TL;DR: The Blockchain

Sumeet H. Chugani

> Whereas most technologies tend to automate workers on the periphery doing menial tasks, blockchains automate away the center. Instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly.
>
> —Vitalik Buterin (Co-founder, Ethereum)

A blockchain is a distributed database or ledger, shared among the nodes of a computer network. Blockchains store information in "blocks" which are linked together via cryptography. Different types of information can be stored on a blockchain, but its primary utility is to serve as a ledger—maintaining a secure and decentralized record of transactions for cryptocurrency systems.

The best-known blockchain, Bitcoin, is decentralized, so that no single person or group has control over the network. Instead, copies of the blockchain are stored across various parts of the network, creating a distributed record of all transactions. This data is immutable—that is, it is unable to be altered by any single user or centralized party. Because there is no ability to alter data recorded on the blockchain, the only trust needed is at the point where a user enters the data. This eliminates the need for trusted third-parties—or intermediaries.

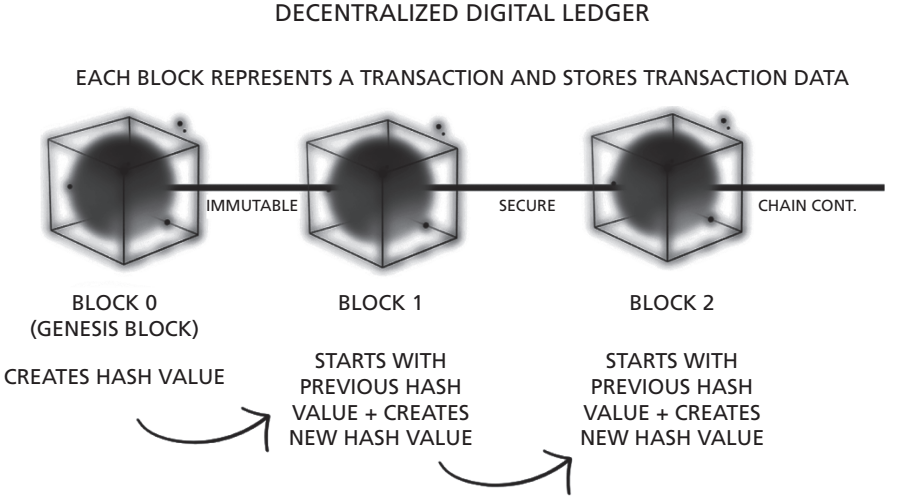
A blockchain has similarities to a database. The key difference with a blockchain is how the data is structured, organized, and accessed. A blockchain consists of "scripts" that conduct the tasks usual for a database: accessing, saving, organizing, and storing information. A blockchain is distributed, meaning that multiple copies are saved on multiple machines, and they all must match to be valid. A blockchain collects transaction information and enters it into a block, akin to a cell and a spreadsheet. Once the block is full, its information is run through an encryption algorithm, creating a hexadecimal number, called the hash.

The hash is then entered into the following block, header and encrypted with other information in the block. This creates a series of blocks "chained" together.

The entire network works simultaneously, trying to solve a hash. Each node generates a random hash, except for the nonce ("number used once"). Each miner starts with a nonce of zero, which is appended to their randomly generated hash. If that number (0+ the randomly generated hash) isn't equal or less than the target hash, a value of one is added to the nonce, and a new block hash is generated. This process continues until one of the miners generates a valid hash, which solves the problem, wins the race and generates a reward in the form of cryptocurrency. Generating random hashes until a specific value is found is the proof of work process. It proves the miner did the work.

Blockchain decentralization is created because a blockchain allows the data in a database to be spread out among several network nodes (computers running software for the blockchain) at various locations. If one node attempts to alter a record, other nodes would prevent it. No single node within the network can alter information held within the database.

Blockchains' uses have grown considerably through creation of various cryptocurrencies, decentralized finance (DeFi) applications, non-fungible tokens (NFTs), smart contracts, and now-banking.



Setting the Table

Sumeet H. Chugani, Stephen T. Gannon, Ciaran McMullan

Is Banking [on] Blockchain the Future of Financial Services? …

> Video killed the Radio Star … put the blame on VCR … in my mind and in my car, we can't rewind, we've gone too far …
>
> —The Buggles (1979)

Blockchains and digital assets are the most highly discussed and controversial technologies hitting financial services in the last 30 years. They also are the most volatile. Beginning in mid-2022, with the implosion of Terra Luna, the crypto market descended into "crypto winter." By mid-2023, that same market was recovering—and by early 2024 the market cap for digital assets touched $2 trillion and the price of Bitcoin surpassed $60,000—with BTC halving on the horizon.

