The Immutable Civic Bedrock: Forging a New Social Contract on a Foundation of Digital Truth

Introduction: Defining the Immutable Civic Bedrock

Contextualizing Layer 1 within the Pyramid of Power

As the global economy transitions into an era characterized by advanced automation and the fragmentation of traditional employment, the 20th-century mechanisms of social power, such as organized labor and collective bargaining, are experiencing a marked decline.[1] In their place, new forms of digital agency are emerging, necessitating a new framework for the social contract. The "Pyramid of Power" is a modular, hierarchical model designed to empower individuals and communities in this new epoch. It outlines five layers of civic infrastructure, from cryptographically-secured identity to forkable governance, that collectively offer a blueprint for a more resilient and equitable digital society.[1]

This report focuses exclusively on the foundational layer of this pyramid: **Layer 1, the Immutable Civic Bedrock**. This layer is the indispensable substrate upon which all higher-order functions—including open value rails, radical transparency, direct democracy, and meta-governance—are built. It addresses the fundamental need for a stable, trustworthy, and verifiable source of truth for core civic information. Without this bedrock, any attempt to construct a digital social contract would rest on "quicksand," vulnerable to manipulation, corruption, and the erosion of public trust.[1] The bedrock establishes the inviolable personal sovereignty that is a prerequisite for meaningful participation in the digital age.

The Three Pillars of the Bedrock

The Immutable Civic Bedrock is composed of three core, interlocking components that together create a tamper-proof foundation for civic life.[1]

1. **Sovereign Digital Identity**: At its heart, the bedrock provides every individual with a secure, portable, and sovereign digital identity. This represents a paradigm shift away from traditional, state-centric identity models, where a person's identity is held and controlled by government databases, towards a user-centric or "self-sovereign" model. In this new model, individuals control their own cryptographic credentials, allowing them to prove who they are and what claims they are entitled to without relying on a central authority that could exclude, surveil, or de-platform them.[1] This is the fundamental "who you are" component of the new social contract.
2. **Inviolable Cryptographic Claims**: Complementing a sovereign identity is the ability to make inviolable claims to property, rights, and other entitlements. This involves recording critical civic data—such as property titles, vital records (births, marriages), legal contracts, and educational credentials—on tamper-evident ledgers secured by strong cryptography.[1] This is the "what you own" and "what you can claim" component, ensuring that an individual's fundamental assets and qualifications are protected from arbitrary seizure or alteration.
3. **The Principle of Tamper-Proof Records**: The key innovation that underpins both identity and claims is *immutability*. The bedrock replaces or augments the fallible trust placed in traditional institutions (courts, bureaucracies, paper archives) with mathematical guarantees.[1] By recording hashes of civic data on distributed or cryptographically linked ledgers, it becomes impossible for any single actor—including the state itself—to unilaterally alter, backdate, or delete records without detection.[1] This permanence creates a "bedrock of trust in society's basic facts and entitlements," thwarting corruption and establishing a single, verifiable source of truth for the most essential civic information.[1]

Thesis and Report Structure

This report posits that the Immutable Civic Bedrock is not merely a technological upgrade of existing bureaucratic functions but a fundamental political and economic restructuring. It recalibrates the relationship between the citizen, the state, and the market by establishing a new basis for individual agency rooted in "cryptographic self-ownership"—the verifiable control over one's own identity and data.[1] Furthermore, it creates the necessary technical and legal preconditions for a system of "algorithmic rights," empowering individuals to assert their claims and defend their interests in an increasingly automated and data-driven society.

To substantiate this thesis, this report will proceed in four parts. Section 2 will examine the first pillar, the sovereign digital self, through a comparative analysis of three distinct and influential models: Estonia's state-governed "digital nation," the European Union's federated "digital identity wallet," and Worldcoin's private, biometric "proof-of-personhood." Section 3 will explore the second pillar of inviolable claims, focusing on Georgia's pioneering blockchain land registry and the broader application of verifiable credentials. Section 4 will provide a technical deep dive into the underlying architectures of trust, including the standards for self-sovereign identity and the unique design of permissioned blockchains like Guardtime's KSI. Finally, Section 5 will offer a comprehensive analysis of the bedrock's transformative impact on the social contract, exploring its role in forging algorithmic rights, reshaping power dynamics in a post-labor economy, and navigating the profound challenges of exclusion and surveillance.

