The New York City Blockchain Plan

December 2025

Table of Contents

Note: *The New York City Blockchain Plan is subject to applicable laws, rules, and regulations, including City procurement rules and processes. The City reserves all rights, including rights to postpone, cancel, or amend the Blockchain Plan at any time. The City shall not be liable for any costs incurred in connection with the Blockchain Plan.*

Cover Photo: Tagger Yancey IV, NYC & Co.

Letter from the CTO

My Fellow New Yorkers:

For the past four years, New York City government boldly embraced technology like never before to enhance public safety, increase affordability, and make government run better. We pursued technology-based solutions not for technology's sake nor to chase trends; we did this, responsibly and thoughtfully, to bring you the best version of New York City we could provide.

When we talk about ways to better serve New Yorkers, the massive promise of blockchain cannot be ignored. New York City is the fintech capital of the world, with incredible resources and talent at its disposal. It would be a disservice to New Yorkers if we did not examine what blockchain could do to unlock a more efficient, modern city government to meet your needs.

I am proud then to announce the New York City Blockchain Plan, a first-of-its-kind framework by a major American city to support exploration and use of this technology across city government. Developed over the past 18 months, this wide-ranging strategy lays the foundation for city agencies to investigate potential opportunities and risks, build public literacy on emerging technologies, and establish mechanisms to track progress and coordinate citywide efforts. In doing so, it advances the blockchain-related goals of Mayor Adams' Executive Order 57.

I look forward to this plan providing a robust foundation to test and deploy city applications of blockchain to benefit New Yorkers in the coming years.

Matthew C. Fraser
Chief Technology Officer

Executive Summary

Blockchain is a fast-growing technology attracting intense global interest and development. Originally designed to enable Bitcoin, the first decentralized form of electronic money, blockchain has grown to power new uses including digital identity management, supply chains, and government operations, among others. Recent policy shifts in digital assets regulation have spurred new growth and experimentation. In 2025, for example, the number of digital assets founders in New York City grew by 30 percent, reflecting rising entrepreneurial activity in the city's blockchain ecosystem.[1] And this local growth tracks with international trends. For example, global digital-asset ownership worldwide grew by nearly 16 percent in 2025, while services have rapidly expanded to offer new features and integrate new technologies.[2] In this context, public and private organizations are committing considerable time and resources to better understand this emerging technology, identify its opportunities and challenges, and chart a responsible path forward.

As a global innovation hub, New York City is uniquely positioned to lead on blockchain exploration. The NYC Blockchain Plan - the first comprehensive city-level report of its kind in the United States – declares our ambitions and lays the foundation for future citywide efforts. This practical framework outlines how New York City should evaluate, pilot and govern blockchain technology, and defines critical steps the city must take to prepare for growing interactions with blockchain outside of government. While the full impact of blockchain on city work might seem distant today, the technology is already raising new questions and opportunities for city service delivery. For this reason, it warrants thoughtful and proactive examination now.

Why this matters for New York City.

As blockchain has matured beyond speculative trading, its potential value for government has become clearer: offering trust in shared records, transparency across stakeholders, tamper-resistant data that's hard to alter, and efficiency through automation. At the same time, blockchain applications introduce certain risks related to privacy, data security, systems integration, cost, and environmental impact. For New York City, the opportunity lies not in adopting blockchain for its own sake, but in creating the structures to responsibly pilot, evaluate, and deploy it where it can genuinely improve government services and enhance equity, accountability, and public trust. As the city looks ahead, opportunities exist to investigate new applications, and develop new frameworks for responsible use.

As blockchain adoption expands across sectors, city agencies will need to adapt to new realities in education, law enforcement and financial management. Building new capacities, methods, and programs will be essential to ensuring agencies can meet their missions in a changing environment.

New York City government has explored blockchain in a set of targeted, experimental efforts for select uses cases – most notably in land records. Agencies are also using blockchain analytics tools to trace illicit activity tied to digital assets, complementing traditional investigative methods. And the city has invested in early educational tools, as well as broader local ecosystem capacity – from supporting a public Ethereum node, to applied learning through local universities, to hosting the NYC Blockchain Week – all in an effort to support literacy and responsible innovation. There is clear opportunity to build on these foundations and take the city's efforts to the next stage.

Key findings from our research.

To better understand the current state of blockchain technology and policy, and in particular, the opportunities and challenges that exist for New York City, the Office of Technology and Innovation (OTI) interviewed over 50 organizations across city agencies, other governments, academia, industry, and civil society. OTI also conducted extensive research, including a review of more than 100 public-sector use cases and policy interventions across all levels of government worldwide.[3]

This research produced the following key findings:

- ***Fit-for-purpose, not first-to-adopt.*** Blockchain is not a one-size-fits-all solution. It is most promising where many parties must share verifiable records and automation can reduce reconciliation and error.
- ***Trade-offs are real.*** Choices among decentralization, security, privacy, scalability, and cost drive whether an implementation is viable in government. These trade-offs must be carefully weighed against each other. And more broadly, blockchain's risks must be weighed against its benefits for a given implementation. All New York City efforts must comply with city privacy, cybersecurity, and climate standards.
- ***Integration and governance decide success.*** The biggest blockers to successful blockchain use are not technological but institutional: legal recognition, legacy system integration, technology governance, and sustained interagency coordination.
- ***Education and capacity building are essential.*** Staff literacy and resident education are prerequisites for responsible exploration. New resources will be needed to ensure that both agencies and the public are prepared to navigate blockchain and digital assets safely and effectively.
- ***The technology and policy landscapes are evolving rapidly***. The blockchain ecosystem is advancing quickly, while state and federal policy frameworks are also developing in parallel. New York City must continuously track both technology and policy changes, to ensure its efforts keep pace, and account for new opportunities and risks as they emerge.

What's in this Plan.

The NYC Blockchain Plan provides foundational information about how blockchain works, its promises and limitations, and how different types and uses of blockchain affect government decision-making. It details how blockchain has been explored in government contexts across the globe, describes the current policy landscape, and reviews key opportunities and challenges for New York City. Finally, it outlines key strategic priorities for the work ahead and details twelve new commitments the city will undertake toward addressing them. A summary of these priorities and commitments is below:

<u>Priority 1: Support City Agencies to Explore and Navigate Blockchain</u>

- 1.1. Launch NYC Blockchain Interagency Working Group: Coordinate standards, share lessons, align on requirements.
- 1.2 Pilot Use Cases: Scope an exploratory pilot on asbestos certification verification with the NYC Department of Environmental Protection (DEP).

- 1.3 Provide Technical Criteria and Guidance: Practical criteria covering feasibility, legal alignment, privacy/security, equity, access, public benefit.
- 1.4 Strengthen the City's Capacity to Address Illicit Activity Risks: expand access to analytics and knowledge resources across relevant teams.

Priority 2: Foster Staff and Resident Literacy

- 2.1 Launch a Literacy & Innovation Series: Case-based learning for agency staff.
- 2.2 Create an Information Hub: Public education, consumer safety, and city updates in one place.
- 2.3 Facilitate Community Safety Resources: Scam-prevention and awareness materials with partners.
- 2.4 Seek Education Partnerships: Support NYC Public Schools (NYCPS) and City University of New York (CUNY) on standards-aligned literacy and hands-on learning with responsible guardrails.

Priority 3: Track, Review, and Adapt

- 3.1 Launch Risk & Opportunity Reviews Process: Periodic reassessment to update priorities and respond to new developments.
- 3.2 Monitor Policy Developments: Translate state/federal shifts into city guidance.
- 3.3 Examine Adjacent Tech: Identity, wallets, and related tools.
- 3.4 Public Progress: Transparent reporting on plan implementation.

The city encourages questions and feedback about this plan, at blockchain@oti.nyc.gov.

Photo: Julienne Schaer, NYC & Co.

Introduction

At a high level, the Office of Technology and Innovation (OTI) developed this report to help New York City understand the current state of blockchain technology, where its opportunities and challenges exist, and how city government should act accordingly. It is designed as both a reference and roadmap, guiding readers through what blockchain is, how it is being used globally, and what it could mean for city work.

More concretely, this plan is written for city agencies, policymakers, and civic partners who make decisions about technology, data, innovation, and service delivery. Technologists will find a concise explanation of the technology, potential government use cases, and key considerations and trade-offs to keep in mind. Policy and legal teams will find a roadmap for responsible governance. Service providers will find an overview of the technology and policy landscape, and how it may stand to impact their efforts to serve and support New Yorkers. Civic organizations, educators, and residents can use this report to understand how the city is approaching blockchain with transparency and public benefit in mind.

Each of the five sections in this Plan builds on the last:

- Section 1: **Blockchain Technology** provides a primer on how blockchain works, the differences between public, private, and hybrid systems, and why these distinctions matter for government. Readers familiar with the technology can skip ahead, but those working in city technology, operational, service delivery, or policy teams are encouraged to review this section closely.
- Section 2: **Use of Blockchain Today** surveys over 100 government use cases worldwide and distills lessons from pilots across levels of government.
- Section 3: **Current Policy Landscape** outlines the rapidly evolving state and federal regulatory environments that shape how the city interacts with blockchain and digital assets.
- Section 4: **Opportunities and Challenges** synthesizes what the research means for New York City, identifying where blockchain may add value, what conditions must be in place for responsible use, and prudent next steps to prepare the city and its residents for interactions with blockchain in other sectors.
- Section 5: **Strategic Priorities and Initiatives** outlines the city's roadmap for responsible exploration and capacity-building. It centers on three priorities: supporting agencies as they evaluate and pilot blockchain applications; building literacy among staff and residents; and tracking progress through ongoing review, monitoring, and reporting. Together, these steps create the foundation for New York City to carefully assess blockchain, strengthen institutional knowledge, and adapt as the technology and regulatory landscape evolve.

1. Blockchain Technology

Before exploring blockchain's implications and potential uses in government, it is essential to understand what the technology is, and what is it not. Many of the opportunities and risks described later in this Plan stem directly from the specific design of a given blockchain. In particular, the differences between public, private and hybrid blockchains, and the inherent trade-offs between security, privacy, and decentralization (the "blockchain trilemma") determine how and where the technology can be responsibly applied.

This section offers an overview of blockchain's key concepts, evolution, and design options. Readers already familiar with the technology may choose to skip ahead to Section 2: Use of Blockchain Today, but for most city staff, as well as a broader range of readers who are relatively new to the subject, a clear grasp of these fundamentals is essential. In particular, understanding how blockchains actually record, secure, and share data, along with the limits of what they can do, will help agencies make informed decisions about any future work.

1.1 What is Blockchain, and How Does It Work?

On a basic level, a blockchain, like other types of databases, records and organizes data. Rather than relying on a single computer or a single person or organization to manage the database, a blockchain functions as a digital "ledger" shared across many computers. Data on a blockchain is held and maintained collectively by these computers, called "nodes," which work together to verify and maintain the ledger's accuracy. In this sense, the system is "decentralized," meaning no single entity controls it.

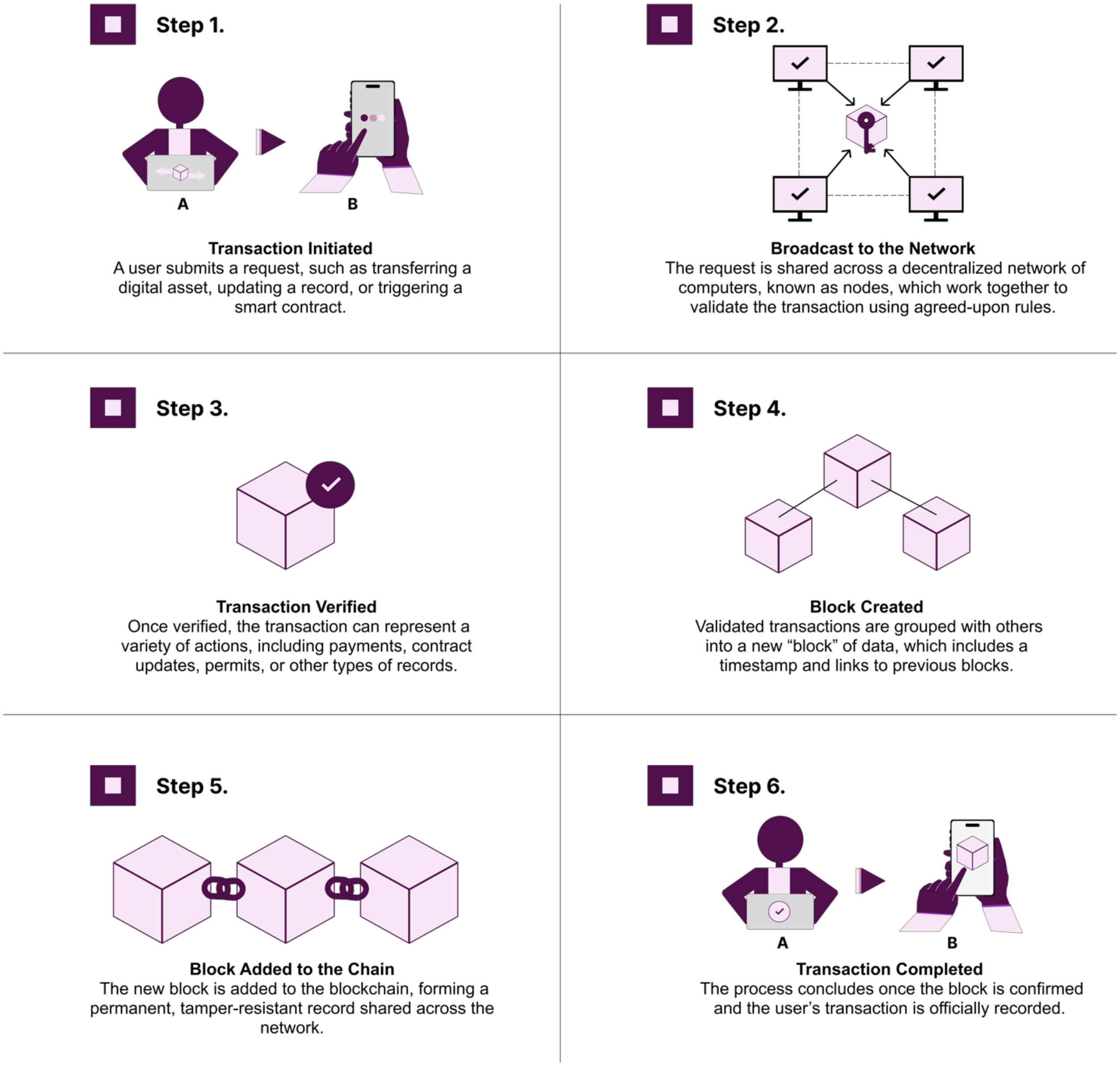
Even though blockchains are decentralized, they are not unstructured. Each system operates according to a set of predefined rules encoded in its protocol. These rules determine who can participate, how transactions are validated, and how new blocks are added to the ledger. In practice, they ensure that the network behaves consistently, allowing thousands of independent nodes to coordinate without a central authority.

