but is yet to hit general multipurpose use.

In a historical context, we can compare where zero-knowledge technology is today to the development of Public Key Infrastructure (PKI) cryptography in the 1990s. Prior to the launch of the early commercial-use browser, Netscape Navigator, PKI had very limited use cases, although it showed promising potential. With the launch of Netscape, public key cryptography found a ready mainstream use case as Netscape implemented SSL — a Secure Socket Layer protocol that underlies the core of internet security today — using RSA public key cryptography. Today, zero-knowledge is in the pre-Netscape era of adoption and is at the cusp of tooling development.

The state of zero-knowledge research and tooling has been advanced by the public blockchain and cryptocurrency ecosystem in their search for solutions for blockchain-scaling and identity solutions that preserve privacy. Nearly 80% of use cases are driven by scaling and 20% by identity. Tools being developed will enable application developers to build use cases leveraging zk-proofs without needing to understand the complex mathematics behind the technology, which will drive mainstream adoption.

Q: What is a good fit for zk-proofs in application?

Zooko: Whether to use zk-proofs or just encryption depends on whether there is a need to validate the encrypted data. If an entity X is going to post some encrypted data on the blockchain, and other third parties are not concerned whether this data needs to be examined for correctness or validity, then a zk-proof is not needed in this scenario — encryption will suffice. But if there is a requirement to provide some assurance about the encrypted data, this can be accomplished using zk-proofs.

In the case of Zcash, a privacy-protecting cryptocurrency that's a fork of the Bitcoin blockchain, the sender, receiver, transaction amount and reference fields are encrypted. But it does not suffice to only encrypt the data, as there needs to be a way for the validators to verify the encrypted data does not have a "double spend" situation (where the sender could send the same coins to two parties). Zk-proofs provide a way to provide confirmation that there's no double spend, without having to reveal the underlying unencrypted data to the verifiers.

© 2023 Citigroup

Blockchain Oracles

Oracles are a prerequisite for scaling blockchain

- Blockchains, by their design, can only access and work on data that is "on-chain." Oracles can be thought of as an application programming interface (API) that helps connect blockchains with the real world and bridge data between the two worlds.
- Oracles are a prerequisite for scaling blockchain as without access to real-world data, use cases across financial markets, insurance, and Web3 will be restricted only to the subset that lives fully on-chain.
- Currently, we find most work on Oracles being done in the decentralized finance (DeFi) space. However, we should start to see more Oracles being built out by regulated financial institutions for market and pricing data.

Oracles: A Prerequisite for Blockchain Use Cases

Blockchain Oracles act like a bridge connecting smart contracts on blockchain to real-time, off-chain data

Blockchains do not have the ability to connect to the outside world, hence they are unable to incorporate external information into their logic. This is where blockchain Oracles come in. Oracles help securely bring takes off-chain data sources and puts it on-chain, so it can then be used in smart contracts.

To put it simply, a blockchain Oracle is a third-party service that serves as a bridge between the blockchain ecosystem (on-chain) and external data sources (off-chain). They function like APIs but in the context of a blockchain.

Let us use an example to convey this concept better. Assume you want to buy a house and register the agreement on the blockchain but pay for it via traditional banking channels through a bank transfer or by bank cheque. A smart contract executed between the parties could help irreversibly execute the transaction based on set of coded conditions. However, since the payment is done off-chain (via traditional banking channels), a blockchain Oracle needs to bring this data on-chain to enable the smart contract to verify proof of successful payment, and then automatically transfer a tokenized ownership deed to the homebuyer.

Figure 29. Prominent Oracles in Select Blockchains

Blockchain	Oracles
Avalanche	API3, Chainlink, DIA, Pyth Network
BNB Chain	API3, Band Protocol, Chainlink, DIA, Flux, Pyth Network
Cardano	API3, Chainlink, Charlie3, Orcfax, PIGY Oracle
Cosmos	Band Protocol
Ethereum	Band Protocol, Chainlink, Flux, iExec RLC, Nest Protocol, Orai, Pyth Network, UMA
Polygon	API3, Chainlink, DIA, Flux, Pyth Network, UMA
Solana	Chainlink, DIA, Gravity, Pyth Network, Switchboard
Terra	Chainlink
Tron	Bridge Oracle, Wink

Source: Alchemy, CoinCentral, LogRocket, Citi GPS

© 2023 Citigroup

How Does a Blockchain Oracle Work?

Oracles help bridge the information gap between on-chain and off-chain data by creating a hybrid smart contract. A hybrid smart contract is comprised of a combination of on-chain contract code and off-chain Oracle node.

In a typical transaction, the on-chain contract code of the Oracle receives data requests from other smart contracts and passes it on to the off-chain Oracle node. The Oracle node is then able to source and verify external information by querying external databases using APIs in order to collect the requested data. This collected data is then transmitted back to the smart contract's storage using the on-chain contract code.[104]

Types of Blockchain Oracles

- **Software and Hardware Oracles:** Software Oracles are most commonly used for price feeds on decentralized exchanges (DEXs). They analyze and deliver digital data such as exchange rates or prices from websites and other databases. For example, a smart contract executed to buy 100 equity shares of Company A, should its price hit a certain target. In this instance, an Oracle would provide accurate and immutable data on the stock price. Oracles are not restricted to just price feeds, but also other data such as weather, geographic, and economic information.

  Hardware Oracles, on the other hand, deliver data from the physical world using information from devices such as temperature sensors, video cameras, motion sensors, smart tags, Radio Frequency Identifications (RFIDs), and other Internet-of-Things (IoT) devices. For example, a hurricane insurance policy linked to a smart contract in conjunction with a hardware Oracle can help monitor external wind speed and notify the insurer should the wind speed cross a certain threshold.

- **Inbound and Outbound Oracles:** The words "Inbound" and "Outbound" in the case of an Oracle refer to the flow of real-world information and data. Inbound Oracles bring real-world information into the blockchain and are among the most commonly recognized types of Oracles today. One example is fetching information on market prices of equities or stocks and providing it to the smart contract for decentralized finance (DeFi) transactions. Inbound Oracles can also be used to provide weather data to a smart contract for automatic insurance claim settlement or providing sports data to settle prediction markets.

  Outbound Oracles take information/instructions from the blockchain to an external source to execute a certain action. For example, a smart contract programmed to unlock an IoT-enabled smart lock of a warehouse following receipt of payment from a particular crypto wallet address.

- **Centralized and Decentralized Oracles:** Centralized Oracles are operated by a single entity, responsible for running the Oracle and being the sole provider of data for the smart contract. Users of a centralized Oracle have to implicitly trust the entity to provide unbiased data sources. While centralized Oracles can be efficient, they are also prone to a single point of failure should they get hacked, manipulated, or shut down.

[104] Ethereum, "Oracles", Accessed March 24, 2023.

© 2023 Citigroup

Decentralized Oracles aim to overcome the limitations of centralized Oracles by relying on multiple Oracle nodes and external data sources. This leads to increased data credibility. They also promise to eliminate the risk of a single point of failure by aggregating multiple data points to arrive at a single point of truth. However, decentralized Oracles can take a relatively longer time to aggregate data from multiple sources, when compared to centralized Oracles.

By offering smart contracts off-chain execution capabilities, Oracles expand the use cases for blockchain technology

- **Compute-Enabled Oracles:** These Oracles help perform complicated computations securely off-chain and relay it to smart contracts on-chain. Computations handled by these Oracles may often be impractical to perform on-chain due to a variety of reasons, including block constraints or the sheer cost of computation.

  Oracle computations help extend the capability of smart contracts by increasing scalability and cost-efficiency. Additionally, they also offer access to features such as verifiable randomness that assigns randomized characteristics to NFTs, off-chain aggregation, and transaction automation. Compute-enabled Oracles can also be used for layer 2 scaling solutions.

- **Human Oracles:** These refer to instances where humans manually provide data feeds to a blockchain Oracle. Human Oracles are often used with complex data that cannot be collected automatically to feed into the blockchain or that require in-depth research. To maintain authenticity of the information being relayed to the smart contract, human beings are involved to verify their identity cryptographically.

- **Contract-Specific Oracles:** These Oracles are often designed from scratch to for use by a single smart contract. However, they are impractical for multiple smart contracts, as multiple Oracles would need to be deployed.

Importance of Oracles in Blockchain and Web3 Applications

Smart contracts running on Ethereum or other blockchains cannot ordinarily access data stored outside the blockchain (i.e., off-chain). Oracles solve this problem by offering off-chain execution capabilities to smart contracts, thus expanding the use-cases for blockchain technology. We highlight some prominent Oracle use-cases below.

> You need some kind of Oracle to tell you, 'Did it actually rain in this particular area?' If you want to have assets that mirror other financial assets, you need an Oracle. If you want a prediction market, you need an Oracle.
>
> – VITALIK BUTERIN, CO-FOUNDER OF ETHEREUM[105]

- **Decentralized Finance (DeFi):** The DeFi industry, whether they are lending markets, liquidity aggregators, derivative protocols, or algorithmic stablecoins, relies extensively on Oracles.

[105] Elizabeth Licorish, "Ethereum Co-Founder Vitalik Buterin on Why Smart Contracts Need Oracles," Chainlink Today, June 7, 2021.

© 2023 Citigroup

Developers rely on Oracles to bring off-chain data into their decentralized applications (dApps). The most widely recognized use case of Oracles are price feeds used in DeFi transactions. Oracles can also be used to provide market prices for collateral assets, enabling platforms to determine how much they can borrow from the system and when to trigger liquidations.

As more traditional assets come on-chain (e.g., tokenized bonds, stocks, real world assets), proof of reserves is likely to become a necessity, with Oracles expected to play an even larger role with external financial market data.

- **NFTs, Gaming, and Web3:** Blockchain Oracles can support dynamic NFTs which can change in appearance or distribution based on external information such as time of the day, weather conditions, etc.

  Additionally, compute-enabled Oracles are also capable of generating a verifiable randomness function (VRF) that assigns randomized traits to NFTs so the rarity of NFTs is randomly assigned when they are minted. VRF can also provide fair random numbers for on-chain gaming dApps and NFTs.

- **Digital Identity:** Oracles can be an effective solution to attest information about a user's identity, certificates, or other documents on-chain that were originally stored or generated off-chain. Blockchain-based identity solutions can also help users monetize their own data, track its usage, and share it easily in a secure manner.

- **Supply Chain and Trade Finance:** Blockchain use in supply chains can help increase trust and transparency. Oracles play a crucial role, as smart contracts on blockchains need to interact with trusted and verified real-world data such as GPS data about shipments, data from supply chain ERP (Enterprise Resource Planning) systems, or customs data about shipped goods.

- **Smart Legal Contracts:** Smart legal contracts (SLCs) can interact with external data sources using Oracles and import data from web services or APIs. This allows the SLC to use external data as part of its decision tree and allows for the recording of the conditions under which the SLC was executed.

- **Insurance Products:** Oracles are relevant in insurance smart contracts for gathering external data, which can be used to confirm that conditions for payment have been met, allowing the insurance company to payout claims automatically, in-line with the pre-defined logic of the smart contract.

  For example, Oracles can gather external information on flight delays, which can then be used to validate automatic claim payments for passengers.

- **Automatic Trade Execution:** As mentioned, Oracles are highly effective in keeping track of changes in stock prices, foreign exchange (FX) markets, or cryptocurrencies and can help execute buy/sell orders in response to external changes. This makes them relevant for managing derivatives, automatic trade execution orders, and other risk management techniques.

As use of blockchain technology continues to grow, we expect to see more sophisticated and secure Oracle solutions. Integration of blockchain with other emerging technology such as artificial intelligence (AI) and smart IoT devices are likely to drive further growth of Oracles, especially in process automation.

© 2023 Citigroup

Potential Risks and Challenges

Oracles are a vital link in the blockchain ecosystem — however, they are not risk free

Oracles are a vital link in the blockchain ecosystem as they provide the underlying data used by self-executing smart contracts. However, Oracles are also prone to several risks, some of which we discuss below.

- **The Oracle Problem:** This refers to the conflict between security, authenticity, and trust in Oracles, which are developed by third parties. Since Oracles provide external data essential for the execution of a smart contract, they are in a position to retain a significant degree of influence over the smart contracts. This potentially removes the trustless nature of smart contracts as part of a decentralized network.

  Further, Oracles are unable to provide trustless verification when dealing with real-world assets on the blockchain. For example, in the case of a transfer of ownership of a house on the blockchain, smart contracts need to rely on additional third parties to verify if the former owner has indeed vacated the house. The need to rely on additional third parties likely further removes the killer feature of trustless applications.

- **Security Mechanism:** Since Oracles act as a bridge connecting external information with on-chain data, they are not part of the main blockchain consensus. This means they are also not part of the security mechanism provided by public blockchains. As a result, a compromised Oracle would likely mean the smart contract relying on it is also compromised.

- **Man-in-the-Middle Attacks:** Oracles are also prone to man-in-the-middle attacks, whereby malicious actors gain access to the data flow between the Oracle and the smart contract, with the intent to modify or falsify the data.

  Man-in-the-middle attacks could also result in interruptions or delays and may even prevent the smart contracts from executing code.

© 2023 Citigroup

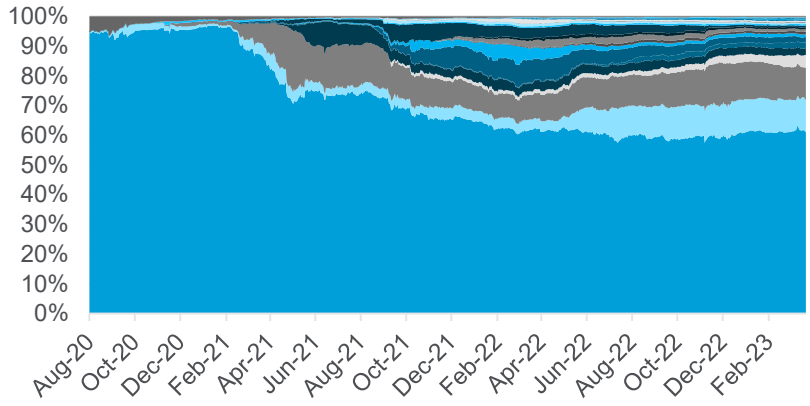
Secure Bridges

- The future is inherently multi-chain, as different blockchains are being built and optimized for different use-cases with varying design choices. This has led to the need for interoperability between chains and the emergence of blockchain bridges as a potential solution.
- Below, we lay out the various design choices in the blockchain ecosystem with respect to bridges and the trade-offs therein. Bridges could potentially be the weak point of a multi-chain world and need careful consideration.
- Bridges fit within a wider requirement for more generic messaging, smart contract calls, and other types of cross-chain communication. This is especially relevant in the context of driving mainstream financial services adoption, where messages and data need to be transferred between different institutions or blockchain ecosystems.

