Bitcoin Policy Institute

BUILDING A TRUSTWORTHY DIGITAL FUTURE:

DIGITAL IDENTITY IN THE LAND OF THE FREE

About the Author

This white paper was written by an anonymous author. The author has worked at multiple publicly traded financial institutions in the fraud detection and prevention spaces; from ground-level tactics to enterprise strategy, product, and policy. They have also held leadership roles at one the nation's largest identity verification companies, designing and operating the strategies and tactics to defend state and federal agencies from identity theft. They have been accountable for tactical implementation and monitoring of KYC / CIP programs, and defended the fraud and identity risk management programs of top-10 crypto exchanges to federal regulators. They believe in the power of decentralized networks, and seek to advance the tools, standards, and technologies that empower individuals.

Author's public signature:

1e98ca920fa6e0260e4e52c7cfeef7533130249bc715a8936dcd843af638332c

About the Bitcoin Policy Institute

The Bitcoin Policy Institute (BPI) is a non-partisan, non-profit think tank. It is dedicated to educating policymakers and the public on Bitcoin and disruptive digital technologies, providing research-based insights to inform sound policy in the United States.

The BPI team comprises experts in economics, law, philosophy, energy, and environmental science, working together to explore the impacts of new technology on existing US public policy interests. The views expressed in this publication do not necessarily reflect the views of all Bitcoin Policy Institute management or its affiliated scholars.

POLICY BRIEF

Building a trustworthy digital future: Digital Identity in the land of the free

Table of **Contents**

Digital Identity: Our Country's Biggest Threat and Opportunity

Identity is the foundation - our "layer zero" - for participating in modern life. Yet in the United States, our relationship with our digital identities has never been more fractured, insecure, and impersonal. While the internet was originally built without a native identity layer, it has nonetheless supported trillions of dollars in economic activity. But today, with AI systems increasingly indistinguishable from humans online, the US's outdated methods for identity verification and authentication are exposing individuals, businesses, and government agencies to growing risks.[1] This is fueling widespread fraud, eroding public trust, and threatening to stall future economic growth.

As identity-related threats increasingly exploit the US's fragmented approach and systems, there's a growing risk that institutions - in an effort to try to mitigate these increasingly acute costs - will seek and adopt solutions that compromise core American values such as individual autonomy and privacy[2]. Despite the severe financial toll of identity fraud[3], our national response and approach must uphold those values and empower individuals to reclaim control over their identities - online and offline.

The core issue with digital identity in the U.S. is that we treat identifiers as authenticators, relying on the presentation of personal information as proof of identity. This assumes such data is private, but decades of widespread data breaches have rendered that assumption false[4]. An equivalent security model would be using knowledge of your home address as the key to your front door. Once you share your address, your security is permanently compromised.

In the absence of a federal solution, U.S. businesses and governments have relied on profit-driven entities like financial institutions and identity verification vendors to confirm digital identities. This reliance creates maligned incentives and forces individuals to depend on corporations to establish and access their own identities, often through permissioned, centrally controlled profiles that can be revoked at any time. As economic growth increasingly moves online, our ability to use the internet safely and confidently remains hampered by our inability to easily, independently, and affordably assert and verify individual identity.

It doesn't have to be this way. In the physical world, Americans regularly assert their identity directly using credentials like driver's licenses, birth certificates, or other privately issued claims - without third-party oversight or reliance. This model protects autonomy and privacy, as individuals can present credentials without involving or notifying the issuer.

By examining how we establish trust in identity in the physical world, we can draw insights and policy recommendations to improve the U.S. digital identity infrastructure. A key outcome of our focus is ensuring that future identity systems and infrastructure enable growth, are aligned with American ideals, and avoid outcomes that aren't in the best interests of citizens.

Verifiable Authorship as an Open and Standardized Public Utility

Understanding the components: digital signatures, decentralized identifiers (DIDs), verifiable data registries (VDRs), and verifiable credentials (VCs)

When shaping digital identity policy in the US, it's helpful to think in terms of "digitizing identity", not creating a separate "digital identity." The goal should be to extend (and ideally enhance) core elements of physical identity, such as autonomy, privacy, and security. As a general principle, the rights and norms that govern identity in the physical world should carry over into the digital wherever possible.

Today, Americans struggle to independently understand and trust that others are who they claim to be online, via phone, email, social media, or other digital channels. As a result, we defer to private companies to verify and assert our identities, effectively outsourcing the representation and verification of our digital selves to for-profit entities. Having the option to delegate such a task may indeed prove useful for many, but it should not be the only practical way to assert our own identity or credibly identify our digital counterparts.

The fact that something is difficult doesn't make it unachievable, **nor does it justify compromising our principles to accommodate subpar solutions**, especially regarding something as important as our identity. Instead, we must recognize that to move away from a world where only private and centralized entities can credibly author, own, verify, and interpret claims related to our identity, we must build and amplify the standards, technology, and tools to enable any person or entity to do so - without relying on or requiring permission from a third-party.

To build a secure, private, and open digital identity infrastructure, we can start by looking at physical-world tools. For centuries, handwritten signatures have served to build trust and authenticate individuals involved in a transaction. In the digital realm, this role must be filled by digital signatures[5]. While analog signatures are imperfect, **digital signatures** - powered by asymmetric public key cryptography - provide strong, verifiable proof of authorship.

At a very basic level, digital signatures are a technological product of a private key and a public key pair. These public and private keys (which are essentially very long numbers) have a direct relationship. Given a random private key, the accompanying public key is derived with mathematical formulas termed "one-way" (nonreversible) functions. This public key acts as a shared identifier that is widely available (and distributed to others without risk), while the private key acts as the "secret" that only the owner / controller holds. When someone signs a digital message using their private key, anyone with the public key can verify both the message's provenance (or origin) and integrity (that it hasn't been altered).[6]

This mechanism is foundational to modern digital security methods, powering open protocols like TLS (and its predecessor SSL) which secure web browsing, email, messaging, and file transfers across the internet globally.

