Partnering for the Future: How a New U.S. Government Blockchain Payment System Can Drive Private-Sector Growth

By Tricia Gallagher, former Senior Financial Expert
and International Economist, U.S. Department of the Treasury
April 21, 2025

Overview -

After dismantling bloated federal programs and exposing inefficiencies in government spending,[1] the Trump administration now has an important opportunity to pivot from tearing down to building up federal government programs — beginning by building the foundation for America's next-generation digital financial infrastructure, or payment "rail". This paper outlines how the United States (U.S.) government, led by the U.S. Department of the Treasury (Treasury), can modernize outdated payment infrastructure using blockchain technology while creating significant new business opportunities for U.S. companies.

Today's federal payment systems are aging, expensive to maintain, and overdue for reinvention. Thanks to **permanent and indefinite (P&I)** appropriations already in place to support Treasury payment systems, the Trump administration can act immediately. [2] Importantly, the U.S. government will require broad private-sector engagement — including the designation of new Financial Agents and the contracting of fintechs, banks, wallet developers, compliance firms, and technology providers — to help build and operate this government blockchain-based infrastructure.

This effort will extend well beyond the federal level**.** State governments, which already deliver disaster relief, public benefits, and identity verification, are uniquely positioned to also lead on innovation. With access to federal funds and matching incentives, states can contract with local and national partners to develop interoperable digital IDs, last-mile delivery tools, and user-friendly payment interfaces. This is where community banks, fintechs, and smaller innovators can thrive.

To begin, the administration can focus on disaster relief payments — a use case that involves multiple layers of government, and preconditions and compliance requirements that must be verified before funds can be released. This is where blockchain is well suited to introduce efficiencies.

The Trump administration must lead this development effort and construct a **U.S. Government Blockchain Roadmap** — one that lays out a strategic, phased approach and timeline for modernizing public-sector financial payment systems. A predictable path forward will give the private sector confidence to invest, innovate, and compete. With the right foundation, public-sector

[1] Office, A. (2025, March 11). *Fraud & Improper Payments*. Gao.gov; U.S. Government Accountability Office. https://www.gao.gov/fraud-improper-payments

[2] United States Government Accountability Office. (2017, January 25). *Revenue Collections and Payments: Treasury Has Used Financial Agents in Evolving Ways but Could Improve Transparency. GAO-17-176*. https://www.gao.gov/assets/690/688595.pdf

modernization can become a catalyst for private-sector growth, connecting public investment with market opportunity.

Public-Sector Blockchain as a Catalyst for U.S. Innovation -

Disaster Relief Payments — Ideal Initial Use Case: Blockchain is not a technology meant to replace all forms of payment, nor should it. The U.S. already has robust, resilient, and highly efficient traditional payment infrastructures that move money quickly and securely. However, blockchain has the potential to revolutionize payments that require complex messaging, conditional approvals among multiple stakeholders, and regulatory compliance, where automation, transparency and efficiency are all critical. This is where blockchain's true power lies.

Disaster relief federal grant disbursements managed by the Federal Emergency Management Agency (FEMA) are an ideal first use case for the application of blockchain in government payments because they are often weighed down by opaque, manual approval processes that stretch across multiple layers of government from federal, state to sometimes local. These payments often involve intricate verification steps, compliance hurdles, and a web of intermediaries that slow down fund distribution or the delivery of critical aid when speed is paramount. Blockchain changes this dynamic by reducing intermediaries and introducing real-time transparency and fund disbursement, allowing all government stakeholders to securely track and verify transactions at the same time on a shared distributed ledger.

Through the use of smart contracts, funds move quickly and seamlessly by self-executing code on the blockchain that automatically carries out transactions or actions once predefined conditions are met. Blockchain technology cuts costs, fraud and improper payments, and improves the efficiency in the government's disbursement of disaster relief funds through programmable, tokenized, transparent fund flows.

There is also a strategic advantage to starting with disaster relief because this is a program the American people see and feel. Faster, smarter disaster aid makes a real difference — to individuals, families, small businesses, and entire communities. Understanding the potential this assistance can have to human lives and communities can be an important driving force towards greater adoption of digital payments and supporting digital IDs, implementation efforts that can be led at the state level.