Despite the robust performance, 2022 and 2023 brought into sharp focus striking business model weaknesses in early-stage blue-chip crypto firms (Terra Luna, Voyager, Celsius, BlockFi, and Three Arrows, to name a few) as well as shining light on outright fraud (FTX). Despite continued institutional investment, crypto's institutional failures such as IMB and Maersk's "TradeLens" venture can't be ignored. They are, however, a source of learning. The TradeLens project was too complex and unable to overcome dependence on globally ubiquitous bills of lading. And, the project failed to recognize the disruptive nature of blockchain innovation, as described by Clayton Christensen in The Innovator's Dilemma (Harvard Business School Press, 1997, 2000, 2016).

Blockchain and digital asset innovation can be viewed as similar to innovation in social media. Established players are ill-equipped to build the tools, technologies, and platforms to drive innovation and mass adoption. Startups are well suited for the task. Their decision-making cycles are short, internal changes required for adaptation are minimal, and new technology can be quickly assimilated. This is evident in payments, gaming, and social

media and recently in crypto-specific advancements like decentralized identity and decentralized physical infrastructure networks.

Progress rarely moves in a straight line. When MTV opened its service in August 1981 alongside The Buggles' Classic, few anticipated Compact Discs (CDs), and streaming was … science fiction. Even when the future is uncertain, developers build toward real-world use cases and cross the bridge from early adopters to mainstream users. This is the financial evolutionary process, in which the strong [and the compliant] will survive and thrive.

In the midst of the build, we must understand how banks are dealing with blockchain technology and digital assets. Given that banks are centralized bodies regulated by a central government, one may pose why they need blockchain and/or digital assets at all. Below, Ciaran McMullan raises those exact questions.

One answer is security. Blockchain decentralization improves security by lowering the threat of a single point of failure or cyber-attack. A second is inclusion, by giving access to banking services in underserved or remote areas typically out of the reach of traditional centralized platforms. A third is speed of transactions, particularly globally since blockchains unlike most centralized systems, operate 24/7/365. A fourth is efficiency in the improvement of corporate operations. A fifth is the advent of tokenization into the capital markets. A sixth is to manage the generational shift to a more digital-based economy. (One survey indicates 77% of millennials are interested in cryptocurrencies and want to learn more.) A seventh is to be able to assist small and medium-sized businesses (SMBs) adopt blockchain technology with an eye toward solutions, such as Robinhood's Connect (easier customer onboarding for conversion of fiat to crypto), Corner Market (introducing blockchain benefits to small businesses) and Metis (a Layer-2 solution offering a user-friendly, no-code environment for SMB blockchain adoption). An eighth is to be prepared for the convergence of digital assets and monetary policy, often expressed in terms of the potential adoption of Central Bank Digital Currencies (CBDCs). Finally, it is simply prudent to be prepared for what is coming next. One does not want to be building battleships when your competitors are designing aircraft carriers. The recent joint request by bank trade groups asking the SEC to amend Staff Accounting Bulletin 121 to allow banks to act as custodians for Bitcoin ETFs appears to be a recognition of a willingness to adopt crypto solutions that make sense for bank business models.

There are arguments to be made for and against blockchains and digital assets. We summarize many of them in this Preface as well as in this book as a whole. We don't presume in this publication to resolve all of them. The debate rages on today by policy-makers, in courts, in legislatures, in boardrooms and, perhaps most importantly, on the Slack, Reddit, and Discord channels of digital asset developers. This book is to identify those arguments and to frame the legal issues which have and which are likely to arise. However, one cannot safely think that the issues have been mastered or even fully understood. These are cutting-edge issues, driven by evolving technology and moving regulations, that likely have already changed by the time this book's ink dries. But handling change and crafting solutions is where lawyers excel. This is just the beginning, so let's get started with a quick overview of some of the basics.