Just as digital signatures separate the secret from the identifier (using private and public keys), we can harness the power of cryptography to achieve the same **separation for our personal identifiers from our authenticators.** In most real-world interactions, a person's name serves as their primary identifier. But as noted earlier, using personally identifiable information (PII) as both an identifier and authenticator is a flawed paradigm, and exposes individuals to privacy risks and fraud. Fortunately, thanks to technology-agnostic standards from the World Wide Web Consortium (W3C), we now have a globally recognized method for creating identifiers that contain no personal data. These are known as **Decentralized Identifiers (DIDs)**.[7]

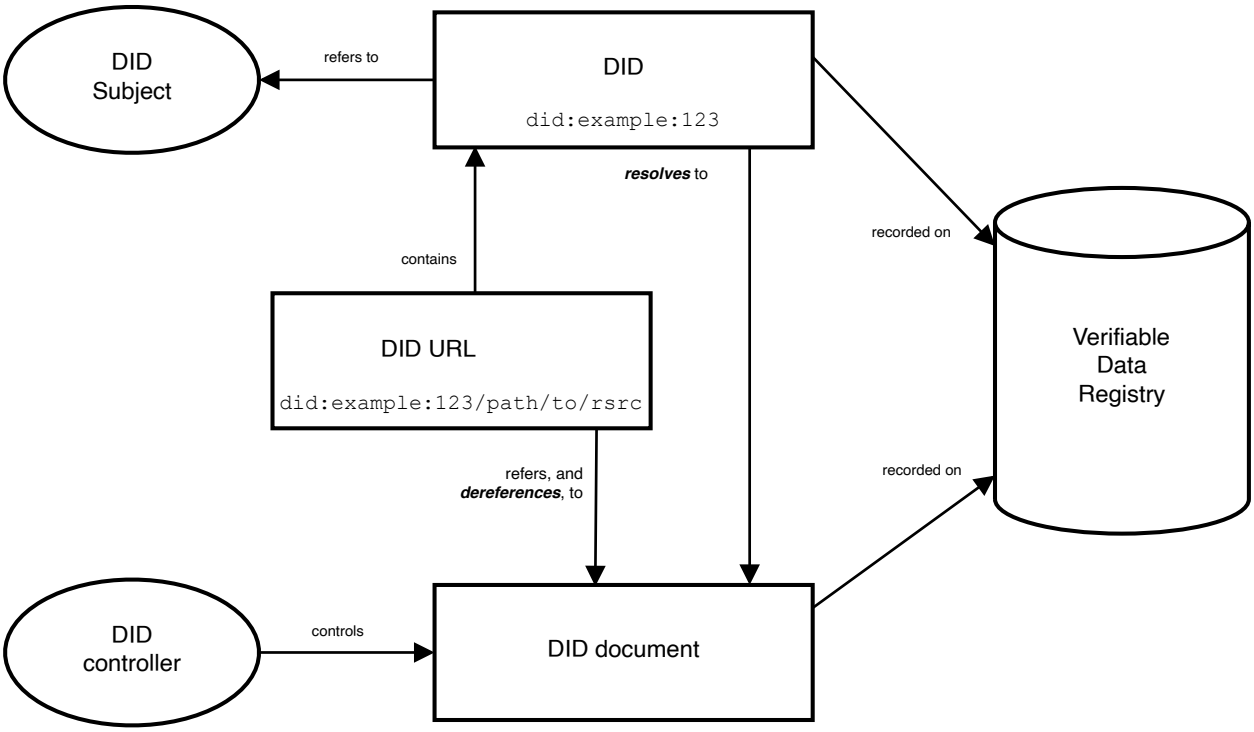
Just as each book in the world can be uniquely identified by its ISBN number (international standard book number), and every U.S. vehicle by its VIN (vehicle identification number), a DID is simply a universal resource identifier that includes a globally unique text string.[8] Each DID is also accompanied by a declaration specifying the associated DID Method - a set of rules for how the DID is created, resolved, and managed - of which more than 200 have been published by businesses and governments to date.

A DID and its associated DID Method allow others to retrieve a DID Document, which contains essential information about the identifier. This document outlines the authentication mechanisms for the DID, including the type of cryptography used to generate its public-private key pair. It provides the public key needed for others to verify the DIDs' digital signature, while the private key (kept secret by the DID controller) acts like a password, enabling the controller to prove ownership and sign securely.

Source: W3C Decentralized Identifiers (DID) v1.0[7]

To access a DID's associated DID Document, modern digital identity systems rely on a **Verifiable Data Registry (VDR).** A VDR serves as a system that facilitates the creation and verification of identifiers, which often is as straightforward as a public database[9]. Its core function is to resolve DIDs into their corresponding DID Documents and public key.

VDRs can take many forms, each with trade-offs. The Bitcoin network is arguably the most decentralized, secure, immutable, and permissionless VDR today. Other examples include peer-to-peer networks like BitTorrent, decentralized file systems, distributed ledgers, and both permissioned and public databases such as web domains managed by the Domain Name System (DNS)[10], government registries, and other open data systems.



Source: W3C Decentralized Identifiers (DID) v1.0[7]

The promise of Decentralized Identifiers lies in their ability to be wholly controlled by individuals or entities without reliance on intermediaries to assert or verify identity-related claims. DIDs operate independently of centralized systems, relying solely on the trust and governance model of the verifiable data registry to which they're anchored. Critically, even if a DID's private key is compromised, it reveals no personal information - unlike traditional identity "secrets" such as Social Security numbers, which, once breached, are permanently exposed.