Benefits of Blockchain Technology for Disaster Relief Payments:

- **Smart contracts** can revolutionize government payments by **automating fund releases** as soon as predefined conditions are met, accelerating disbursements and boosting efficiency.
- **Blockchain** can dramatically **cut the costs** of government payments **by eliminating intermediaries** and streamlining transactions.
- The **distributed nature of blockchain** ensures **transparency and real-time information sharing** across federal, state, and local governments, enhancing coordination and preventing duplicative aid.
- The **immutability of tokenized blockchain** ensures flows are not only transparent but permanent and easily auditable.

- **Digital IDs**, a cornerstone of blockchain, **expand financial access for the unbanked**, or those without access to banking services, and guarantee that aid reaches its intended recipients, **reducing improper payments and fraud**.
- **Careful securely designed interoperability** can extend the reach of the blockchain ecosystem and help engage community banks, fintechs, NGOs, and global donors, enabling tokenized crowdfunding and **broadening the reach of disaster relief efforts**.

Crucial Distinction: Tokenized Deposits, Stablecoins, and Cryptocurrency: For blockchain-based payments to scale in the U.S., they must integrate with the existing traditional financial system. This makes it essential to distinguish among tokenized deposits, stablecoins and cryptocurrencies, all of which are based on blockchain technology.

- **Tokenized deposits** are digital versions of commercial bank deposits, or federal government deposits held in the government's account at the Federal Reserve. Issued by regulated banks and backed by central bank reserves, they settle in central bank money. This ensures they preserve the *singleness of money*—allowing 1:1 convertibility with traditional deposits, without pricing differences or devaluation risk.
- **Stablecoins**, while designed to hold a stable value, can lack transparency around their reserves and may not guarantee 1:1 redemption. Backing assets vary and may not be fully liquid or easily verified. Some stablecoins are issued by non-bank entities without access to deposits or the Federal Reserve's master accounts, raising concerns they could operate outside the regulated traditional banking system. These gaps create risks of financial instability as interoperability and consistent valuation of stablecoins can break down. With the right regulatory framework in place to address these gaps and concerns, stablecoins can play a useful role in payment-related activities, particularly at the "last mile" in delivering digital assets quickly and efficiently to end recipients.
- **Cryptocurrencies** are not tied to sovereign currencies or central authorities. Their prices fluctuate with market sentiment and supply dynamics—such as Bitcoin's fixed cap of 21 million—making them too volatile for reliable payments.

For purposes of a blockchain-based U.S. government payment system, this paper speaks only to the use of tokenized federal government deposits or "tokenized deposits" held at the Federal Reserve in the U.S. Department of the Treasury's (Treasury) General Fund.

Today's Treasury Core Payment Infrastructure: The infrastructure supporting federal government payments is foundational to Treasury's operations and the broader stability of the U.S. economy. Yet, its core platform—the Treasury Web Application Infrastructure (TWAI), built and maintained by the Federal Reserve's IT arm—remains sorely outdated and costly to operate. Treasury has long recognized the need to move key systems off the TWAI, but efforts have stalled due to the complexity of the task and the risk of disrupting critical infrastructure that underpins trillions in annual transactions. For this reason, a phased and careful approach to updating the U.S. government payment infrastructure must be taken.

The U.S. government will importantly need partners in this effort. Currently, Treasury designates the Federal Reserve (Fed) as its Fiscal Agent responsible for managing the TWAI. Also, a narrow set of large financial institution incumbents compete in a limited fashion for designation as

Treasury's Financial Agents in support of the Treasury core payment and collection activities. Unfortunately, these current arrangements, particularly with the Fed, have not delivered the full innovation or infrastructure improvements the federal government payment systems urgently need. To modernize, Treasury must open the door to greater competition—inviting a broader range of banks, nonbanks and consortiums to serve as Financial Agents that help design and implement next-generation blockchain-based payment systems capable of replacing legacy systems.

How Federal Funds Flow—and Where Inefficiencies Persist: Each year, the federal government transfers trillions of dollars to state governments which serve at the frontline in administering programs such as Social Security, Medicare, and disaster relief. Once funds are authorized by Congress and appropriated, federal agencies enter into grant agreements with states in accordance with each program's design and desired outcome. These agreements typically specify the total award amount, program purpose, documentation requirements, compliance obligations, and preconditions for fund release.