Need for Interoperability in a Multi-Chain World

Since Bitcoin was launched in January 2009, there has been a sharp rise in the number of blockchains, ranging from generalized smart contract platforms such as Ethereum to application-specific chains. According to data from Coingecko, there are currently hundreds of blockchains in existence. Value is still concentrated on a few chains, but diversity has increased in recent years.

Figure 30. Total Value Locked per Blockchain



Source: DeFiLlama, Citi GPS

The future of blockchain is inherently multi-chain, as varying use-cases have different design needs

The blockchain industry is still young, but in our view, it is unlikely that one blockchain will act as the sole settlement layer in the future. The future is inherently multi-chain, as varying use cases have very different design needs (e.g., consensus mechanism, security, monolithic versus modular, throughput). However, building blockchains in isolation optimized for specific stated purposes may result in incompatibility, which in turn increases the risk of fragmentation. To ensure that the value will not be stuck on isolated islands, blockchains need to be able to talk to each other. Enter bridges.

© 2023 Citigroup

How Do Bridges Work?

Blockchain bridges refer to protocols or intermediaries that enable users to move assets from one blockchain to another

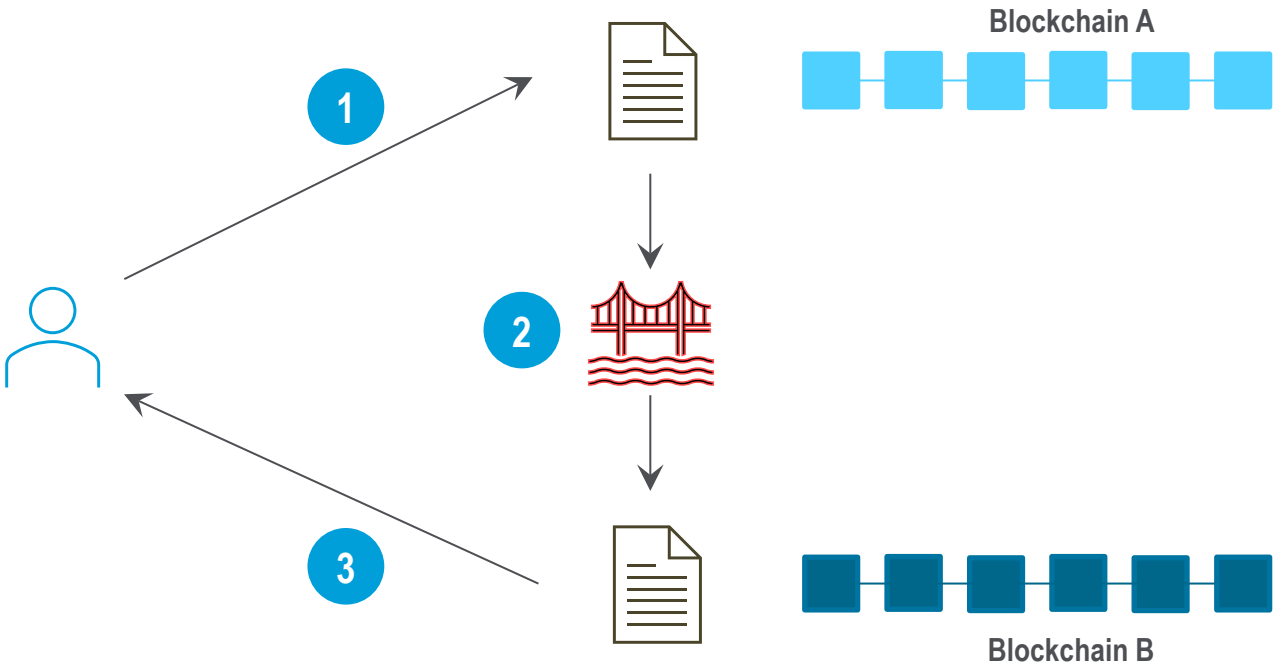
Blockchain bridges have emerged as a potential solution to the rising need for interoperability. Bridges refer to protocols or intermediaries that enable users to move assets from one blockchain to another. One popular model is the lock-and-mint model.

In the lock-and-mint model, a user has a token on Blockchain A but wants to use it on Blockchain B. A bridge can help make this possible (illustrated in Figure 31).

- **Step 1:** The user sends tokens from Blockchain A to a smart contract controlled by the bridge that locks the tokens.
- **Step 2:** The bridge has a smart contract deployed on Blockchain B, which will mint an equivalent number of tokens on Blockchain B. This is often a "wrapped" version of the original token.
- **Step 3:** The tokens will then be sent to the address of the user. The user can now use the tokens on Blockchain B (e.g., lend it, post as collateral).

If a user wants their tokens back on Blockchain A, they need to send the wrapped tokens to the bridge-controlled smart contract that will burn the wrapped tokens on Blockchain B, unlock tokens on Blockchain A and send them back to the user.

Figure 31. Lock-and-Mint Bridges



Source: Citi GPS

Figure 31 is a simplified example and there are different ways a bridge operates. In many cases, the asset does not move from one blockchain to another. It is locked and burned on one chain, while new tokens are simultaneously unlocked and minted on the other chain. Mechanisms like this allow users to utilize a "wrapped" version of Bitcoin (BTC) on the Ethereum blockchain.

© 2023 Citigroup

There are other variations possible, such as the deposit and withdraw model. In this case, a bridge is managing a pool with tokens on each chain. Here the user deposits tokens in the pool on the source chain, and the bridge will then send the equivalent number of tokens from the liquidity pool to the destination chain at the user address. The advantage is that the user receives the native token, not a wrapped version. It thus does not have to rely on the security of the bridge anymore once the transaction is finished. Wrapped Bitcoin (WBTC) is currently the largest bridge, with nearly $3.5 billion in total value locked, based on data from DeFiLlama.[106]

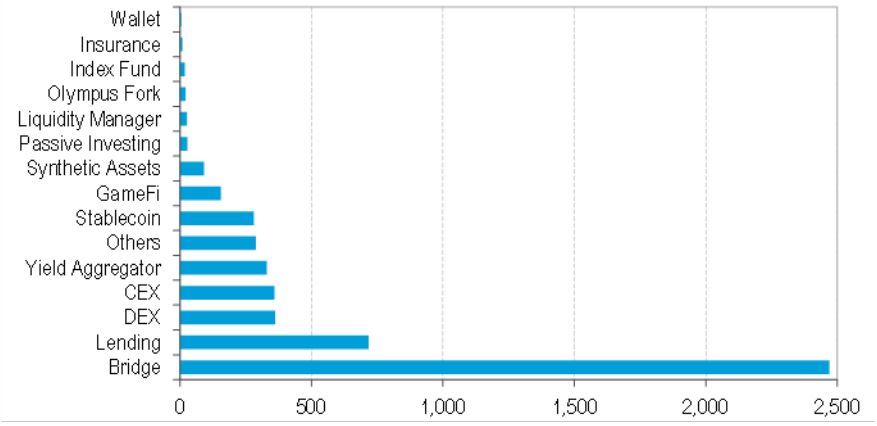
A problem with each bridge launching their own version of wrapped tokens is that they are not fungible. As a result, liquidity gets fragmented. For example, WBTC is not the only wrapped version of BTC; several others, such as hBTC, tBTC and iBTC, also exist. To solve this, LayerZero launched the Omnichain Fungible Token (OFT), a new token standard that aims to overcome this problem.

Bridge Exploits

The popularity of bridges has led to a number of exploits, which were by far the largest category of stolen funds, amounting to nearly $2.5 billion in 2022

Like all nascent technologies, blockchains are prone to vulnerabilities and so are blockchain bridges. The popularity of bridges has also led to a number of exploits, which by far were the largest category of stolen funds, amounting to nearly $2.5 billion in 2022 (Figure 32).

Figure 32. Exploits by Type, $ millions



Source: Token Terminal, Citi GPS

The largest exploit occurred with Ronin, a bridge built for the game *Axie Infinity*, where more than $600 million were stolen.[107] Likewise, PolyNetwork was also exploited for over $600 million, followed by BSC Bridge.

In a multi-chain world, interoperability protocols are a key piece of the infrastructure. Any weakness here can be traced to core design choices of how assets are bridged between networks.

[106] Data from DeFiLlama as of March 8, 2023.
[107] REKT.News, "Ronin Network – REKT," March 29, 2022.

© 2023 Citigroup

Moving Beyond Asset Bridges

Most bridge solutions were initially focused on moving tokens across blockchains. However, the long-term potential of interoperable blockchains goes beyond this functionality.

Besides moving tokens across blockchains, blockchain bridges' use cases include DeFi lending and NFTs…

Potential use cases include DeFi lending and borrowing in a chain-agnostic way, where the loan and collateral sit on different blockchains, as well as decentralized exchanges that pool liquidity from different chains. Other examples include NFTs that would allow users to access their utility, but from on another chain or a governance mechanism that allows users to vote cross-chain.

These use cases require solutions that allow for more generic messaging, smart contract calls, and other types of cross-chain communication. In other words, general cross-chain message solutions are needed. These protocols allow any arbitrary data to be sent across blockchains, not just tokens. Several projects such as Connext, Hop, and LayerZero are working on generic interoperability protocols.

…and they also play a crucial role in driving blockchain adoption of regulated financial institutions

This becomes especially important in the context of driving blockchain adoption among regulated financial institutions. Different consortium initiatives or bank-led blockchains would result in an ecosystem where messaging, data, and asset-transfer between blockchains are critical to establish interoperability to achieving scale on use-cases straddling different institutions. This goes hand-in-hand with standardization requirements as well. ISO 20022 standards for SWIFT messages have set an open global standard for financial information. It is critical that inter-blockchain messaging and bridging also evolves to open standards that fit the needs of the regulated financial industry.

Different Types of Interoperability Protocols

Three broad types of interoperability protocols exist based on the type of verifier

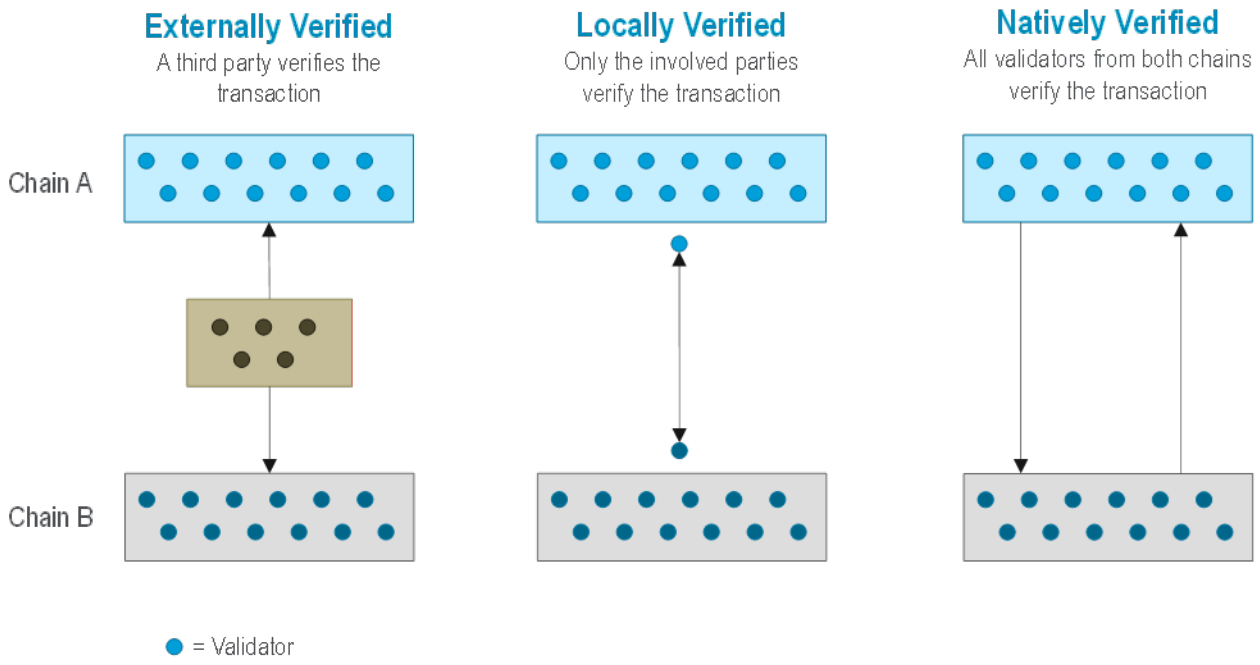
While bridges and cross-chain protocols broadly do the same thing — i.e., enable communication between blockchains — there are several ways of achieving this, and they cannot be all be put in one bucket.

However, there is no perfect design, and each choice poses some trade-offs. Looking at the different types of interoperability protocols, we believe it all boils down to the verifier, i.e., who is verifying the data that someone is trying to send across chains? In our view, there are three types of verifiers:

- **Externally Verified:** An external party verifies transactions between blockchains. These validators do not belong to either of the two blockchains but are part of the bridge. Users are required to trust the new set of validators instead of the validators of the underlying blockchains.
- **Locally Verified:** Only parties involved in the transaction will verify the message versus all validators of each chain.
- **Natively Verified:** All validators of the two blockchains verify the message. This is typically done by running a light client node of both chains.