How Blockchains Store and Secure Data

As decentralized networks, blockchains operate through a series of steps. First, when new data is submitted by a user or system interacting with the blockchain, it is recorded as a transaction. Participating nodes use a set of mutually agreed-upon rules to confirm that these transactions are valid and accurate.[4] Once verified, transactions are grouped into a "block" that contains encoded information (such as transaction details and user information), a timestamp, and a reference to the previous block. This block is then shared with the broader network, triggering additional verification. Once enough nodes confirm its validity, the block is permanently added to the chain of records - hence the term "blockchain."[5]

Under this process, data cannot be altered within one block without modifying all the blocks that come after it, a task that is computationally very complex, and so energy- and resource-intensive that it becomes economically impractical.[6] Because of this, blockchains are often described as "immutable."[7]

How Does Blockchain Work?



Step 1.

Transaction Initiated
A user submits a request, such as transferring a digital asset, updating a record, or triggering a smart contract.

Step 2.

Broadcast to the Network
The request is shared across a decentralized network of computers, known as nodes, which work together to validate the transaction using agreed-upon rules.

Step 3.

Transaction Verified
Once verified, the transaction can represent a variety of actions, including payments, contract updates, permits, or other types of records.

Step 4.

Block Created
Validated transactions are grouped with others into a new “block” of data, which includes a timestamp and links to previous blocks.

Step 5.

Block Added to the Chain
The new block is added to the blockchain, forming a permanent, tamper-resistant record shared across the network.

Step 6.

Transaction Completed
The process concludes once the block is confirmed and the user’s transaction is officially recorded.

Figure 1. Graph adapted by the NYC OTI from PricewaterhouseCoopers, Making Sense of Bitcoin, Cryptocurrency and Blockchain, (last accessed October 2025). https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html

How Are They Accessed

To use a blockchain, participants need two key pieces of information, collectively referred to as digital "keys." A "private key" works like a highly secure password that authorizes transactions. A "public key" functions like an account number that others can see and use to send data or assets. Just like a person's username and password for a banking application grants access to that person's bank account, the private key grants full control over the data or assets belonging to a user and must be kept secure. To protect private keys, people store them in digital "wallets" – either software wallets connected to the internet or hardware wallets stored offline for extra security.[8] At a high level, this system ensures that only authorized participants can access or transfer data and assets, helping maintain trust in the network.

Who Can Participate

The decentralized approach to managing data and the immutability of such data are essential characteristics of all blockchains. Additionally, many blockchains have other common features. For example, the most widely used blockchains are "open," meaning anyone can join them.[9] Many are also considered "neutral," in that they are designed to treat all users, transactions, and data the same way.[10] And these blockchains are often described as "borderless," since they can be accessed globally, just as the internet is.[11]

How They Enable Automation

In addition to the core functions of recording and organizing data, many blockchains can also be programmed with built-in rules that automatically carry out specific actions, reducing the need for intermediaries and lowering the risk of errors or fraud. These programs, known as "smart contracts," are self-executing agreements that are triggered once pre-defined conditions are met.[12] This capability gives most blockchains another key feature –automation, which can streamline processes such as verifying transactions, managing digital credentials, or enforcing compliance rules without manual oversight. Smart contracts can make data management more efficient, transparent, and reliable, which are qualities especially relevant for workflows that depend on accuracy and trust.

Key Benefits

Overall, the core benefits of blockchain technology lie in its ability, under the right conditions, to promote trust, transparency, and efficiency. Because transactions are time-stamped and recorded on a shared ledger that all participants can see, information is traceable and verifiable. Blockchain technology's tamper-evident design helps ensure records have not been altered, which can strengthen trust and accountability. Blockchains allow all participants to access the same information simultaneously, which can support transparency, and help multiple parties collaborate without depending on a single authority. These properties can improve accountability, while also reducing manual work, and potentially lowering costs. And blockchains' ability to automate certain functions can help users save time that might otherwise be allocated to manual verification, reconciliation, or paperwork.

Key Risks

In addition to these varied potential benefits, blockchain technology's characteristics and capabilities can also create a range of risks and challenges, which will be discussed in detail shortly. Key among these are data privacy and security concerns, system integration complexities, scalability limitations, the need for specialized technical expertise, and social and environmental impacts.

In light of this mix of potential benefits and risks, the city's research indicates that blockchain is not a one-size-fits-all solution. Careful consideration of the specific use case, as well as relevant technical, operational, organizational, and social factors is required to responsibly assess when and how it may be appropriate to use.

The proceeding sections will detail both how blockchain has evolved and added new capabilities over time, and some of the ways in which specific design choices can influence how different blockchains perform in terms of speed, scalability, privacy, and security. Understanding these differences is key to evaluating how a blockchain might be applied in government.

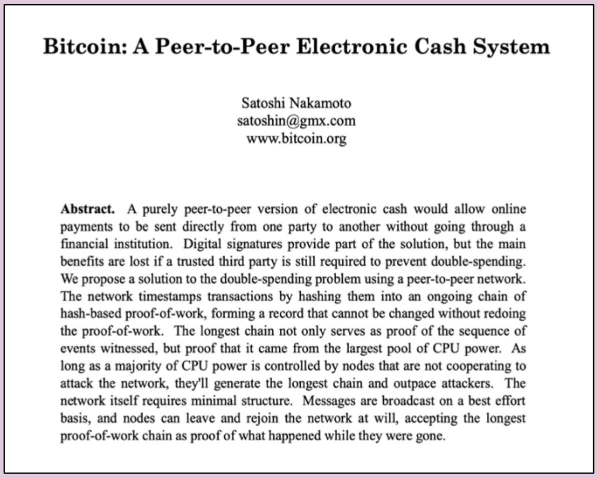
1.2 Beyond Bitcoin: The Evolution of Blockchain

The first use of blockchain emerged from a 2008 white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System," which outlined a system for transferring digital value directly between users without relying on a trusted third party.[13] The paper's author(s), Satoshi Nakamoto[14] launched a system based on this design in January of 2009, mining the first Bitcoin block, known as the "genesis block." In Bitcoin, "mining" refers to using computing power to validate transactions and add them to the blockchain in exchange for new coins, launching a new model for peer-to-peer digital money.

Bitcoin introduced the first fully decentralized digital currency and solved a longstanding challenge in digital payments called the "double-spend problem."[15] In earlier, traditional financial systems, preventing someone from spending the same unit of value more than once typically required a trusted third party, such as a bank or payment processor, to verify transactions and maintain account balances. For some, this reliance on intermediaries was considered a problem – banks could block transactions, charge fees, or exclude users altogether, whether for commercial, regulatory, or discretionary reasons. Nakamoto's innovation used a

Key Term: Cryptocurrency

The first and most commonly-referenced application of blockchain technology is as the infrastructure supporting "cryptocurrencies" such as Bitcoin. A cryptocurrency is a purely digital form of money that exists within a decentralized, blockchain-based network, and is primarily used for payments, as a store of value, or as an investment. Unlike traditional currencies, cryptocurrencies are not issued or controlled by a central authority, such as a central bank. Instead, they rely on cryptographic keys for ownership and transfer, and on distributed consensus mechanisms to validate transactions, regulate issuance, and secure the system.



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Image: Cover page of the original Bitcoin white paper, published by Satoshi Nakamoto in 2008.

consensus mechanism called Proof-of-Work (PoW) to replace the need for this centralized oversight. Instead, transactions could be verified by a distributed network of participants (the "nodes" described above), allowing for secure, peer-to-peer payments without a central authority.[17]

In its early years, Bitcoin was often called "internet money" due to its ability to function as a digital cash system for anyone who had access to the internet. However, its underlying technology, blockchain, and the open-source spirit of its developer community sparked interest beyond digital currencies. The ability to establish and verify ownership of "digital assets" across a decentralized system inspired new blockchain designs for broader purposes.

Accordingly, blockchain technology has evolved significantly since its introduction, moving over time to being a broader platform for digital applications, financial systems, and even new models of online interaction. Today, thousands of different blockchain networks exist, many of which are designed with their own distinct features and use cases in mind. Each stage of this evolution introduced technical innovations, that sought to address limitations of earlier designs while expanding what blockchain could do.

Key Term: Digital Assets

Today, blockchain supports a much broader set of applications beyond cryptocurrency. In these uses, information stored on a blockchain can take two main forms. In some cases, it is a straightforward digital record, such as a log of transactions, a registry of permits, or a record of supply chain steps. In other cases, the information represents a "digital asset," something that carries value or conveys rights, such as land titles. Digital assets can include unique items such as "tokens," which are a digital representation of assets, currency, or access rights.[16] Some tokens are unique and not interchangeable, known as non-fungible tokens (NFTs), often used for items like digital art or collectibles. Others are representations of real-world items or rights, such as credentials, licenses, access rights, or public benefits. Cryptocurrencies themselves are one type of digital asset. The process of creating these digital assets on a blockchain is often called "tokenization."

From Bitcoin's Origins to Ethereum's Innovation

Ethereum, launched in 2015, expanded blockchain's functionality by enabling not only the recording of transactions, but also the execution of programs on the blockchain. As noted above, these programs can range from simple rules to more complex applications. Commonly referred to as "smart contracts," they work to automatically enforce conditions or agreements without human intervention. Building on this capability, developers have created decentralized applications (dApps), which are applications that run on a blockchain and rely on smart contracts as their core building blocks. Together, these innovations opened the door to new uses of blockchain, such as decentralized finance (DeFi),[18] gaming, and digital identity tools.

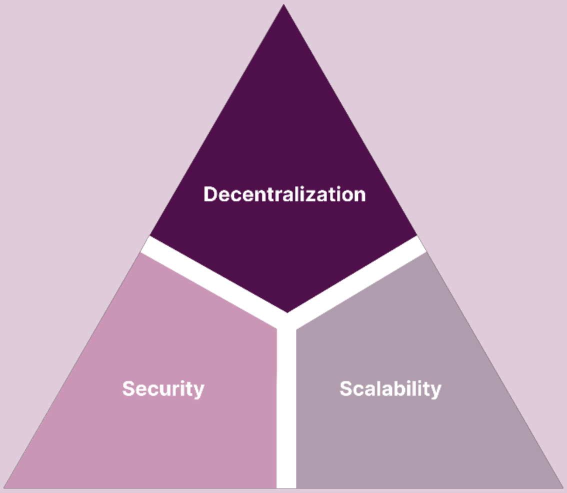
As adoption of Ethereum grew, so did its network activity, which in turn surfaced challenges around scalability, including rising transaction fees, congestion, and slower processing times during peak usage.[19] In response, developers sought to scale the network to handle growing demand. However, increasing transaction capacity often required either reducing the number of nodes involved in validation, leading to less decentralization, or using lighter and potentially less secure validation methods. The emergence of these trade-offs, potentially compromising either security or decentralization for scalability, is a challenge commonly referred to as the "blockchain trilemma."

The "Blockchain Trilemma"

Each blockchain model offers unique trade-offs, commonly referred as the "blockchain trilemma": the challenge of balancing decentralization, security, and scalability.

Most blockchains can optimize for two of these goals, but often at the expense of the third. For example, a highly decentralized and secure network (such as Bitcoin) may face limitations in speed and cost-efficiency, while a system designed for scale (such as Ethereum) may introduce more centralized controls or reduce security assurances.

These design tensions are not just technical. They shape real-world decisions about how blockchain systems function, who controls them, and how resilient they are. Section 4 of this document explores these considerations in greater detail, with a focus on how they relate to government priorities.



The Scalability Challenge: Development of Layers 2 and 3

To address the scalability challenge, many blockchain developers in recent years have created what are known as Layer 2 (L2) solutions.[20] These are protocols built on top of the base blockchain (Layer 1) that handle transactions off-chain, then post the results back to the main network. By shifting activity off the base layer, L2s can process transactions faster and at lower cost, while still relying on the security of the underlying blockchain. This approach represents a key direction in blockchain's evolution, with significant growth in the adoption of Layer 2 networks such as Optimism, Arbitrum, and Base.[21]

At the same time, critics argue that the reliance on a smaller set of operators in L2s may concentrate control and introduce new risks and vulnerabilities in the smart contracts that connect L2s to the main blockchain. This raises questions about whether scalability has come at the expense of decentralization and security.

Building upon Layer 2 solutions, focused on easing congestion and lowering costs on existing blockchains, Layer 3 (L3) solutions go a step further by tailoring networks for particular uses, such as gaming, finance, or healthcare, without forcing every application to compete on the same base chain. By providing more customized environments and smoother user experiences, such as faster confirmations and lower and more predictable fees, L3s aim to lower technical barriers and make blockchain applications more practical and accessible for everyday users.[22]

A detailed diagram illustrating these different layers, and how they work together is included in Appendix II.

Blockchain has evolved to integrate a range of complementary technologies and applications in recent years. Appendix III provides a deeper look at these advancements, including key enabling tools such as cryptographic security mechanisms, digital wallets, and oracles, as well as emerging frameworks like decentralized autonomous organizations (DAOs).

1.3 Public, Private, and Hybrid Blockchains: Why It Matters

A critical factor shaping a blockchain’s performance, scalability, privacy, security, and usability, is how it is structured at its core: whether as a public, private, or hybrid system. These design choices determine who can access and validate data, how control is distributed, and what level of transparency or confidentiality the system can offer. For governments, these differences are not merely technical. They determine whether a blockchain can meet public requirements for accountability, compliance, data protection, and interoperability. The next section introduces these three main types of blockchains, explains their key characteristics, and highlights their implications for public-sector use.

Public Blockchains

“Public” blockchains, like Bitcoin or Ethereum, are designed to be open networks where anyone can participate without approval. Because no single organization controls them, they are generally considered to be decentralized. As noted above, they are also described as neutral (open to anyone regardless of identity) and borderless (able to operate across jurisdictions much like the internet). These features make them powerful tools for transparency and censorship-resistance, but they also raise questions about how such systems could be adopted or governed at scale.

Public blockchains rely on “consensus mechanisms” like Proof-of-Work (PoW) or Proof-of-Stake (PoS) to validate transactions. While these systems are designed to maintain decentralization, the degree to which they do so can vary: PoW networks like Bitcoin maximize decentralization at the expense of speed and efficiency, whereas PoS systems such as Ethereum aim to increase scalability and lower energy use, sometimes by relying on a smaller set of validators.

In general, public blockchains are most useful for systems that require transparency, broad participation, or censorship resistance. However, if used in contexts where confidentiality is important, public chains may integrate additional measures to protect data privacy. These can include a variety of techniques, including: a) encryption; b) “zero-knowledge proofs,” which are mathematical methods that prove something is true without revealing the underlying data; or c) use of off-chain storage, which can keep sensitive data outside the blockchain, while only recording references or proofs on-chain.[23] Through the use of these additional tools, public blockchains can be configured to support secure, private interactions, even though they do not offer privacy by default. However, even with the use of these tools, public blockchains may not currently be suitable for use cases that require strict confidentiality or compliance with data protection laws or policies. Appendix III explores these challenges in more detail.

Proof-of-Work vs. Proof-of-Stake

Blockchains rely on “consensus mechanisms” to validate transactions and maintain the integrity of the ledger. Two primary approaches are Proof-of-Work (PoW) and Proof-of-Stake (PoS).

Proof-of-Work (PoW)

PoW is the consensus mechanism used by Bitcoin. It relies on a process known as “mining,” where network participants (“miners”) compete to solve complex mathematical problems. The first to solve the problem earns the right to validate the next block of transactions and is rewarded with newly-issued cryptocurrency.