When individuals and entities are able to control and resolve DIDs built on open, global standards, they're able to securely and privately author and verify the provenance of any message independently. However, in many cases, including higher-value commercial transactions (such as those that require identity verification), counterparties often require more than a simple self-assertion of identity. **Enter credentials.**

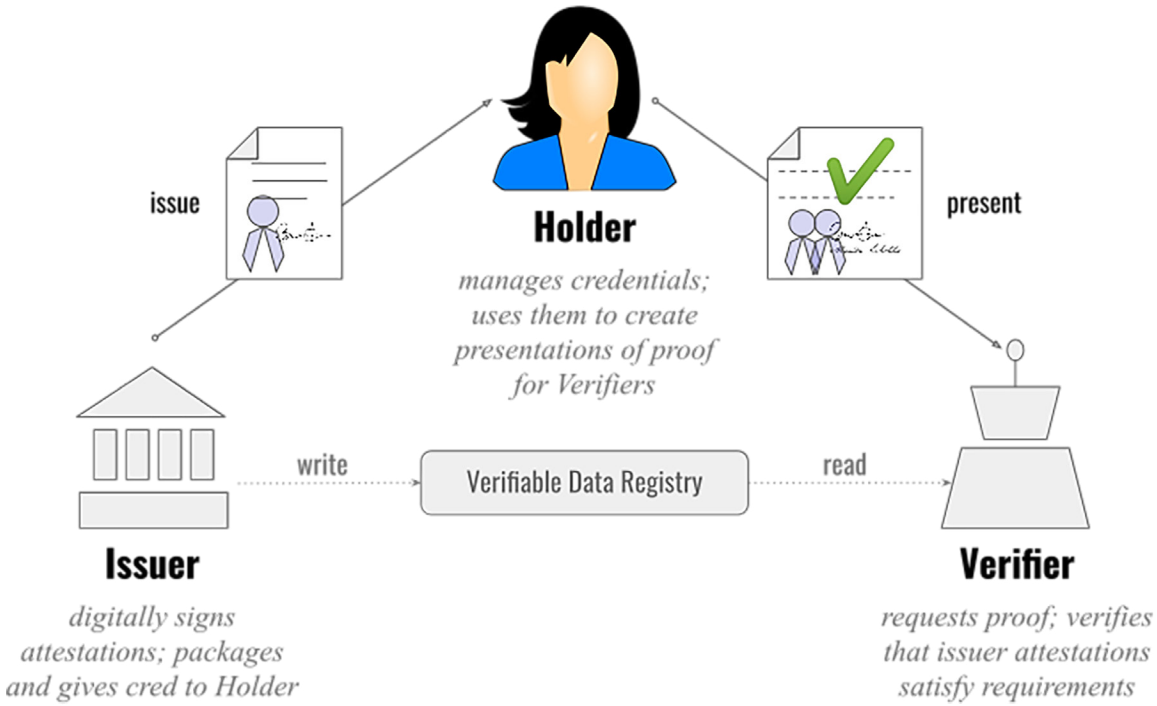
Credentials help us verify the claims of others with whom we are interacting, whether that be about their identity or otherwise. Although credentials come in an unlimited number of forms, one of the most common examples in the U.S. is the driver's license, which asserts both identity and driving eligibility. These credentials bring trust and assurance that the claim being made is authentic, as it is certified (or "signed") by the issuer.

For thousands of years, credentials and other "official" messages have been ratified using physical security features such as signatures, water marks, or specialized wax seals. However, over time, humans (and their tools) have gotten better at counterfeiting physical security features, leading to rising levels of fraud and large-scaled deception. Because it can be difficult to achieve absolute certainty about a credential's authenticity, the rigor of a relying party's inspection process typically depends on the associated risks and / or requirements specific to the given situation.

Verifiable Credentials (VCs) are the digital evolution of traditional credentials, offering the same high-level of authenticity assurance regardless of the context in which they are used. They are standardized, tamper-evident data packages containing claims whose provenance and integrity can be instantly verified. Like DIDs, VCs are based on open W3C standards[11] and use digital signatures to prove the issuer's authorship. Together, DIDs and VCs enable anyone to issue, hold, and verify claims - including those related to identity.

This new model of digital identity is built around a simple concept known as the "trust triangle," in which each participant takes on one or more key roles. To understand how this open framework functions, we must first define some foundational terms and concepts:

- **Issuer:** An entity that generates ("issues") claims, which are packaged as a credential and given to the holder
- **Holder:** An entity who possesses and can present credentials, and is usually the subject of the credential they are holding
- **Verifier:** An entity that receives information shared with them by a holder who authenticates ("verifies") the source and integrity (i.e. if the claim has been tampered with) of the credential



Source: Wikipedia [11]

Verifiable Credentials eliminate the risk of counterfeit credentials by providing cryptographic proof that the issuer authored the credential and that it remains unaltered. This dramatically reduces the cost, risk, and time involved in issuing, holding, and verifying claims. As a result, organizations like Harvard University, the Department of Homeland Security, and numerous professional associations have adopted this model for diverse use cases across a variety of industries.[12, 13]

An ideal implementation of this model occurs when issuers create credentials that reference a subject's DID, rather than including sensitive personal information.This enables verifiers to authenticate the credential and the fact that it was issued to the presenting DID controller, without ever receiving the holder's personal data. This privacy-preserving outcome is further enhanced by **selective disclosure**, where holders reveal only specific attributes from a credential, even if the full credential contains personal information.

Consider the common case of age-restricted access. To enter a bar in the U.S., patrons must prove they're over 21 years of age. Today, this typically involves presenting a driver's license, which reveals far more personal information than is necessary to verify the holder's age - including name, address, photo, and other personal details. The bar employee is responsible for judging the authenticity of the credential by visually evaluating the security features of a piece of plastic.

Now imagine a state DMV issuing a digital credential to a citizen, based on the same trusted verification processes used for physical credentials. While this digital credential may include sensitive information, it's designed to allow selective disclosure.[14] Using her phone's digital wallet, the citizen creates a ***Verifiable Presentation***[15] of her DMV-issued credential - choosing to reveal only the necessary attestations, such as being over 21 and her DMV photo. To share this information, she first authenticates herself to her device (likely using a security code or device-bound biometric), then presents a scannable code to the bar employee. With a phone or offline-capable verification tool (which is running open source software), the bar employee can then scan the code and cryptographically verify that:

- The DMV's DID issued and signed the credential.
- The holder's DID signed both the credential and the Verifiable Presentation.
- The credential claims are unchanged, include the subject's photo, and confirm she is over 21.

In this model, the bar can confidently accept the DMV's claim without collecting or storing the citizen's personal data. If necessary, the bar employee can inspect the cryptographically signed photo to confirm the holder's identity. There's no need to examine physical security features - instead, open cryptographic protocols validate that the credential was authored by the DMV and has not been altered. Additional assurances can also be established and passed along as a part of this process, such as the fact that the device that the holder presented to the DMV when the credential was issued to them is the same device that is presenting the credential now, further reducing the risk that a credential could be misused if it were to become compromised.