© 2023 Citigroup

Figure 33. Three Types of Verifiers



Source: Connext, Citi GPS

Each of these types pose certain advantages and disadvantages. Before expanding further on this, we look at the "interoperability trilemma," as formulated by Arjun Bhuptani, the founder of Connext.[108]

The Interoperability Trilemma

Interoperability protocols can fully satisfy only two of three properties simultaneously — they can be trustless, generalizable, or extensible

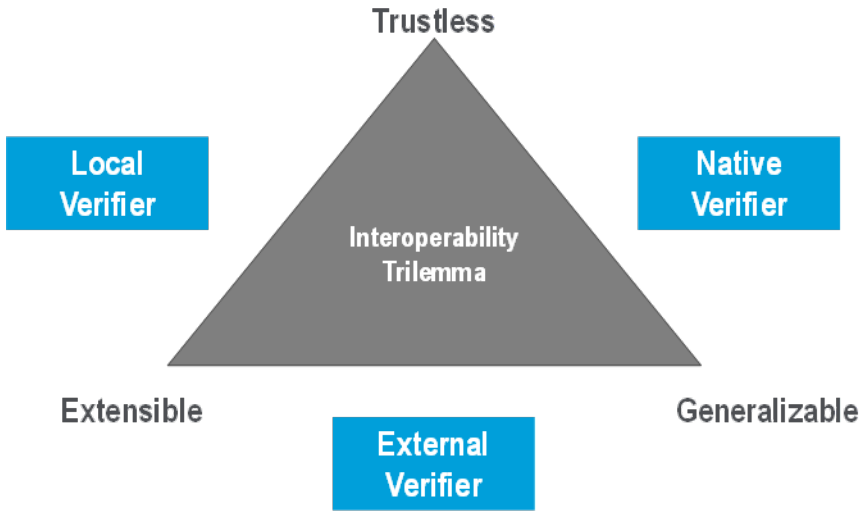
The interoperability trilemma states that interoperability protocols can only fully satisfy two of three of the following properties simultaneously. They can be:

- **Trustless:** A trustless protocol does not introduce additional security assumptions. In other words, it inherits the security from the underlying blockchains. Users do not have to rely on a third party to execute transactions. In general, the more trust-minimized, the more secure a bridge is.
- **Generalizable:** The bridge cannot only transfer assets between chains but can communicate any kind of arbitrary data.
- **Extensible:** It is very easy to extend the bridge to other blockchains.

[108] Arjun Bhuptani, "The Interoperability Trilemma," Connext Blog, October 1, 2021.

© 2023 Citigroup

Figure 34. Interoperability Trilemma and Different Verification Models



Source: Connext, Citi GPS

In reality, trustlessness is a spectrum. Externally verified bridges are trusted solutions, since they rely on external validators. Natively verified bridge solutions are more trustless since the trust remains on the blockchains associated with the cross-chain transaction.

Each of the verification models depicted in Figure 34 (external, local, native) satisfies two of the three properties of the trilemma.

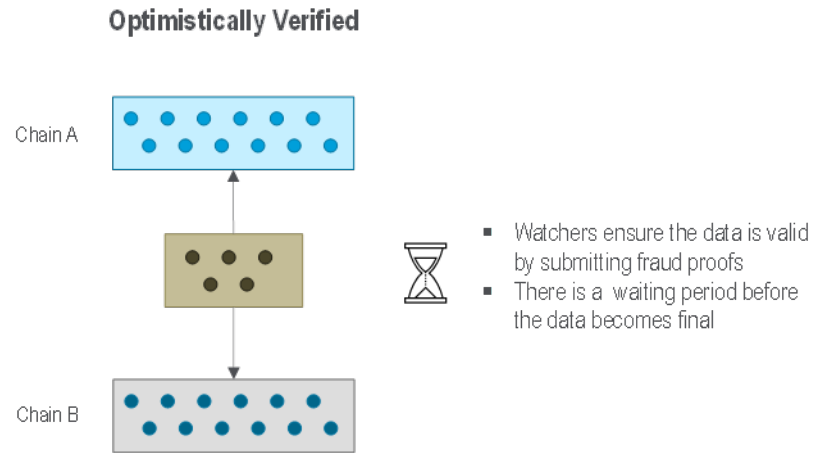
- **Externally Verified Protocols:** These allow for general cross-chain messaging and can be relatively easy be expanded. The downside is that users need to fully trust the external verifiers. Despite the tendency of lower security, this is the most popular type of bridge, also because they are typically cheaper and are easier to deploy. Examples: Multichain.
- **Locally Verified:** These are relatively trustless and are easy to extend to other blockchains. The disadvantage is that these systems typically don't support generalized data messaging. Examples: Hop, Connext V1.
- **Natively Verified:** These are the most trustless type and allow for generalized cross-chain messaging. On the other hand, these types are difficult to extend due to the heterogeneity of the blockchain designs. Examples: IBC, Polkadot.

There are some protocols that aim to solve the trilemma through optimistic bridges. Optimistic bridges use fraud proofs to send data across blockchains, which is similar to how optimistic rollups aim to solve the blockchain scalability trilemma.

In such a framework, users can send any kind of data across chains, but it is not immediately finalized. Instead, there is a time window where "watchers" can submit fraud proofs if they observe fraudulent data. If no such proof is submitted within the time window, data sent to the destination chain can be considered finalized. It is worth noting, however, that optimistic bridges introduce a new trade-off, namely: latency.

© 2023 Citigroup

Figure 35. Optimistic Bridges



Source: Connext, Citi GPS

Looking Ahead

While the interoperability landscape continues to evolve with new technology, we expect natively verified protocols to dominate, as they are more trustless

We believe interoperability protocols could become an increasingly important piece in the crypto infrastructure. It is likely that natively verified protocols will dominate, as they are more trustless. That said, it remains to be seen how the interoperability landscape will evolve. Some exciting areas include:

- Applying zero-knowledge technology to interoperability is an area being explored that could allow interoperability protocols to be truly trustless.
- Applications may apply across chains through cross-chain apps. Currently, applications are mostly multi-chain (deployed on multiple blockchains), but not cross-chain (i.e., they are not really composable).
- Bridges could be modular, similar to many blockchains that have become modular.

© 2023 Citigroup

[D.] Legal Enablers

Smart Legal Contracts

We enter into multiple contractual agreements on a daily basis without even realizing, such as when buying a cup of coffee, taking public transport, or purchasing a favorite item online. Although invisible, contracts form a major part of our day to day lives. They are ubiquitous.

In other activities, both in our personal and business lives, they appear in a much more visible way. Think about the last time you made an investment — perhaps you bought some shares or crypto or bought a home — or perhaps you got a new job or signed an agreement with a supplier. Putting it into context, 60%-80% of business transactions are governed by contracts.[109]

When you reflect on contracts, they are often associated with long negotiation processes to agree on the clauses and contents, multiple reviews and re-drafting of different versions until finally an agreement is reached, which is usually lengthy and often written in complex legalistic language that is difficult to understand. While law firms and enterprises use technology tools that greatly help the contract creation process, the end result is a written document, often in the form of a PDF file, that requires following through exactly as described.

Contracts are ubiquitous; they govern 60%-80% of business transactions

The lengthy completion and execution process of contracts means they are ripe for disruption

The painful process behind contract creation, involving lengthy text and complex language, means that sometimes contracts are not read at all and just signed (i.e., when was the last time you read the terms of service when you downloaded an app?). Yet when something goes wrong, it comes down to the details of the contract: what was agreed, what was the intention of the contracting parties, and what was the contract governance. Make a mistake and not only will it cost you, but you may be missing out on a massive opportunity. Poor contract management alone is estimated to cost companies 9% of their bottom line, according to World Commerce & Contracting.[110] In a study on outsourcing contracts, KPMG writes that most organizations are leaving significant value on the table and missing out on 40% of the identified potential of the contract because of poor contract management.[111]

So, contracts are everywhere, whether we like it or not. Each of them creates a legal relationship between two (or more) parties but leaves it to those parties to figure out for themselves how they manage it. Therefore, we should pay attention to how we fulfill contracts, as they are relevant both in a business context and in our personal lives. Contracts have been ripe for disruption for quite some time and developments in technology have taken contracts to the next level promising automation speed and security.

[109] Based on an infographic by Selectica, appearing in Cotrill Research, "Contract Manager Software by the Numbers," September 6, 2013.
[110] World Commerce & Contracting, "Poor Contract Management Continues to Costs Companies 9% of Their Bottom Line," April 29, 2020.
[111] KPMG, *A Clearer View From the Top: Nordic Shared Services and Outsourcing Pulse Survey 2019*, 2019.

© 2023 Citigroup

What do contracts 2.0, or smart legal contracts (SLCs), bring to the table? And what, if anything, do they have to do with blockchain? According to Aaron Powers, Co-founder and CEO of Hunit, they will provide a whole new set of rails for global commerce and finance to run on.

We put SLCs under the microscope in this chapter and dive deep into their anatomy. We learn that blockchain has certain benefits compared to conventional web platforms, and as such, would be the most favorable technology underpinning SLCs. These benefits include: the independence of decentralized ledgers, which fits well with the nature of legal agreements; the enhanced levels of security due to the use of cryptography and hashing techniques; the provision of a single source of truth through their consensus mechanism; and being tamper-proof.

SLCs are not widely adopted yet, but trillions of SLCs could be entered annually

Although such contracts are not yet widely adopted, we anticipate their uptake will accelerate as work has already started on analyzing and removing regulatory barriers to innovation. The UK is leading the way in this area, as the UK Law Commission completed their advice to the UK government in November 2021 confirming SLCs can be accommodated in current legal frameworks. There are other favorable regulatory developments on the horizon, particularly with emerging rules around trade digitization, paving the way for SLCs such as the Electronic Trade Documents Bill. This bill was only introduced in October 2022 and at the time of writing is with the House of Lords in the report stage. Completion is likely a few years away, and we do not have a timeline on implementation.

There are multiple use cases ranging from property to service-level agreements. However, we believe that given the nature of these contracts — they are based on conditional logic (i.e., if X happens then Y follows) — they will be suited for more basic agreements. With respect to value, while no specific SLC figures exist, Sir Geoffrey Vos, a senior judge in England on civil matters, alluded to the possibility that "trillions" may be used annually.[112]

> "I would expect English law and UK dispute resolution to prove a popular foundation for the trillions of smart legal contracts that we may then expect to be entered into annually."
>
> – SIR GEOFFREY VOS, MAY 6, 2019[113]

Origin of Smart Legal Contracts

Nick Szabo: A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on the other promises

The concept of smart contracts is not new — it goes back three decades. It was coined by Nick Szabo, an American computer scientist, in an article he wrote back in 1994 and expanded on in 1996.[114]

[112] Trustnodes, "Trillions of Smart Legal Contracts May Be Expect Says Senior Judge," May 6, 2019.
[113] Ibid.
[114] Nick Szabo, "Smart Contracts," 1994; Nick Szabo, "Smart Contracts: Building Blocks for Digital Markets," 1996.

© 2023 Citigroup

In the latter, Szabo uses the following definition: "A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on the other promises."[115] His definition gives us a good idea of the main smart contract ingredients: namely, a set of promises, a digital format, and protocols.

Going back in time and thinking about where the world was in 1994-96 from a technology perspective, smart contract technology was not at the forefront of what was being developed: 1994 was the year of the Web with the first International World Wide Web conference held at CERN in May and 1996 was the year of the DVD.[116] Smart contracts entered the spotlight with Ethereum as a key building block of decentralized applications. According to the Ethereum organization, *"A 'smart contract' is simply a program that runs on the Ethereum blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain*." The organization further explains smart contracts as being "computer programs stored on the blockchain that allow converting traditional contracts into digital parallels."[117]

Smart Contracts vs. Smart Legal Contracts

What do smart contracts look like, and are they synonymous with SLCs? Let us take a closer look at both. From a visual perspective, smart contracts look like a string of code. Below is an example of a smart contract written in Solidity language.

[115] Nick Szabo, "Smart Contracts: Building Blocks for Digital Markets," 1996.
[116] CERN, "A Short History of the Web," Accessed March 29, 2023.
[117] Ethereum Organization, Introduction to Smart Contracts

© 2023 Citigroup

Figure 36. An Example of a Smart Contract Written in Solidity

Source: Gustavo Ansaldi Oliva, Ahmed E. Hussain, and Zhen Ming (Jack) Jiang, "An Exploratory Study of Smart Contracts in the Ethereum Blockchain Platform," Empirical Software Engineering, Vol. 25, 1864-1904, 2020.

However, while the terms are often used inaccurately and interchangeably, smart contracts and SLCs are not the same thing. There is no universally agreed-upon definition, and the terminology is evolving. For the purposes of our report, we draw a distinction: SLCs are a type of smart contract — a subset of smart contracts — but with different characteristics than smart contracts.

- SLCs may or may not use blockchain — in contrast to smart contracts, which use blockchain. We discuss blockchain below.
- SLCs are intended (in form and structure) to create legally binding agreements that are compliant with the legal and regulatory requirements of their intended jurisdiction. Legal enforceability is rarely a consideration in smart contracts.

© 2023 Citigroup

The UK Law Commission specifically defines smart legal contracts as "a legally binding contract in which some or all of the contractual obligations are defined in and/or performed automatically by a computer program"

As described by the UK Law Commission, smart contracts can be used to define and perform the obligations of a legally binding contract. The Commission specifically defines smart legal contracts as "a legally binding contract in which some or all of the contractual obligations are defined in and/ or performed automatically by a computer program."[118]

- Due to smart contracts' lack of legal enforceability, the syntax of the code used in a smart contract is the subject of agreement between two parties — they do not have legal enforcement as a fallback. In contrast, SLCs include agreement upon both the intent of the parties and how automation will be used in the fulfillment of that intent. This allows for the involvement of the court system in the event of dispute, mis-execution, or malfunctioning computer code.
- In contrast to smart contracts, smart legal contracts are more dynamic to changing circumstances — to achieve legal compliance, they must include terms that allow them to be paused, modified, or rectified.
- While both smart contracts and SLCs can connect to and use outside data sources (referred to as Oracles when used for smart contracts), the legal enforceability of SLCs enhances their ability to use human assistance in their self-execution. Roles like auditors, inspectors, or agents can use Oracles to certify under penalty of law that actions have occurred that are specified in the legal agreement but are outside of the capability of an SLC to verify.