PoW’s structure discourages fraud because altering past records or taking over the network would require an attacker to have control over the majority of the total network computing power, known as its “hashrate.” This would demand enormous electricity and hardware resources, making attacks highly expensive and impractical. In most cases, it is far more profitable to follow the rules and validate transactions correctly than to try to cheat the system.

Proof-of-Stake (PoS)

PoS is a consensus mechanism where validators are chosen based on the amount of cryptocurrency they hold and commit, or "stake," as collateral. In Ethereum’s PoS system, users stake “ether” (Ethereum’s native currency) to become validators, propose blocks, and vote on their validity to verify transactions and keep the network running.

Like PoW, PoS relies on a system of rewards and penalties to encourage honest behavior. Because validators risk losing their staked assets if they attempt to cheat, they are financially incentivized to act honestly.

Private Blockchains

“Private” blockchains, by contrast, may restrict access, limit participation, or rely on centralized controls. They often offer faster transaction speeds and lower costs because they involve fewer validating nodes and operate under known, trusted participants. Many blockchain implementations today, particularly in government or enterprise settings, use private or permissioned networks, where only approved participants can access or update the ledger.

These models resemble traditional IT systems and are often favored over public blockchain solutions for reasons such as policy or legal compliance, data confidentiality, or operational control. Permissioned blockchains also consume less energy than proof-of-work networks, because they rely on a smaller set of trusted validators rather than open mining competitions.[24]

Private chains can be a practical choice when transparency is less important than performance, or when sensitive data must be tightly controlled. That said, privacy in these systems still depends on how data is encrypted and stored, not simply on restricting access. Some experts argue that private blockchains end up resembling conventional databases with added complexity, since they restrict access, rely on trusted administrators, and may not fully deliver the transparency or decentralization that make public blockchains distinctive.[25] Debate continues over whether private blockchains offer significant advantages over conventional databases.[26]

Hybrid Blockchains

Hybrid blockchains combine elements of both public and private models, offering flexible architecture. In a hybrid model, some parts of the blockchain may be publicly accessible to promote transparency and accountability, while other parts remain restricted to authorized users to ensure privacy and control. For example, a licensing system could publish non-sensitive permit status updates on a public ledger, while keeping applicant data private and permissioned. This configuration might allow an organization to benefit from blockchain's openness without compromising compliance or data protection. More broadly, for organizations exploring emerging technologies in the context of evolving policy and standards, hybrid models can potentially offer a practical, phased approach to test blockchain's potential while managing associated risks. However, hybrid models can also introduce governance challenges, for instance, deciding which data is public versus private, and who has the authority to make those decisions.

In practice, each blockchain model presents trade-offs, and the choice of design will depend on the intended use case, and whether priority is given to resilience, cost efficiency, public trust, or compliance with data protection rules.

A diagram detailing how characteristics compare across each type is included in Appendix IV.

Photo: Michael Appleton, New York City Mayoral Photography Office

2. Use of Blockchain Today

As described above, use of blockchain is no longer confined to cryptocurrencies. Across industries, it is being tested and deployed in areas as varied as supply chain tracking,[27] digital identity management, health care data management,[28] among others. Large corporations have piloted blockchain to verify the provenance of goods from coffee beans to airplane parts; universities have experimented with credential verification; and nonprofits have used it to coordinate humanitarian aid. These diverse applications demonstrate the underlying technology's flexibility as a tool for securing records, coordinating multiple parties, and improving transparency.

Governments have taken note of these trends. While their priorities differ from private industry, with public trust, accountability, and legal compliance being paramount, public-sector actors are exploring many of the same core ideas. In some cases, government-led experiments draw directly on lessons from industry and civil society, while in others they test use cases unique to government.

To better understand the current state of blockchain-related exploration in the public sector, the city conducted a review of approximately 100 government efforts worldwide. These spanned local, state, and national levels of government across North America, Latin America, Europe, Asia, Africa, and the Middle East, as well as initiatives led by international organizations such as the United Nations. This review combined publicly available information, including official reports, press releases, and evaluations, with selected interviews with government representatives and industry leaders directly involved in these projects.[29]

The research also included input from a broader range of stakeholders in academic institutions, civic organizations, and industry who are engaged in blockchain policy, technology development, and the broader blockchain ecosystem. These perspectives helped contextualize government efforts within the wider landscape of innovation, regulation, and public dialogue, offering a clearer view of how different sectors are responding to the technology's evolution.

2.1 Blockchain in Government - Use Cases Explored Around the World

Governments around the world are increasingly exploring blockchain technology as a potential tool to improve public service delivery. Motivations range from increasing the efficiency of bureaucratic processes, to automating compliance tasks, to enhancing transparency and verifiability in government systems.

Though blockchain can in theory offer new solutions for government, significant risks and challenges remain related to data privacy, security, integration with legacy systems, legal compliance, and alignment with broader social and environmental goals. As a result, while industry adoption of blockchain and digital assets has grown rapidly, particularly in the financial sector, public-sector experimentation has followed a more cautious, exploratory path, focusing on learning, piloting, and evaluating feasibility.

Indeed, the city's research indicates that as of early 2025, most government efforts in the U.S. remain in early or pilot phases, often limited to specific departments or functions. Scaled use cases are particularly rare in large cities comparable to New York. Governments are approaching blockchain as a toolset that must be carefully adapted to specific needs, institutional contexts, and legal environments.

Moreover, a key area where governments are focusing work is in adapting internal methods, systems, or resources to the growth in use of blockchain, and particularly cryptocurrency *outside* of government. These efforts recognize a changing technology, policy, and social landscape related to this technology, and seek to evolve public sector approaches accordingly.

This section highlights a selection of initiatives across governments in the U.S. and around the world. This is not an exhaustive list, but rather a reflection of the diversity of approaches and examples of how governments are engaging with blockchain and digital asset technologies. These examples are intended to inform and illustrate, not to suggest that New York City is currently pursuing or will pursue these specific use cases.

Digital Credentials & Property Ownership Records

A number of governments have explored how blockchain can improve the way personal and property-related credentials are issued, verified, and shared. From land- and vehicle titles, to marriage certificates and digital IDs, many official records remain paper-based and fragmented across systems, with associated processes prone to delays and vulnerable to fraud. Even though significant risks and challenges remain, blockchain technology is being explored to offer potential benefits through tamper-evident verification, real-time authentication, and greater transparency.

Projects have varied in scope and focus. The California Department of Motor Vehicles (DMV), for example, has used blockchain to digitize car titles, issuing over 40 million titles as NFTs and linking them to identity wallets to reduce fraud and streamline transfers.[30] The government of Buenos Aires, Argentina has deployed a fully decentralized digital ID system, allowing more than 3.6 million residents to manage over 90 official documents through a city-run digital wallet integrated with zero-knowledge technologies.[31] Baltimore, Maryland is using blockchain to manage historical and current records for over 228,000 properties, starting with vacant lots.[32] By recording title histories, liens, and ownership data on a blockchain-based system, in parallel with legacy systems, city officials aim to improve transparency, reduce legal search time, and eventually support property tokenization.[33] Washoe County, Nevada has used

Photo: Julienne Schaer, NYC & Co.

blockchain to authenticate digital marriage certificates. In doing so, they sought to solve a challenge for residents and tourists needing timely proof of marriage, while decreasing their transaction turnaround time.[34] To support verification without revealing personal information, the system hashes each document and records the hash, rather than the data itself, on a private blockchain. Originally built on Ethereum, the project transitioned to a private chain due to rising transaction costs and demand for more privacy.[35]

Public Resource Management

Blockchain has also been explored as a tool to strengthen transparency, efficiency, and coordination in the use of public resources. From budgeting and procurement to emergency response and long-term digital preservation, various blockchain pilots are being implemented with hopes of improving accuracy, enhancing accountability, and supporting real-time visibility into the use of public funds.

For example, the Federal Emergency Management Agency (FEMA) has explored blockchain-based systems to modernize disaster response workflows, toward delivering faster aid and tracking where resources go in an area where speed, accuracy, and trust are critical.[36] At the local level, the city of Reno, Nevada is using blockchain to digitize and authenticate its register of historic places to streamline recordkeeping, reduce administrative delays in adding or updating listings, and ensure the accuracy and tamper-resistance of historic property documentation. [37] Similarly, the Internet Archive's "Democracy's Library" project, developed in partnership with a range of U.S. public institutions, leverages decentralized blockchain storage to preserve government websites, datasets, and research publications, protecting their data from tampering or loss over time.[38]

Digital Assets and Financial Applications

Financial uses of blockchain are among the most developed across sectors, but also among the most complex for governments. The regulatory landscape for digital assets is both complex and dynamic. Challenges such as price volatility and public perceptions create risks that governments must weigh carefully. While blockchains themselves can enhance traceability and transparency, cryptocurrencies raise concerns around stability and potential misuse.

Apart from exploring the direct use of blockchain technology, some governments have adjusted internal systems to accept cryptocurrency payments for taxes or fees. For example, the Canton of Zug in Switzerland allows residents to pay taxes using Bitcoin and Ether.[39] These options are supported by a broader national framework that provides legal clarity around digital assets and blockchain.[40] In a few cases, such as Lugano, Switzerland, municipalities have launched local tokens to encourage regional economic activity. This particular arrangement involved a third-party processor and did not require the government to manage the blockchain network themselves.[41] In the U.S., the city of Williston, North Dakota, is one of the first municipalities to accept cryptocurrency for utility bill payments via a third-party processor.[42] Adoption among residents has been low, but the city of Williston reports that the use case carries minimal risk for their purposes, and it continues to offer this option.[43] Colorado has also permitted residents to pay a wide range of state taxes with cryptocurrency since 2022.[44]

Some governments have also explored integrating digital assets into their broader fiscal strategies. Governments exploring "strategic reserves" of Bitcoin or other digital assets generally frame these efforts as ways to diversify fiscal holdings, hedge against inflation, or securely manage assets acquired through seizures.[45] The U.S. Federal Government, via presidential Executive Order 14233 of 2025, called for the creation of a Strategic Bitcoin Reserve and Digital Asset Stockpile, aiming to store and oversee digital assets acquired through legal proceedings.[46] At the state level, Texas has passed legislation to create its own strategic Bitcoin reserve,[47] and Pennsylvania,[48] Wyoming,[49] and Ohio[50] are considering similar steps.

Meanwhile, other governments are beginning to experiment with issuing government bonds using blockchain technology. For example, Lugano, Switzerland has issued multiple municipal bonds through distributed ledger platforms.[51] In the U.S., Quincy, Massachusetts, became the first city to issue blockchain-based bonds in 2024.[52]

Blockchain Analytics

Another key area where governments are building and leveraging new capacity to interact with blockchain is in law enforcement. Unlike traditional financial systems where records can be deleted, altered, or obscured, activity on public blockchains cannot be erased. Even though criminals may attempt to conceal their activities using techniques such as "mixers,"[53] privacy coins,[54] or cross-chain transfers,[55] the underlying ledger remains available for analysis. Due to this structure, blockchain provides transparent and immutable records that can enable tracing of illicit financial flows, provided agencies have the right capacity and investigative tools.

Blockchain analytics refers to the use of software platforms that allow investigators to follow the flow of funds, identify patterns of activity, and connect blockchain addresses to real-world actors.[56] These platforms typically combine transaction monitoring, risk scoring, and address attribution databases with investigative methods to interpret activity across blockchain networks.[57] By leveraging these tools, governments around the world have disrupted criminal enterprises – from tracing ransomware payments and darknet market activity to identifying funds tied to sanctions evasion, terrorist financing, and child exploitation.[58]

In recent years, law enforcement organizations in Spain, the United Kingdom, and North America have successfully recovered millions of dollars in ransomware proceeds, [59] tracked billions in stolen cryptocurrency from hacked exchanges, [60] and dismantled networks laundering money for organized crime.[61]

Effectively leveraging blockchain analytics remains challenging for many governments, however. Many departments and agencies still lack the technical expertise, software, and dedicated staff needed to fully utilize these tools. Successful investigations typically require trained analysts, specialized analytics platforms, and workflows for integrating blockchain insights into broader investigative processes. In addition, while blockchain records are inherently transparent, tracing illicit activity can be challenging when funds are routed through intermediaries or services designed to obscure their origin, such as unregistered brokers or mixers.[62]

To mitigate these challenges, some cities, such as Miami, Florida have institutionalized the use of blockchain analytics as part of their law enforcement toolkit. For example, investigators are increasingly trained to interpret blockchain data alongside traditional financial intelligence, integrating it into anti-money laundering, cybercrime, and counterterrorism efforts. [63] This shift reflects a growing recognition that digital assets create new types of forensic evidence that must be met with new techniques, resources, and capabilities.[64]

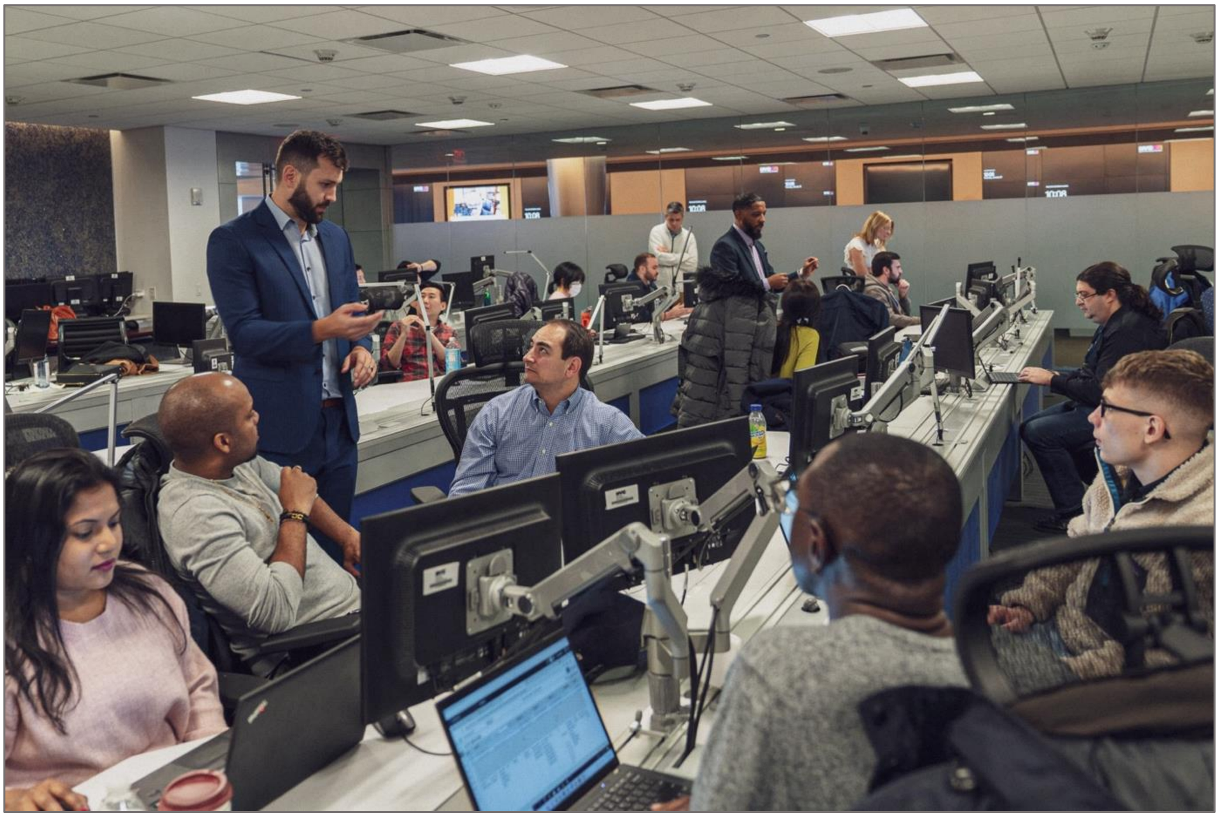


Photo: Andres Lopez-Ovejero, NYC Office of Technology & Innovation

Educational Efforts

Around the world, governments and civic organizations are investing in blockchain and digital asset education as part of a broader financial literacy, technical skill-building, and workforce readiness agendas. Singapore and California have each partnered with universities to train public officials and students in the fundamentals of blockchain technologies. Public educators in selected states and municipalities have introduced new materials for students to learn about digital assets and related financial literacy topics. These efforts reflect a growing recognition that understanding blockchain's mechanics, opportunities, and risks is becoming an important component of technical and financial education.