A key benefit of this model is that the verifier (i.e., the bar) doesn't need to "phone home" to the issuer (the DMV) to validate the authenticity of the credential. Like physical credentials, digital credentials should minimize external dependencies. This protects user privacy by ensuring that issuers of digital credentials cannot track when, where, or how holders use those credentials, just as the issuer of a physical credential is not notified when a holder presents a physical credential to a verifier.

Verifiable Credentials help restore the physical-world principle that merely possessing someone's personal information is not enough to prove identity. In the digital context, verifiers can require a signed credential that the individual securely holds and presents. If a credential is lost, stolen, or compromised, the citizen can re-authenticate with the issuer to obtain a new one, and revoke the validity of the old credential in a way that protects their personal information.

"Trust" in a World of Decentralized Claims

Understanding the limits of cryptographic certainty

Digital signatures allow us to verify if a given DID authored a message, but not whether the DID controller is who they claim to be. If a third party issues a credential linking a DID to a person, how do we trust that the issuer got it right? Cryptography provides certainty about who (which DID) signed a message at a technical level, but not whether the underlying claim of a credential is true. In other words, cryptographic trust establishes the source of a claim but not its veracity. In applying these tools to establish trust in a human context, we must recognize that belief in or **reliance on any claim issued by a third-party ultimately depends on social trust, which cryptography alone cannot provide.**

So how can we build social trust in a DID controller's identity, and the reliability of their claims, or those of their credential issuers? The answer begins with recognizing that **trust is not binary**. In both physical and digital contexts, the level of information and assurance required varies depending on the situation and the needs of the relying party.

In his article "Musings of a Trust Architect: Building Trust in Gradients,"[16] Christopher Allen argues that trust in the physical world is built in gradients, and thus a progressive trust framework should also inform the guiding principles for building digital trust. The current concept of trust on the internet is narrow and binary, which is a natural product of the internet's maturation path. At the dawn of the web, not only were controls governing online interactions far less rigid (or non-existent), but being denied access to an online service was more of an inconvenience than an impediment to daily life, as most of those online services were either discretionary or had alternative methods of authentication based in the physical world through which we could remedy our issues. As the internet has scaled, however, online access to many services has become increasingly centralized and rigid due to the involvement of large commercial intermediaries - they either let us in, or they don't. This centralization of access provisioning coincided with the internet's evolution into a de facto public utility for most Americans, with the amount and variety of "essential" digital interactions growing exponentially, many of which now have no physical (in-person) means of remedying access issues related to identity verification.

As Mr. Allen notes, today's binary approach to digital trust - offering only "blind trust or total skepticism" - has inadvertently heightened the risk of critical online interactions. This absolutist framework leaves individuals dependent on tech giants to assert and verify identity, with little room for autonomy or inspection of the assurances being made, let alone self-assertion. This model is both overly restrictive and prone to failure, and it fails to mirror how trust is built and managed in the physical world; gradually, contextually, directly (peer-to-peer), and with degrees of confidence.

In the physical world, the context of an interaction shapes what information each party requires to move forward throughout the engagement lifecycle. Trust is typically built over time, with information and assurances revealed progressively as circumstances demand. Context also determines how much confidence - or assurance - is required to trust the information exchanged, including the fundamental claim that someone is who they say they are. These methods and timelines best-practices should inform how we approach digitizing identity moving forward.

Social Trust and Governance Frameworks

Enabling biomimetic systems of federated, open, and verifiable digital claims

If we zoom out, we start to see that the credibility of any claim (be it a digitally signed attestation or otherwise) is a function of the context and ecosystem from which the claim originates. Building and evaluating trust this way is time-consuming, and difficult to scale for individuals who don't want to rely on centralized intermediaries.

To alleviate this difficulty, we need to introduce the missing piece of the "trust triangle" articulated above - trust and governance frameworks. These frameworks help us simplify daily life by delegating the inspection and verification of an issuer's underlying processes to others we trust. They can also be viewed as the business, legal, and technical rules that enable us to standardize and scale social trust.[17]

Although they come in many forms, these frameworks help us establish and maintain trust in the counterparties issuing claims. These frameworks may outline underlying diligence and issuance procedures, what happens when there's a dispute, and what rights different parties may have in a given context. It's also important to note that **trust and governance frameworks are not always necessary** to create a thriving network of credibly reliable identity claims.

If trust and governance frameworks help us simplify reliance on others' claims, how should we evaluate which frameworks and ecosystems are more trustworthy - especially in relation to digital identity? One key factor to consider is the level of decentralization within a given trust or governance framework. Consider the role of a Verifiable Data Registry (VDR), which can anchor a Decentralized Identifier (DID). The Bitcoin network, for instance, serves as a highly robust VDR for several reasons:

- It has no central authority or corporate owner.
- All past ledger entries are fully open source and verifiable.
- The process for adding new entries is also transparent, open source, and publicly auditable.

The Bitcoin network is just one of many possible VDRs, but analyzing it helps illustrate key factors that influence the trustworthiness of VDRs and related components - such as DID methods and trust frameworks. For contrast, consider one of the most widely used VDRs today: the Domain Name System (DNS). DNS is a globally trusted "lookup" service that translates human-readable domain names like btcpolicy.com into IP addresses.

The DNS system is governed by ICANN (Internet Corporation for Assigned Names and Numbers), but unlike Bitcoin, its trust and governance framework is not open source. Instead, it relies on human oversight and a federation of for-profit entities accredited through a private, multi-step process managed by ICANN to control how DNS entries are created and maintained.[10] This isn't to suggest the process is flawed or insufficient, but to highlight that even foundational VDRs which serve as critical roots of trust for daily digital life differ in transparency, rigor, and security. Some trust frameworks and governance systems are publicly documented and verifiable, while others are less transparent. **Whether a given system meets our needs depends on our specific context**, which informs whether its trust and governance model provides the level of decentralization, assurance, and openness we may require.