When a state requests funds, the federal agency, such as FEMA, reviews the request, verifies compliance with the grant's conditions, and, if satisfied, authorizes the release. At Treasury, Certifying Officers, who are legally responsible for ensuring payments are lawful, proper, and accurate, then certify and approve the disbursement of funds to the states.

Prior to the Cash Management Improvement Act (CMIA) of 1990, [3] federal transfers were often advanced to states well before the funds were needed, resulting in idle balances, lost federal interest income, and adding to mounting federal borrowing costs. At the same time, states frequently earned interest on unspent federal dollars. In response to these inefficiencies, and a broader push for fiscal discipline and modernization, Congress enacted CMIA to streamline cash flows and promote intergovernmental fairness. [4]

While CMIA has improved fund transfer efficiency, practical barriers remain. Chief among them is the lack of transparency around the preconditions federal agencies require before releasing funds, which can create bottlenecks. This is especially pronounced in disaster relief, where urgent funding needs may be delayed by unclear or shifting agency requirements.

U.S. Businesses Stand to Gain from Revenue Capture -

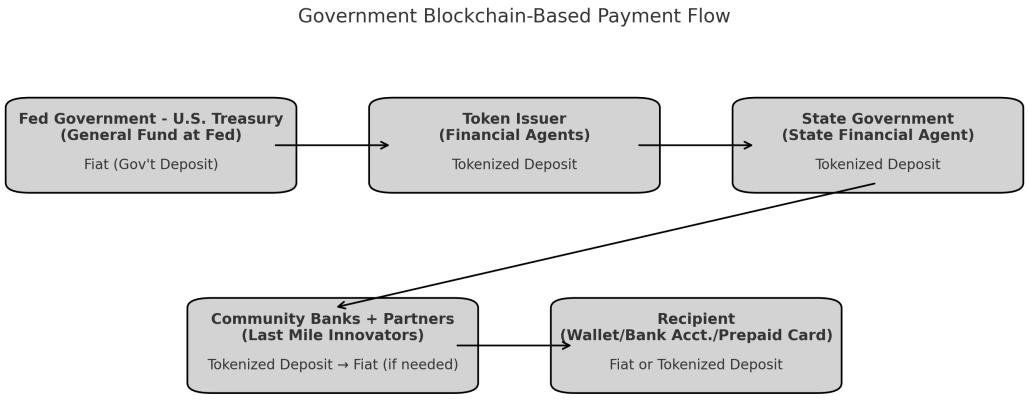
The time is right for the Trump administration to lay out a new framework for federal and state government engagement with the private sector—including large financial institutions, payment processors, community banks, fintechs and startups—to help build scalable, blockchain-based public infrastructure. These public-private partnerships, spanning both federal and state levels, are essential to driving innovation, enhancing service delivery, and unlocking private-sector growth.

A national Roadmap for public-sector investment in blockchain technology opens up immense opportunities—but to realize them, clear guidance is needed on which entities are eligible to partner

[3] *Cash Management Improvement Act - CMIA Statute*. (2018, March 19). Bureau of the Fiscal Service. https://fiscal.treasury.gov/cmia/resources-cmia-statute.html

[4] Financial Management Service, Fiscal Service, Department of the Treasury. (2002, May 10). *Rules and Procedures for Efficient Federal-State Funds Transfers. Federal Register*, *67*(91), 31880-31894.

with government, and under what terms. The diagram below illustrates the key roles in a potential government blockchain-based payment system, highlighting the varied points of entry for different market participants.



Federal Financial Agents: A Role for Scaled Institutions and Strategic Partnerships: At the federal level, Financial Agents—designated by Treasury rather than competitively procured—play a critical role in maintaining the integrity and stability of the U.S. payment system. Traditionally, regulated depository institutions authorized to hold master accounts at the Federal Reserve may settle federal payments. These same large regulated financial institutions have already successfully integrated blockchain and tokenization into their existing platforms, demonstrating that these technologies are not experimental concepts but working solutions being used in real-world financial transactions. Payment processors and select fintechs, meanwhile, have also scaled tokenized networks and blockchain technology solutions.

To tap into this innovation while preserving settlement integrity, the Trump administration could encourage new models of partnership. By allowing regulated banks to formally collaborate with non-deposit-taking payment processors or fintechs, the federal government can leverage both trust and technological agility to design next-generation payment rails. These partnerships could provide the backbone for blockchain architecture used across the federal and state levels.