Benefits

The benefits of blockchain and digital assets are well known. Blockchains, smart contracts, and digital assets offer a full-stack payment system providing security, immutability,

flexibility, and speed. Moreover, tokenized real-world assets have begun to take their place within financial services. For example, in late 2023, the municipal government in Shanghai, China [population 24 million, seventh largest in the world] released a road map to achieve blockchain breakthroughs by 2025. China intends to construct a basic service platform for the municipality which will support government affairs, cross-border trade, supply chain finance, transportation, an industrial Internet of Things, carbon management, metaverse, data element circulation and zero-knowledge proofs. And, new use cases continue to emerge. For example, stablcoins continue to be useful tools within which to conduct commerce across blockchains and their transparency has been increasing. Moreover, certain analysts believe XRP could play a role amid calls for gold-backed stable coins. In fact, the World Bank, the IMF and the World Gold Council have been openly discussing the need for a gold-backed stablecoin through which central banks might tokenize gold reserves.

Challenges

Blockchains challenges are well-known. Proof of work blockchains can be slow and difficult to scale. Different blockchains usually are not compatible with one another. Cross-chain linkages can be vulnerable to hacking. Adverse users can take the pseudo-anonymity of blockchain, complicate it with devices such as mixers, and use it as a method of transferring illicit funds. Dispute resolution frameworks have not been fully crafted including, for example, the legal standing of blockchain stored documents. Thus, overall, there is now and will be ample work for lawyers to do in analyzing and solving the various legal issues which will arise as the framework for this technology is evolving.

Talent/Liquidity/Capital

No industry sector will succeed without an ability to attract talent and generate liquidity. For now, blockchain and digital asset projects continue to attract talent and capital as past negatives are addressed. Problems of scalability, speed and security are being tackled. For example, transaction speed per second on some blockchains has now crossed the 100,000 transaction per second threshold. Entities such as Chainalysis, Elliptic, Crowd Strike and others have improved the tools to mitigate crypto sanctions evasion risk. The security of blockchains have improved and law-enforcement officials have become more effective at tracing stolen funds. Energy consumption concerns are also being addressed as proof of stake, consensus mechanisms, grow in number, and as proof of work technologies increasingly rely on the use of renewable energy and can become primary tools for removing carbon pollutants such as methane.

The recent approval of eleven spot bitcoin ETFs has significantly broadened liquidity for the industry, and improved credibility. Projects such as JP Morgan's Onyx are now scaling. Institutions such as BNY Mellon (custody); Fidelity (crypto funds); Deutsche Bank (custody, tokenized assets); Visa (payments), DTCC (clearing) and PayPal (stablecoins) all have entered the fray with their own products and projects. While the New York State Department of Financial Services (DFS) recently granted Wisdom Tree a charter to operate as a limited purpose trust company, allowing it to custody digital assets as well as issue, exchange, and manage the reserves of DFS-approved stable coins. It is unlikely that disciplined institutional players would fund blockchain and digital asset projects without an expectation of returns.

While debates remain, the markets have confirmed blockchain and digital assets are more than a mere bubble. The recent performance of the sector, on the other hand, tends to demonstrate its resilience and likely staying power. In a broader sense, the availability of spot Bitcoin ETF in the U.S. has advanced this trend and could potentially lead to the creation of more complex derivative products that rely on compliance-friendly spot ETFs, as a source of liquidity. Institutional adoption and support remains strong and one-third of institutional investors increased their crypto allocations in 2023.

Further, the reemergence of tokenization suggests that the capital efficiency of having an instantaneous settlement on repos, bonds, and other capital markets instruments is becoming more relevant. For example, in February 2024, Citibank used Layer-1 blockchain Avalanche's Spruce Subnet to explore the tokenization of private equity funds to re-architect capital markets. Citi worked with traditional financial entities WisdomTree and Wellington Management to carry out its proof-of-concept trial that was issued on Avalanche's Spruce, an Evergreen subnet designed for large financial institutions looking to use public blockchain infrastructure. tZero, Securitize, and Polymath are some of the market leaders in this space, using their platforms to transform private market securities through the use of smart contracts on the blockchain to create digital shares that can be traded on Alternative Trading Systems (ATSs).

Decentralization

The promise of decentralization continues to have powerful appeal. Banks must deploy numerous and expensive intermediaries to provide their services in an efficient, and safe and sound manner. The lower cost of immediate settlement and customer empowerment offered by blockchain projects continue to be attractive to small investors around the globe. Among the best-known use cases are remittances powered by crypto providing greater financial security to individuals living in countries with unstable financial systems. Moreover, while there is little risk in the short term of a global de-dollarization or a substantial decline in the use of the dollar as the world's reserve currency (an advantage which former French President Giscard d'Estaing referred to as the "privilege exorbitant"), it also is true that policymakers across the globe are looking closely at the weaponization of global finance as a result of the increased U.S. sanctions on Russia. This has accelerated interest in developing new cross-border payment solutions as more countries are striking bilateral agreements to reduce their dependence on the dollar. For example, perhaps ominously, both France and Brazil have started to settle commodity trades in Chinese renminbi. In addition, trials continue to be conducted with CBDC's to avoid today's cumbersome system of correspondent banks. Decentralization is not yet even a small wave, but it is an identifiable ripple in the water that appears to be gaining momentum.