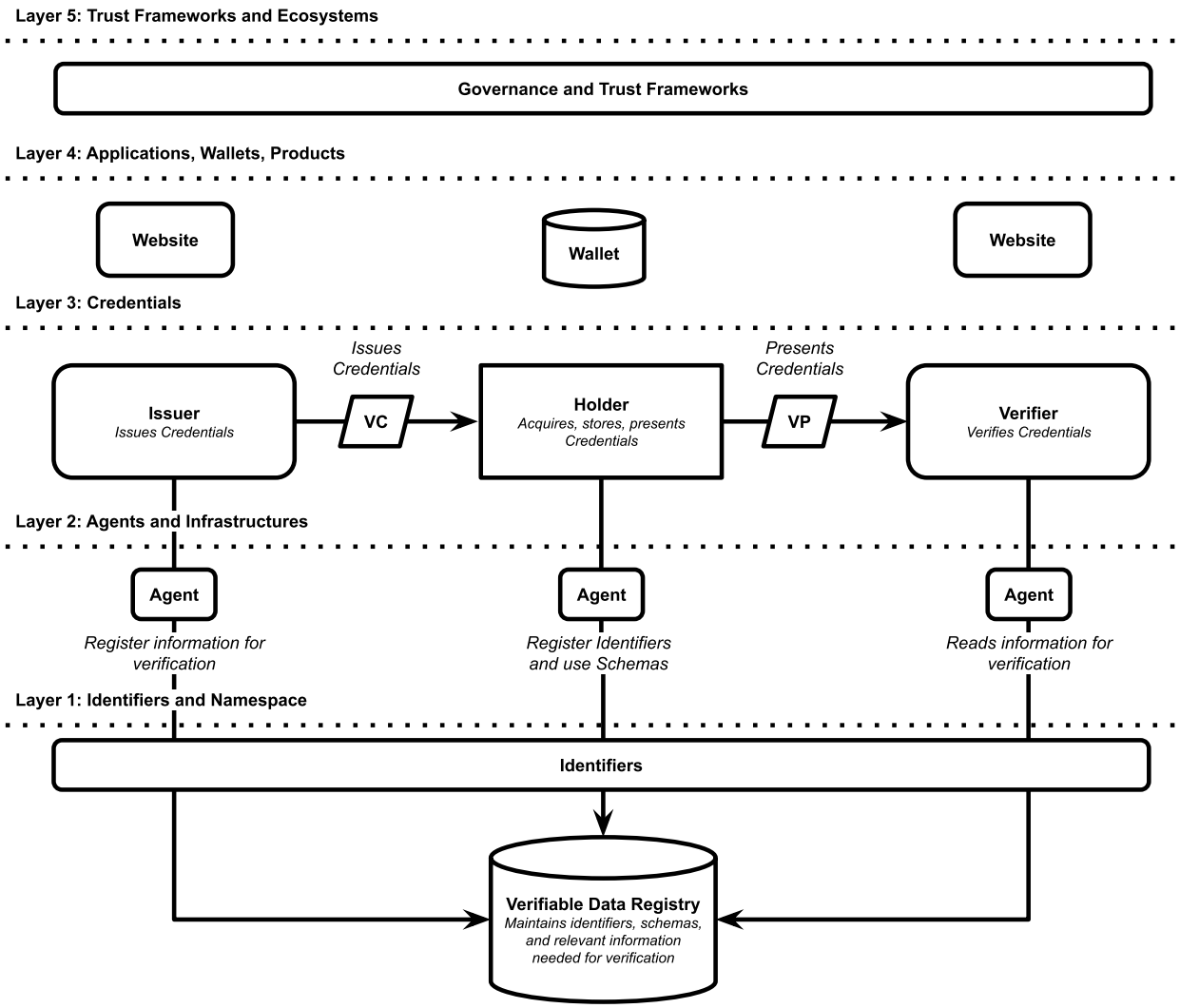
Beyond VDRs, we can look to other entities that serve as "authoritative" sources / issuers of important claims, such as a state Department of Motor Vehicles (DMV). The DMV's operations rely on both human oversight and automated systems, managing entries in a permissioned, private database. While some public oversight may exist due to the nature of the department's remit and funding sources, the internal processes governing the management of the database are not publicly disclosed or fully available for independent, open scrutiny.

Wikipedia offers a different model; one that is distributed and quasi-open. Anyone can propose edits, but new entries and modifications are subject to approval by delegated domain moderators who interpret whether content meets Wikipedia's principle of being "verifiable." What qualifies as "verifiable?" That's left to the moderator's judgment, based on whether a source meets their own standards of veracity and assurance, given the domain and context. In this way, even Wikipedia operates through layered, delegated trust frameworks - another illustration of **trust frameworks all the way down.**

Trying to simply rank the trustworthiness of an "identity system" and its governance framework is ultimately a fool's errand because identity and assurance requirements are always context-dependent. Still, some meaningful efforts have been made to evaluate decentralized trust models. For example, the W3C recently published a rubric for assessing DID methods, addressing key criteria like rulemaking, design, operations, enforcement, auditability, security, and privacy.[18] As we zoom out, it may be more useful not to fixate on how a trust or governance framework operates, but rather when we might need to rely on it, and whether it may meet the needs of that particular moment.

What becomes clear is that in order to satisfy the evolving digital needs of individuals, governments, and industry moving forward, **many trust and governance frameworks will be required** across domains and sectors. Some may benefit from oversight, sponsorship, or partnership with state or government agencies, while others clearly will not, and need not. At the same time, many digital identity challenges can be effectively addressed through the use of open tools like DIDs and VCs, even without formalized governance structures involving government agencies.

Broadly enabling this ecosystem will allow verifiers (including individuals) to define their own requirements for the types of claims or credentials they require in various contexts. In response, a diverse and competitive market of claims and assurance provider networks will emerge, each offering different levels of specialization, robustness, governance, and trustworthiness from users. Over time, these providers and networks will serve as vital signalers and roots of trust in our digital life, shaped and continuously tested by the dynamics of the open market.