State-Level Agents, Community Banks, and Fintechs: Where Innovation Meets the End User: Because state and local governments are on the frontline administering public services such as disaster relief, they have closer knowledge of both the needs of their citizens and the capabilities of community banks, and local digital ID providers and fintechs. This positions them well to partner with firms specializing in user interfaces. Some of these smaller players may not hold master accounts at the Fed, but they are ideally positioned to deliver innovative tools for verifying identities and routing payments to intended recipients, while building novel user-facing applications that run on government blockchain infrastructure. This is a space where competition can thrive.

Critically, while federal Financial Agents are "designated" due to national interest in preserving critical government payment infrastructure, in the downstream, state governments can competitively contract with private-sector partners. With federal funds—such as those from the Permanent and Indefinite (P&I) appropriation—states can invest in their own extended state-level blockchain-based infrastructure. These federal funds could be conditioned on state matching, incentivizing local investment in digital payments, identity systems, and financial inclusion tools.

Community and regional banks are uniquely positioned to benefit in support of this state-level development effort due to their deep ties to local communities and ability to reach the unbanked. Meanwhile, fintechs can offer modular, user-friendly services that lower costs and improve compliance, security and government responsiveness, without requiring agencies to build from scratch. Importantly, federal and state regulators will need to provide the guardrails and safeguards needed to encourage partnerships between these two important players.

Digital Identity Providers: The Linchpin of Scalable Blockchain Payments: Blockchain-based payments only work if governments know **who** they are paying. From disaster relief to stimulus credits to Social Security, secure identity verification is foundational to ensuring funds are delivered accurately and fraud is minimized. Digital ID providers, especially those offering privacy-preserving, interoperable solutions, will play a central role in this ecosystem.

State governments can lead by partnering with digital ID issuers and verifiers to integrate identity into payment flows. These systems will be critical not just for eligibility enforcement and anti-fraud controls, but also for ensuring taxpayer accountability and trust in the system.

Public Sector Blockchain Technology: A Primer -

The Promise of Web3: Cryptocurrencies and blockchain technology emerged from a 2008 white paper by Satoshi Nakamoto, whose identity remains unknown to this day. The paper was built on the cypherpunk movement of the 1980s, which advocated privacy and freedom from central control and surveillance through the use of cryptography and decentralized networks. Distrust of central authorities was also fueled by the 2008 financial crisis involving the "too big to fail", along with concerns over personal data capture by big tech companies like Amazon, Google, and Meta.

Today's Web2 internet is built on centralized servers controlled by large corporations that monetize user data. Web3 offers a new vision: a decentralized internet where data, transactions, and applications run on blockchain-based distributed networks and users control their data. It introduces new forms of digital ownership through blockchain-based tokens**,** and it democratizes governance through distributed shared decision-making. In its ideal form, Web3 aspires to create a global, uninterrupted peer-to-peer network, shifting control away from centralized institutions or intermediaries to individuals. Accordingly, Web3 and blockchain have the potential to disrupt incumbent players in today's traditional financial industry and alter market dynamics entirely.

While promising, Web3's fully decentralized vision is incompatible with today's established financial and monetary systems, which require some form of centralized oversight. A staged, hybrid approach towards implementing blockchain, or progressive decentralization, is therefore necessary i.e., gradually introducing decentralization within centralized governance structures. This hybrid

model balances the benefits of a decentralized system such as transparency, financial inclusion and greater user control over data with governance, accountability, compliance, and financial stability.

In government-sponsored blockchain-based payment systems, full decentralization is neither feasible nor desirable. What matters is a shared transparent ledger, modular design, open architecture, and the ability to evolve. The U.S. government's role is not to decentralize everything, but to build the backbone of a blockchain ecosystem and let the private sector innovate on top.

Nodes and Hashing: Blockchain networks allow for the secure exchange of tokenized value—ranging from bank deposits to financial or physical assets—across a distributed network. These networks rely on cryptographic tools, hashing algorithms, and programmable smart contracts and are designed to be resilient with no single point of failure.