2.2 Cross-cutting Challenges and Lessons

The city's research uncovered a range of opportunities and constraints in adopting blockchain in government. These lessons reflect an ongoing process of aligning new tools with real-world needs, institutional capacities, and legal frameworks. In this context, most governments exploring blockchain use are moving forward incrementally, testing the technology where it shows clear promise, while continuing to refine approaches as the technology and policy environment evolve. The research also showed that a range of considerations come into play for governments seeking to build capacity related to their interactions with the technology as it becomes more common across sectors.

Clear Value Proposition for Adoption

One consistent theme that emerged during our conversations with stakeholders was the importance of a clearly-defined value proposition for adopting blockchain. Some stakeholders described cases where they initially pursued blockchain integration but later abandoned it after offering few meaningful advantages over existing systems. In such instances, decision-makers viewed blockchain as a tool that could replicate existing functions but introduced additional complexity without delivering significant new benefits. In this sense, stakeholders advised against adopting blockchain simply for the sake of innovation, emphasizing that projects should be fit-for-purpose and grounded in real operational or service-delivery needs.

Integration with Existing Systems

Legacy systems often are deeply embedded in public operations. Re-engineering or connecting them to new platforms can be complex and disruptive. Several interviewees stressed the importance of aligning new blockchain applications with existing workflows and interoperability standards from the outset, to ease such challenges.

Maintaining Parallel Systems

Governments also took a cautious approach by running blockchain pilots alongside existing systems. These were not only required to comply with existing regulations but also served as a broader risk management strategy, ensuring continuity in case blockchain systems failed to deliver.

Cost and Scalability

Blockchain systems can be resource-intensive to design and maintain, including expenses beyond transaction fees, such as infrastructure, development, and integration with existing systems. While there is evidence to suggest that certain component costs have been declining as the technology matures – for example the average transaction fees on networks like Ethereum – overall system costs remain significant.[65] Accordingly, stakeholders emphasized that starting with small-scale, lower-risk pilots can not only help to manage costs but also allow agencies to demonstrate tangible value before scaling up.

Inter-Departmental Coordination

Coordinated inter-departmental implementation and management surfaced as another challenge. Many stakeholders emphasized that blockchain only delivers value in collaborative environments, whereas use by one agency alone has offered limited benefits. However, building and maintaining multi-stakeholder infrastructure requires dedicated resources, leadership commitment, and sustained collaboration, all of which can be difficult to achieve. Even when interest exists, shifting priorities within government can undermine momentum.

Institutional Capacity and Readiness

Teams with in-house expertise or strong external partnerships were better able to frame the right questions, assess risks, and make informed design decisions related to blockchain efforts. By contrast, organizations without this capacity often depended heavily on vendors, which could create challenges for integration or long-term sustainability. A key lesson across projects surveyed was the importance of building internal knowledge and partnerships, if efforts are to move beyond one-off experiments and have the potential to become durable parts of government systems. Moreover, readiness also depended on broader institutional resources, including procurement processes, staff training, and leadership engagement. Cities that could mobilize finance, legal, and IT teams together were better positioned to assess blockchain uses cases holistically, communicate risks and benefits to policymakers, and prepare for emerging interactions with the technology, such as accepting payments in digital assets or leveraging blockchain analytics for law enforcement.

User Readiness

On the end-user side, challenges included accessibility and adoption, particularly in communities with low digital literacy or limited access to smartphones and digital wallets. This is a challenge that may need to be addressed via broader interventions before a public-facing implementation is considered, in particular, to avoid inequitable access to or use of systems.

Legal, Regulatory, and Public Goals Alignment

Legal and regulatory alignment may also pose a challenge, particularly for financial use cases, or interactions with them across sectors. For blockchain to be considered for broader adoption, clear laws and governance frameworks are essential. Even technically successful pilots may run into limits due to the absence of legal guardrails. Momentum is now building in several jurisdictions to establish clearer laws around blockchain and digital assets, which may help reduce these barriers over time.

In addition, public-sector uses must align with broader social and environmental goals, ensuring that blockchain technologies advance equity, transparency, accessibility, and sustainability, alongside innovation.

Keeping up with an Evolving Landscape

Many stakeholders finally flagged a need to continuously assess new developments in blockchain technology itself, and its use across sectors, given the rapid pace of change. In this context, being prepared to adapt approach on an ongoing basis is a fundamental need for navigating the use and interaction with this emerging technology.

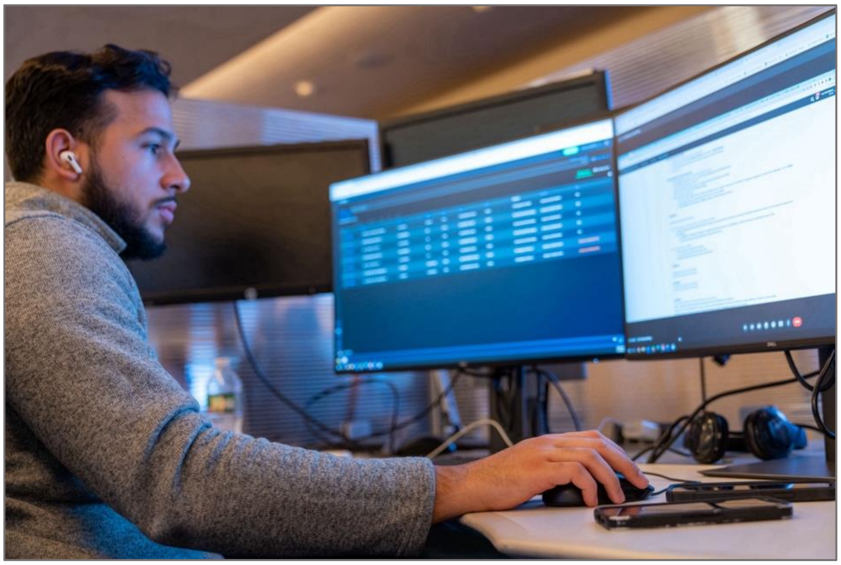


Photo: Andres Lopez-Ovejero, NYC Office of Technology & Innovation

2.3 New York City Exploration of Blockchain

The city is actively examining how blockchain might be used in government, and what new resources or capacities may be needed for the city's interactions with blockchain across sectors.

The city's Economic Development Corporation (NYCEDC) has been a longtime leader in advancing the city's blockchain ecosystem – supporting innovation, entrepreneurship, and workforce development initiatives in this emerging sector. Most recently, NYCEDC, in partnership with the Office of Talent and Workforce Development and City University of New York (CUNY) Queens College, created NYC Node, the City's first investment in blockchain infrastructure.[66] Housed at the Tech Incubator at Queens College, NYC Node operates an Ethereum archival node and provides applied learning opportunities, workshops, and research resources for CUNY students and faculty.

This builds on NYCEDC's earlier efforts to position NYC as a global blockchain hub. Since 2018, NYCEDC led initiatives including supporting NYC Blockchain Week, which convened global leaders across technology and finance; establishing the NYC Blockchain Center, a dedicated hub offering education, mentorship, and business support for blockchain entrepreneurs;[67] and launching the BigApps Blockchain challenge, which engaged over 600 New Yorkers and invited local companies to collaborate with government to prototype public sector blockchain applications. Collectively, these initiatives reflect NYCEDC's sustained commitment to positioning New York City as a global leader in emerging technology and innovation.

Between 2021 and 2022 the New York City Department of Finance (DOF) tested the use of blockchain for recording land titles. While technically feasible, the pilot surfaced challenges, including high costs relative to benefits, integration with existing systems, and the absence of legal recognition for blockchain-based title transfers under New York law. In addition, the data base of Land Records is already immutable. As a result, the pilot did not demonstrate a clear business or legal case for broader adoption at the time of the test.

In recent years, New York City's Department of Health and Mental Hygiene (DOHMH) has explored the use of blockchain to modernize the issuance of birth certificates through a range of national-level discussions. However, the general consensus is that blockchain is unnecessary and would not provide significant improvements over other technologies or methods. In addition, recognition of the need to develop a national solution and widespread acceptance of a digital version of these critical records has shifted local efforts to national collaboration on digital issuance.

Local public education institutions are beginning to explore blockchain and digital asset technologies as part of broader efforts to build technology skills, financial literacy, and workforce readiness. NYC Public Schools (NYCPS) has explored integrating emerging technologies like blockchain and digital assets into computer science and financial literacy curricula. This has included, for example, both school-year and summer programs that help students understand what digital assets are, how they work, and what risks and opportunities they can present.

At the university level, CUNY has piloted innovative projects that integrate blockchain applications, such as the use of tokens, digital wallets, and digital credentials, into coursework. These hands-on experiences give students a practical understanding of how decentralized systems work and how they can be applied across sectors, from finance to digital identity.

Together, these educational efforts illustrate how New York City institutions are beginning to prepare students for a future where blockchain and related technologies play a growing role in the workplace and economic life.

Overall, New York City is still at an early stage of examining this emerging technology. This Plan is intended to help orient the city's approach going forward by identifying where blockchain could genuinely add value, supporting knowledge and capacity-building inside government, and ensuring that exploratory efforts are conducted responsibly. Strengthening internal expertise and cross-agency collaboration will be essential for assessing blockchain's risks and opportunities and determining whether the city should pursue additional pilots in the future. Equally important, the city should continue to build capacity to manage interactions with blockchain outside of government, so that agencies are equipped to respond effectively and responsibly. Sections 4 and 5, below, will explore specific opportunities and challenges for New York City, as well as productive next steps, in greater detail. First, however, it is important to review the current state of the policy landscape around blockchain, to understand how evolving laws and regulations may shape what is possible for city government and how New York City should position its own efforts.

Photo: Benjamin Kanter, New York City Mayoral Photography Office

3. Current Policy Landscape

Legislative policy and government regulations often evolve more slowly than emerging technologies, and blockchain is no exception. While there has been increasing legislative and regulatory activity at the state and federal levels – particularly around digital assets such as cryptocurrencies and stablecoins, there has been limited policy development related to blockchain as a broader technology, and at the local level in New York City. As such, this section focuses primarily on financial policy developments at other levels of government. While these efforts have limited direct bearing on the city's prospective use of blockchain for non-financial applications, they may influence how agencies interact with digital assets across sectors. For that reason, these policy developments remain important for the city to track and understand, especially as the U.S. regulatory landscape continues to evolve rapidly.

New York City Context

In New York City, blockchain and digital assets are not directly regulated at the municipal level. However, their adoption and use by the city will be governed by a range of existing city laws and policies that apply to all IT systems. These include measures related to procurement, information privacy, and cybersecurity, among others.

In particular, New York City agencies are broadly required to comply with the city's Identifying Information Law (ILL) and its associated Citywide Privacy Policies.[68] This includes consideration of the city's privacy principles, which should be honored in all aspects of agency decision-making and operations impacting information privacy.[69] Likewise, agency efforts must comply with Citywide Cybersecurity Policies and Standards, including any updates to these measures over time as the technology and threat landscapes evolve.[70] These requirements also extend to how data generated or processed through new systems, such as blockchain-based applications, is classified, governed, and audited, ensuring consistent protection and oversight.

More broadly, the city has a range of existing goals and responsibilities that must be taken into account in planning and deploying any new technology tool – including ensuring transparency, in how new systems operate, privacy, and environmental sustainability.[71]

In some cases, individual city agencies may also have existing specific policy or guidance that must be taken into account. The NYPD, for example, has already developed formal guidance for the use of blockchain analytics tools through its Public Oversight of Surveillance Technology (POST) Act's Cryptocurrency Analysis Tools: Impact and Use Policy.[72] These NYPD frameworks ensure transparency, accountability, and appropriate oversight when leveraging blockchain technology for investigative purposes.

Taken together, these existing laws and policies will help form the framework that will govern blockchain use across the city. They must be thoughtfully integrated into any future policy efforts the city undertakes on this subject. Robust compliance and alignment with these measures will be critical to ensuring any city blockchain efforts are undertaken responsibly, and minimize risks to residents.

U.S. State Policy Actions

Several U.S. states have outlined policies in the last decade related to digital financial assets that are focused on financial regulation, anti-money laundering measures, and consumer protection. New York, for example, became the first state to establish a licensing framework for virtual currency businesses through the BitLicense program in 2015.[73] Administered by the New York State Department of Financial Services (DFS), BitLicense aims to safeguard consumers and promote responsible innovation by requiring companies engaged in activities such as buying, selling, storing, or transferring virtual currency to obtain a license, meet capital requirements, and comply with anti-money laundering and consumer protection rules.

Environmental regulation has also emerged as a distinct policy category related to digital assets. In 2022, New York State enacted a cryptocurrency mining law establishing a two-year moratorium on new permits for certain proof-of-work mining permits facilities, particularly those drawing on fossil-fuel-based power plants. The law also directed the NYS Department of Environmental Conservation (DEC), in consultation with the NYS Department of Public Service, to prepare a Generic Environmental Impact Statement (GEIS) on assessing the industry's impacts.[74] This legislation was a first-of-its-kind in the United States, reflecting concerns that energy-intensive mining could conflict with state climate goals.