Pillar I: The Sovereign Digital Self and the Spectrum of Identity

From State Ledger to Personal Wallet: The Evolution of Digital Identity

The concept of digital identity has undergone a significant evolution, moving progressively from centralized, state-controlled systems towards more decentralized, user-centric models. Historically, digital identity has been fragmented and siloed, with governments, banks, and technology companies each maintaining their own proprietary databases.[2] This approach creates friction for users and raises significant privacy and security risks. In response, governments have developed national digital ID schemes to streamline access to public services, but these often retain a centralized architecture.[3]

The contemporary landscape reveals a fundamental tension between state-led models, which prioritize national efficiency, security, and administrative control, and the emerging paradigm of self-sovereign identity (SSI), which prioritizes individual empowerment, privacy, and user control over personal data.[5] This tension is not merely technical but deeply political, reflecting a contest over the source and locus of identity in the digital age. The following case studies illustrate a spectrum of approaches, from a highly efficient state-monopoly model to a federated regulatory framework and a radical private-sector initiative aiming to bypass the nation-state entirely.

Case Study: Estonia's Digital Nation - The State-Governed Apex

Estonia stands as the world's most advanced digital society, having built a comprehensive, state-governed identity ecosystem that is deeply integrated into every facet of civic and commercial life.[7]

System Overview

For over two decades, Estonia has provided its citizens with a state-issued digital identity (e-ID). With an adoption rate of 99% among residents, the system is ubiquitous and serves as the cornerstone of the nation's e-government services.[1] The e-ID ecosystem is multi-faceted, offering several secure authentication methods: a mandatory, chip-based national ID card; a SIM-based Mobile-ID for smartphones; and an app-based Smart-ID.[9] These tools enable Estonians to perform nearly all bureaucratic tasks online, including filing taxes (98% are filed online), managing bank accounts, accessing personal health records, signing legally binding documents, and even voting in national elections.[9] The system has generated immense efficiency gains, with digital signatures alone estimated to save each citizen an average of five working days per year.[9]

e-Residency Program: A Transnational Digital Identity

In 2014, Estonia extended its digital infrastructure to the world with its pioneering e-Residency program. This initiative offers a government-issued, transnational digital identity to any non-resident, allowing them to establish and manage an EU-based company entirely online.[1] Over 100,000 individuals from more than 170 countries have become e-residents, effectively "plugging into" Estonia's efficient and trustworthy legal and digital framework.[1] The program represents a revolutionary step in decoupling economic identity from physical geography, demonstrating that a nation-state can scale its jurisdiction digitally and compete in a global marketplace for governance services.[8]

Governance and Trust Model

Estonia's success is not merely technological; it is rooted in a deep political commitment to digital transformation and a governance model designed to foster public trust. A core tenet is the "once only" principle, which mandates that the state can only ask a citizen for a piece of information once; thereafter, it must be securely shared between government agencies as needed.[11] This interoperability is enabled by X-Road, a decentralized, open-source data exchange layer that connects the nation's public and private sector databases without creating a single, monolithic central database.[11]

While the identity system is government-issued and therefore centralized in its authority, it builds trust through radical transparency. A key feature is the "Data Tracker," a portal where citizens can monitor who has accessed their personal data, when, and for what purpose.[1] This accountability mechanism serves as a powerful deterrent against misuse by officials and provides citizens with a degree of oversight, mitigating some of the concerns typically associated with state-controlled identity systems.

Case Study: The European Digital Identity Wallet (eIDAS 2.0) - The Federated, Regulatory Model

The European Union is pursuing a different path, creating a federated and interoperable digital identity framework through comprehensive regulation. This approach seeks to balance the sovereign authority of its member states with the need for a seamless, user-centric, cross-border digital single market.