Nodes are essentially network-connected computers or devices that each maintain a copy of the blockchain and help verify and record new transactions. Nodes collectively contribute to validating, propagating, and storing data on the blockchain. Through **governance or consensus protocols**, nodes agree on which new transactions and data blocks are valid and can be added to the ledger. This protocol ensures that all nodes reach a shared understanding of the blockchain's current state at any given time. Once agreement is reached and a block is added, it becomes immutable—it cannot be changed without consensus from the entire network, which preserves data integrity and auditability.

Blockchain security is reinforced by cryptographic hashing to secure and link blocks of information. Each block contains transactional data, such as who sent funds, who received them, and the amount. A hash function transforms this data into a fixed-length, unique string like a digital fingerprint. Even a minor alteration in the data generates a completely different hash, making any tampering immediately apparent. Each block includes its hash plus the hash of the previous block, creating a chronological chain. Changing one block would break the link to the next, thereby compromising the integrity of the entire chain—unless every subsequent block is revalidated. In a permissioned, private system, such tampering would not only be computationally difficult, but also immediately detectable by the network's vetted participants.

Consensus and Governance Protocols: Governance protocols for blockchain systems vary depending on how much trust exists between participants. In **public, permissionless blockchains** like Ethereum, participants are pseudonymous and untrusted by default. They are open ecosystems that allow anyone to join the network, validate transactions, or deploy applications. Therefore, these systems require robust consensus mechanisms that are resistant to manipulation. For example, **Proof-of-Work (PoW)** and **Proof-of-Stake (PoS)** protocols are designed to prevent any single participant from having outsized control or 51% of the network or network power.

Under PoW, miners expend computational energy to solve complex mathematical puzzles. The first to solve the puzzle earns the right to add the next block and receive a reward—this process incentivizes honest behavior and secures the network. PoS, which is more energy-efficient, selects validators based on the amount of cryptocurrency they "stake" or lock up as collateral. Both models are based on economic incentives and disincentives and borrow from game theory to maintain decentralized trust.

However, these protocols are not suitable for a government-sponsored blockchain ecosystem. Protocols for public, permissionless blockchain systems were designed for environments that lack trusted participants and generally are not aligned with the strict legal and regulatory needs of government.

Private, permissioned blockchain systems—like those envisioned for a U.S. government payment platform—rely on a governance model with **known and vetted participants**. These participants, which include government agencies and regulated financial institutions, can validate and order transactions without relying on mining or staking. Instead, they can operate in an **"append-only" mode** where they can write new data but cannot alter or delete previous entries. This ensures immutability while maintaining transparency and regulatory oversight.

Governance in Government Blockchain Ecosystems: A key challenge for policymakers is defining governance in public-sector blockchain-based financial ecosystems. As Christian Catalini, founder of the MIT Crypto-economics Lab, describes it—in Web3 and blockchain, intermediaries are taken out of the picture and put back in but in a different form, ultimately changing the nature of intermediation. All blockchain systems, both public or private, require governance over access, decision-making, and accountability. In highly-permissioned, government-controlled ecosystems, identifying who governs, how changes occur, and how oversight is maintained is critical to ensuring trust and stability.

Governance should answer:

- Who can write to the ledger and validate transactions?
- How are roles assigned and changed?
- How are disputes resolved and updates implemented?

In private, permissioned blockchain systems, governance is centrally coordinated. A designated authority manages who may join, assigns roles and permissions (e.g., who can read, write, or validate), and enforces compliance through built-in controls. These systems rely on vetted participants, strict access controls, and clear responsibilities. Governance protocols are designed to prevent fraud, collusion, or disruption—even among trusted parties—and ensure auditability and accountability.

A private permissioned blockchain offers operational control, enabling governments to ensure proper use of public funds. They also ensure systems are interoperable, standards-based, and open source—preserving sovereignty and accountability while benefiting from technical innovation.

Businesses that help build early public-sector blockchain use cases will be well positioned to scale across government agencies and into international aid and relief logistics. Blockchain infrastructure for disaster relief isn't just a one-off — it's a model for rethinking how money moves domestically and globally.

Digital Identification (ID): A trusted digital identity system is essential to any blockchain-based payment infrastructure built by the U.S. government. Whether for disaster relief or tax refunds,

digital IDs allow individuals to securely prove who they are, reducing fraud, accelerating disbursements, and improving compliance. But how that ID system is designed matters.