Anatomy of a Smart Legal Contract

SLCs can be broken down into three categories with varying degrees of automation lending themselves to different levels of adoption in practice:

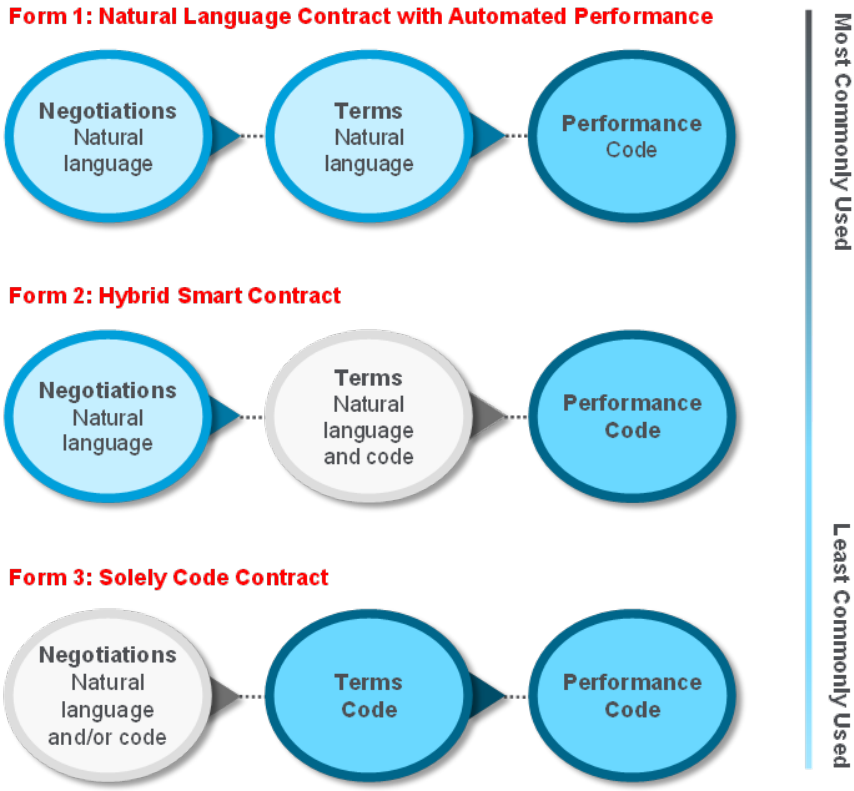
SLCs fall into three categories with different degrees of automation and adoption

- The SLC that would lend itself to being most widely adopted is a natural language contract combined with code. It uses the code of a computer program to execute the contractual obligations (note: the code does not define the contractual obligations).
- At the other end of the spectrum are code-only contracts, where both contractual terms and execution are done by the code. There is no natural language version underpinning the contract. Their use is rare in practice.
- Somewhere in the middle are hybrid contracts, where some of the terms are defined in code and some of the contractual obligations are executed by the code.

[118] UK Law Commission, *Smart Legal Contracts: Summary*, November 2021.

© 2023 Citigroup

Figure 37. The Three Types of Smart Legal Contracts[119]



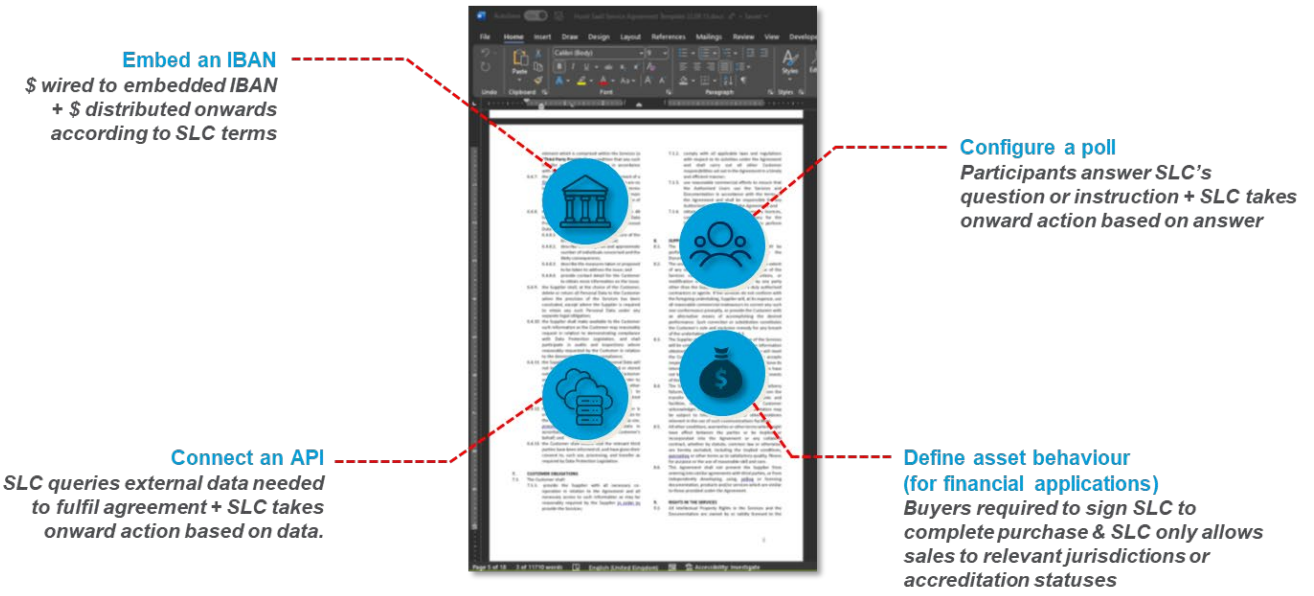
*We have edited the above illustration per our understanding
Source: The UK Law Commission, Citi GPS

On the face of it, if we look at the black and white text (i.e., the natural language) in the image below, SLCs look very similar to ordinary legal agreements. Their anatomy and functionality, however, is quite different.

[119] Ibid.

© 2023 Citigroup

Figure 38. Four Key Features of Smart Level Contracts



Source: Hunit, Citi GPS

- **Payment Identifiers:** SLCs can create and embed International Bank Account Numbers (IBANs), or any other identifiers such as blockchain "public keys" for "on-chain" payments, in the text of the contract, which are exclusively managed by the SLC and its terms. This means payments made to an SLC (via the IBAN) will be handled quickly and accurately and will result in the SLC verifying that a payment requirement has been met. For example, an SLC-based corporate bond may receive a gross sum amount for the borrower's interest payment and distribute payments onward to each individual bondholder. The payment automation is created through a banking integration service, which creates the bridge between the SLC and the global banking system.

- **Polls/Questions:** The SLC contains polls (or an equivalent series of questions). These polls require that identified parties (i.e., signatories to an agreement or service providers to it) answer questions for parts of the contract that cannot be digitized, as they are based on subjective assessments or require some sort of external activity to take place. It is this part of the SLC that requires human involvement. This is important, as many legal agreements contain terms that cannot effectively be fulfilled without the assistance of human actors. For example, a contract may be subject to X number of audits taking place every year before payment can be sent. The poll might therefore ask: Have X number of audits taken place? A human would answer the question, and depending on the answer, the next stage of the contract can be performed.

- **The SLC Connects APIs:** This allows the SLC to use external data as part of its decision tree and enables the recording of the conditions under which the SLC was executed. It can also make an SLC's data, such as its terms or its execution history or status, available to external systems through APIs. This is important for enterprises that have a large portfolio of contracts on their books. A "data lake" of contract data on which other technologies like machine learning can be applied to extract insights and make business decisions.

© 2023 Citigroup

Insights can include how contracts are being performed, where they are failing, where there are disputes, where an enterprise may have a concentration of exposure to legal risk, and where there are repeated failures like an SLC being breached multiple times. These insights can be put on a contract heatmap, on the back of which business decisions can be made to improve performance (such as choosing a different supplier if the current one is repeatedly breaching the terms of the contract).

SLCs do not need DLT to perform

For SLCs using blockchain, the bridge between the contract and the external data set can be provided by an Oracle application. These applications bring off-chain data on the blockchain for the SLC to deploy. Without them, an SLC running on a blockchain would be restricted to only accessing on-chain data. We explain how these are incorporated in the insurance use case below.

- **SLCs Define Asset Behavior:** This is important for financial applications. Not all financial assets can be sold everywhere in the world and to every type of investor. Some cannot be sold to retail investors, for example, or may have restrictions on secondary sales that include first rights of refusal for existing investors or the execution of a deed of adherence to the SLC governing the terms of the investment. The SLC can include terms in the code to make sure all the necessary checks have taken place before an asset can be purchased in a primary or secondary transaction.

Do Smart Legal Contracts Need DLT?

The short answer is that SLCs do not need distributed ledger technology (DLT) to perform, as expressed clearly by the UK Law Commission.[120] SLCs could, for example, be deployed on a conventional cloud-based web service.

> "Smart legal contracts can be performed automatically by computer programs without the use of DLT."
>
> – THE UK LAW COMMISSION

It is therefore not surprising that when the UK Law Commission consulted on smart legal contracts, their analysis was not limited to those which deploy DLT, and this conclusion was informed by the large majority of consultees who agreed that any analysis of SLC should be technology neutral.

It is equally unsurprising that SLC industry consortia, such as the Accord Project, take a more tech-neutral approach to SLCs and as such do not solely focus on DLT. The Accord Project is a non-profit organization that builds open-source code and documentation specifically for SLCs.

[120] Ibid.

© 2023 Citigroup

It is anticipated DLT will be more widely adopted for SLCs due to the additional benefits the technology provides

Where SLCs deploy DLT, the sections of the legal agreement that include self-executing automation are recorded in code that can be run by the chosen DLT network. Non-automated (natural language) portions of the agreement and the records that result from the network's running of the SLCs automation are also recorded by the DLT network. DLT network protocols such as Ethereum, Hyperledger, Corda, and Stellar all may be potentially used for SLCs. Early indications are that the sector's preference falls towards permissioned (i.e., access controlled — see below for further detail) DLT networks where security and costs can be more carefully managed.

It is anticipated that DLT will be more widely adopted for SLCs due to the additional benefits it provides compared to conventional web platforms, namely:

- **Longevity and Independence:** Legal agreements can last a long time. Think about a bond that has a duration of multiple years, or a mortgage loan that is taken out over a 25-year term. Decentralized ledgers are able to exist as long as one of the parties — a node on the ledger — maintains a copy of the ledger.
- **Enhancing Trust and Eliminating Silos:** An SLC's data records and automation are counterparty-neutral: equally accessible to both parties while not under the control of either. This increases transparency of the state of an agreement's completion, enhances the accuracy of an agreement's completion, and improves trust both between the parties and in the outcome of the legal agreement.
- **Tamper-Proof:** Records stored on a DLT cannot be tampered with after the fact. This is important because it means that the contracting parties can safely rely on them without worrying about the risk that they may have been tampered with or modified unilaterally.
- **Security:** While Web3 servers can be compromised and breached, the DLT architecture that runs on top of them uses powerful encryption and multi-party consensus protocols. DLT architectures maintain their security, even if there is a hack at the server on which they are running.
- **Single Source of Truth:** A blockchain has a built-in way of authenticating entries to the database, called "consensus," ensuring that there is a "single source of truth" that has been confirmed by the parties to the network. When it comes to transactions, by way of example, they are verified without a central counterparty in the middle. Instead, they are verified on a peer-to-peer basis using a consensus mechanism to ensure this common single source of truth. This is particularly important in the context of legal agreements when things go wrong and there is a legal dispute. The parties to the dispute can be certain about which is the true legally binding agreement on which to base their case.

If DLT is deployed in SLCs, then there is a choice of which type of DLT to use. It can be a permissioned or a permissionless system, or possibly somewhere in between. (It does not have to be one or the other, and as DLT develops, it may be possible to incorporate permissioned elements into permissionless DLT systems.)

- **Permissioned Systems** would be appropriate where knowing the identity of the parties is important to execute the contract.
- **Permissionless Systems** would be more appropriate in cases where it is acceptable for any node to see data on the ledger, in contrast to permissioned systems, which limit visibility to the transacting parties.

© 2023 Citigroup

Use Cases of Smart Legal Contracts

Although SLCs are in their infancy in terms of adoption, we are on the cusp of change: Regulatory barriers are being removed, and the technology is use-case agnostic

We understand from speaking with experts that SLCs are still at their infancy in terms of adoption, but we are on the cusp of change. First, as the use cases are vast and varied, the technology is use-case agnostic. Second, various regulatory and legal barriers are being removed, with the UK leading the way, as discussed below.

Key use cases are covered below. While they are very different to each other (as noted, the beauty of SLCs is that they are use-case agnostic), what they have in common is the automation of a specific process or task once certain conditions are met (in other words, once certain events have been triggered). SLCs contain clauses that rely on data to check if conditions have been met and outline terms for payment or transfer of ownership. They can also be used for the transferring of funds into one's wallet once certain conditions have been met. Payment can be in fiat, in a crypto asset, or in a Central Bank Digital Currency (CBDC), as and when these become widely available. It will depend on what payment instrument the user decides to use and what payment instrument the service provider decides to offer (an insurance provider may only choose to offer payout in fiat, for example).

Notably, although an SLC's automation may eliminate the operational need for certain roles like agents or notaries, in many cases, these roles are required by current regulations and cannot be eliminated in their entirety. In the below example of an SLC escrow agreement, the buyer and seller both enjoy the benefits of SLC use, but a regulated escrow agent is still required to officiate the transaction. In this case, the SLC allows the escrow agent to perform its role in a far more efficient and risk-free manner. While this may appear to be an unnecessary complication, the escrow agent fulfills the critical role of accepting legal liability for any error that may arise in the transaction.

- **Real Estate and Proptech:** In the property purchase process, an SLC can be programmed such that the money be transferred to the seller, once legal title in the property is registered to buyer. Or in a leasehold scenario, an SLC can be programmed to say your lease comes to an end on a certain date unless you pay money on day X, in which case your lease will automatically review for another year. For real estate purchases requiring lending and borrowing through a mortgage, an SLC would remove the need for intermediaries in the chain. The SLC can be programmed to issue a mortgage offer the moment all checks and documentation has been received.