Framework and Objectives

The legal foundation for this initiative is the eIDAS 2.0 regulation (Regulation (EU) 2024/1183), which entered into force in May 2024.[14] It amends the original eIDAS framework and mandates that all 27 EU member states must offer their citizens a European Digital Identity Wallet (EUDI Wallet) by 2026.[15] The primary objective is to enable any EU citizen to use their national digital ID to securely access public and private online services across the entire Union, breaking down digital borders and fostering a more integrated economic and civic space.[1]

Key Features

The EUDI Wallet is designed to embody the core principles of self-sovereign identity within a state-sanctioned framework. Key features include [14]:

- **User Control**: The wallet resides on the user's personal device (e.g., a smartphone), giving them full control over their data.
- **Selective Disclosure**: Users can share specific attributes from their credentials without revealing the entire document. For example, they can prove they are over 18 to access an age-restricted service without disclosing their exact date of birth or address.
- **Free and Open**: The wallet will be free of charge for all natural persons, and the core application software components are mandated to be open source, promoting transparency and security.
- **Legal Validity**: The wallet will support qualified electronic signatures, which hold the same legal weight as handwritten ones across the EU.
- **Interoperability**: It will be built on common technical standards to ensure that a wallet issued in one member state is recognized and accepted in all others.

This model represents a sophisticated hybrid: the credentials within the wallet (e.g., national ID, driver's license) are issued by trusted government authorities, but the wallet itself is a tool of personal empowerment, placing the user in control of their data interactions.

Implementation Status

The eIDAS 2.0 framework is actively being implemented. As of late 2024, the European Commission has adopted the first set of implementing acts that establish the technical architecture, reference framework, and common standards for the wallets.[14] Member states are now in the process of developing their respective wallets, with large-scale pilots underway to test various use cases, such as mobile driving licenses and e-prescriptions. The full, mandatory rollout is anticipated by 2026.[14]

Case Study: Worldcoin - The Private, Biometric, and Controversial Frontier

At the most radical end of the identity spectrum is Worldcoin, a private-sector project that aims to create a global, universal identity system completely detached from the nation-state. Its approach is technologically ambitious, globally scoped, and ethically contentious.

Mission and Technology

Worldcoin's stated mission is to build a globally-inclusive identity and financial network to address a critical challenge of the AI age: distinguishing humans from bots online.[18] This "proof-of-personhood" is intended to enable a host of future applications, from preventing Sybil attacks in online governance to facilitating the fair distribution of Universal Basic Income (UBI).[1]

The core of its technology is the "Orb," a custom-designed, spherical biometric imaging device that scans a person's iris.[18] The iris scan is converted into a unique, abstract numerical representation called an IrisCode. This code is checked against a global database to ensure the person has not signed up before. If unique, the system issues a cryptographically secure "World ID" to the user's smartphone app.[20] The project claims this process is privacy-preserving by default, as the iris images are typically deleted from the Orb after the IrisCode is created, and the World ID itself is not linked to the user's biometric data or real-world identity, using zero-knowledge proofs to enable anonymous verification.[18]

Privacy and Ethical Controversies

Despite its privacy-preserving design claims, Worldcoin's methodology has sparked significant global controversy and regulatory scrutiny.[22] Data protection authorities in numerous countries, including the UK, France, Germany, Kenya, and Indonesia, have launched investigations or halted the project's operations.[23]

The central concerns include [22]:

- **Collection of Sensitive Biometric Data**: The iris is one of the most stable and unique biometric identifiers. Critics question the necessity of collecting such sensitive data for the stated purpose and worry about the security of the central database of IrisCodes, which could become a target for hackers. Unlike a password, a compromised biometric template cannot be changed.
- **Informed Consent**: Investigations have focused on whether users, particularly in developing countries where the project has been actively promoted, are giving truly

informed consent. The practice of offering a small crypto token (WLD) in exchange for a scan has been criticized as potentially coercive, inducing people to trade sensitive personal data without fully understanding the long-term implications.
- **Regulatory Compliance**: Authorities are examining whether Worldcoin's practices comply with stringent data protection laws like the EU's GDPR, which classifies biometric data as a "special category" requiring a clear legal basis and explicit consent for processing.

Sybil Resistance as a Core Value Proposition

The project's primary justification for its use of biometrics is to solve the problem of Sybil resistance at a global scale.[24] A Sybil attack occurs when a single actor creates numerous fake identities to gain disproportionate influence in a network—for example, to claim multiple shares of a UBI distribution, to cast multiple votes in an online poll, or to overwhelm a social network with automated bots.[24] By creating a unique, non-transferable proof-of-personhood anchored to an individual's physical body, Worldcoin aims to provide a robust defense against such attacks, which are becoming easier to mount with advanced AI.[1] This makes it a potentially crucial piece of infrastructure for any future system that requires a one-person, one-share or one-person, one-vote principle to function fairly.