Infrastructure

Besides transaction speeds, the industry is tackling weaknesses of interoperability and liquidity. For example, the Depository Trust Clearing Corporation (DTCC), along with Euroclear and ClearStream, recently released a joint industry paper (footnote to citation), highlighting how they can help develop and improve the digital asset markets of the future and play a role in the distributed ledger technology (DLT) based market. DTCC recently

acquired Securrency, a crypto infrastructure, firm, providing institutional grade compliance, and interoperability. The CEO of Securrency, Nadine Chaker, commented on the acquisition: "We are excited to bring DTCC's infrastructure capabilities with Securrency's technology to embrace a future with a digitization of capital markets that is at the forefront of innovation … [W]e will unlock opportunities to reimagine compliance, liquidity, efficiency, and interoperability in trading real world assets on the blockchain." The point, of course, is to have disparate platforms begin to interact with one another. Moreover, the continuing challenges of digital assets in connection with scalability and interoperability are being improved with Layer 2 solutions to either handle transactions off chain or in connection with other solutions such as sharding, batching, or consolidating on the main blockchain.

Regulatory Uncertainty

While the legislative and regulatory environment in the United States continues to be uncertain, there is an expectation that pending cases will be resolved, at least at the trial level, in the coming year and that those decisions will provide some guidance (even if not fully consistent) to the industry. There also is no shortage of proposed legislative solutions being offered, as we review in Chapter 1. Moreover, regulation outside the U.S., including the EU, the U.K., Singapore, Dubai, Brazil, and Canada continues to advance and add stability to what entrepreneurs can expect in the global market. The approval of spot Bitcoin ETF applications by the SEC may be the precursor to greater regulatory clarity removing much of the friction that otherwise has inhibited capital from flowing into this asset class. For example, the growth of Bullish, a digital asset exchange founded in 2021 and run by Tom Farley, former president of the NYSE. Bullish has been regulated from the beginning, just not by U.S. regulators. It secured a distributed ledger technology license from the Gibraltar Financial Services Commission in November 2021 before opening access to customers in select jurisdictions across Asia Pacific, Europe, Africa, and Latin America. It also has exploring licensing options in Hong Kong and Germany. It is audited by accounting firm, Deloitte, evidencing its commitment to transparency. It's customers go through a rigorous KYC, AML, and sanctions screening process before being on-boarded to the exchange. It also is well capitalized, often using its balance sheet to provide liquidity. Thus, despite the lack of U.S. licensing, Bullish was recently ranked fourth, by spot volume, for bitcoin by the Coin Metrics Market Data Feed. This may be the blueprint for what lies ahead—integrity, ample, mature management, transparency, and reasonable regulation.

We Are in the Starting Blocks

Much remains to broaden and deepen the adoption of blockchain and digital assets. Of course, the industry is in its infancy—approximately the same point at which air travel found itself in 1920. Over-indexing what may appear to be spectacular successes or failures (but which may only be point-in-time factoids) is mistaken. There is a path to broader adoption and success, but it remains uphill. And, it is marked with legal issues at each and every turn. The U.S. regulatory framework simply has not been written, and for some time is likely to be written by U.S. judges, and not by regulators. While this presents its challenges, other markets are showing the way to a convergence of innovation, products, benefits, and reasoned regulation that eventually will migrate to the United States. Thus,

this book is, more than anything, about what the very early innings in this industry look like now and how best to advise your clients on how to navigate through an ecosystem that is developing and changing even as this is written.

Banking's integration of Blockchain will be a high mountain—with a sharp angle of ascent. This book details those challenges that appear today, how they can be overcome, and the future of Banking [on] Blockchain.

… Or, Will Blockchain and Digital Assets Be a Passing Fad?

In many environments, the strengths of blockchain and digital assets also act as barriers to broader adoption. For blockchain and digital assets to go mainstream in banking, thoughtful criticisms must be recognized, analyzed, and answered. This debate must be viewed as productive since it focuses attention on the current gaps in a blockchain-based system which require problem-solving today and in the near future.