Source: https://www.w3.org/reports/identity-web-impact/#architecture, inspired and adapted by ToIP (https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf)

Digital Life in The Home of The Free

A future built on decentralization, individual privacy, security, and autonomy

This vision stands in stark contrast to today's model, where our digital identities are often permissioned and centrally-controlled by corporations. Instead, we should aspire to an America where individuals fully control their digital identity and can easily derive and satisfy the requirements of any context (digital or otherwise) in ways that enhance the privacy and autonomy of themselves and their counterparties.

While aligning our national approach and standards to those of our economic and geopolitical allies may offer important compatibility benefits, the US must ensure our practices, systems, and networks reflect our ideals above all else. We must ensure that our approach is not overly focused on aligning with external models, because many of those external efforts are not aligned with empowering citizens and protecting their privacy - but instead risk entrenching state or corporate power structures whose motives and ideals do not reflect our own.

To counter the growth of authoritarian models and digital power structures globally, as well as uphold democratic values, the United States must urgently champion open, global digital identity standards and practices. Doing so will embed core American principles - liberty, individual sovereignty, and privacy - into the fabric of the digital world (domestically, and beyond).

By codifying these ideals, standards, and decentralized approaches as protocols of freedom (for online and offline life), the US can help shape the future of digital interactions globally in its image. Embracing this approach will reinforce 21st century federalism, empower individuals with greater control over their digital lives, dramatically reduce fraud at a national level, and foster a more secure, trustworthy, and open digital future. It is a strategic imperative to ensure that the global evolution of digital identity reflects and reinforces American ideals.

In an effort to manifest this future, we submit policy recommendations on the following page for discussion and consideration in the United States.

Policy Recommendations

1. *Rethink what digital identity is / should be under the law, and what gaps may remain*

- **Consider what the appropriate frameworks might be for legally classifying our digital identities.**
    - Evaluate and consider the notion of principle authority as rooted in commercial agency law, and how that may be potentially applied to digital identity. Per Christopher Allen, "By saying that a Principal has the ultimate authority to control their digital identity, then that Principal may then delegate their authority under existing fiduciary Laws of Agency and Custom."[19]
    - As articulated by Joe Andrieu, viewing our digital identities as property is likely suboptimal, and "Ownership is just one way to make rights enforceable. One that commoditizes the asset and subjects it to the whim of the state and those who control property. If we care about the liberation of the digital self, we must resist turning identity into property."[20]
    - Amplify the notion that our identity is not given to us by the state, instead, the state affirms our identity via credentials, which are a product of verification and authentication practices.[21, 22]
- **Consider existing state and federal legislative proposals:**
    - Explore and enhance the model legislation set forth in Utah that describes the notion of "State Endorsed Digital Identity", granting autonomy and privacy to citizens while ensuring equal access for those who choose not to participate.[49, 50]
    - Consider the importance of Wyoming's protection of disclosure of private keys. Importantly, this does not prohibit law enforcement from legally compelling someone to use their private keys (e.g., to prove ownership of a digital asset). [23]
    - Advance the "no-regrets" legislation from representatives Bill Foster Rep and Clay Higgins which instructs TSA to compile a report on its acceptance of digital IDs and its impact on US homeland security, which includes assessing the "related benefits and risks, and how such current and emerging ecosystems may better protect homeland security and increase the competitive advantage of the United States." [24]
    - Senators Kyrsten Sinema and Cynthia Lummis may not actively be pursuing it after 3 years of advocacy, but policy makers should consider and advance many of the very sensible and bi-partisan recommendations in their Improving Digital IDentity Act (introduced in 2022), which calls for the creation of a task force which will recommend strategies that address privacy, equity, and interoperability concerns. It also calls for an evaluation of what resources may be required for federal agencies to move forward. This bill was also reintroduced by Representative Bill Foster in Q4 2024.[25]

- **Evaluate if existing laws (such as ESIGN[46] and UETA[47]) enable a citizen's digital signature to have the full standing and protections they deserve and require.**

    - Examine if there are specific legal or technical definitions which could benefit from refinement, such as in Wyoming's Digital Identity Act.[26]
    - Examine what frameworks, standards, or investments could be made to accelerate the enablement of citizens to issue, hold, present, and verify credentials in a variety of legal contexts.

2. *Provide federal guidance and leadership on mobile driver's license (mDL) standards to ensure that privacy is on-par with physical credentials*

- **Ensure state issuance of mobile driver's licenses aligns with American norms**

    - Evaluate the appropriateness of US states to be issuing authoritative identity documents in the format prescribed in ISO 18013-5, which can enable a "server retrieval mode"; which reaches out to the issuing authority every time a citizen attempts to utilize their credentials, enabling tracking and surveillance ("phoning home").[27]
    - If states do decide to use this standard, consider adopting language that prohibits DMVs and other state agencies from issuing credentials which leverage this particular variant of the standard, as it does not align with the privacy rights and norms that citizens have with non-digital credentials.
    - Revise and expand the intent behind Executive Order 14144 ("Strengthening and Promoting Innovation in the Nation's Cybersecurity"), which seeks to ensure that federal agencies who are verifying citizens for the purpose of accessing federal benefits programs do not rely on mDLs (or other digital identity documents) that enable the issuer to surveil the usage of those credentials.[28]
    - Ensure that any state which is planning to begin issuing digital credentials to their citizens follow appropriate and expected open legislative processes that ensure public transparency and enable public review and comment periods.
    - Commit to the notion that the issuance of an authoritative identity document is a public act, and therefore should be overseen as such. Additionally, consider applicable protections to ensure that citizens are not "locked in" to a specific technology service provider by the state in order to hold and utilize their credentials.
        - Much of this can be avoided by issuing global standards-compliant credentials as opposed to bespoke vendor substitutes.

- **Explore and enable frameworks and protections to buttress individual privacy**

  - Derive appropriate laws and regulations to ensure that state-issued credentials cannot be tracked across verifiers. Explore how open standards (like AnonCreds) can emulate commercial solutions that solve for verifiable one-time use applications like TruAge.[27, 29, 30]
  - Consider when and where it may be appropriate to mandate restrictions on data storage and use related to the verification of state-issued credentials. Evaluate if there are specific contexts in which it may be appropriate to require verifiers to register with a relevant authority (ensuring that when a verifier is requesting sensitive information, citizens are able to accurately and easily identify who they are). This will help to prevent scams and abuse related to the sharing or presentation of sensitive information.