Comparative Analysis of Identity Models

The divergent approaches of Estonia, the EU, and Worldcoin highlight the critical trade-offs in designing a digital identity system. There is no single "best" model; rather, each represents a different set of political, social, and technological priorities. The table below provides a structured comparison of these three landmark initiatives.

Feature	**Estonia (e-ID)**	**EU (EUDI Wallet)**	**Worldcoin (World ID)**
Governance Model	State-led, centralized issuance, national scope with transnational	Federated, regulatory-driven, transnational (EU-wide) public-private	Private (Tools for Humanity/World Foundation), decentralized network, global

	extension (e-Residency).	ecosystem.	ambition.
Technology Stack	PKI, chip/SIM/app-based authenticators, X-Road interoperability layer, KSI Blockchain for integrity.	DIDs/VCs (W3C standards), open-source wallet software, relies on notified national eID schemes.	Custom biometric hardware (Orb), iris scanning, zero-knowledge proofs, blockchain protocol (Ethereum L2).
Basis of Trust	Institutional trust in government, legal framework, transparency tools (Data Tracker).	Regulatory compliance (eIDAS 2.0), technical standards, user control over data sharing.	Cryptographic proof of unique humanness, protocol transparency, decentralization goal.
Primary Use Case	Comprehensive e-government, secure commercial transactions, digital democracy (i-Voting).	Cross-border access to public/private services, secure authentication, digital signatures.	Sybil resistance for Web3, UBI distribution, distinguishing humans from AI, private logins.
Key Strength	Proven, high-adoption, comprehensive integration into society.	Interoperability, strong legal foundation, balances state authority with user control.	Solves the hard problem of global, unique proof-of-personhood at scale.
Key Controversy	Centralized state control (though mitigated by transparency), potential single point of failure.	Implementation complexity across 27 member states, potential for inconsistent user experience.	Severe privacy concerns over biometric data collection, ethical questions about rollout, regulatory

			scrutiny.

These case studies reveal that "sovereign identity" is not a monolithic concept but a spectrum of control and authority. Traditional identity is a monopoly of the nation-state, granting documents like passports that define legal personhood. Estonia's system represents the digitization and optimization of this state monopoly; it is hyper-efficient and user-friendly, but identity remains a grant from the state.[9] The EU's eIDAS 2.0 framework marks a significant evolution. It acknowledges the need for user control and privacy by adopting the technical architecture of self-sovereign identity, but it keeps the authority to issue the underlying credentials firmly in the hands of its member states, creating a federated system where state power and individual rights are held in a delicate balance.[14] Worldcoin represents a radical departure, attempting to bypass the state entirely. It seeks to create a new, global identity primitive based not on a political fact (citizenship) but on a biological one (the uniqueness of an iris).[18] Consequently, these are not merely different technological solutions; they are competing political philosophies about the ultimate source and locus of identity. The choice of which model to adopt is an inherently political decision about the future role of the state in a globalized, digital world.

Pillar II: Inviolable Claims and Cryptographically Secured Rights

The Problem of Trust: Corruption, Fraud, and Bureaucratic Friction

Beyond the question of "who you are" lies the equally critical question of "what you own" and "what you can claim." In many parts of the world, the systems designed to record and protect these claims—particularly land titles—are deeply flawed. Paper-based registries are susceptible to physical destruction, forgery, and fraudulent alteration. Even centralized digital systems can be compromised by corrupt insiders who can illicitly edit or delete records, dispossessing legitimate owners.[25] This lack of secure property rights creates enormous economic friction, prevents individuals from using assets like land as collateral, and erodes public trust in government institutions.[25] The promise of cryptographic ledgers is to provide an incorruptible, publicly verifiable record of these fundamental claims.

Case Study: Georgia's Blockchain Land Registry - A Bulwark Against Corruption

The Republic of Georgia provides one of the earliest and most-cited examples of a government using blockchain technology to secure a core civic function: its national land registry.