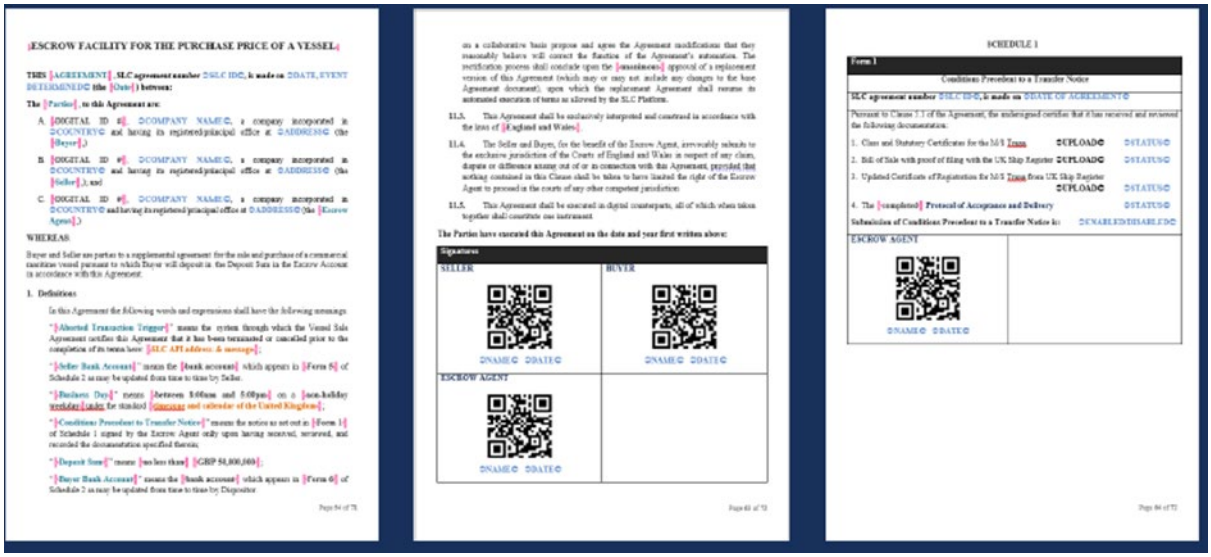
  SLCs can also be used in combination with the tokenization of real-world assets. Tokenization in this context enables digital ownership and transfer with each token representing a fraction — like a share — in the ownership of the overall asset. SLCs can contain all the clauses and conditions that need to be met to trigger an event occurring (e.g., fractional ownership is recorded and ownership is transferred to the buyer once payment has been made and received).

  While tokens and tokenization have been a core use of smart contracts and decentralized finance, they are an interesting use case for SLCs because the tokenization of conventional assets like real estate requires the use of a legally viable ownership structure. In this example, the underlying real estate may be owned by an SPV corporation, which uses tokens to represent equity shares. An SLC-based shareholder agreement would establish this legal structure and would define the terms of purchase and ownership of the corresponding tokens, ensuring that a novel form of real estate ownership (token purchase) is harmonized with the legal framework of property title possession and transfer.

© 2023 Citigroup

Escrow Payments: Linked to the property use case where escrow is used to buy and sell property, an escrow is where a third party holds money or property until certain terms of the contract have been met. The firm Transpact brought this to life by automating the escrow payout process using SLCs. Two parties agree on the terms of the contract in natural language, and the buyer pays Transpact. Once the SLC conditions are met, the funds are automatically released. If the conditions are not met, the funds are returned to the buyer. The whole cycle is automated and self-running. Figure 39 below illustrates what an SLC escrow agreement looks like.

Figure 39. Visual Illustration of a Smart Legal Contract Escrow Agreement

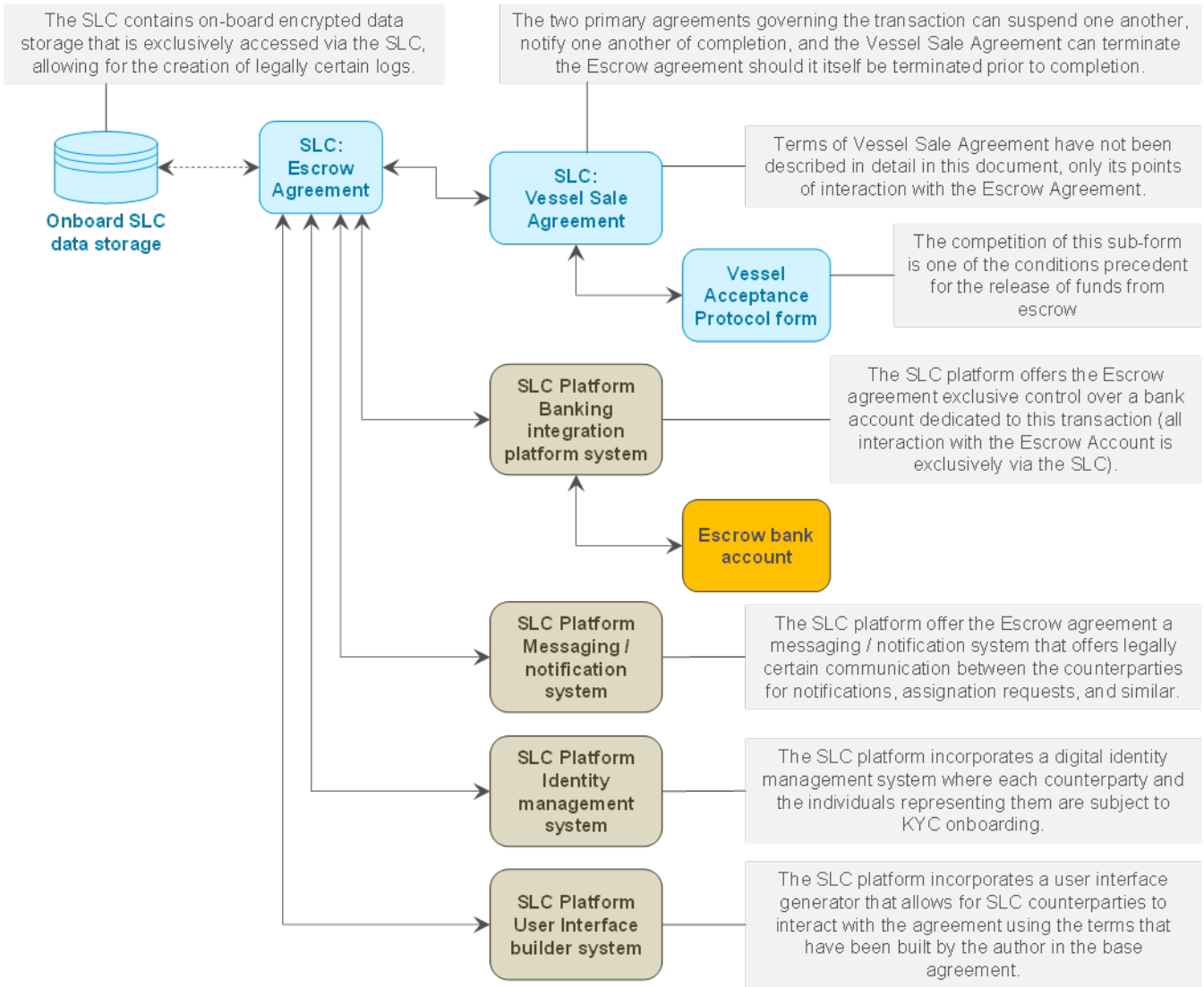


Source: Hunit

This process is underpinned by a technical ecosystem that makes the SLC escrow agreement possible for an escrow agent to assist in the sale of a vessel. In Figure 40 below, the boxes in blue show objects that exist in a multi-node distributed ledger network. The boxes in brown show objects provided by the SLC platform provider (not based on a DLT network), and the orange box shows an external third-party service.

© 2023 Citigroup

Figure 40. Smart Legal Contracts Technical Ecosystem for Escrow Agreement



Source: Hunit

Continuing with the example above of an escrow agreement used when purchasing a vessel, the SLC can be deployed in different steps and interaction points. We cover some of the main ones below:

- To disburse the escrow funds once certain predefined conditions have been met (for example, a technical inspection of the vessel may need to be completed), an SLC will contain identifiers such as IBANs, as described in the anatomy of the SLC. If the conditions are met, the SLC will allow for the transfer of funds.
- An SLC can be used to check that all the conditions have been satisfied (e.g., the necessary documentation has been received, any inspections have taken place, and required forms have been signed). The buyer and seller can then submit a request for the SLC to transfer the funds.
- The transaction closes once buyer and seller have submitted a transfer request for the SLC to transfer funds, any transfer notices have been signed, and funds have been received. The escrow agreement then terminates.

© 2023 Citigroup

Notably, in addition to the interaction points above, the SLC's platform messaging service can also be used for parties of a contract to send each other notifications of contractual significance. Such messaging services help establish a clear, auditable, and legally protected record of communication that includes time stamps.

- **Insurance:** SLCs can be used to automate the payment of claims. Think about the last time your flight was delayed. The SLC would clearly define what event needs to take place for a payout to occur (e.g., the flight needs to be delayed over X number of hours). To do so, the SLC connects to airport databases, tracks flight numbers and timings (e.g., an Oracle could be used to connect to an off-chain database such as a flight tracker, check by how many hours the flight is delayed, and then transmit this information on-chain for the SLC to use), and triggers a payout as soon as a flight is delayed at level that satisfies the insurance policy, as illustrated in Figure 41 below.

  The same logic applies to other types of insurance claims beyond travel as long there is a need for an insurance payout contingent on a specific event occurring. However, that not all types of insurance-related use cases can be fully automated. There are insurance claims that require a physical inspection of an asset (e.g., a building) before payout. In these cases, the SLC can rely upon an agent to perform the physical inspection and certify to the SLC that payout is due.

Figure 41. Simplified Smart Contract Coding Example[121]

Source: European Insurance and Occupational Pensions Authority (EIOPA)

- **Supply Chains:** These have been put to the test and have been under stress on the back of the COVID-19 pandemic. Their reliance on multiple parties and paper-based documentation makes them ideal candidates for SLCs. Trade-related documentation can be turned into SLCs so that the payment is executed when specific events occur in the supply chain (e.g., the delivery of goods triggers payment or instruction for further goods to be manufactured or re-ordered, or payment is triggered after the expected date of delivery for the goods).

  In addition to payment execution (and similar to the above-mentioned escrow example), the SLC can be used to record an event or message when something happens, such as an unforeseen event that can have an impact on the contract.

[121] European Insurance and Occupational Pensions Authority (EIOPA), *Discussion Paper on Blockchain and Smart Contracts in Insurance*, 2021.

© 2023 Citigroup

For example, a container with goods critical to your supply chain is on a ship. The ship has an accident, or someone breaks into the container. This information would need to be monitored (separate from the SLC with the help of monitoring technologies used in supply chains) and then recorded on the blockchain ledger used by the SLC. Depending on the event that has occurred, further human investigation may be required before funds can be released.

- **Managing Breaches in Service Level Agreements:** This could be an agreement with any supplier or provider of a service, such as a technology service like a cloud service provider. Coming back to the different types of SLCs, part of the agreement will be written in natural language, and another part of the agreement will be in computer code. The point is that the SLC would have built-in code to instruct a payout or make a credit (or whatever has been agreed between the contracting parties) when there is a breach in the service level. The service being provided would need to be monitored from a trusted source, and data on the services would need to be collected and recorded to identify any drop in agreed service levels. The trusted source would have to link with the part of the SLC that is in computer code. Where a breach in the service level occurs, the contract executes. If the contract already has embedded payment identifiers, payout occurs (see the section "Anatomy of a Smart Legal Contract"). This means that the parties to the contract would not have to take any action themselves to request an instruction for payment.

- **Derivatives Agreements:** The International Swaps and Derivatives Association (ISDA) has been working for several years on promoting the digital standards that will ultimately serve as the basis for the development of smart contracts in the derivatives industry.[122]

  ISDA's work in developing common legal and documentation standards aims to reduce transacting inefficiencies within the derivatives ecosystem and will provide a foundation upon which new technologies can be developed and implemented. ISDA's recently published *Digital Asset Derivatives Definitions* provides a good example of how increased contractual standardization can support the development of smart contracts.[123] The key operative provisions within these Definitions have been drafted using a controlled semantic structure, expressing most contractual provisions as a series of parameterized conditions and consequences. This allows the operational mechanics of the Digital Asset Definitions to be distilled into a series of "if/then" statements, facilitating their translation into computer code for future implementation within DLT-based infrastructure and smart contracts.

  Digitization of documentation, with supporting processes and data, allows the key commercial and operational terms within legal agreements to be more closely aligned with, and consistent with, the operational and business processes they support, allowing for increased automation of those processes.

[122] ISDA, "Joint Association Letter on a Digital Future for Financial Markets," July 29, 2020.
[123] ISDA, "ISDA Launches Standard Definitions for Digital Asset Derivatives," January 26, 2023.

© 2023 Citigroup

ISDA Create (a tool made by ISDA and Linklaters providing an end-to-end solution automating the creation, negotiation, and execution of derivatives contracts) plays a central role here by facilitating the online creation and negotiation of derivatives documentation and transforming previously unstructured legal agreement data into structured data.[124]

ISDA Create can then translate this structured data into operational data within the "Common Domain Model"— a machine-readable and machine-executable data model for derivatives products, processes, and calculations — for implementation within computable or smart contracts.[125]

ISDA has also published legal guidelines for the development of smart derivatives contracts with respect to equities, foreign exchange, interest rate and credit derivatives.[126] These papers provide an introduction to the various derivatives products for readers who are designing and implementing technology solutions for these products; they highlight which aspects of these contracts are likely to provide the best opportunities for automation within a smart contract.

As noted, there are limitations as to when SLCs can be deployed. Some contractual obligations may not be suitable for automation by a computer program because they are not based on conditional logic (i.e., if A happens then B follows) and are therefore difficult to translate into code. These include situations that require humans to exercise their discretion and judgement. We therefore anticipate that SLCs will be deployed for more basic contracts or use human input, as discussed, to make these determinations.

Regulatory Considerations

The current law of England and Wales is sufficiently flexible to accommodate SLCs

Like with all technological innovations, SLCs can only be adopted and eventually scaled if they are not hindered by rules and regulation.

The UK Law Commission has addressed the question of regulating smart legal contracts with respect to English law. Their findings are important not just in the context of the UK, but also on the global stage given the importance of English law in business transactions.

> "The flexibility of our common law means that the jurisdiction of England and Wales provides an ideal platform for business and innovation, without the need for statutory law reform."
>
> – THE UK LAW COMMISSION

According to an Oxera report:

"*English Law was selected as the most frequently used governing law by 43% of 600 survey respondents, and was often used in transactions with little or no other link to the UK. Similarly, it is estimated that English law comprises 40% of all governing law in global corporate arbitrations.*"[127]

[124] ISDA, "ISDA Create," accessed March 25, 2023.
[125] ISDA, "ISDA Common Domain Model," October 14, 2019.
[126] ISDA, "Memoranda: ISDA Smart Contracts," October 16, 2019.
[127] Oxera, *Economic Value of English Law*, prepared for Legal UK, October 5, 2021.

© 2023 Citigroup

Furthermore, the report highlights that English law governed approximately £250 billion of global mergers and acquisitions in 2019.