3. *Seize the moment and elevate NIST's role in setting domestic and international standards related to digital identity*

- **Invest in and amplify NIST and the power of their digital identity standards**

  - Fully fund NIST's digital identity group and give them explicit and actionable directives which focus on advancing standards and trust frameworks for those who want to issue and rely on digital claims, including:
    - Producing assessments of other peer countries' approaches to digital identity through the lenses of technology, trust frameworks, standards, and overall outcomes for citizens. Ensure the assessment includes a framework that accounts for all significant forms of state-sponsored initiatives related to digital identity and trust, such as Singapore's "Trade Trust" organization, which was set up to "enable everyone to confidently trade with anyone, anywhere."[31]
    - Doubling down on standards development and coalescence of approaches, including "approved" cryptographic methods across the trust spectrum, including:
      - Privacy preserving capabilities and their associated cryptographic methods and functions, including those that power Zero-Knowledge Proofs (ZKPs).
      - Standards that power data minimization best practices like OIDC4VP, an open standard aimed at enabling holders to selectively present the attributes from a verifiable credential. [48]
      - The advancement of standards and credential schemas that codify basic ideas like proof of personhood and known customer credentials to ensure the US has a diverse spectrum of claims and assurance for holders and relying parties.[2, 32]
  - Produce an open source wallet code base, for distribution and use by anyone which incorporates relevant standards and approaches for issuers, holders, and verifiers. Provide working code examples that allow issuers, verifiers, and holders to effectuate their role in the trust triangle.

- **Expand NIST's ability to partner with private and public organizations**

    - Explore funding for and / or targeted partnerships with experts in the space who are working to solve for digital trust in financial services, logistics, healthcare, and beyond via open standards and governance / trust framework templates, including non-profit and for-profit enterprises like The Linux Foundation's Decentralized Trust group, The W3C, Blockchain Commons, Decentralized Identity Foundation, Trust Over IP Foundation, and Ayra.[33 - 38]
    - Explore and evaluate partnerships with specific and economically relevant trade associations or states in order to build digital trust in targeted sectors and / or high-value use cases, like "KYC" in financial services. NIST should provide working code examples which will satisfy the basic requirements of relevant stakeholders of a given working group, including a draft of a governance framework.
        - In all industries, the ability to standardize the assurance of the claims that are being relied on (or minimally point to standards and a functional governance framework around the issuance of those claims) will likely enable the procurement of insurance, which is required to scale for most commercial endeavors.
    - Consider ways to accelerate the vetting and codification of emerging cryptographic trust approaches, like KERI and others.[39]

4. *Leverage our leadership role at FATF (Financial Action Task Force) to advance American ideals and build more effective AML / CFT (Anti-Money Laundering and Countering the Financing of Terrorism) frameworks*

- **Use our leadership position in FATF to proliferate and codify American ideals around:**

    - The freedom to transact, which is missing from the UN's Universal Declaration of Human Rights. This right is likely a logical dependency to achieve the other rights outlined by the UN.[40,41]
    - **Financial privacy**; ensuring that a sustained lack of action does not continue to lead to the increasingly recursive surveillance of Americans via static thresholds for "high-risk" transactions as articulated 55 years ago in the Bank Secrecy Act.[42]
    - **Biometrics not being used as identifiers**. Biometrics are excellent authenticators (i.e. binding a person to a given device, which is linked to an identity or credential) for citizens to use to secure their devices, but should not be used as identifiers in identity systems. The reason behind this is a citizen's biometric markers are permanent, and cannot be reissued if compromised. Advance the notion that biometrics should be used locally on a citizen's device, and not used as an identifier.[43]
- Consider Senator Mike Lee's Saving Privacy Act, and how we can ensure that the fourth amendment is appropriately applied to our digital lives in the US and beyond.[44]

5. *Bring federal regulators together to provide explicit guidance on how reusable identity can thrive in financial services, and the US broadly*

- As it stands today, regulated financial institutions are seemingly allowed to rely on identity-related claims of their mutual customers - but in practice most don't.[45] This acts as a significant constraint to the proliferation of "reusable identity" for citizens, which in turn requires them to re-verify and assert their identity every time they want to open an account or switch to a new service provider; increasing costs, creating walled gardens, and leaving identity resolution to the profit-driven motives of individual providers.
  - The reasons behind this hesitation relate to banks' inability to have confidence in the underlying verification processes of their peer banks (trust and governance frameworks can help solve these problems), but the bigger issue from risk and compliance managers may well be lack of confidence that applicable regulators will allow this broadly.
- Instruct the Department of the Treasury, the OCC (Office of the Comptroller of the Currency), FDIC (Federal Deposit Insurance Corporation), and all other relevant federal regulators to form a working group to craft and publish a unified and explicit set of guidance on how to achieve a compliant form of CIP reliance in the US for account opening use cases. Require the guidance to provide details related to verification and authentication requirements, standards, oversight regimes, and all other relevant expectations in order for banks to issue and rely on claims related to identity verification across a given or varying set of contexts.
  - If the working group is not able to achieve these goals, document outstanding gaps and / or issues and provide the ability for an adjoining industry working group to propose solutions to meet identified gaps. Instruct the working group to commit to a public process until there is a satisfactory resolution.

References and Endnotes:

[1] As trust related to identity continues to erode online, growing numbers of service providers are requiring their users to provide identifying information to prevent DDoS (Distributed Denial of Service) attacks from bots and AI tools controlled by malicious actors. This trend increasingly requires users to provide incredibly sensitive biometric information to interact with basic online services to demonstrate that they are humans.