Context and Objectives

In the post-Soviet era, Georgia was plagued by systemic corruption, with property records being a frequent target for manipulation.[1] As part of a broader anti-corruption drive, the government sought to leverage technology to restore public trust and provide absolute security for property rights. In 2016, the National Agency of Public Registry (NAPR) partnered with the blockchain technology company Bitfury to pilot a system that would make its land titles immutable.[1]

Implementation

The project's technical architecture was a pragmatic and innovative hybrid solution. Rather than replacing its existing, efficient digital registry system, the NAPR augmented it with a blockchain layer.[28] Each property transaction was timestamped on a private, permissioned blockchain built using Bitfury's Exonum framework. A cryptographic hash (a unique digital fingerprint) of each transaction was then anchored to the public Bitcoin blockchain.[1] This design offered the best of both worlds: the speed and control of a permissioned system for day-to-day operations, and the ultimate, globally-verifiable security and immutability of the world's most powerful public blockchain.[1] By 2017, the pilot had successfully recorded over 300,000 land titles and other property documents using this method.[1]

Impact and Current Status

The project was widely hailed as a success in achieving its primary goal: eliminating the possibility of surreptitious, post-facto alteration of property records.[1] By making the history of every title publicly auditable via the Bitcoin blockchain, it dramatically increased public confidence that ownership records were secure from tampering by either external hackers or corrupt internal officials.[1] While the initial pilot demonstrated the viability of the technology, public information on its nationwide expansion since 2020 is limited. More recent developments in Georgia's digital asset space appear to have shifted focus toward broader cryptocurrency regulation and the exploration of smart contracts for real estate transactions, building on the foundation of trust established by the land registry project.[30]

Beyond Land: Verifiable Credentials as Portable Proofs of Claims

The principle of securing claims with cryptographic proof extends far beyond real estate. The same technological framework can be applied to a vast range of personal attributes and entitlements, transforming them from static entries in siloed databases into portable, user-controlled, and instantly verifiable assets.[1]

This is most powerfully realized through the concept of Verifiable Credentials (VCs). A university, for example, can issue a graduate a VC representing their diploma. This digital diploma is cryptographically signed by the university and held in the graduate's personal digital wallet. The graduate can then present this VC to a potential employer, who can instantly and mathematically verify its authenticity without needing to contact the university's registrar's office.[1] This process drastically reduces administrative friction, combats credential fraud, and empowers the individual with direct control over their own records. Pioneering institutions like MIT have already begun issuing blockchain-secured digital diplomas, and governments have explored the technology for securing official records. For example, Colombia ran a pilot to record academic diplomas on a blockchain to curb rampant fraud.[1] These examples illustrate a future where all manner of personal claims—professional licenses, medical histories, credit scores, and civic memberships—can be issued as secure, portable VCs, forming a rich and verifiable tapestry of an individual's identity and qualifications.

The experience with blockchain-based land registries, however, reveals a critical limitation that tempers the technology's promise. While blockchain can guarantee the integrity of a record *after* it has been entered onto the ledger, it cannot inherently validate the accuracy of the information at the moment of entry.[1] This is often referred to as the "garbage in, garbage out" problem. If a corrupt official, a flawed process, or inaccurate source data leads to the registration of a fraudulent land title, the blockchain will immutably and perfectly preserve that fraudulent record. The technology itself cannot distinguish between a legitimate and an

illegitimate claim at the point of origin.

This reality reframes the role of blockchain in governance. It is not a panacea that automatically eliminates corruption, but rather a powerful and unforgiving auditing tool. By creating a permanent, transparent, and incorruptible audit trail, it makes any malfeasance at the human-computer interface impossible to hide or deny after the fact. The knowledge that any fraudulent entry will be permanently recorded for all to see creates a powerful social and behavioral deterrent for the officials responsible for data entry. Therefore, the primary impact of an immutable ledger is not just technical data security; it is the enforcement of accountability, shifting the focus of anti-corruption efforts from preventing record tampering to ensuring the integrity of the people and processes at the system's edge.

The Technological Substrate: Architectures of Trust and Immutability

The construction of an immutable civic bedrock relies on a stack of sophisticated technologies designed to create, manage, and verify digital identity and claims in a secure, decentralized, and privacy-preserving manner. Understanding these core architectural components is essential to grasping how the bedrock functions.

The W3C Standards: A Common Language for Digital Trust

To ensure global interoperability, the World Wide Web Consortium (W3C) has developed a set of open standards that form the technical foundation for self-sovereign identity.