In its November 2021 advice to the UK government, the Law Commission considers whether current well-established principles of contract law (by analyzing the requirements that form legally binding contracts) can accommodate SLCs. It concludes that the current law of England and Wales is sufficiently flexible to accommodate SLCs. [128] The UK Law Commission's findings build on earlier work conducted by the UK Jurisdiction Task Force (UKJT), which concluded the same in their Legal Statement.

In Europe, the European Commission proposed a draft regulation in February 2022, the so-called Data Act, with the aim of harmonizing rules on fair access to, and use of, data.[129] This Act does not distinguish between smart contracts and SLCs. The SLC terminology is new. It will be interesting to see how the market responds to this Act and if there will be developments to align the definitions as the Act goes through the various drafts and stages in the EU's legislative process.

The Act serves to fill regulatory gaps and is drafted with the spirit of removing barriers to smart contract adoption by setting standards and requirements regarding smart contracts of data sharing. Furthermore, in Italy, the Federation Autonoma Bancari Italiani (FABI, a federation whose mission is to protect bank workers) has weighed in on SLCs, explaining that they are different from smart contracts and that they would have to adhere to Articles 1321 and 1325 of the civil code.[130]

In Asia, the Court of Appeal in Singapore, in the case Quoine Pte Ltd v. B2C2 Ltd, the judges had to decide how to apply the law of mistake (a principle of contract law) to contracts formed by deterministic algorithms.[131] Although the case did not involve smart legal contracts, it may form how the law is applied to smart legal contracts using deterministic algorithms in the future. The majority judgment demonstrates how traditional principles of contract law can be adapted to apply to contracts run by technology without the need to rip up and re-write the rulebook.

These regulatory developments are positive news for SLC adoption. It comes as a relief that SLCs can be accommodated within existing regulatory frameworks without large-scale reform. Reform not only takes time but also creates an uncertain environment, and operating in a regulatory vacuum hinders business adoption.

Beyond regulatory considerations, SLCs do not come without risks:

- **Unreliable External Inputs:** SLCs rely on external data sources to determine if the terms have been fulfilled for the contract to perform. It is therefore key for the source of the data to be trusted, accurate, and secure.

[128] UK Law Commission, *Smart Legal Contracts: Summary*, November 2021.
[129] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)," PDF, February 23, 2022; The Data Act decines smart contracts as: a computer program stored in an electronic ledger system wherein the outcome of the execution of the program is recorded on the electronic ledger.
[130] Federazione Autonoma Bancari Italiani (FABI), "Smart Legal Contract," (Italian language), video, accessed March 22, 2023.
[131] In the Court of Appeal of the Republic of Singapore, "Judgment," PDF, Quoine Pte Ltd v. B2C2 Ltd, Civil Appeal No. 81 of 2019, accessed March 22, 2023.

© 2023 Citigroup

- **Inaccurate Codes and Bugs:** It is possible for coders to misinterpret the intention of the contracting parties, resulting in the code not performing as expected (or indeed, intended). It is also possible for code to contain bugs. Anyone seeking to use SLC should be aware of these risks upfront. The UK Law Commission explains that the difficulties involved in rectifying codes will probably depend on the technical specifications of the smart contract platform, including whether there is a built-in rectifying functionality.

> The extent of any practical difficulties in rectifying coded terms will likely depend in the technical specifications of the particular smart contract platform, such as whether it has relevant built-in functionality to rectify the coded terms.
>
> – THE UK LAW COMMISSION

- **Cyber Risks:** Codes are subject to cyberattacks and hacks. Anyone deploying SLCs needs to be mindful of such risks and consider putting in place appropriate mitigation measures if such events occur. This can be through the introduction of escape hatches that can stop the contract subject to consent from the contracting parties. The natural language version of the code should flesh out cyber risks and mitigating action, and any SLC enterprise platform should conform to international standards on information security (i.e., ISO 27001 standards) or equivalent.

SLCs and the Future

What the SLC market lacks is a set of principles or standards. These principles would prevent bias in code, ensure that the set of coders is diverse, and make clear that developers can be held to account if they aid and abet violations of the law.

We have already seen signals that would be in line with a direction of travel that holds smart contract developers to account. For example, Brian Quintenz, Commissioner at the Commodity Futures Trading Commission (CFTC), addressed the question of who should be held responsible if a smart contract is not executed in compliance with rules, saying, “a strong case could be made that the code developers aided and abetted violations of CFTC regulations,” and that “the CFTC could prosecute those individuals for wrongdoing.”[132]

[132] Commodity Futures Trading Commission, “Remarks of Commissioner Brian D. Quintenz at the 38th Annual GITEX Technology Week Conference,” Public Statements & Remarks, October 16, 2018.

© 2023 Citigroup

> Instead, I think the appropriate question is whether these code developers could reasonably foresee, at the time they created the code, that it would likely be used by U.S. persons in a manner violative of CFTC regulations. In this particular hypothetical, the code was specifically designed to enable the precise type of activity regulated by the CFTC, and no effort was made to preclude its availability to U.S. persons. Under these facts, I think a strong case could be made that the code developers aided and abetted violations of CFTC regulations. As such, the CFTC could prosecute those individuals for wrongdoing.
>
> – BRIAN QUINTENZ, COMMISSIONER AT THE COMMODITY FUTURES TRADING COMMISSION (CFTC)

Indeed, this approach of apportioning liability has been used in U.S. state legislation, either recently passed or still under consideration, providing legal status to Decentralized Autonomous Organizations (DAOs) in Utah and New Hampshire.[133] These DLT-based organizations devolve all decision making to their members via voting mechanisms and lack the typical structures of directors and chairpersons. Under these state laws, the members of a DAO voting for an action that results in the DAO acting illegally will be held personally liable.

For the technologists, one element to highlight, which we believe will have a more important role in the future, is the so-called "reasonable coder" who can foresee how a code in development may violate regulations. Logically, these coders will be in demand, as they will be called upon to assist the courts when interpreting coded terms in a contract. Coded terms can be subject to interpretation, and there can be a divergence between what the code means and how it executes. To this end, the Law Commission confirms that reasonable coders will be relied upon instead of computers when it comes to interpretation issues.

For the legal profession, upgrading contracts to SLCs will require thought — perhaps more so than before — on eventualities and on how risks will be allocated when things go wrong, and baking these into the contract. This includes doing a thorough analysis of what could happen in the future, setting out the different steps and procedures to get there, and including these in the SLC using polls. As SLCs become more widely used, it will also be interesting to observe to what degree they replace lawyers in certain areas of corporate contract work. Think about escrows or asset purchases: A solicitor will not be required to check if the funds have been received before proceeding to payment.

The UK Law Commission has set out a non-exhaustive list of issues contracting parties may wish to consider for their SLCs

The UK Law Commission has set out a non-exhaustive shopping list of issues that contracting parties may wish to consider for their SLCs.[134] It would make sense for anyone wishing to deploy such contacts in the future to review these issues to avoid disputes and limit any uncertainty as to how the contract would be treated under law. The list also includes what should be considered where the SLC deploys DLT.

[133] Utah State Legislature, "H.B. 357 Decentralized Autonomous Organizations Amendments," accessed March 24, 2023; BillTrack*50*, "NH HB645," accessed March 24, 2023.
[134] UK Law Commission, "Smart Legal Contract, Summary," November 2021.

© 2023 Citigroup

Further regulatory change is on the way in the UK with the Electronic Trade Documents Bill, which was introduced into Parliament in October 2022.[135] This Bill is a big step forward in the move to digitize paper-based trade documentation and to making digital documents legally recognized. Similar regulatory change is taking place in Singapore with the Electronic Transactions (Amendment) Act, which recognizes electronic equivalents of transferable trade documents such as bills of lading, promissory notes, and bills of exchange. If these documents are digitized, legally recognized, and combined with DLT, then we have a good starting point from which to automate the documents and turn them into SLCs.

While the developments happening in the UK and in Singapore are encouraging, as trade is a global business, any legislative change will need to happen on a global scale and in multiple jurisdictions. This will enable digital documents to be traded successfully, as they go through multiple countries during their life cycle and should be accompanied by the building of new infrastructure for using them, as well as by major players coming together to form industry consortia.

The creation of regulatory sandboxes could help SLCs gain mass adoption

Looking into the future, what could help SLCs gain mass adoption — and thus take blockchain adoption into the billions — is the creation of regulatory "sandboxes" to test out the application of technologies under the watchful eye of regulators. We have witnessed these come to fruition since 2016, with the Financial Conduct Authority being the first regulator to market. These sandboxes have been replicated and tailored by regulators around the word. The initiative has now gone global with the introduction of the Global Financial Innovation Network (GFIN) — a global sandbox, in other words. Different technologies have been tested in such sandboxes, from AI to privacy-enhancing technologies that comply with anti-money laundering and know your customer (AML/KYC) rules. It is not a far cry to imagine an SLC sandbox coming to market in the future. This is an important space to watch.

[135] UK Parliament, "Electronic Trade Documents Bill," PDF, accessed March 22, 2023.

© 2023 Citigroup

A Conversation With Aaron Powers on How Smart Contracts Can Transform Finance

Aaron Powers is the CEO and Co-founder of Hunit. Hunit allows any law office, financial group or enterprise to create distributed ledger-based, self-executing smart legal contracts without having to write a single line of code. Hunit works with aims to unlock new opportunities for the growing private investment market and the legal professionals serving it. Hunit operates across the UK, Norway and the U.S. Hunit's embedded technology development partner, Revelry Labs, which has deep blockchain and financial industry experience.

Q: What are smart legal contracts (SLCs)? How are they different from real world legal contracts?

Aaron: Legal contracts are everywhere. KPMG estimates 60%-80% of all business operations are either driven by legal obligations or are somehow constrained by them. But, despite pervading all commercial and financial transactions, they are the world's last great analog holdout.

Smart legal contracts are like standard natural language agreements but include embedded automation that transforms the contract from an archive of intention into an active business tool — the legal agreement and the tools used to execute it become one and the same. In other words, smart legal contracts are like an operating system for global commerce and finance to run on. As further benefits, smart legal contracts incorporate Web3 primitives such as immutability, transparency, and trustlessness.

This means we can integrate a smart legal contract with the global banking system. For example, if at a certain point in time of a contract's execution, one party needs to send money to the other, this can be achieved by sending the payment to the smart legal contract, which in turn records receipt. This money can then be distributed onwards according to the terms of the agreement.

Smart legal contracts can also interact with external data sources and import data from web services or APIs (Application Programming Interfaces). At the same time, structured data generated by the smart legal contract, as it executes its life cycle, can be made available to external systems (e.g., enabling portfolio dashboarding for large institutions with big portfolios of legal agreements).

A smart legal contract complies with the regulatory framework that defines what is and is not a legal agreement. SLCs also recognize important elements like the preemptive rights of courts and bankruptcy trustees. Aspects such as title law and force majeure events all need to be incorporated into smart legal contracts.

Q: Why do we need smart legal contracts? What are the use cases of smart legal contracts?

Aaron: The future of finance with tokenization, decentralized finance (DeFi) and the metaverse require natively digital legal solutions. At a basic level, smart legal contracts are use-case agnostic and will serve as the layer that marries these new digital ecosystems and the legal frameworks that governs them.

However, there are trillions of conventional legal agreements signed every year that can be recorded as SLCs. We do not need to wait for DeFi to move mainstream for SLCs to start adding value to society — one can use smart legal contract for business and consumer agreements today. This could be something as mundane as non-disclosure agreements or for sophisticated use in financial instruments, especially in areas that have not been effectively digitized, such as alternative assets.

We estimate, there are nearly $1.4 trillion of newly issued PDF-based private market investment instruments annually that can be transformed by SLCs. The status quo necessitates significant manual intervention and high costs for fulfilling these agreements. Furthermore, this creates the risk of costly errors.

© 2023 Citigroup

In my opinion, smart legal contracts represent one of the great breakout moments for Web3 — they have the potential to bring this technology to more people and companies than any other Web3 application. In the long-run, there is only one use case for smart legal contracts — to record and improve upon the wide variety of legal agreements in use today. However, in the more immediate term, industries driven by large numbers of financial transactions that don't currently have effective digital infrastructure represent their first market inroads. This includes sectors like private market financial instruments, power markets, shipping, and construction.

Q: Are smart legal contracts recognized in the UK legal system? How do they interact with existing law?

Aaron: The UK Law Commission started a public consultation to look at smart legal contracts and how they could work with the existing UK law. While our initial discussions were very constructive and highlighted the feasibility of smart legal contracts, regulators were concerned with a few key areas.

To solve for these concerns, we successfully worked with the support of the UK Jurisdictional Task Force, a division of the Ministry of Justice, as well as the Solicitors Regulation Authority (SRA). During this period, we defined at a very practical level how a smart legal contract needs to behave in order for it to exist under current regulations.

The final piece in the puzzle was the Digital Trade Documents Act in the UK, which is removing the requirement for certain types of documents to be presented in physical form in order for them to be valid and effective. This allows for the dematerialization of all documents such as bills of lading and other bearer bond-type structures.

Today, smart legal contracts are ready to use in the UK and we are working to deploy them everywhere.

Q: Where are we in the U.S. in the context of smart legal contracts? Are legal systems flexible in non-common law countries to accommodate smart legal contracts? Where is continental Europe in terms of SLC?

Aaron: The U.S. poses a unique challenge as we have essentially 50 different, but similar legal regimes. However, both, the UK and the U.S. are common law systems. Thus, the work done to gain regulatory support in the UK largely translates to the U.S., although there are still a few aspects that need to be reviewed and changed.

Importantly, in a common law environment, it is the court precedents that create the regulatory approach to different areas. This may not be as proactive as what we are seeing in the UK, but inroads are being made in the U.S. For financial applications, the SEC is continually clarifying its position on the use of Web3 technology and all big players in the space are looking hard at the aspects of smart legal contracts.

There are a number of EU countries that have passed the requisite legislations around dematerialization of documentation, digital signatures etc. Of course, in a Napoleonic legal environment, there is a need for the boxes to be drawn ahead of time. At this point, we have some use cases that potentially touch on uses in France and we have not found ourselves butted up against any structural issues.

© 2023 Citigroup

However, the warmest welcome we have received for smart legal contract technology so far has been in the UK. Nonetheless, it is my opinion that the wave of smart legal contracts is fast approaching, and it would be difficult in 2023 to argue that the analog agreement structure will continue in the medium to long term (either in finance or elsewhere).

Q: Can you elaborate on the use-cases for smart legal contracts?