Other states, such as Vermont,[75] Illinois,[76] and Arizona,[77] have passed legislation recognizing blockchain records and smart contracts, enabling their use in legal agreements, notarization, and digital recordkeeping. Wyoming has been an early mover in establishing regulatory frameworks for digital assets and decentralized autonomous organizations (DAOs), aimed at providing legal clarity for token issuance, digital asset custody, and corporate governance for DAOs.[78] Beginning in July 2026, California will require companies dealing in digital assets to be licensed by its Department of Financial Protection & Innovation (DFPI), to ensure consumer protection, financial stability, and regulatory oversight over digital asset activities in the state.[79]

U.S. Federal Policy Actions

At the federal level, oversight of digital financial assets is distributed across multiple agencies, including the Securities and Exchange Commission (SEC),[80] Commodity Futures Trading Commission (CFTC),[81] Federal Trade Commission (FTC), and Department of the Treasury. To date, each of these agencies has pursued its own approach. For example, the SEC has brought enforcement actions against unregistered token offerings and pursued cases of fraud while the CFTC has asserted jurisdiction over digital asset derivatives and treated Bitcoin and Ether as commodities. The Treasury (through FinCEN) has extended anti-money laundering and "travel rule" requirements to virtual asset service providers.[82] In parallel, the FTC has emphasized consumer protection, issuing guidance, bringing enforcement actions, and creating reporting mechanisms for digital-asset scams and deceptive practices.[83] However, the absence of a unified federal framework has often resulted in fragmented guidance and uneven enforcement, leaving both public institutions and private actors uncertain about how to comply or plan ahead.[84]

Federal involvement at the executive level began under the Biden Administration. On March 9, 2022, President Biden issued Executive Order 14067 “Ensuring Responsible Development of Digital Assets,”[89] which set out a government-wide strategy to coordinate research and policy on digital assets. The order outlined multiple goals, including protecting consumers, promoting financial stability, advancing U.S. leadership in digital finance, mitigating illicit finance risks, and encouraging responsible innovation, while directing federal agencies to study regulatory gaps and develop coordinated policies. While the order provided a first step toward greater coordination, efforts to translate its goals into comprehensive legislation stalled amid congressional gridlock, and shifting market conditions following major industry failures.[90] This left uncertainty around licensing requirements, banking services for the crypto industry, taxation, and enforcement priorities for digital asset firms.[91] Some government and industry stakeholders have argued that this gap created space where banking regulators informally discouraged financial institutions from serving digital asset firms.[92]

In 2025, the Trump Administration revoked Executive Order 14067 and issued Executive Order 14178, “Strengthening American Leadership in Digital Financial Technology” which called for the establishment of a Presidential Working Group on Digital Asset Markets and the creation of a Strategic Bitcoin Reserve and U.S. Digital Asset Stockpile.[93] On July 30, 2025, the Trump administration also released a digital asset report outlining policy approaches to market structure, banking, stablecoins and payments, taxation, and anti-money laundering.[94] Together the actions signal a high level of federal interest in rapidly advancing national digital asset policy, though key implementation factors, including multi-agencies’ jurisdictional regulatory authorities, remain.

Current Use Cases for Stablecoins

Originally developed for crypto trading, stablecoins have expanded into a range of everyday financial uses. Backed by assets like the U.S. dollar, stablecoins are currently mostly used in decentralized finance (DeFi), peer-to-peer payments, international trade, and as a store of value in countries experiencing economic instability.[85]

Cross-border remittances are a use case that many have argued could be impactful.[86] Stablecoins allow money to be sent quickly and at a fraction of the cost of traditional remittance methods. For instance, according to Chainalysis,[87] sending $200 from Sub-Saharan Africa can cost more than 60 percent less when using stablecoins than through conventional channels, helping families access funds faster and more affordably.

Advocates also point to their potential role in expanding financial access to help those who face barriers to opening traditional bank accounts.[88]

Taken together, these uses illustrate both the opportunities and ongoing debates around how stablecoins may reshape access to and the movement of money.

In July 2025, the U.S. GENIUS Act (S. 1582) was signed into law.[95] This is the first federal statute to directly regulate a class of digital financial assets. The new federal law defines U.S. dollar-backed stablecoins, establishes a federal licensing regime for permitted issuers (including banks, approved fintechs, and certain state-chartered entities), and mandates monthly reserve disclosures and independent audits for large issuers. It also prohibits interest payments to holders and requires stablecoins to be fully backed on a 1:1 basis by liquid, low-risk assets such as cash, short-term treasuries, or certain deposits. While this represents a significant shift toward greater regulatory clarity in one segment of the digital asset market, some observers have raised concerns that the law could concentrate stablecoin issuance among a few large institutions, potentially limiting innovation, reducing competition, and increasing systemic risk in the broader financial system.[96]

A short summary of the current state of international policy, for comparison, is included in Appendix V.

Photo: Michael Appleton, New York City Mayoral Photography Office

4. Opportunities and Challenges

Building on the city's global review of government use cases, policy developments, and stakeholder input, this section distills what these findings mean for New York City. Drawing on the city's analysis and stakeholder interviews, including a range of city agencies, the following outlines key opportunities and challenges for how the city can both responsibly evaluate potential use cases of blockchain in its own operations and service delivery, and strengthen its capacity to manage interactions with blockchain technologies outside of government.

4.1 Opportunities for NYC Government

Opportunity Areas for Blockchain Adoption

Streamline Operations

Blockchain has the potential to help simplify and automate certain city functions, particularly those involving recordkeeping, contract management, and auditing. Smart contracts, for example, could potentially verify milestones or execute transactions automatically, reducing administrative overhead and opportunities for error. In addition, blockchain's shared ledger design could reduce the need for multiple parties to independently reconcile records, allowing agencies to work from a single, verified source of truth. This could help cut down on duplication, shorten processing times, and reduce reliance on intermediaries to validate information. As blockchains continue to improve, their ability to combine automation with tamper-evident, real-time recordkeeping may provide advantages over traditional systems, especially in contexts where multiple agencies or stakeholders must coordinate and verify the same data.

Enhance Transparency, Trust, and Accountability

For city governments, blockchain could offer a new level of transparency related to use of public funds, service delivery, and decision-making. Blockchain analytics tools are making it easier to interpret complex transaction flows, offering a full lifecycle view that can potentially complement traditional oversight methods. By publishing relevant records on tamper-evident ledgers, agencies could reinforce public trust in how services are delivered and resources are managed.

Strengthen Security and Reduce Fraud

Because blockchain transactions are cryptographically secured and logged in a tamper-resistant way, they might offer built-in protections against certain types of fraud and data manipulation. For example, once a record is logged, it is difficult to alter without detection, which could help discourage document forgery or back-dated entries. In some circumstances, blockchain systems might also make digital assets or records easier to recover than cash-based or paper systems, since transfers are auditable and tied to a persistent ledger. Advances in blockchain safety tools, such as automated auditing of smart contracts, might further support fraud prevention. While no system is immune to risk, blockchain's structural features may add an extra layer of defense when combined with robust governance.

Reduce Long-Term Costs

While blockchain adoption requires upfront investments in new tools, as well as integration, training, and governance, over time it may deliver cost savings in certain applications. Automation can reduce the administrative burden of managing routine transactions, while more efficient blockchain networks, particularly those with low energy use and minimal transaction fees, are becoming more cost-competitive. It is important to note, however, that the potential for savings is highly dependent on context, and careful cost-benefit analysis will be needed before any citywide deployment of a blockchain solution.

Opportunity Areas for City Interactions with Blockchain

Open New Avenues for Payments

There may also be opportunities to modernize how the city manages incoming and outgoing payments, by building the capacity to interface with blockchain-based payment systems as they become more widely used across sectors. On the disbursement side, for example, programmable tokens could allow the city to support direct and efficient payments to vendors or partners, reducing administrative steps and settlement delays. While any financial applications would need to carefully navigate regulatory and risk concerns, blockchain could expand the menu of options available for secure and timely transactions.

Expand Capacity for Blockchain Analytics

As blockchain use grows across industries, city agencies will increasingly encounter data, assets, and activity that is recorded on public ledgers. Strengthening data processing capacity, including access to blockchain analytics tools, training, and partnerships, can enhance the city's ability to detect illicit finance and ensure compliance with consumer protection and public safety goals.

Promote Public Literacy

With more New Yorkers engaging in digital assets, there is an opportunity to expand public understanding of blockchain's risks and benefits. By supporting financial and technical literacy initiatives, the city can help residents make informed decisions, avoid scams, and participate safely in the broader blockchain ecosystem. Moreover, blockchain and related technologies are reshaping sectors from finance to digital identity. Collaborating with educational institutions and workforce programs to integrate blockchain fundamentals, hands-on learning, and responsible-use principles can strengthen citywide innovation capacity and talent development.

4.2 Challenges for City Government

Challenge Areas for Blockchain Adoption

The following challenges highlight areas where careful planning, governance, and risk mitigation will be essential as the city considers direct blockchain adoption. Some challenges also extend beyond the technology itself, including key management, vendor oversight, and long-term operational resilience.

Coordination in a Complex City Environment

New York City's size and institutional landscape can make coordinated adoption particularly challenging. Many blockchain use cases, such as property or identity systems, require participation from multiple agencies, private actors, state or federal partners, as well as resident end users. Without strong coordination, fragmented adoption could create confusion, inefficiency, or inequity.

Technical and Integration Constraints

While blockchain technology has matured, scalability, interoperability, and integration remain real barriers to blockchain adoption. City systems handle millions of transactions daily, and few blockchain platforms can deliver that scale without trade-offs. Equally important, most government systems rely on legacy infrastructure. Unless blockchain applications can integrate seamlessly, they risk becoming isolated pilots rather than lasting solutions. Careful alignment with existing city IT systems and standards will be critical to any implementation.

Any assessment of potential solutions should also incorporate vendor due-diligence, including secure onboarding, data-handling expectations, and clear exit strategies, to ensure long-term integrity and continuity of city operations.

Privacy and Cybersecurity

Blockchain's transparency creates challenges when sensitive or personal information is involved. Immutable public ledgers could expose resident data in ways that conflict with privacy protections or city laws or policies, especially because once data is recorded, it cannot be deleted. Data locality also presents challenges, as blockchain transactions may span multiple jurisdictions at once, raising questions about compliance with national or local laws. Smart contracts raise further questions: they may contain vulnerabilities, and if not carefully designed and audited, they can also introduce risks such as coding errors or malicious exploitation. And with permissioned or centralized blockchains, there is also the risk of single points of failure, if the managing authority is compromised, sensitive data or assets could be at risk.

In order to address these issues, new risk assessment and incident response plans will be required for blockchain integrations, since existing frameworks are not designed with blockchain-specific vulnerabilities in mind. And because cryptographic algorithms eventually become obsolete or vulnerable, blockchain projects must account for future upgrades to avoid creating technical debt and long-term security risks.

Additionally, blockchain systems introduce key-management challenges that are distinct from traditional IT models. Agencies and vendors will require clear policies for safeguarding private keys, mitigating insider threats, and establishing secure, user-friendly pathways to recover access if credentials or wallets are lost.

These considerations highlight the need for robust privacy, security, and governance measures whenever blockchain is explored for city use.

Environmental Impact

Photo: Michael Appleton, Mayoral Photography Office

Blockchain is a computationally intensive technology that has received significant attention for its environmental footprint. The most energy-demanding systems, such as those using the Proof-of-Work (PoW) consensus mechanism, require large amounts of electricity to validate transactions through competitive "mining." This process involves running high-powered computers continuously to solve cryptographic puzzles, a design that ensures security but at high energy cost. As a result, global PoW-based networks have been shown to consume electricity at a rate comparable to small nations.[97] Other mechanisms, such as Proof-of-Stake (PoS) or permissioned systems, generally consume less energy.[98]

Blockchain's energy use has also been argued to have impact on broader utility markets. A recent study showed, for example, that increased grid demand from mining operations led to increased monthly electricity bills for both residents and businesses in upstate New York. [99]

Various industry efforts have begun to address these significant environmental concerns at different points in the blockchain lifecycle. For example, there is evidence to suggest that Ethereum's 2022 transition from PoW to PoS reduced its estimated annual energy consumption from roughly 78 terawatt-hours to less than 0.01 terawatt-hours per year, a decline of more than 99 percent.[100] Other initiatives have attempted to increase renewable sources of energy to power blockchain technologies and limit the most energy intensive activities to more optimal times of day. [101] Still, any figures to show sustainability claims should be viewed with caution, given the challenges of independently verifying emissions and water consumption data across decentralized networks. Unfortunately, while some mining operations have indeed shifted toward renewable sources or develop methods to repurpose waste heat, crypto mining overall continues to commonly rely on fossil fuels.

Together, these issues underscore the need for public-sector stakeholders to critically evaluate environmental trade-offs before engaging in blockchain-related activity. For a city like New York with ambitious climate goals, any implementation must carefully weigh emissions impacts (direct and indirect) against potential benefits. This is especially true for large-scale applications that require frequent transactions. Ultimately, agencies must ensure that any exploratory or operational use of blockchain aligns with city's sustainability commitments, such as those outlined in PlanNYC: Getting Sustainability Done and Local Law 97, which mandate significant reductions in greenhouse gas emissions across city operations.

Trust and Usability

Building and maintaining trust is essential for any government technology. Blockchain is no exception. While most of the city's prospective blockchain use cases described in this report are non-financial, broader public perceptions, shaped by the volatility and scandals of the digital-asset sector, can still shape how residents and agencies view the technology. Skepticism may stem not only from associations with cryptocurrency, but also from concerns about privacy, complexity, and accessibility.

Beyond reputation, blockchain systems themselves present real usability challenges. Managing wallets, keys, or digital credentials can be confusing and technical, especially for residents unfamiliar with these concepts. Designing user-friendly interfaces and clear recovery processes will be critical if blockchain applications are to be equitable and inclusive.

Trust also depends on transparency and accountability. Users must be confident that systems are secure, data is handled appropriately, and technology use is transparent, and serves a clear public purpose. For permissioned or centralized blockchains, transparency is particularly important to avoid single points of failure or misuse of authority.

For any city-led effort to succeed, trust must be built not only through careful design and deployment, but also through outreach, education, and thoughtful policy.

Legal and Regulatory Uncertainty

Although regulatory frameworks are advancing at federal and state levels, many rules governing blockchain remain unsettled - particularly for uses involving digital financial assets. For city government, this creates uncertainty that could affect both how the city interacts with external uses of blockchain, as well as any prospective direct city uses that integrate financial components in the future. While non-financial transactions can move forward more smoothly, the evolving regulatory environment means that any applications touching payments or financial transactions will require particular caution and coordination with state and federal regulators until clearer guardrails are in place.

In addition, because policies across domains where blockchain may be integrated have not generally been designed with these emerging systems in mind, governments and organizations can face legal ambiguity and compliance hurdles that can slow or complicate deployment, even for non-financial applications.

Challenge Areas for City Interactions with Blockchain

In addition to these challenges that can arise with regard to direct blockchain adoption, there are also a range of challenges that may arise as city agencies encounter growing blockchain use *outside* of government. Key among these are challenges related to skills and knowledge, inter-agency coordination, and a rapidly changing technology and policy landscape.

Institutional Knowledge and Coordination Gaps

Across governments the city studied, a consistent challenge to developing new resources or programs to respond to blockchain's integration across sectors was limited internal understanding of how blockchain and other emerging technologies function, what risks they present, and how they intersect with existing government systems and policies. Without dedicated expertise or coordination structures, agencies may find it difficult to evaluate blockchain's impacts on their work, engage with external partners, or develop new programs or tools, such as systems to integrate new payment mechanisms or capacity to analyze cryptocurrency transactions for law enforcement.

Building shared literacy, technical capacity, and cross-agency structures will be critical to ensure the city can responsibly assess, engage with, and manage interactions involving blockchain now and in the future.

Rapidly Evolving Technology and Policy Landscape

The pace of change in blockchain technology, as well as the policies surrounding it, creates additional uncertainty for governments. New platforms, protocols, and security and privacy standards continue to emerge, and industry adoption patterns shift quickly. Regulatory frameworks at the state and federal levels are also still evolving, particularly for digital assets. This dynamic environment means a solution that appears promising today may require revision or replacement tomorrow. For New York City, responsible exploration requires continuous monitoring, flexible planning, and the ability to adapt policies, resources, and workforce skills as the technology and its use evolves.