Decentralized Identifiers (DIDs)

A Decentralized Identifier (DID) is a new type of globally unique identifier designed to be controlled by the user, independent of any centralized registry like a domain name system or a government database.[33] A DID is essentially a string of text, for example

did:example:123456789abcdefghi, that serves as a stable, persistent address for an entity (a person, organization, or thing). The DID itself contains no personal information; it simply

points to an associated "DID Document," a public file that contains cryptographic public keys and service endpoints necessary to interact with the DID's owner.[34] This architecture allows an individual to have a verifiable digital identity that they create, own, and control, without needing permission from any external authority.[36]

Verifiable Credentials (VCs)

Verifiable Credentials (VCs) are the digital equivalent of physical credentials like driver's licenses or university diplomas.[37] A VC is a set of claims (e.g., "Name: Jane Doe," "Date of Birth: 01-01-1990," "Degree: B.S. in Computer Science") made by an issuer about a subject (the holder). This set of claims is packaged into a standardized data format (typically JSON) and is cryptographically signed by the issuer.[33] This digital signature makes the credential tamper-evident; any change to the data would invalidate the signature. This allows a third party to mathematically verify both the authenticity of the issuer and the integrity of the claims.[38]

The Trust Triangle

DIDs and VCs work together within a three-party ecosystem known as the "Trust Triangle," composed of Issuers, Holders, and Verifiers.[36]

1. **Issuer**: A trusted entity (e.g., a government, university, or employer) that creates a VC, signs it with its private key, and issues it to a Holder.
2. **Holder**: The individual who requests the VC from the Issuer and stores it in their personal digital wallet (e.g., a smartphone app).
3. **Verifier**: An entity that needs to confirm a claim about the Holder (e.g., a bar needing to check age, an employer needing to verify a degree). The Holder presents the VC to the Verifier.

Crucially, the Verifier can check the validity of the VC by using the Issuer's public key (found via the Issuer's DID) without needing to contact the Issuer directly. This model decentralizes the verification process, enhances user privacy (as the Holder controls the flow of information), and increases efficiency.

Ledgers for Governance: Permissioned vs. Public Blockchains

While the W3C standards define the data formats, the underlying ledger technology used to anchor DIDs and VCs can vary. The choice of blockchain architecture has significant implications for governance, privacy, and control.

Public (Permissionless) Blockchains

Public blockchains, such as Bitcoin and Ethereum, are open networks where anyone can join, view the ledger, submit transactions, and participate in the consensus mechanism that validates them.[39] Their primary strengths are radical transparency, censorship resistance, and true decentralization, as they are not controlled by any single entity.[39] However, for many government services, these features can be liabilities. The complete transparency of public ledgers is often incompatible with data privacy requirements for sensitive citizen information. Furthermore, their permissionless nature means governments have no control over the network's participants or governance, and scalability can be a concern.[40]

Permissioned (Private/Consortium) Blockchains

Permissioned blockchains are closed networks where participation is restricted to a set of known, vetted entities.[41] An access control layer governs who can read the ledger, submit transactions, and validate blocks.[40] This model offers several advantages for civic applications:

- **Privacy**: Data can be kept confidential among the authorized participants.
- **Control**: The governing entities can enforce legal and regulatory compliance.
- **Performance**: With fewer validators, these networks can often achieve higher transaction throughput and faster finality.

For these reasons, most government-led blockchain projects, including Georgia's land registry and the infrastructure securing Estonia's data, have opted for permissioned or hybrid models. They provide the cryptographic integrity and auditability of a blockchain while retaining the necessary control and privacy for managing official civic data.[1]

Technical Deep Dive: Guardtime's KSI Blockchain - The Architecture

of Mathematical Certainty

Estonia's approach to data integrity relies on a unique, highly specialized technology called Keyless Signature Infrastructure (KSI), developed by the Estonian company Guardtime. KSI is a permissioned blockchain, but its design differs fundamentally from conventional blockchains.