Aaron: The technology behind smart legal contracts is use-case agnostic. As an example, our own shareholder agreement is about 50 pages with about 17 instances where automation makes sense and could provide value. The rest of the agreement is in natural language terms that either have limited operational impact or include disclaimers, acknowledgements, etc. With a few exceptions, the automation that is being embedded can be used across a broad spectrum of agreement types — it is the natural language of the agreement that gives the automation its context. Think of how many types of agreements contain conditions precedent or have a procedure to deliver something in response to payment — the same underlying automation can be reused over and over.

To give you some ideas about how self-executing legal agreements can change business, think of a non-disclosure agreement where confidential materials are either sent via or displayed by the NDA itself. Once the non-disclosure period or agreement terms have ended, access can be denied automatically. This can reduce manual intervention of deleting files or restricting access and actually make the NDA an enforceable document.

Within finance, we are currently working to deploy a set of fund offering documents. These are agreements a limited partner would sign when investing in a hedge fund. Thanks to automation, smart legal contracts can provide efficiencies in the areas of Know Your Customer, accreditation, and onboarding, etc. SLCs help automate processes around subscriptions into the fund, performing delivery versus payment for fund shares. In this use, smart legal contracts help create economies of scale for fund managers and admins.

We can also extend this use case further to trading parameters, albeit the latter is still under development. We know hedge funds have different parameters they commit to with investors — for example, minimum diversification, max leverage, etc. The current paradigm is that these commitments are made, trades are executed on the trading desk, and at the end of every week, the compliance department checks through to make sure trades were not out of balance. In case of breaches, one needs to evaluate the size and extent of breach and if it warrants for users and regulators to be notified. This can be a long back-and-forth process.

Using smart legal contracts, trading platforms will receive their trading parameters from the contract itself, creating an end-to-end digital link between the agreement signed with the investor and the trading desk's performance. This can lead to a significant reduction in risk, whilst also improving efficiency.

A consumer-focused example is from the automotive sector. We are exploring the use of smart legal contracts for business model innovation. A buyer or lessee can sign a smart legal contract while purchasing or leasing a new car. This smart legal contract can then be integrated with banking systems, allowing for loan repayment or lease payments to be paid automatically from the customers bank account (possibly using the EU's Second Payment Services Directive, or PSD2 architecture).

© 2023 Citigroup

So far, so normal. But taking it a step further, the smart legal contract can also be integrated with the car's diagnostics, gathering various data points on kilometers driven, service intervals, malfunctioning equipment, etc. This additional information can then be linked to the fee structure for the leased car, with potential penalties for late servicing, accidents, etc. Using external data connections, smart legal contracts can also be used to ascertain if the car is properly insured, and failure to do so could possibly disable the car ignition altogether.

An important point to mention is that under today's model, customized agreements drive big increases in cost and manual tasks. But when the automation used to fulfill smart legal contracts is embedded in the agreement itself, they are a cost-effective solution for a car manufacturer to offer a wide variety of commercial models around mobility services.

My last example relates to litigation finance. A typical company in the retail litigation space may offer between 1,500 and 2,000 small-scale loans per month. These companies then periodically issue securities on the back of a cohort of these loans to specialized investors with the aim to replenish their capital. These cohorts often necessitate intensive manual work tying the life cycle of the loan to the actual progress made on individual cases. A large cohort of maybe 5,000 loans can further complicate matters. Lastly, one also needs to manually track individual cases in the cohort to determine which ones have been settled and calculate the amount of principal owed back.

A three-way smart legal contract can be initiated between the lender, the legal services provider, and the claimant. These can then be grouped into a special purpose vehicle (SPV), that issues a debt instrument. Extensive amounts of data can then be collected and structured to automate regular payments, making the process far more efficient and transparent. In my opinion, this type of transparency would have avoided the 2008 sub-prime crisis as the rating agencies and investors would have seen exactly what was being collateralized.

Q: What recourse mechanism is available when a smart legal contract goes wrong? How do you handle bugs and errors in code?

Aaron: The quality of the code in a smart contract is of paramount value — it is your first and last defense.

Smart contracts also need to have fatalistic execution. If you had a force majeure button on a smart contract for forward sales of cryptocurrency, it would be calamity as there would be no repercussion for pressing it — as there is no legal significance in the smart contract.

But if a party to a smart legal contract claims force majeure and pauses its execution inappropriately, they can expect to find themselves in court. In other words, having the legal system as the backstop for smart legal contracts allows the technology to offer ways to update an agreement or fix things that are going wrong. During a dispute, should the parties agree, or the court mandate, the automation can be turned off. We term this as rectification automation. Additionally, if both parties mutually agree to make rectifications to the contract, they can amend the smart legal contract in a very similar way as one would for a traditional agreement.

© 2023 Citigroup

Taking it a step further from conventional agreements, smart legal contracts allow users to agree to incorporate, at the outset, potential resolution mechanisms for anticipated breaches of terms. Most commonly, breaches either involve delay in payment of an agreed sum of money or denial of payment altogether. The parties to the agreement can agree on potential ways to address these breaches at the time of initiating the smart legal contract itself. The smart legal contract can then automatically execute such actions if a breach occurs. Think of a secured bond that automatically starts the liquidation of a pledged asset 45 days after a missed repayment — investors don't have to organize a costly litigation and the issuer doesn't have the opportunity to drag things out in court. This would reduce the time needed to recover capital from years to weeks and think of what that kind of change means to a model for pricing risk.

© 2023 Citigroup

Appendix 1: How Real-World Assets Are Tokenized

In the real world, there are non-fungible assets, which are unique and irreplaceable, and fungible assets, which may be interchanged for other assets of similar or identical qualities and quantities. In most cases, the fungibility of the real-world asset token corresponds with its underlying real-world asset. For example, when a share of stock or gold is tokenized, it is typically minted as a fungible token, but a piece of land typically becomes a non-fungible token (NFT) as it has unique attributes including but not limited to its acreage and geographic location.

Theoretically, any assets with monetary value in the real world can be tokenized, and there are various ways to create real-world asset tokens.[136] The process and complexity of tokenizing certain types of real-world assets may vary but could generally be summarized by the following steps.

1. **Due Diligence**

   The owner of the real-world asset thoroughly reviews, audits, and appraises the asset value and relevant information that would be encoded on-chain.[137] The owner also conducts due diligence on the jurisdiction including regulations and legal guidelines, different blockchain networks and types of token, custodians for the underlying real-world assets, tokenization platforms, and marketplaces or exchanges where the token will be listed, to ensure both the terms and conditions and the tokenization process are best suited for the real-world asset and remain legally compliant. In more complex cases — such as tokenizing real estate assets or private equity funds — additional factors, including the investment time horizon, fractionalization ratio, and ownership structure, also go into consideration.[138] There is now a growing number of platforms that offer "tokenization as a service" to help facilitate the process for asset owners.

2. **Digitization**

   As due diligence concludes and decisions are made on the various aspects of tokenization, the relevant information, the asset's unique attributes, and the agreed terms and conditions can proceed to be digitized on-chain through the methods selected during the due diligence period and written into the smart contract. These can either be embedded in the token or deployed on the blockchain to automate functions such as transferring ownership, distributing dividends, or allowing the token to be exchanged for other cryptocurrencies or fiat currencies.[139]

[136] Ravi Chamria, "Comprehensive Guide on Tokenized Real-World Assets," Zeeve, November 23, 2022.
[137] Ibid; Ben Plomion, "How to Tokenize an Asset: A Step-by-Step Guide to NFTs Backed by Physical Assets," Dibbs, accessed March 22, 2023.
[138] Ravi Chamria, "Comprehensive Guide on Tokenized Real-World Assets," Zeeve, November 23, 2022.
[139] Andrei Larion, "Real Estate Tokenization," University of Florida, Warrington College of Business, August 26, 2022.

© 2023 Citigroup

3. **Custody**

To add a layer of security for token holders, a third-party typically provides custody of the token's underlying real-world asset to make sure the asset is safely stored and appropriately maintained. For example, luxury wine needs to be stored in a temperature-controlled cellar, and gold needs to be stored in a vault.

Furthermore, real-world assets are subject to entropy, meaning that all objects that physically exist will eventually degrade and perish. However, tokens (i.e., the digital representation of the real-world assets) are not subject to such physical law. As the physical status of the underlying real-world asset continues to evolve, it is important that the custodian or another party reflects the changes on-chain to ensure transparency and ease of valuation and auditing. Various start-ups are developing technology using the Internet of Things (IoT) and Oracle networks to convey real-time data of the tokenized real-world asset, such as gold purity, soil acidity, or foot traffic, which can be applied to measure and convey the status of the asset.[140]

Proof-of-reserve has also become an increasingly crucial component of custody since the series of bankruptcies and scams negatively affected the crypto world in the second half of 2022. Investors now often demand exchanges to prove that the digital assets they hold in custody on behalf of their customers are backed 1:1. Similarly, investors may also demand proof their real-world asset tokens are backed 1:1 by the real-world assets stored under custody.

Notably, the custody of the underlying real-world assets is differentiated from custody of the token. Token holders are usually free to choose where to keep their private key, whether in a hot wallet (connected online) or a cold wallet (data stored offline) to prevent loss and theft.

4. **Distribution**

The last step is to issue the tokens, which will be transferred to new investors for the first time, and to list the tokens on selected marketplaces or exchanges so there is a secondary market, and their holders have access to liquidity.[141] Marketing is another component during this process and is particularly important for projects that aim to raise capital or sell assets not yet widely recognized in traditional finance.

[140] Chainlink, "Tokenizing Real-World Assets On-Chain," Chainlink Tech Talk #10, YouTube, December 26, 2022; Menghua Wong, Xuedong Liang, and Zhi Li, "Research on the Evaluation Index System of the Soil Remediation Effect Based on Blockchain," *Land*, Vol. 10, No. 11, November 2021.

[141] Ravi Chamria, "Comprehensive Guide on Tokenized Real-World Assets," Zeeve, November 23, 2022; Ben Plomion, "How to Tokenize an Asset: A Step-by-Step Guide to NFTs Backed by Physical Assets," Dibbs, accessed March 22, 2023.

© 2023 Citigroup

Appendix 2: Digital FMIs Scaling Infrastructure

New Digital Disruptors

As distributed ledgers are creating new opportunities across the value chain for financial securities, we are seeing a wave of new digital market infrastructures entering the market by either introducing new functionality or disrupting traditional operating structures. These include:

- **Digital Securities Trading and Settlement Market Infrastructures:** Built on Distributed Ledger Technology (DLT) or with significant parts of their infrastructure utilizing tokenized, smart contract-driven flows, these seek to either target new emerging asset models (fractional, tokenized) or offer cheaper clearing and settlement functionality for traditional assets. Examples include BondEvalue in Singapore, Archax in the UK, and Paxos in the U.S.
- **Tokenization Agents:** These focus on the issuance/origination of securities on DLT, either as a digital-native token or a tokenized outstanding security. Examples include agents such as Tokeny, Securitize, and Securrency.
- **Documentation and Workflow Infrastructures:** These offer the option to centralize the whole documentation process pre-issuance by facilitating the exchanges between all the involved parties and automating some of these parts. Examples include Agora, Origin, NowCM and previously Nivaura (recently acquired by NowCM).
- **Marketplaces and Tokens Distribution Platforms:** These provide access to a broader investor base, expanded to all accredited investors that can directly access the digital token through an online platform offering features for an easier investment process (e.g., 24/7 access, fractionalization, and instant settlement).
- **Wallet Providers and Digital Custodians:** These enable custody of digital securities on DLT-based wallets.
- **Digital Collateral Infrastructures:** Focused on digitizing collateral flows in order to make them smoother, cheaper and seamless globally, examples of digital collateral infrastructures include HQLA^X (which is building a digital collateral network initially in Europe), JPMorgan's Onyx repo platform, and Broadridge's DLT Repo.

© 2023 Citigroup

Figure 42. Selected New Digital FMIs and Platrofmrs Disrupting Traditional Capital Markets

	Company	Overview	Key Partnerships
Trading and Settlement Market Infrastructures	BondEvalue	Singapore-based Fintech focused on digitizing the bond market and allowing for fractionalized trading of bonds	▪ **Citi:** Investor and Custodian ▪ **Northern Trust:** Asset Servicing
	Archax	London-based digital securities exchange	▪ **Ownera, Tokeny, Securitize, Securrency** (among others)
	Paxos Trust Company	Blockchain infrastructure provider providing trading and settlement solutions	▪ **Bank of America, Credit Suisse, Interactive Brokers, Binance**: Clients
Tokenization Agents	Tokeny	Luxembourg-based institutional grade platform allowing for the issuance, transfer, and management of digital securities	▪ **Euronext**-backed
	Securitize	Platform for digital securities issuance and live trading of security tokens	▪ **Morgan Stanley, Nomura, Coinbase Ventures**: Investors ▪ **KKR**: client for a fund tokenisation
	Securrency	Platform for digital securities issuance and marketplaces	▪ **WisdomTree, Money Group, Ownera, State Street, US Bank**
Documentation and Workflow Infrastructures	Agora	Blockchain-based voting ecosystem	▪ **Binance and Synaps**
	NowCm	NowDocs automates the documentation process for issuances	▪ **Natixis, BNP Paribas, Credit Agricole**: Clients ▪ **Societe Generale, Amundi, Banque de France**: Investors
Digital Collateral Infrastructures	HQLA^x	Distributed ledger for securities finance and repo transaction to improve collateral mobility	▪ **Citi, Goldman Sachs, BNY Mellon, Deutsche Börse**
	Onyx by J.P. Morgan	Blockchain-based platform for payments transactions, tokenization, and exchange of digital assets	▪ **J.P. Morgan**

Source: Citi GPS

Traditional FMIs Upscaling

Faced with a direct disintermediation threat, traditional FMIs have been working on upgrading their infrastructures and data models:

- **Central Securities Depositories (CSDs):** As we have seen in the EIB digital pilot bond, the need for a CSD was successfully tested for in the initial pilots, and CSDs may be needed for a potential future market environment.
- In 2021, Deutsche Börse and Clearstream (an international CSD that is part of Deutsche Börse Group) developed D7, a platform that operates within German and European regulatory frameworks and offers and supports same-day issuances for digital securities, automated straight-through processing, and decentralized and atomic settlement and custody systems. LBBW (Landesbank Baden-Württemberg) and Vontobel performed automated issuances on the platform as well as KfW (a €20 million digital bond with a two-year duration and a coupon of 2.381%).
- In the U.S., the Depository Trust & Clearing Corporation (DTCC) announced its Project Ion platform, which leverages DLT to improve settlement processes. A primary goal of the platform is to support T+0 settlement, on top of T+1 and T+2 settlement cycles, in a regulatory-compliant manner. The platform, which is private and permissioned, went live in pilot form in parallel with existing settlement infrastructure.