Photo: Ed Reed, New York City Mayoral Photography Office

5. Strategic Priorities and Initiatives

Based on the city's survey of the technology and policy landscapes, review of lessons learned from government implementations around the world, and a detailed assessment of the specific opportunities and challenges blockchain presents for New York City, the city has outlined 12 commitments across three priority areas to advance the city’s capacity and efforts on blockchain. These priorities are designed to guide responsible exploration, build literacy among staff and residents, and ensure that ongoing city efforts remain aligned with broader commitments and responsibilities. Initiatives included below are presented with a specific timeframe for completion.

Priority 1: Support Agencies to Explore Blockchain and Navigate its Use Across Sectors

Support city agencies with the tools, structures, and knowledge needed to evaluate when blockchain is the right fit and effectively address their interactions with external blockchain use.

Commitments:

1.1 Launch NYC Blockchain Interagency Working Group: Led by OTI, coordinate agency interests, align on data and technical standards, and facilitate knowledge-sharing across departments. The group will help agencies understand the potential benefits and challenges of leveraging blockchain in city operations, identify barriers to entry, and define early steps for exploration (e.g., how to start scoping a use case). (Q1 2026)

1.2 Pilot Use Cases: Partner with the New York City Department of Environmental Protection (DEP) to scope and launch an exploratory pilot focused on blockchain-based asbestos certification verification, while continuing to engage other interested agencies on potential applications such as digital credentials, permits and licenses, or broader data management efforts. Lessons from the DEP pilot will be documented and shared for review and consideration by other agencies. (Q4 2025-Q2 2027)

1.3 Provide Technical Criteria and Guidance: Publish “Blockchain in City Operations: Use Case Evaluation Guide” to help agencies effectively and responsibly assess feasibility, legal requirements, and alignment of blockchain applications with city priorities. This guide will incorporate values and safeguards discussed in this plan (e.g., equity, privacy and data security, access, public benefit, etc.) and will be focused on process, outcomes, and governance criteria rather than single-use standards. (Q4 2026)

1.4 Strengthen the City’s Capacity to Address Illicit Activity Risks: Bolster city efforts to address blockchain-enabled illicit activity including options such as supporting access to analytical tools, and developing and sharing knowledge-building resources across relevant teams and functions about how blockchain-based systems might be misused to obscure activity or enable fraud. (Q1 2026-Q4 2026)

Priority 2: Foster Staff and Resident Literacy on Blockchain and Associated Technologies

Build staff knowledge and public understanding of blockchain technologies to support informed participation and decision-making.

Commitments:

2.1 Launch the NYC Blockchain Literacy & Innovation Series: Led by OTI in collaboration with relevant city partners, build agency staff capacity through case studies, expert talks, and tailored resources. The series will provide baseline literacy and practical insights for departments exploring blockchain use cases, helping staff understand both opportunities and risks for public-sector work. (Q2 2026-Q4 2027)

2.2 Create an Information Hub: Roll out an online hub to publish educational materials and safety tips related to consumer interactions with digital assets, as well as updates on the city's broader blockchain work. This hub would be developed in consultation with relevant agency and external partners, such as NYC Public Schools (NYCPS), NYC Police Department (NYPD), and other financial literacy or public safety awareness providers. (Q1 2026-ongoing)

2.3 Facilitate Community Safety Resources: Partner with relevant city agencies or community groups to develop or promote public-facing literacy materials to help residents navigate interactions with blockchain, avoid scams, and make informed consumer choices. (Q1 2026-ongoing)

2.4 Seek Education Partnerships: Work with NYCPS and the CUNY to support educational and workforce initiatives that integrate blockchain and digital asset concepts. Assist NYCPS in identifying ways to align computer science and financial literacy efforts with current developments in blockchain and digital asset technologies. Partner with CUNY to explore experiential learning opportunities that enable students to engage directly with blockchain tools and applications, such as digitals assets and tokens, as part of applied coursework. These partnerships will strengthen citywide literacy and workforce readiness in alignment with New York City's broader innovation and technology education goals. (Q1 2026 - Q4 2027)

Priority 3: Track the City's Progress in Implementing this Plan, and Continuously Evaluate New Opportunities and Risks

Keep close tabs on institutional progress and make space for periodic reassessment of priorities, risks, and new technologies.

Commitments:

3.1 **Launch Blockchain Risk & Opportunity Review Process:** Establish an ongoing review process, led by OTI, to monitor emerging blockchain technologies, policy shifts, and use cases. The process will identify potential risks and opportunities for city operations, update priorities and initiatives accordingly, and share insights with agencies through regular briefings and guidance materials. Agencies will be able to contribute information on relevant developments and request analytical support or coordination as needed. (First Review: Q4 2026)

3.2 **Monitor Policy Developments:** Track and analyze policy developments at the state and federal levels and assess their implications for NYC public-sector efforts. Share findings with city stakeholders as appropriate. (Ongoing)

3.3 **Examine Adjacent Technologies:** Continuously track adjacent technologies such as digital identity, digital wallets, zero-knowledge proofs, and others, to evaluate their relevance to NYC's blockchain planning. Share insights with agencies. (Q1 2026-ongoing)

3.4 **Publish Progress and Review Regularly:** Track and publish the city's progress in implementing this plan. (Q4 2026)

Photo: Michael Appleton, New York City Mayoral Photography Office

6. Conclusion

Blockchain presents a range of opportunities and challenges for New York City. This technology can enable new forms of transparency, accountability, and efficiency that may benefit city operations and service delivery. But it also presents a range of risks and challenges around privacy, scalability, regulatory uncertainty, and environmental impact that must be carefully navigated. Varied city interactions with blockchain across sectors will also continue to evolve alongside the broader landscape, and this area too will require ongoing attention to ensure that appropriate resources and capabilities are in place.

The experiences of other governments demonstrate that successful blockchain efforts are grounded in a clearly defined value proposition, supported by strong internal expertise, and pursued with appropriate care from both a social and technological perspective. The city's three strategic priorities, outlined in this report, are designed to build the necessary foundation to navigate this emerging space effectively and responsibly, now and in the future. Ultimately, this Plan aims to provide a framework for thoughtful exploration, ensuring that city use and interaction with blockchain serves the public interest, complies with existing laws and policies, and supports the city's broader strategic goals. By preparing proactively, the city can ensure it is ready to manage both the risks and opportunities of a technology landscape that will likely become more integrated into public and private systems. In doing so, New York City can position itself as a leader in setting responsible standards for the use of blockchain technologies in government.

Appendices

Appendix I: Stakeholders Interviewed for this Plan

New York City Agencies:

- Department of Buildings
- Department of Environmental Protection
- Department of Finance
- Department of Health and Mental Hygiene
- Department of Records & Information Services
- Department of Transportation
- New York City Office of Talent and Workforce Development
- New York City Police Department
- New York City Public Schools
- NYC Mayor's Office of Talent and Workforce Development
- NYC Mayor's Office of Contract Services
- Department of Citywide Administrative Services
- Department of City Planning

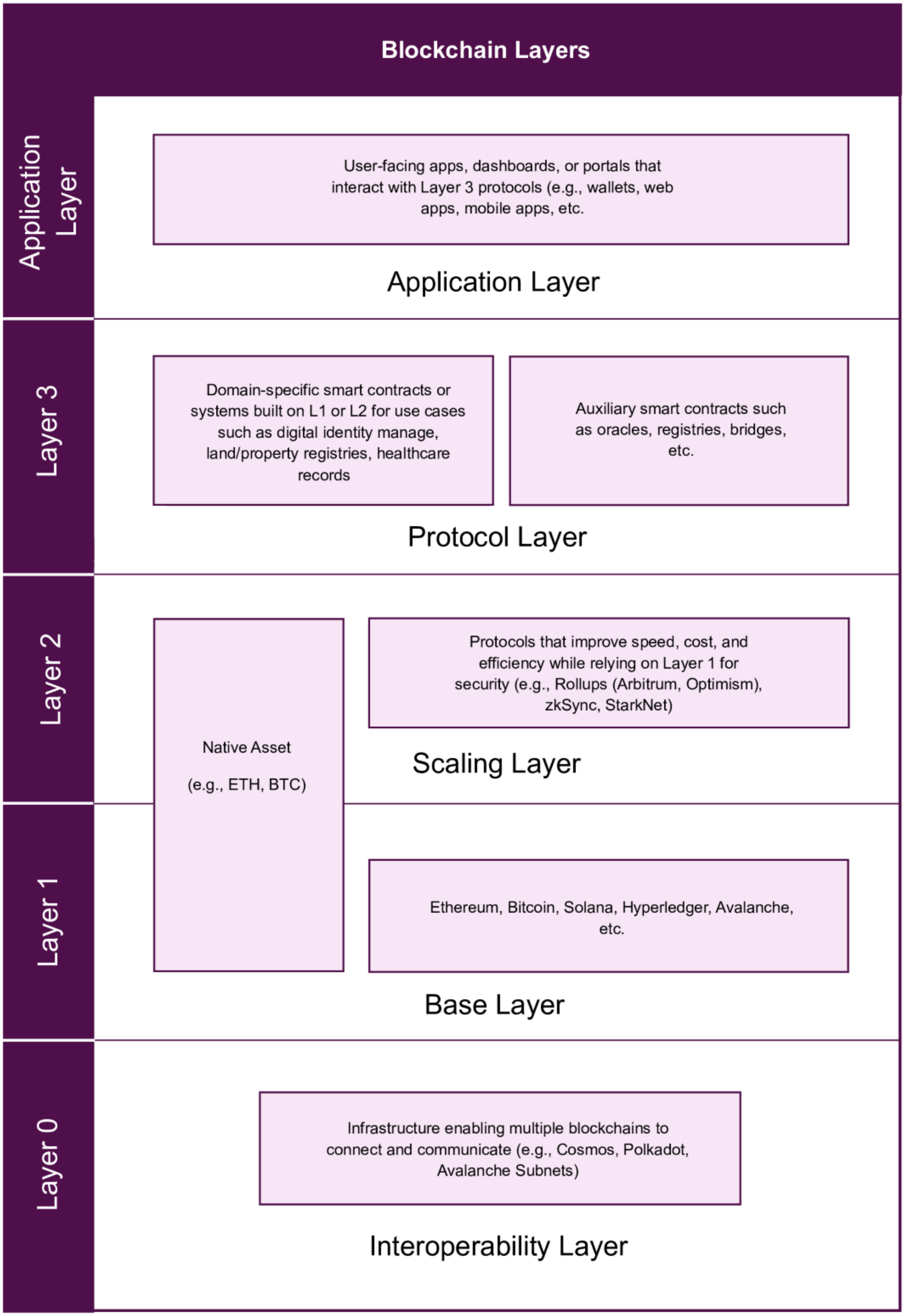
External Organizations:

- Arbitrum
- Ava Labs
- City of Baltimore
- Blockchain Foundation
- California Department of Motor Vehicles
- California Government Operations Agency
- Central Bank of Brazil
- Chainalysis
- Circle
- Coin Center
- Cornell University
- Crypto Council for Innovation
- Democracy Earth Foundation
- Electric Coin Company
- Elliptic
- Ernst & Young (EY)
- Ethereum Foundation
- Filecoin Foundation
- Google (Google Cloud)
- Human Rights Foundation
- The Initiative for Cryptocurrencies and Contracts (IC3)
- International Business Machines (IBM)
- Klynveld Peat Marwick Goerdeler (KPMG)

- Medici Land Governance
- Microsoft
- New York State Department of Financial Services
- Office of New York State Assembly Member Clyde Vanel
- Outdid
- Solidus Labs
- Stanford University
- State of Wyoming
- Stellar Development Foundation
- Switzerland - The Canton of Zug, Economic Promotion Office
- Switzerland State Secretariat for International Finance
- Tech:NYC
- The City College of New York
- The Giving Block
- University College London
- University of San Francisco
- University of Zurich
- World ID (Tools for Humanity)

Appendix II – Blockchain Layers Diagram

This diagram of blockchain ecosystem layers, shows how base infrastructure, scaling solutions, protocols, and applications build on one another to support both financial and non-financial use cases. Graphic adapted by the OTI from the Federal Reserve Bank of St. Louis' "Decentralized Finance: On Blockchain – and Smart Contract-Based Financial Markets" report (2021)[102] and the White House's Strengthening American Leadership in Digital Financial Technology report on digital assets (2025).[103]



Blockchain Layers

Application Layer

User-facing apps, dashboards, or portals that interact with Layer 3 protocols (e.g., wallets, web apps, mobile apps, etc.

Application Layer

Layer 3

Domain-specific smart contracts or systems built on L1 or L2 for use cases such as digital identity manage, land/property registries, healthcare records

Auxiliary smart contracts such as oracles, registries, bridges, etc.

Protocol Layer

Layer 2

Native Asset

(e.g., ETH, BTC)

Protocols that improve speed, cost, and efficiency while relying on Layer 1 for security (e.g., Rollups (Arbitrum, Optimism), zkSync, StarkNet)

Scaling Layer

Layer 1

Ethereum, Bitcoin, Solana, Hyperledger, Avalanche, etc.

Base Layer

Layer 0

Infrastructure enabling multiple blockchains to connect and communicate (e.g., Cosmos, Polkadot, Avalanche Subnets)

Interoperability Layer

Appendix III – Additional Blockchain Concepts and Technologies

This appendix provides additional context on advanced blockchain concepts and technologies that are not central to current city operations but help illustrate how the broader ecosystem is evolving. These topics, including Web3, decentralized autonomous organizations (DAOs), zero-knowledge proofs, and oracle networks, showcase how blockchain systems have expanded beyond digital assets to support new models of digital services, governance experimentation, and privacy-preserving data exchange.

While these developments remain largely early-stage and outside the scope of near-term city adoption, understanding them helps New York City remain informed as emerging technologies mature, particularly in areas related to identity, data governance, public participation, and digital infrastructure.

Web3 and New Models of Governance

As Ethereum's functionality expanded, it gave rise to an entirely new stage in blockchain's evolution: the emergence of decentralized applications (dApps) and the broader "Web3" movement. Because Ethereum is open-source, developers anywhere in the world could build on its base layer, creating applications that interact directly with the network. Smart contracts became the foundation for dApps, which often look like regular websites or apps but are powered by blockchain instead of centralized servers.

This marked a shift from blockchain as primarily a financial tool toward a broader vision of decentralized digital services. Collectively, these applications form part of what is often called "Web3," which aims to shift control of digital services and data away from centralized platforms toward decentralized ownership and governance. Supporters believe this model can give users greater control over their information, reduce dependence on large technology companies, and create more transparent and community-driven systems.[104]

Building on these innovations, another related concept emerged: Decentralized Autonomous Organizations (DAOs).[105] DAOs use smart contracts to establish rules for collective governance, allowing groups of participants to coordinate, pool resources, and make decisions without a central managing entity. While DAOs remain experimental and face challenges around regulation, legal recognition, and inclusivity, they illustrate how blockchain is being used not just to build applications, but also to test new models of digital governance, organization and collaboration.

These models may inform future conversations about public participation, digital identity, digital public infrastructure, and how communities could collaborate or organize around shared civic goals in digital environments.