Keyless Signature Infrastructure (KSI)

The most distinctive feature of KSI is that it does not use asymmetric (public/private key) cryptography for its signatures.[43] Traditional digital signatures rely on a private key, which, if compromised, can be used to forge signatures. KSI, by contrast, uses only one-way hash functions. This makes the system "keyless" and immune to threats that target key management, including future attacks from quantum computers that are expected to be able to break current public-key cryptography.[44]

Temporal Scaling

KSI's second major innovation is its scaling model. Typical blockchains scale linearly with the number of transactions (O(n)), meaning the ledger grows larger with every transaction added. KSI scales linearly with *time* (O(t)).[44] It achieves this through a massive aggregation process. Every second, the KSI network takes the hashes of all data events submitted to it from across its global clients and uses a hash tree (Merkle tree) to combine them into a single root hash value for that one-second interval. This single root hash is the only thing added to KSI's "calendar hash chain." This architecture allows the system to handle a virtually unlimited number of transactions per second while the blockchain itself grows at a small, constant rate (approximately 3GB per year).[45]

How it Ensures Immutability

The calendar hash chain is maintained and verified by a distributed network of consensus nodes. The root hash values are also published in widely witnessed public media (like legacy print newspapers or public blockchains), creating an irrefutable and globally accessible trust

anchor.[43] In Estonia's e-government system, whenever a record in a state database is created or modified, its hash is registered with the KSI network. The system returns a KSI signature that cryptographically links the data's state to a specific point in time on the calendar chain.[1] If an attacker—be it an external hacker or a malicious insider—later tries to alter that database record, its new hash will no longer match the original hash stored in the KSI signature. Any independent verifier can immediately detect the discrepancy, making unauthorized tampering evident.[48] This provides a mathematical proof of data integrity, replacing the need to trust system administrators with verifiable, digital truth.[48] This technology is used to secure numerous critical Estonian registries, including those for healthcare, business, property, and the court system.[49]

A critical architectural pattern emerges from both the SSI and KSI models: the decoupling of the underlying data from the cryptographic proof of its integrity. This separation is a paradigm shift that resolves the inherent tension between the need for transparency and the right to privacy. In the SSI model, a holder can use their Verifiable Credential to generate a zero-knowledge proof, allowing them to prove a specific fact (e.g., "I am over 18") without revealing the full source document (their ID card).[33] Similarly, in the KSI model, the actual government data never leaves the secure state database; only its anonymous hash is sent to the global KSI network for timestamping.[44] In both systems, the verification process is conducted on the cryptographic proof, not the raw data itself. This architectural separation is a key innovation that enables systems to be simultaneously trustworthy and privacy-preserving, overcoming a major political and social obstacle to the adoption of digital civic infrastructure.

Analysis: The Bedrock's Role in a New Social Contract

The establishment of an immutable civic bedrock is more than a technical project; it is a profound intervention in the distribution of power within a society. By providing individuals with verifiable control over their identity and data, it lays the groundwork for a new set of rights and a re-negotiated social contract fit for an automated, data-driven world.

Forging Algorithmic Rights: From Data Subject to Data Sovereign

In contemporary society, both public agencies and private corporations increasingly rely on algorithmic systems to make high-stakes decisions affecting people's lives. These systems determine eligibility for welfare benefits, calculate credit scores, screen job applications, and

even inform judicial sentencing. However, their inner workings are often opaque "black boxes," and they can perpetuate and amplify historical biases present in their training data, leading to new forms of systemic discrimination.[53] Individuals affected by these decisions often have little recourse, as they lack the means to inspect the logic or challenge the data used to judge them.

An immutable civic bedrock, particularly one built on the principles of self-sovereign identity and verifiable credentials, provides the technical toolkit to establish and enforce "algorithmic rights".[55] When an individual possesses a set of irrefutable, cryptographically-signed VCs about their own life (e.g., income statements, employment history, educational qualifications), they are no longer merely a passive "data subject" whose information is held by others. They become an active "data sovereign" who can present verifiable proof to audit and contest an algorithmic decision.[57] For example, if an automated system denies an individual a loan, they could present VCs to prove their financial history is sound, forcing the system (or its human overseers) to justify its decision based on verifiable inputs rather than opaque correlations. This capability for contestation shifts the balance of power, creating a mechanism for due process and accountability in an age of automated governance.

Reshaping Power Dynamics in a Post-Labor Economy

The social contract of the 20th century was largely built around the centrality of labor. Full-time employment provided not only income but also social identity, benefits, and a basis for political power through unions and collective action.[1] As automation and AI continue to diminish the economic value of many forms of human labor, this traditional foundation of individual leverage is eroding.[58]

In this emerging post-labor economy, personal data is increasingly understood as a new and valuable form of capital.[59] The vast datasets generated by human activity are the essential raw material that fuels the AI and machine learning systems driving economic productivity.[61] An immutable civic bedrock functions as the foundational property rights system for this new data-based capital. A self-sovereign identity acts as the "deed" that establishes an individual's ownership over their personal data, and immutable ledgers serve as the registry that secures these claims.[1] This provides individuals with a new source of economic agency and bargaining power. Instead of relying solely on the sale of their labor, individuals could potentially license, pool, or collectively bargain over the use of their data, capturing a share of the value it creates.