© 2023 Citigroup

- **Stock Exchanges and Trading Venues:** With increasing number of new digital exchanges and marketplaces, traditional venues have been upscaling their value-add to cater to digital securities leveraging local regulations when possible.

  Switzerland's SIX Digital Exchange (SDX) is the digital exchange arm of the SIX Swiss Exchange, leveraging the flexibility offered by Swiss regulation for the issuance and secondary trading of digital securities. SDX has performed a few pilots where a digital bond was issued on DLT, listed both on the traditional and digital exchange at the same time, and available for trading on both.

- **Custodians:** With the growing need for custody for digital securities and the temptation of self-custody, select major custodians have been setting up digital custody capabilities.

  Traditional custodians have the additional experience and capability to upscale their role and manage the private keys of the DLT instruments and assets for holding and transfers. They also provide connectivity to the relevant networks and protocols as well as the balance sheet backing in case of any issue.

© 2023 Citigroup

Appendix 3: DAOs as a Foundation for Web3

DAOs have the potential to drive blockchain adoption by providing new, innovative ways for communities to govern and manage themselves. The decentralized and democratic economic model of DAOs helps grant individuals flexibility to rent their talent or time to specific projects in order to earn rewards by leveraging fractional ownership in a community-governed ecosystem.

DAOs can facilitate inclusive access, providing small investors and contributors with access to the DAO's content and a voice in organizational decisions. They can also potentially help unlock access to private investment opportunities previously available only to wealthy investors.

DAOs could also play a crucial role in the Open Metaverse (i.e., a Web3-based version of the Metaverse). Using DAOs, content creators can own and monetize their original creations, and the value can be manifested as NFTs (non-fungible tokens) or tokens.

- **More Autonomy, Better Monetization:** Increased lifestyle flexibility and control have enabled today's creator economy of artists, vloggers, podcasters, and the like to flourish through short-term contracts. As DAOs proliferate, instead of having one employer and a defined working week, individuals may be able to contribute several hours a week to multiple DAOs, resulting in more autonomy in the monetization and scheduling of work hours.

  DAOs are likely to attract self-motivated individuals who share an organization's specific vision. Thus, DAOs are well-suited to strengthen workers' engagement by rewarding them with ownership in projects, mitigating the principal-agent dilemma, where there is a conflict of interest or priorities between employers (i.e., the principals in this example) and their employees (i.e., agents). **DAOs could grant more autonomy over where, when, and how an employee works.**

- **Freedom to Pursue More Fulfilling Work:** According to a report by Gallup, only 21% of the global workforce today is engaged at work.[142] DAOs could offer employees freedom to choose projects where: (1) they share the company's mission or vision, (2) the role aligns with their core competences, and (3) talented and like-minded co-workers are present. The technology-centric nature of DAOs may also help automate trivial tasks using smart contracts that could further free up employee time for more critical and creative work.

- **Different Compensation Streams and Structures:** DAOs could enable ownership and governance in an Open Metaverse, driving newer monetization methods for contributors. For instance, a DAO employee can contribute to content moderation of the virtual world where kids play, learn, socialize, and earn native DAO or Metaverse tokens, thereby making the employee the owner and aligning their interests with that of the DAO and the Metaverse.

[142] Gallup, *State of the Global Workplace: 2022 Report*, June 2022.

© 2023 Citigroup

As Web3 infrastructure proliferates and offers the possibility of redefining traditional paradigms of gaming, social media, money, and finance over the next five to 10 years, we are likely to see more of these communities being governed by DAOs. In the coming years, DAOs could challenge the way we think about organizations by putting emphasis on self-governing businesses. And even if existing corporate structures do not wither away, DAOs represent a mindset and an ethos that may influence existing structures to become more participatory.

© 2023 Citigroup

As our premier thought leadership product, **Citi Global Perspectives & Solutions (Citi GPS)** is designed to help readers navigate the most demanding challenges and greatest opportunities of the 21st century. We access the best elements of our global conversation with senior Citi professionals, academics, and corporate leaders to anticipate themes and trends in today's fast-changing and interconnected world.

All Citi GPS reports are available on our website www.citi.com/citigps

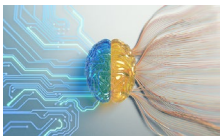
The Cyber Problem
Causes and Consequences of the Rise in Cyber Skill Demand
March 2023

The Creator Economy
Getting Creative and Growing
March 2023

Generative AI
ChatGPT and Search
February 2023

Supply Chain Finance
Uncertainty in Global Supply Chains Is Going to Stay
January 2023

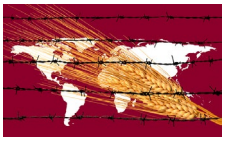
State of Global Electric Vehicle Adoption
A Trip Around the World
January 2023



Disruptive Innovations IX
Ten More Things to Stop and Think About
December 2022

Antimicrobial Resistance
The Silent Pandemic
December 2022

Climate Finance
Mobilizing the Public and Private Sector to Ensure a Just Energy Transition
November 2022



Food Security
Tackling the Current Crisis and Building Future Resilience
November 2022

Energy Transition: Vol 1
Mixed Momentum on the Path to Net Zero
November 2022

Energy Transition: Vol 2
Building Bridges to Renew Momentum
November 2022

China's Inward Tilt
The Pursuit of Economic Self-Reliance
October 2022

Philanthropy v2.0
Reinventing Giving in Challenging Times
October 2022

Food and Climate Change
Sustainable Foods Systems for a Net-Zero Future
July 2022

Home of the Future 2
PropTech – Towards a Frictionless Housing Market?
June 2022

Global Supply Chains
The Complexities Multiply
June 2022

Space
The Dawn of a New Age
May 2022

Investing for Outcomes
Why Impact Is Relevant Beyond Impact Investing
April 2022

Metaverse and Money
Decrypting the Future
March 2022

Global Art Market Disruptions
Pushing Boundaries
March 2022

Women Entrepreneurs
Catalyzing Growth, Innovation, and Equity
March 2022

Eliminating Poverty
The Importance of a Multidimensional Approach
February 2022

Global Supply Chains
The Complicated Road Back to "Normal"
December 2021

Philanthropy and the Global Economy
Opportunities in a World of Transition
November 2021

Education: Learning for Life
Why L&D Is the Next Frontier in Global Education
November 2021

Home of the Future
Building for Net Zero

October 2021

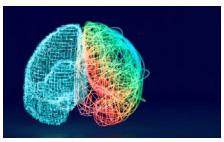
Global Carbon Markets
Solving the Emissions Crisis Before Time Runs Out
October 2021

Disruptive Innovations VIII
Ten More Things to Stop and Think About
October 2021

Holistic Digital Policy
Nation States Must Lead in Building Equitable Human-Centric Digital Economies
October 2021

Biodiversity
The Ecosystem at the Heart of Business
July 2021

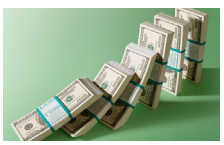
Natural Gas
Powering Up the Energy Transition
July 2021



Technology at Work v6.0
The Coming of the Post-Production Society
June 2021

Hard to Abate Sectors & Emissions
The Toughest Nuts to Crack
May 2021

Future of Money
Crypto, CBDCs and 21st Century Cash
April 2021



Systemic Risk
Systemic Solutions for an Interconnected World
April 2021

The Global Art Market and COVID-19
Innovating and Adapting
December 2020

If you are visually impaired and would like to speak to a Citi representative regarding the details of the graphics in this document, please call USA 1-888-800-5008 (TTY: 711), from outside the US +1-210-677-3788

IMPORTANT DISCLOSURES

This communication has been prepared by Citigroup Global Markets Inc. and is distributed by or through its locally authorised affiliates (collectively, the "Firm") [E6GYB6412478]. This communication is not intended to constitute "research" as that term is defined by applicable regulations. Unless otherwise indicated, any reference to a research report or research recommendation is not intended to represent the whole report and is not in itself considered a recommendation or research report. The views expressed by each author herein are his/ her personal views and do not necessarily reflect the views of his/ her employer or any affiliated entity or the other authors, may differ from the views of other personnel at such entities, and may change without notice.

You should assume the following: The Firm may be the issuer of, or may trade as principal in, the financial instruments referred to in this communication or other related financial instruments. The author of this communication may have discussed the information contained herein with others within the Firm and the author and such other Firm personnel may have already acted on the basis of this information (including by trading for the Firm's proprietary accounts or communicating the information contained herein to other customers of the Firm). The Firm performs or seeks to perform investment banking and other services for the issuer of any such financial instruments. The Firm, the Firm's personnel (including those with whom the author may have consulted in the preparation of this communication), and other customers of the Firm may be long or short the financial instruments referred to herein, may have acquired such positions at prices and market conditions that are no longer available, and may have interests different or adverse to your interests.

This communication is provided for information and discussion purposes only. It does not constitute an offer or solicitation to purchase or sell any financial instruments. The information contained in this communication is based on generally available information and, although obtained from sources believed by the Firm to be reliable, its accuracy and completeness is not guaranteed. Certain personnel or business areas of the Firm may have access to or have acquired material non-public information that may have an impact (positive or negative) on the information contained herein, but that is not available to or known by the author of this communication.

The Firm shall have no liability to the user or to third parties, for the quality, accuracy, timeliness, continued availability or completeness of the data nor for any special, direct, indirect, incidental or consequential loss or damage which may be sustained because of the use of the information in this communication or otherwise arising in connection with this communication, provided that this exclusion of liability shall not exclude or limit any liability under any law or regulation applicable to the Firm that may not be excluded or restricted.

The provision of information is not based on your individual circumstances and should not be relied upon as an assessment of suitability for you of a particular product or transaction. Even if we possess information as to your objectives in relation to any transaction, series of transactions or trading strategy, this will not be deemed sufficient for any assessment of suitability for you of any transaction, series of transactions or trading strategy.

The Firm is not acting as your advisor, fiduciary or agent and is not managing your account. The information herein does not constitute investment advice and the Firm makes no recommendation as to the suitability of any of the products or transactions mentioned. Any trading or investment decisions you take are in reliance on your own analysis and judgment and/or that of your advisors and not in reliance on us. Therefore, prior to entering into any transaction, you should determine, without reliance on the Firm, the economic risks or merits, as well as the legal, tax and accounting characteristics and consequences of the transaction and that you are able to assume these risks.

Financial instruments denominated in a foreign currency are subject to exchange rate fluctuations, which may have an adverse effect on the price or value of an investment in such products. Investments in financial instruments carry significant risk, including the possible loss of the principal amount invested. Investors should obtain advice from their own tax, financial, legal and other advisors, and only make investment decisions on the basis of the investor's own objectives, experience and resources.

This communication is not intended to forecast or predict future events. Past performance is not a guarantee or indication of future results. Any prices provided herein (other than those that are identified as being historical) are indicative only and do not represent firm quotes as to either price or size. You should contact your local representative directly if you are interested in buying or selling any financial instrument, or pursuing any trading strategy, mentioned herein. No liability is accepted by the Firm for any loss (whether direct, indirect or consequential) that may arise from any use of the information contained herein or derived herefrom.

Although the Firm is affiliated with Citibank, N.A. (together with its subsidiaries and branches worldwide, "Citibank"), you should be aware that none of the other financial instruments mentioned in this communication (unless expressly stated otherwise) are (i) insured by the Federal Deposit Insurance Corporation or any other governmental authority, or (ii) deposits or other obligations of, or guaranteed by, Citibank or any other insured depository institution. This communication contains data compilations, writings and information that are proprietary to the Firm and protected under copyright and other intellectual property laws, and may not be redistributed or otherwise transmitted by you to any other person for any purpose.

IRS Circular 230 Disclosure: Citi and its employees are not in the business of providing, and do not provide, tax or legal advice to any taxpayer outside of Citi. Any statements in this Communication to tax matters were not intended or written to be used, and cannot be used or relied upon, by any taxpayer for the purpose of avoiding tax penalties. Any such taxpayer should seek advice based on the taxpayer's particular circumstances from an independent tax advisor.

© 2023 Citigroup Global Markets Inc. Member SIPC. All rights reserved. Citi and Citi and Arc Design are trademarks and service marks of Citigroup Inc. or its affiliates and are used and registered throughout the world.

NOW / NEXT

Key Insights regarding the future of Blockchain

CURRENCY

Out of the 100+ central banks involved in central bank digital currency (CBDC) research, development, and pilot, only three central banks have officially launched its CBDC – Nigeria, the Bahamas, and Jamaica. / Major central banks, including India, the UK, China, and the European Union are planning to launch a CBDC during the 2020s.

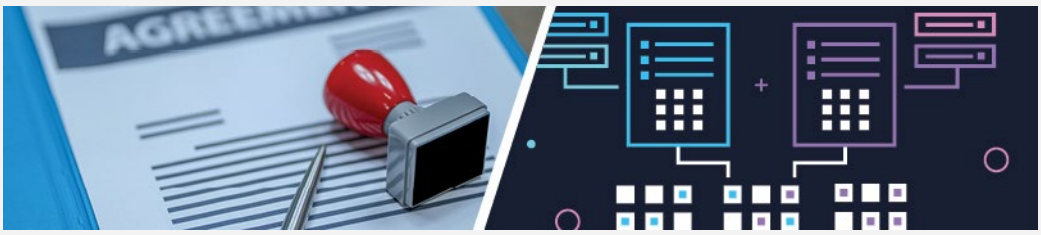
Click Here to Add Graphic

INFRASTRUCTURE

Today, different parts of the financial market infrastructure run on different rails. For example, payments run on a different tech stack than asset discovery, pre-trade matching, clearing, and settlement. / The end state is a vision of a digitally native financial asset infrastructure with smart contract and DLT-enabled capabilities. And potentially using a shared "golden-source" infrastructure.

REGULATION

Smart legal contracts are not yet widely adopted but work is starting – with the UK leading the way –on analyzing any regulatory barriers to innovation. / The creation of regulatory sandboxes to test out application of technologies under the eye of regulators could help smart legal contracts gain mass adoption.



© 2023 Citigroup

© 2023 Citigroup