Traditional digital ID systems are **centralized**: a government agency, bank, or tech platform verifies a user's identity and stores their personal data in a central database. These IDs are typically digital versions of physical credentials, such as driver's licenses or passports. While they offer institutional authority and trust, users must often reverify across services, have little control over their data, and remain vulnerable to breaches, outages, or misuse. Once compromised, personal data may be permanently exposed.

Decentralized identity systems use blockchain and cryptography to shift control back to users. Here, identity credentials are verified and cryptographically signed by trusted issuers (e.g., governments, banks, universities), but stored in digital wallets under the user's control. The user chooses what credentials to share and with whom, using a private key.

In this model, users manage their identity through a **key pair**: a **private key** (kept secret by the user) and a **public key** (visible on-chain). Public keys act as pseudonymous identifiers and are linked to encrypted credentials that users can selectively disclose—for example, proving they are over 18 without sharing a birthdate. Sensitive data stays off-chain to preserve privacy. Trust in the credential comes from the issuer's validation and signature; control and privacy come from the user's ability to manage access.

This all operates within a broader **identity framework** — the rules and infrastructure for creating, verifying, and managing digital identities. A key innovation is the use of **Decentralized Identifiers (DIDs)**, which allow users to carry a single identity across platforms and services. One DID might be used to sign into a portal, verify a business license, and access disaster assistance — all without re-authenticating. Trust is embedded in the architecture.

For government-backed blockchain systems, a **hybrid model** is most appropriate:

- **Issuance and verification** by trusted authorities (e.g., state governments) under federal standards
- **Control and sharing** managed by individuals through secure wallets

This model preserves trust and accountability while protecting privacy and avoiding centralized surveillance risks.

Starting with a use case like federal disaster relief, the U.S. can demonstrate the benefits of secure digital ID while unlocking business opportunities for fintechs, wallet developers, compliance firms, and ID providers. Most importantly, it lays the groundwork for broader digital public infrastructure built around security, privacy, and individual control.

States are well positioned to lead. They already issue driver's licenses and manage ID systems for public benefits. Under federal standards, states can deploy secure digital IDs bound to verifiable credentials, enabling instant eligibility checks for aid, benefits, or tax refunds. This opens new business opportunities for companies to develop wallets, integrate biometrics, and offer secure

storage solutions. Digital ID infrastructure creates an emerging market for fraud prevention, compliance tools, and government-grade ID platforms — all areas where American firms can lead.

Policy and Design Considerations, and Roadmap -

Modernizing U.S. government payment systems with blockchain doesn't require a full overhaul from the start. A phased approach, beginning with disaster relief and other high-impact programs allows the government to test functionality, demonstrate results, and minimize disruption. The system must be designed with security and interoperability at its core which in turn drives the adoption expansion strategy. Today, connecting blockchain networks across jurisdictions and systems increases risk exposure through APIs, bridges, and third-party connectors, making it essential to begin with trusted nodes and strict access controls**,** and to scale only as resiliency is successfully established in security models.

Success will depend on governance and private-sector participation from the start. This means clear rules, defined roles, and an open, transparent process for designating new Financial Agents and awarding contracts. As new firms enter the ecosystem and compete with established incumbents, the government must ensure that the process remains competitive, fair, and accessible — particularly for the types of fintechs, regional and community banks, and compliance providers positioned to bring innovation into public-sector services.

States must be empowered. With appropriate funding mechanisms, including use of **P&I appropriations and federal matching incentives**, states can partner with private-sector providers to build their own modular blockchain-based payment systems, digital ID layers, and last-mile delivery tools. These efforts will not only improve how aid and public benefits reach citizens, but also expand markets for American technology firms and community financial institutions.

The federal government's role is to tie all the pieces together. It needs to launch a **U.S. Government Blockchain Roadmap** that sets out a strategic, staged vision and implementation timeline for modernizing public payment systems. This roadmap must connect an overarching federal payment infrastructure with state-level implementation and digital ID systems. A clear national strategy will give businesses the confidence to invest and innovate, knowing the government is committed to long-term transformation.

An important component of this government blockchain strategy is a **national digital ID strategy** that is privacy-preserving, secure, and built for public-sector use cases rooted in user control and not surveillance. By taking action now, the U.S. can modernize outdated systems, offer new business opportunity, and build a payment infrastructure that is secure, inclusive, and future-ready.