The fundamental characteristics of a blockchain are at the center of these concerns. At the most basic level, a blockchain is a distributed copy of a simple debit/credit ledger. The most important design principle of Satoshi's blockchain was that it had to be trustless, meaning it had to securely transfer a digital asset, and users needed to trust it without the need for a central authority. Moreover, it had to be: (1) pseudo- anonymous, (2) immutable, (3) censorship resistant, (4) consensus-based, to maintain the integrity of the system, and (5) public, meaning anyone could see the history of all Bitcoin transactions since the inception of the system.

Are the Core Features of Blockchain Incongruous with Modern Banking?

Pseudo-Anonymity

Pseudo-anonymity impedes the efficient application of anti-money laundering regulations, a key requirement for any banking entity. Unlike any other medium of exchange, crypto is the only one that offers the ability to move extremely high-value amounts, extremely quickly and irreversibly. While most blockchain analytics firms track the use of illicit on-chain transactions, they often overlook the much larger problems created by obfuscation methods (such as mixers) and off-chain criminal proceeds that are laundered using crypto.

Immutability

The complexity of modern life and the speed with which technology has enabled decision-making, especially around payments and investments, dictates the ability to investigate and, where necessary, reverse transactions (such as in the case of fraud) is both critical and, in many cases, expected. Because reversing entries on a blockchain is either disallowed or extraordinarily difficult, this factor can make blockchain applications unattractive to retail customers and to regulators concerned with consumer protection.

Censorship-Resistant

While this feature can be attractive from a privacy point of view, the lack of a central authority allows any actor, good or bad, to execute transactions on the blockchain which under the AML/CFT/Sanctions environment has law enforcement and operational implications.

Consensus-Based

This characteristic of the blockchain is critical to ensuring there is no need for a centralized third party. However, the process of seeking consensus may not be attractive to retail customers who prefer the reliability of familiar systems.

Lack of Scalability

As it exists today, blockchain's append only, distributed structure is fundamentally incapable of a greater level of efficiency than a centralized, programmable database. Basic knowledge of queuing theory in mathematics illustrates the fact that the mining/consensus aspect of the technology may render it slower than a centralized system. Blockchain's highest and best use is the self-custody, ownership and transfer of a digital asset without the need for central authority. Banking and financial services, however, are increasingly high-volume businesses with a growing desire for instantaneous payment and finality. Given the characteristics of blockchain described above, significant additional work needs to be done to be able to handle high volume transactions with a short time scale finality. Those that are achieving higher speeds have done so by removing key aspects of the blockchain, such as decentralization and unhackable security. And, of course, once centralization is introduced into a blockchain environment, the argument for the blockchain itself diminishes.

Current Technology May Still Be Fit for Purpose

Centralized programmable databases/ledgers have been the basis of the banking system for decades and have proven to be efficient and robust. However, today's technology is not what hinders faster settlement, but rather the agreements, pricing and procedures utilized by participants in the process. Blockchain's solution to this particular problem is not technological, but rather is the removal of the trusted intermediaries required within our modern regulatory and financial structure via, for example, smart contracts.

Moreover, global payment systems have upped their game significantly. WISE allows for international remittances in a matter of seconds, and HSBC can instantaneously transfer high value amounts between accounts in multiple jurisdictions. At the domestic level, The Clearinghouse's Real Time Payments and the FRB's "FedNow" will soon make immediate payments ubiquitous for customers and businesses alike. Thus, it is puzzling why so much investment is being poured into overcoming the fundamental inadequacies of the "base" blockchain when fully functional alternatives exist today.

What, Then, Is Driving the Interest?

There can be no contesting the fact that significant amounts of capital [and space on the internet] have migrated into this relatively new corner of financial services. There are four things which account for this, and not all of them are good.

New Blockchains

First, new actors began to build their own blockchains with additional features and computational power above that offered by Bitcoin, Ethereum being the most well-known.

Designed by Vitalik Buterin, it goes beyond using the blockchain and its associated cryptocurrency (Ether, or ETH) as a store of value by designing the Ethereum blockchain (also known as the Ethereum Virtual Machine or EVM) to be used as a platform for development using smart contracts, as well as enabling the creation of non-native cryptocurrencies and non-fungible tokens (NFTs). Buterin's groundbreaking work encouraged others to design their own blockchains, such as Cardano and Solana. Hundreds of blockchains began to emerge, each with its own theory of value creation and investment.