[2] "Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online" - https://arxiv.org/abs/2408.07892

[3] Estimates from the Department of Labor's Office of the Inspector General estimate that anywhere from 11% - 21.5% of Pandemic Unemployment Assistance and other related aid likely went to fraudsters. See https://www.oig.dol.gov/public/testimony/02082023.pdf

[4] Over 4,100 data breaches have been publicly disclosed in the last year. See https://www.breachsense.com/breaches/

[5] Electronic Signatures - Enabling trusted digital transformation World Bank - https://openknowledge.worldbank.org/entities/publication/d56f94c3-c1c8-4b17-b479-fd68f9551b1c

[6] Public Key Infrastructure: Implementing High-Trust Electronic Signatures World Bank - https://openknowledge.worldbank.org/server/api/core/bitstreams/8626c5c7-f50f-4614-a81d-7a680d5e0648/content

[7] Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations W3C - https://www.w3.org/TR/did-core/

[8] Universal resource identifiers are strings of characters that identify a resource on the internet, similar to a digital "address", which are used to identify anything described using the Resource Description Framework (RDF) from the W3C

[9] A Verifiable Data Registry is "a system that facilitates the creation, verification, updating, and/or deactivation of decentralized identifiers and DID documents" - https://www.w3.org/TR/did-core/

[10] DNS is a globally trusted "lookup" system - taking in a human readable domain name like "btcpolicy.com" and returning an IP address. The DNS system is governed by ICANN, but unlike Bitcoin, the trust framework that governs ICANN (and thus modifications to the DNS ledger) is not open source - https://www.icann.org/resources/pages/accreditation-2012-02-25-en

[11] Verifiable Credentials - https://en.wikipedia.org/wiki/Verifiable_credentials

[12] Certified Electronic Credentials at Harvard - https://credentials.harvard.edu/about

[13] News Release: Homeland Security Awards Contracts to Six Startups to Identify, Develop, and Implement Privacy-Enhancing Digital Wallets Technologies - https://www.dhs.gov/science-and-technology/news/2024/07/08/homeland-security-awards-contracts-six-startups-identify-develop-and-implement

[14] Selective disclosure in digital credentials: A review
https://www.sciencedirect.com/science/article/pii/S2405959524000614

[15] "A verifiable presentation is a tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification. Certain types of verifiable presentations might contain data that is synthesized from, but do not contain, the original verifiable credentials (for example, zero-knowledge proofs)." -
https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations

[16] Musings of a Trust Architect: Building Trust in Gradients Christopher Allen
https://www.lifewithalacrity.com/article/progressive-trust/

[17] Identity & the Web, 2.1. Terminology - https://www.w3.org/reports/identity-web-impact/#terminology

[18] DID Method Rubric v1.0 https://w3c.github.io/did-rubric/#abstract

[19] Principal Authority: A New Perspective on Self-Sovereign Identity - https://www.blockchaincommons.com/articles/Principal-Authority/#the-rights-of-self-sovereign-authority

[20] SSI: The Bleeding Edges - https://docs.google.com/presentation/d/1BbkBX-tUgifiS_VKcqCZYRTQAGF5pK-JEYQwmHYbMcI/edit#slide=id.g76a3502c7f_0_319

[21] Utah SB0260 - https://le.utah.gov/~2025/bills/static/SB0260.html

[22] Utah Blazes New Trail for SSI: SEDI -
https://rufftimo.medium.com/utah-blazes-new-trail-for-ssi-sedi-441d8ce65ab8

[23] Wyoming SF0105 - Disclosure of private cryptographic keys (2021) - https://wyoleg.gov/Legislation/2021/SF0105

[24] https://clayhiggins.house.gov/wp-content/uploads/2024/06/TSA_digital_ID_xml3.pdf

[25] S.884 - Improving Digital Identity Act of 2023 - https://www.congress.gov/bill/118th-congress/senate-bill/884/text

[26] Wyoming SF0039 - Digital Identity (2021) - https://wyoleg.gov/Legislation/2021/SF0039

[27] State Legislatures Need to Block Creation of Nightmarish National Identity System - https://www.aclu.org/news/privacy-technology/state-legislatures-need-to-block-creation-of-nightmarish-national-identity-system

[28] Strengthening and Promoting Innovation in the Nation's Cybersecurity - https://www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity

[29] Anoncreds - https://www.lfdecentralizedtrust.org/projects/anoncreds

[30] TruAge FAQ - https://www.mytruage.org/faq.html#scan-my-license

[31] https://www.tradetrust.io/

[32] Known Customer Credentials - https://github.com/TBD54566975/known-customer-credential

[33] Linux Foundation Decentralized Trust - https://www.lfdecentralizedtrust.org/

[34] W3C - https://www.w3.org/

[35] Blockchain Commons Advocacy - https://advocacy.blockchaincommons.com/

[36] Decentralized Identity Foundation - https://identity.foundation/

[37] Trust Over IP - https://trustoverip.org/

[38] Ayra - https://ayra.forum/about/

[39] The Hitchhiker's Guide to KERI. Part 2: What exactly is KERI? - https://medium.com/finema/the-hitchhikers-guide-to-keri-part-2-what-exactly-is-keri-e46a649ac54c

[40] Musings of a Trust Architect: The Case for an International Right to Freedom to Transact - https://www.lifewithalacrity.com/article/RightToTransact/

[41] Universal Declaration of Human Rights - https://www.un.org/en/about-us/universal-declaration-of-human-rights

[42] How Inflation Erodes Financial Privacy - https://www.cato.org/blog/how-inflation-erodes-financial-privacy

[43] Bodily Harms: Mapping the Risks of Emerging Biometric Tech - https://www.accessnow.org/wp-content/uploads/2023/10/Bodily-harms-mapping-the-risks-of-emerging-biometric-tech.pdf

[44] S.5242 - Saving Privacy Act - https://www.congress.gov/bill/118th-congress/senate-bill/5242/text

[45] 31 CFR 1020.220(a)(6) - https://www.ecfr.gov/current/title-31/part-1020#p-1020.220(a)(6)

[46] 15 USC 7001 - Electronic Signatures in Global and National Commerce Act - https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf

[47] Uniform Electronic Transactions Act - https://en.wikipedia.org/wiki/Uniform_Electronic_Transactions_Act

[48] OpenID for Verifiable Presentations - draft 28 - https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[49] Utah S.B. 260 Individual Digital Identity Amendments - https://le.utah.gov/~2025/bills/static/SB0260.html

[50] Utah Blazes New Trail for SSI: SEDI - Timothy Ruff - https://rufftimo.medium.com/utah-blazes-new-trail-for-ssi-sedi-441d8ce65ab8

Bitcoin Policy Institute

www.btcpolicy.org