Key Technologies Underpinning Blockchain Systems

Blockchain relies on a set of foundational technologies that enable its capabilities related to decentralization, security, and verifiability. At the heart of these systems is cryptographic hashing, a technique that ensures that once information is recorded on a blockchain, it cannot be altered without detection. A hash is a fixed-length string of numbers and letters generated whenever data is entered into the system.[106] Even the smallest change in the input produces a completely different hash, making tampering immediately obvious.

As noted earlier, control and access to blockchain data are managed through digital keys and digital wallets. A public key serves as a visible account identifier, while a private key enables its owner to authorize transactions. To guarantee authenticity, digital signatures verify that the person using a private key is indeed its rightful owner.[107] Digital wallets act as the interface for users to manage these keys, securely store account identifiers, and interact with blockchain applications. Importantly, beyond cryptocurrency, wallets are now being explored as platforms for digital identity management, storing credentials that can be used to access government services, verify eligibility, or log in to secure systems.

As digital identity solutions evolve globally, including municipal and national pilots, understanding these tools may be useful for long-term planning related to secure access to public services, credential management, and resident privacy.

Beyond the Basics: Advanced Tools for Security and Real-World Integration

Other cryptographic tools provide additional layers of security and flexibility. For example, multi-signature (multi-sig) authorization requires multiple parties to approve a transaction before it is processed. This is different from consensus mechanisms, which validate transactions across the entire network. Multi-sig operates at the user or account level, making it useful for shared accounts, treasury controls, or organizational governance.[108] Similarly, zero-knowledge proofs (ZKPs) [109] as explained earlier, enable selective disclosure and privacy-preserving verification.

Another crucial technology supporting blockchain systems is oracles. Blockchains are intentionally isolated from the outside world to preserve security and integrity. Oracles bridge this gap by transmitting data from external sources, such as financial markets, weather services, or IoT sensors, into blockchain systems. This capability enables smart contracts (programs that automatically enforce rules or agreements) to respond to real-world events. For example, an oracle could provide shipping data that triggers automated payments, or environmental readings that update permits in real time.[110]

As governments explore secure digital credentials, privacy-preserving verification, and trusted automation, these mechanisms may inform future approaches to secure data exchange and regulated automation in city processes.

Appendix IV: Diagram Comparing Public, Private, and Hybrid Blockchains

FEATURE	PUBLIC BLOCKCHAIN	PRIVATE BLOCKCHAIN	HYBRID BLOCKCHAIN
Access	Open to anyone; no approval required	Restricted; only approved participants can join	Mix of open and restricted access depending on data or function
Governance	Decentralized, no single entity in control	Centralized; administrators manage the network	Shared governance; split between public transparency and private control
Consensus Mechanisms	Typically PoW or PoS; prioritizes decentralization over speed	Usually simpler consensus; prioritizes efficiency	May combine consensus mechanisms
Transparency	High – anyone can verify transactions	Limited – visibility restricted to authorized users	Selective – some data public, some private
Privacy	Pseudonymous; privacy requires extra tools (e.g., zero-knowledge proofs (ZK proofs), encryption, off-chain storage)	Stronger data confidentiality through restricted access, but still depend on encryption and storage design	Balances transparency and confidentiality (e.g., public record of status, private details restricted)

Figure 4. Main Types of Blockchain. Adapted from: University of Cambridge, Global Blockchain Benchmarking Study, 2017.[111] Table modified by NYC OTI to reflect government contexts.

Appendix V: International Policy and Standards

Globally, blockchain policy varies widely. Some jurisdictions are pursuing proactive or comprehensive frameworks and others taking narrow or reactive approaches. The European Union's Markets in Crypto-Assets Regulation (MiCA),[112] adopted in 2023, creates a unified licensing and disclosure regime for crypto-asset service providers across all EU member states. MiCA also sets out rules for stablecoins, including reserve requirements and redemption rights, which in some respects parallel aspects of the U.S. GENIUS Act.

Beyond the European Union, countries are adopting a mix of regulatory approaches to digital assets. Singapore[113] and Switzerland[114] are taking proactive steps to provide clear guidelines for crypto businesses, creating licensing and compliance frameworks that support innovation while addressing risks such as money laundering and consumer protection. Other nations, such as China and India, have taken a more restrictive stance, banning or heavily limiting crypto activities altogether.[115] These divergent approaches highlight the ongoing challenge for international coordination, as regulators balance fostering innovation with protecting financial stability and public trust.

Notes

[1] a16z Crypto, *Builder Energy Dashboard (interactive tool)*, a16z Crypto, (last accessed November 3, 2025), available at: https://builderenergy.a16zcrypto.com/

[2] a16z Crypto, *State of Crypto Report 2025*, a16z Crypto, 2025, available at: https://a16zcrypto.com/posts/article/state-of-crypto-report-2025/

[3] For a full list of organizations interviewed, see Appendix I.

[4] These rules are known as "consensus mechanisms" in the context of blockchain - the concept of consensus mechanisms is explained in greater detail in SECTION 1.4, below.

[5] PwC, "Making Sense of Bitcoin, Cryptocurrency and Blockchain," PwC, August 26, 2025, available at: https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html

[6] There is additional explanation of this characteristic of blockchains in the Key Technologies section.

[7] While current cryptographic standards make altering blockchain data practically infeasible with current computers, future advancements in quantum computing could compromise existing encryption standards. Attacks by quantum computers remain an emerging yet likely distant risk. That said, research and early deployment of post-quantum encryption are already underway to prepare for this possibility. To learn more, visit, e.g., National Institute of Standards and Technology (NIST), *Post-Quantum Cryptography Project*, (last accessed August 26, 2025), available at: https://csrc.nist.gov/projects/post-quantum-cryptography, archived at: https://web.archive.org/web/20251013000000/https://csrc.nist.gov/projects/post-quantum-cryptography, accessed on November 12, 2025.

[8] Andreas M. Antonopoulos and David A. Harding. *Mastering Bitcoin: Programming the Open Blockchain*. 3rd ed., O'Reilly Media, December 2023. https://github.com/bitcoinbook/bitcoinbook?tab=readme-ov-file

[9] For more detail on the various ways this can be configured, see section 1.4.

[10] Vitalik Buterin, "Credible Neutrality As A Guiding Principle," Jan 2, 2020, available at: https://balajis.com/p/credible-neutrality

[11] Antonopoulos and Harding, *Mastering Bitcoin*, 2023.

[12] Despite the name, "smart contracts" are not necessarily legal contracts in the traditional sense. They are pieces of code stored on a blockchain that automatically execute pre-defined actions when certain conditions are met. Their enforceability as legal agreements depend on the surrounding legal framework and how they are used.

[13] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. October 31, 2008, available at: https://bitcoin.org/bitcoin.pdf

[14] "Satoshi Nakamoto" is a pseudonym. To date, the true identity of the author(s) of the *Bitcoin: A Peer-to-Peer Electronic Cash System* whitepaper remains unknown. It is not clear whether Nakamoto was an individual or group, and no verified public evidence has ever confirmed their identity.

[15] National Institute of Standards and Technology (NIST), "*Double Spend (Problem) – Glossary*" CSRC, 2025, available at: https://csrc.nist.gov/glossary/term/double_spend

[16] Antonopoulos, Andreas M., and Gavin Wood, *Mastering Ethereum*, 1st ed., O'Reilly Media, 2017, available at: https://github.com/ethereumbook/ethereumbook

[17] Antonopoulos and Harding, *Mastering Bitcoin*, 2023.

[18] Decentralized finance (DeFi) refers to a set of blockchain-based financial tools and services that operate without traditional intermediaries such as banks or brokers. DeFi applications use smart contracts to enable activities like trading, lending, and payments directly between users on decentralized networks. These systems are typically open-source and permissionless, allowing anyone with internet access to participate and verify transactions. While DeFi aims to increase transparency, reduce reliance on centralized institutions, and expand access to financial services, it also introduces risks related to cybersecurity, market volatility, and technical complexity.

[19] Etherscan, "Ethereum Average Gas Price Chart," Etherscan, 2025, available at: https://etherscan.io/chart/gasprice

[20] Chainlink. "What Is Layer 2?," Chainlink, 2025, available at: https://chain.link/education/what-is-layer-2

[21] L2BEAT, “The State of the Layer Two Ecosystem,” L2BEAT, 2025, available at: https://l2beat.com/summary/

[22] Chainalysis, “Introduction to Layer 3 in Blockchain,” Chainalysis, 2025, available at: https://blog.chainalysis.com/reports/introduction-to-layer-3-in-blockchain

[23] ConsenSys, “Busting the Myth of Private Blockchains,” ConsenSys, 2025, available at: https://consensys.net/blog/blockchain-explained/busting-the-myth-of-private-blockchains/

[24] European Union Blockchain Observatory & Forum, *Energy Efficiency of Blockchain Technologies: A Thematic Report*, European Commission, December 2019, available at: https://blockchain-observatory.ec.europa.eu/document/download/4e612a85-eac1-44fd-b7b6-bf97e51abaea_en?filename=Energy%20Efficiency%20of%20Blockchain%20Technologies_1_0.pdf

[25] Cointelegraph, "Permissioned Blockchain vs. Permissionless Blockchain: Key Differences,” Cointelegraph, August 8, 2025, available at: https://cointelegraph.com/learn/articles/permissioned-blockchain-vs-permissionless-blockchain-key-differences

[26] Viktor Charpentier and Tom Johansson, *Blockchain Database: Technical Background and a Reconnaissance on an Implementation Within the Banking Industry*, KTH Royal Institute of Technology, 2017, available at: https://kth.diva-portal.org/smash/get/diva2:1127299/FULLTEXT01.pdf

[27] Daniela Barbosa et al., *Hyperledger in Action: Supply Chain and Trade Finance*, Linux Foundation, 2023, available at: https://www.linuxfoundation.org/hubfs/Hyperledger_Supply_Chain_Trade_Finance_ebook_03.pdf?hsLang=en

[28] Treiblmaier, H., “*Harnessing Blockchain to Transform Healthcare Data,” Blockchain in Healthcare Today*, 2024, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11073478/

[29] A complete list of organizations interviewed for this Plan is included in Appendix I.

[30] Reuters, “California DMV Puts $42 Million in Car Titles on Blockchain to Fight Fraud,” July 30, 2024, available at: https://www.reuters.com/technology/california-dmv-puts-42-million-car-titles-blockchain-fight-fraud-2024-07-30/?utm_source=chatgpt.com

[31] Gobierno de la Ciudad Autónoma de Buenos Aires, “miBA con tecnología QuarkID: la Ciudad de Buenos Aires incorporó blockchain a su sistema de identidad digital,” Buenos Aires Ciudad, 2025, available at: https://www.buenosaires.gob.ar/miBA-quarkid-blockchain-identidad-digital

[32] Baltimore City Government, “Baltimore City Title Search Portal,” Baltimore City Government, 2025, available at: https://titlesearch.baltimorecity.gov/

[33] GovTech, “Baltimore Uses Blockchain to Target Blighted Properties,” *GovTech*, June 24, 2025, available at: https://www.govtech.com/civic/baltimore-uses-blockchain-to-target-blighted-properties

[34] Washoe County Recorder's Office, “Digitally Certified Record Copies,”. Washoe County Government, 2025, available at: https://www.washoecounty.gov/recorder/blockchain.php

[35] Insights shared in stakeholder interview with Washoe staff in May 2025.

[36] Federal Emergency Management Agency (FEMA), *Strategic Foresight 2050 Final Report*, FEMA, 2025, available at: https://www.fema.gov/sites/default/files/documents/fema_strategic-foresight-2050-final-report.pdf, archived at: https://web.archive.org/web/20251013000000/https://www.fema.gov/sites/default/files/documents/fema_strategic-foresight-2050-final-report.pdf, accessed on November 12, 2025.

[37] City of Reno, “Biggest Little Blockchain: Historic Registry Pilot Program,” City of Reno Government, 2025, available at: https://int-renopublic.azurewebsites.net/

[38] Internet Archive, “Democracy’s Library: Preserving Government Data with Decentralized Storage,” Internet Archive, November 21, 2023, available at https://upload.fil.org/p/democracys-library-one-petabyte-later

[39] Canton of Zug, “*Tax Payments with Cryptocurrencies,”* Canton of Zug, March 1, 2023, available at: https://zg.ch/de/steuern-finanzen/steuern/steuerbezug/taxpaymentswithcryptocurrencies

[40] Swiss Federal Council, *Legal Framework for Distributed Ledger Technology and Blockchain in Switzerland*, Government of Switzerland, December 14, 2018, available at: https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf

[41] City of Lugano, “LVGA Token: A Local Cryptocurrency for Regional Economic Activity*,”* City of Lugano, 2025, available at: https://my.lugano.ch/en/lvga/

[42] City of Williston, *City of Williston Accepts Cryptocurrency Payments for Utility Bills*, (last accessed August 26, 2025), available at: https://cityofwilliston.com/news_detail_T18_R1029.php
[43] Insights shared in stakeholder interview with Williston staff in May 2025.
[44] Colorado Department of Revenue, "Cryptocurrency Payments," Colorado Department of Revenue, 2022, available at: https://tax.colorado.gov/cryptocurrency
[45] Chainalysis, "Bitcoin Strategic Reserves: Behind the Changing Architecture of Sovereign Finance," Chainalysis, May 29, 2025, available at: https://www.chainalysis.com/blog/bitcoin-strategic-reserves/
[46] The White House, "Establishment of the Strategic Bitcoin Reserve and United States Digital Asset Stockpile," The White House, March 6, 2025, available at: https://www.whitehouse.gov/presidential-actions/2025/03/establishment-of-the-strategic-bitcoin-reserve-and-united-states-digital-asset-stockpile/
[47] Texas Senate Bill 21, 89th Legislature, Regular Session. *Relating to the establishment and administration of the Texas Strategic Bitcoin Reserve for the purpose of investing in cryptocurrency and the investment authority of the comptroller of public accounts over the reserve and certain other state funds,*" Texas Legislature Online, 2025, available at: https://capitol.texas.gov/tlodocs/89R/billtext/html/SB00021I.htm
[48] Pennsylvania House Bill 2664, 2023-2024 Regular Session, *An Act providing for authorization for State Treasurer to invest in Bitcoin or digital assets and for authorization for systems to invest in exchange-traded products*, Pennsylvania General Assembly, 2024, available at: https://www.palegis.us/legislation/bills/2023/hb2664
[49] Wyoming House Bill 201, 2025 General Session, *An act relating to public funds; authorizing the investment of state funds and permanent funds in Bitcoin; specifying requirements for the investment in Bitcoin; requiring rulemaking; requiring reports; providing definitions; and providing for an effective date,* Wyoming Legislature, 2025, available at: https://legiscan.com/WY/bill/HB0201/2025 US Strategic Bitcoin Reserve Monitor+5
[50] Ohio Senate Bill 57, 136th General Assembly, *Enact the Ohio Bitcoin Reserve Act*, Ohio Legislature, 2025, available at: https://www.legislature.ohio.gov/legislation/136/sb57
[51] Ledger Insights, "Lugano, SIX issue digital bonds on SDX," *Ledger Insights*, May 21, 2025, available at: https://www.ledgerinsights.com/lugano-six-issue-digital-bonds-on-sdx/
[52] Bond Buyer, "Quincy, Massachusetts, issues first-ever blockchain bond deal in U.S.," *Bond Buyer*, April 25, 2024, available at: https://www.bondbuyer.com/news/quincy-massachusetts-issues-first-ever-blockchain-bond-deal-in-u-s
[53] U.S. Secret Service, *Public Alert: Cryptocurrency Mixing*, June 2025, available at: https://www.secretservice.gov/sites/default/files/reports/2025-06/Public-Alert-Cryptocurrency-Mixing.pdf
[54] Chainalysis, "Privacy Coins: Anonymity-Enhanced Cryptocurrencies," Chainalysis, (last accessed August 26, 2025), available at: https://www.chainalysis.com/blog/privacy-coins-anonymity-enhanced-cryptocurrencies/
[55] Warren Liang and Britney Johnson Mary, "Tracing Illicit Crypto Flows: Blockchain Analytics Techniques for Identifying Sanctions Evasion Networks," 2024, available at: https://www.researchgate.net/publication/395456196_Tracing_Illicit_Crypto_Flows_Blockchain_Analytics_Techniques_for_Identifying_Sanctions_Evasion_Networks
[56] U.S. Department of Justice, *Report of the Attorney General's Cyber Digital Task Force on Cryptocurrency White Paper*, January 2021, p. 59, available at: https://www.justice.gov/usao/page/file/1403671/dl?inline=
[57] Examples of such tools include Chainalysis, Elliptic, Solidus Labs, TRM Labs, among others.
[58] Endong Liu (University of Birmingham), Mark Ryan (University of Birmingham), Liyi Zhou (University of Sydney), and Pascal Berrang (University of Birmingham), "Evasion Under Blockchain Sanctions," *arXiv*, July 15, 2025, available at: https://arxiv.org/abs/2507.11721
[59] Europol, "Crypto Investment Fraud Ring Dismantled in Spain After Defrauding 5,000 Victims Worldwide," (last accessed August 26, 2025), available at: https://www.europol.europa.eu/media-press/newsroom/news/crypto-investment-fraud-ring-dismantled-in-spain-after-defrauding-5-000-victims-worldwide
[60] Chainalysis, "How Chainalysis Helped Uncover an NCA Officer's Theft of Seized Bitcoin," Chainalysis, July 16, 2025, available at: https://www.chainalysis.com/blog/nca-officer-theft-of-seized-bitcoin-july-2025/