The Hype Machine Began to Operate

In the late 20-teens and early 2020s blockchain and digital assets became among the most popular projects to write about on the internet. The amount of electronic ink spilled on this topic was stupendous. That intense focus and attention naturally drove interest amongst the investment class.

Venture Capital Provided Support for the Hype

As projects began to develop and promised spectacular returns, and as interest rates stayed low and liquidity remained plentiful, Venture Capital stepped behind blockchains and digital assets in a very substantial manner. In part, this was driven by the venture capital community's emphasis on (and comfort with) risk-based assets, as well as its well-known fear of missing out (FOMO, or the greater fool theory). The inadequate level of due diligence conducted with respect to projects such as Terra/Luna and FTX confirms what was at play. At the time, however, "move fast and break things" made sense.

Traditional Industry Players Added Credibility by Launching Their Own Blockchain Projects

As blockchain and digital asset products began to proliferate, they became part of the mainstream corporate innovation discussion. As a result, many of the world's largest companies decided to analyze blockchain technology and its potential to fundamentally improve their operations. Many of those companies made public announcements, hoping to ride the positive market sentiment around blockchain, which, in turn, added credibility to the sector.

Permissioned Blockchains

Many blockchain projects have launched at industrial scale. Few have landed fully intact. The vast majority of use cases being explored by the banking and financial services industry are using a *derivative* of blockchain technology called permissioned blockchains.

As mainstream players started to investigate the utility of blockchain and digital assets, they found it necessary to forfeit some of the fundamental characteristics of a blockchain in order to apply it to current corporate issues. In general, they eschewed many of blockchain's fundamental characteristics, including pseudo-anonymity, censorship resistance, public accessibility, and consensus-based approval.

While permissioned blockchains have many useful characteristics, the current variant is not the blockchain designed by Satoshi's Bitcoin innovation in 2009. In fact, permissioned blockchains are much more akin to a multi-user access, centralized and programmable

database. In many cases, these permissioned blockchains are used for tokenization, such as with deposits and bonds, though they have not yet caught on at scale nor resulted in meaningfully liquid markets. Moreover, tokenization with respect to real estate and other real world assets continues to require reform of existing laws and systems for enforcing ownership—an area for legal innovation, to be sure. However, this kind of fractionalization will have to compete with prior legal innovations such as REITs. multi-member LLC, as well as product offerings from FinTech pioneers such as Robinhood and Block's CashApp.

Failed Large-Scale Corporate Projects

The success rates of large-scale commercial projects still leaves much to be desired. Recently, the *Journal of The British Blockchain Association* analyzed over 500 blockchain firms, finding that only 6.2% of projects provided evidence of a real business problem being identified, and even fewer projects (5.8%) analyzed the project architecture against alternative technologies, and only 1.5% used filtered, that is, hard evidence, to consider program outcomes.

There also are several high profile failed corporate projects where the lessons learned are available.

- Australian Stock Exchange (ASX). This project was designed to replace ASX's existing settlement system, known as CHESS. It was launched in 2015 and shut down in 2022, causing ASX to take a $200 million pre-tax write off. ASX's former CFO said: "It would have been easier to just build a new version of CHESS in some other modern language rather than blockchain."
- Lygon. Once lauded as the future of banking, this was a joint venture between various Australian banks to digitize bank guarantees using blockchain technology. It collapsed at the end of 2023.
- Maersk/IBM. This joint venture launched a new platform called TradeLens to track global trade and shipping. It was launched in 2018 and shut down in 2023. According to the *Wall Street Journal*, "the technology is complex, requires more computing power and is more expensive to run than existing databases."
- Commonwealth Bank/NDIS. This project was intended to automate benefit payments for the Australian government's National Disability Insurance Scheme (NIDS). Launched as a nationwide pilot program in 2018, it was subsequently discontinued. An independent review of the project was carried out by the National Science Agency and found "While these results for the proof of concept are positive, they could also likely be achieved by a centralized database solution."

In the end, none can argue with the laudable goal of financial democratization, which could be achieved through greater decentralization and fractionalization. The question is whether the underlying tools, that is, blockchains and digital assets, include the basic utilities needed to achieve these goals *at scale*. Thus, one needs to ask whether, once the excitement of speculation has faded, are the long term use cases for blockchains and digital assets capable of delivering value exceeding the required technological investment? After

all, banks exist to return capital and profits to their investors. Thus, until that question can be answered affirmatively, the impact of blockchains and digital assets banking and financial services will remain open to challenge.

The Blockchain Hype Story—Visualized