[61] Chainalysis, "U.S. and Canada Join Forces to Combat Crypto Scams," Chainalysis, July 30, 2025, available at: https://www.chainalysis.com/blog/us-and-canada-join-forces-to-combat-crypto-scams/

[62] United Nations Office on Drugs and Crime (UNODC), *Cryptocurrency Investigations* (training resource), UNODC, (last accessed November 7, 2025), available at: https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/investigation/cryptocurrency.html; Financial Action Task Force (FATF), *Virtual Assets: Red Flag Indicators of Money Laundering and Terrorist Financing*, FATF/OECD, September 2020, available at: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html.

[63] Miami-Dade Police Department, "Cyber Crimes Bureau," Miami-Dade County, (last accessed August 26, 2025), available at: https://www.miamidade.gov/global/police/about-cyber-crimes-bureau.page

[64] Chainalysis, "Blockchain Analysis for National Security and Law Enforcement Agencies: A Primer," July 21, 2022, available at: https://www.chainalysis.com/blog/blockchain-analysis-national-security-law-enforcement-agencies-a-primer/

[65] Etherscan, "Average Daily Transaction Fee Chart of ETH*,"* Etherscan, (Last accessed August 26, 2025), available at: https://etherscan.io/chart/avg-txfee-usd

[66] NYC Economic Development Corporation, *NYC Node: Blockchain Applied Learning Program,* NYCEDC, April 8, 2024, available at: https://edc.nyc/press-release/nycedc-nyc-talent-and-cuny-queens-college-launch-nyc-node-blockchain-applied-learning

[67]NYC Economic Development Corporation, *Industry Programs Update 2019,* NYCEDC, October 2019, available at: https://edc.nyc/sites/default/files/2019-10/nycedc-industry-programs-update-v02.2.pdf

[68] New York City Office of Technology and Innovation, *Citywide Privacy Protection Policies and Protocols*, June 13, 2025, available at: https://www.nyc.gov/assets/oti/downloads/pdf/reports/cpo/2025%20Citywide%20Privacy%20Protection%20Policies%20and%20Protocols_web.pdf

[69] *Ibid.*

[70] New York City Office of Technology and Innovation, *Cybersecurity Requirements for Vendors and Contractors*, New York City, available at: https://www.nyc.gov/content/oti/pages/vendor-resources/cybersecurity-requirements-for-vendors-contractors

[71] These principles are reflected across several existing city frameworks. For example, transparency is emphasized through the NYC *Open Data Law* (Local Law 11 of 2012). Privacy obligations stem from the *Identifying Information Law (Local Law 245 of 2017)* and the *Citywide Privacy Protection Policies and Protocols (CPO Policy)*, which govern how agencies collect, use, and share personal data. Environmental sustainability goals are established in *PlaNYC: Getting Sustainability Done (2023)* and *Local Law 97 of 2019*, which set citywide greenhouse-gas-reduction targets and require agencies to consider environmental impact in technology and operations. Together, these frameworks provide the baseline expectations that any emerging technology, including blockchain, must align with.

[72] New York City Police Department, *Cryptocurrency Analysis Tools: Impact and Use Policy*. NYPD, April 11, 2021, available at: https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/cryptocurrency-analysis-tools-nypd-Impact-and-use-policy_4.9.21_final.pdf

[73] New York State Department of Financial Services, *Virtual Currency Business Licensing,* New York State DFS, (last accessed August 26, 2025), available at: https://www.dfs.ny.gov/consumers/virtual-currency-business-licensing

[74] New York State, *Environmental Quality Review Act: Public Scope Document on Cryptocurrency Geothermal Projects*, (last accessed August 26, 2025), available at: https://dec.ny.gov/sites/default/files/2024-04/cryptogeisfinalpublicscope.pdf

[75] Vermont General Assembly. *Vermont Legislative Documents,* Vermont General Assembly, (last accessed August 26, 2025), available at: https://legislature.vermont.gov/

[76] Illinois General Assembly, *Blockchain Technology Act, 205 ILCS 730,* Illinois General Assembly, (Last accessed August 26, 2025), available at: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4077&ChapterID=36

[77] Arizona State Legislature, *House Bill 2417: Blockchain-Related Legislation,* Arizona State Legislature, (last accessed August 26, 2025), available at: https://www.azleg.gov/legtext/55leg/1R/bills/HB2417P.pdf

[78] Wyoming State Legislature, *Senate File 0038, 2021 General Session,* Wyoming State Legislature, (last accessed August 26, 2025), available at: https://www.wyoleg.gov/Legislation/2021/SF0038 . There is more information on DAOs broadly in Appendix III, Additional Blockchain Concepts and Technologies.

[79] California Department of Financial Protection and Innovation (DFPI), *Digital Financial Assets,* DFPI, (last accessed August 26, 2025), available at: https://dfpi.ca.gov/digital-financial-assets/

[80] U.S. Securities and Exchange Commission (SEC), *Crypto Task Force,* SEC, (last accessed August 26, 2025), available at: https://www.sec.gov/spotlight/crypto

[81] U.S. Commodity Futures Trading Commission (CFTC), *Digital Assets,* CFTC, (last accessed August 26, 2025), available at: https://www.cftc.gov/DigitalAssets

[82] U.S. Department of Justice, *Report of the Attorney General's Cyber Digital Task Force on Cryptocurrency White Paper*, January 2021, p. 59, available at: https://www.justice.gov/usao/page/file/1403671/dl?inline=, archived at: https://web.archive.org/web/20240325020544/https://www.justice.gov/usao/page/file/1403671/dl?inline=, accessed on November 12, 2025.

[83] Federal Trade Commission (FTC), *What to Know About Cryptocurrency Scams*, (last accessed November 12, 2025), available at: https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-scams, archived at: https://web.archive.org/web/20240905014623/https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-scams, accessed on November 12, 2025.

[84] PwC, *Global Crypto Regulation Report 2025: Navigating the Global Landscape,* PwC, March 2025, available at: https://legal.pwc.de/content/services/global-crypto-regulation-report/pwc-global-crypto-regulation-report-2025.pdf

[85] They are often argued to offer the stability of traditional currency combined with the speed and efficiency of digital assets, see, e.g., their widespread use in DeFi liquidity and lending markets (a16z Crypto, State of Crypto Report 2025) and early experiments using stablecoins for trade settlement and cross-border payments (IMF, Digital Money and Cross-Border Payments, 2024).

[86] Chainalysis, "Stablecoins 101: Behind Crypto's Most Popular Asset," Chainalysis, December 11, 2024, available at: https://www.chainalysis.com/blog/stablecoins-most-popular-asset/

[87] *Ibid.*

[88] European Parliament, *Stablecoins: Financial Stability, Monetary Policy, and Financial Inclusion Implications*, European Parliamentary Research Service, 2021, available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698803/EPRS_BRI(2021)698803_EN.pdf

[89] The White House, *Executive Order on Ensuring Responsible Development of Digital Assets*, March 9, 2022, available at: https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/, archived at: https://web.archive.org/web/20240323022035/https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/, accessed on November 12, 2025.

[90] Congressional Research Service, *Digital Assets and the Federal Response*, CRS Report R47450, April 18, 2023, available at: https://crsreports.congress.gov/product/pdf/R/R47450

[91] PwC, *Global Crypto Regulation Report 2025, 2025.*

[92] See, e.g., Yahoo Finance, Proof of Operation Chokepoint 2.0*,"* Yahoo Finance, December 8, 2024, available at: https://finance.yahoo.com/news/proof-operation-chokepoint-2-0-194948609.html and U.S. House of Representatives, Committee on Financial Services, Subcommittee on Oversight and Investigations, *Hearing on Operation Choke Point 2.0: The Biden Administration's Efforts to Put Crypto in the Crosshairs,* 119th Congress, 1st session, February 6, 2025, available at: https://www.congress.gov/event/119th-congress/house-event/117858

[93] The White House, *Executive Order on Strengthening American Leadership in Digital Financial Technology*, January 23, 2025, available at: https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/, archived at: https://web.archive.org/web/20250201000000/https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/, accessed on November 12, 2025.

[94]The White House, *Strengthening American Leadership in Digital Financial Technology*, July 30, 2025, available at: https://www.whitehouse.gov/crypto/, archived at:

https://web.archive.org/web/20251014000000/https://www.whitehouse.gov/crypto/, accessed on November 12, 2025.

[95] United States Congress, *Guiding and Establishing National Innovation for U.S. Stablecoins Act of 2025* (GENIUS Act), S. 1582, 119th Congress, 1st session, enacted July 18, 2025, available at: https://www.congress.gov/bill/119th-congress/senate-bill/1582

[96] New York Times, "*Wall Street Banks Embrace Stablecoins: A Payments Revolution in the Making," New York Times*, August 13, 2025, available at: https://www.nytimes.com/2025/08/13/business/wall-street-banks-crypto-stablecoins.html

[97] Cambridge Centre for Alternative Finance, Cambridge Bitcoin Electricity Consumption Index (CBECI), University of Cambridge Judge Business School, (last reviewed September 12, 2025, updated continuously), available at: https://ccaf.io/cbnsi/cbeci

[98] U.S. Energy Information Administration (EIA), *Tracking electricity consumption from U.S. cryptocurrency mining operations*, February 1, 2024, available at: https://www.eia.gov/todayinenergy/detail.php?id=61364&utm_source=chatgpt.com

[99] Warren Liang and Britney Johnson Mary, "Tracing Illicit Crypto Flows: Blockchain Analytics Techniques for Identifying Sanctions Evasion Networks," 2024 (SSRN working paper), available at: https://download.ssrn.com/22/08/12/ssrn_id4188246_code2116257.pdf

[100] Kapengut, E., & Mizrach, B,"An event study of the Ethereum transition to proof-of-stake," *Commodities* 2(2), pp. 96-110, 2023, available at: https://doi.org/10.3390/commodities2020006

[101] Cambridge Centre for Alternative Finance, *Cambridge Digital Mining Industry Report*, University of Cambridge Judge Business School, April 2025, available at: https://www.jbs.cam.ac.uk/wp-content/uploads/2025/04/2025-04-cambridge-digital-mining-industry-report.pdf and KPMG, *Bitcoin's Role in the ESG Imperative: An Overview of the Opportunities and Creative Approaches That Deliver Value and Drive Trust* (2023), https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2024/bitcoins-role-esg-imperative.pdf

[102] Federal Reserve Bank of St. Louis, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets,* Federal Reserve Bank of St. Louis Review, Second Quarter 2021, available at: https://www.stlouisfed.org/-/media/project/frbstl/stlouisfed/publications/review/pdfs/2021/04/15/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets.pdf

[103] The White House, *Strengthening American Leadership in Digital Financial Technology*, July 30, 2025, p. 22, available at: https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf, archived at: https://web.archive.org/web/20250804112908/https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf, accessed on November 12, 2025.

[104] Ethereum Foundation, "What is Web3 and why is it important?," (last accessed August 26, 2025), available at: https://ethereum.org/web3/

[105] Chainalysis, "*Introduction to Decentralized Autonomous Organizations (DAOs),"* Chainalysis, April 7, 2023, available at: https://www.chainalysis.com/blog/introduction-to-decentralized-autonomous-organizations-daos/

[106] Antonopoulos and Harding, Mastering Bitcoin, 2023.

[107] Andreas M. Antonopoulos, *Introduction to Digital Currencies*, University of Nicosia, 2025, available at: https://www.unic.ac.cy/unic-launches-mooc-in-introduction-to-digital-currencies-msc-in-digital-currency/

[108] Coinbase, "What is Multi-Signature (Multi-Sig)?," Coinbase, August 25, 2025, available at: https://www.coinbase.com/learn/wallet/what-is-a-multi-signature-multi-sig-wallet

[109] Chainalysis, "Introduction to Zero-Knowledge Proofs," Chainalysis, 2025, available at: https://blog.chainalysis.com/reports/introduction-to-zero-knowledge-proofs

[110] Chainlink. "What Is an Oracle in Blockchain? Explained," Chainlink, 2025, available at: https://chain.link/education/what-is-an-oracle

[111] Garrick Hileman and Michele Rauchs, *Global Blockchain Benchmarking Study,* University of Cambridge's Judge Business School / Cambridge Centre for Alternative Finance, 2017, available at: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-09-27-ccaf-globalbchain.pdf

[112] European Union, *Markets in Crypto-Assets Regulation (MiCA),* European Union, (last accessed August 26, 2025), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065

[113] Monetary Authority of Singapore, *Response to Feedback Received on Proposed Regulatory Approach: Regulations and Notices for Digital Token Service Providers under the Financial Services and Markets Act 2022,* MAS, May 30, 2025, available at: https://www.mas.gov.sg/-/media/response-to-feedback-received-from-dtsp-cp.pdf

[114] Swiss Federal Council, *Legal Framework for Distributed Ledger Technology and Blockchain in Switzerland,* Government of Switzerland, December 14, 2018, available at: https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf

[115] Atlantic Council, *Cryptocurrency Regulation Tracker,* Atlantic Council, (last accessed August 11, 2025), available at: https://www.atlanticcouncil.org/cryptocurrency-regulation-tracker