Furthermore, a robust and Sybil-resistant digital identity is a critical prerequisite for the fair and effective implementation of new social safety nets designed for a post-labor world, such

as Universal Basic Income (UBI).[1] To prevent fraud and ensure that distributions are allocated on a one-person, one-share basis, a system must be able to reliably verify that each recipient is a unique human being. Identity systems like Worldcoin are explicitly designed to solve this problem, providing the foundational layer upon which such large-scale redistribution programs could be built.[18]

From Institutional Trust to Verifiable Truth: A Political Theory Perspective

The shift towards a cryptographically secured civic bedrock represents a fundamental change in the philosophical basis of the state-citizen relationship. Traditional political theory, from Hobbes onward, has largely conceived of the state as the central, sovereign authority that creates and guarantees identity, rights, and property. Citizens place their trust in institutions—courts, legislatures, registries—to act as fair arbiters. The immutable bedrock challenges this model by introducing a source of truth that exists independently of institutional discretion.[63]

This new paradigm aligns more closely with a Lockean conception of natural, inherent rights that pre-exist the state. With a self-sovereign identity, an individual possesses a cryptographically defensible claim to their own personhood and data that is not merely granted by the state but is technologically self-evident.[63] The ability to control and present one's own verifiable data becomes a new form of liberty. However, it is crucial to recognize that decentralization is not a synonym for democracy.[65] While SSI technology empowers individuals with greater control over their data, the governance of the overall ecosystem—who is recognized as a legitimate issuer of credentials, what standards are adopted, how disputes are resolved—can either reinforce existing power structures or create new, less transparent ones. True democratic empowerment requires not only individual cryptographic sovereignty but also collective, participatory oversight of the identity infrastructure itself.[65]

Challenges, Critiques, and Unresolved Questions

Despite its transformative potential, the path toward an immutable civic bedrock is fraught with significant risks and challenges that must be addressed to avoid creating a digital dystopia.

- **Exclusion and the Digital Divide**: The most pressing danger is that digital ID systems, if

not designed with radical inclusion as a primary goal, will exacerbate the marginalization of vulnerable populations.[68] Individuals lacking access to technology, digital literacy, stable internet connectivity, or the necessary foundational documents to enroll in the system risk being rendered "invisible" and locked out of essential economic and civic services.[70]

- **The Specter of Surveillance**: The same technology that empowers can also be used to control. A national digital ID system, especially a mandatory and centralized one, can become a tool for unprecedented state surveillance and social engineering.[13] As critics of systems like India's Aadhaar have argued, linking a unique identifier to all aspects of a person's life—financial transactions, travel, healthcare, political activity—creates a detailed profile that can be used for social control, chilling dissent and eroding privacy.[13]
- **Governance and Accountability**: The governance of these complex ecosystems remains a largely unresolved question. In a decentralized network, it is often unclear who is ultimately accountable when systems fail, data is breached, or rights are violated.[2] Establishing clear legal frameworks for liability, data protection, and due process is a critical prerequisite for the responsible deployment of these technologies.

The implementation of an immutable civic bedrock thus presents a profound paradox. On one hand, it offers individuals unprecedented sovereignty and control over their digital existence, empowering them to act as autonomous agents in their interactions with state and corporate power.[63] On the other hand, by creating a perfect, permanent, and machine-readable record of identity and claims, it makes the individual more legible and potentially more governable by algorithmic systems than ever before.[68] This legibility is a double-edged sword: it can be a tool for radical inclusion and efficiency, enabling seamless access to services like UBI [21], or it can become a tool for surveillance and exclusion, for instance, if a digital ID were required for all forms of political speech or assembly.[69] The ultimate outcome—whether this foundation supports a society of liberation or one of control—will not be determined by the technology itself, but by the political choices made about its governance, the legal rights embedded within its architecture, and the democratic accountability of the institutions that oversee it.

Conclusion: The Cornerstone of 21st-Century Governance

Synthesis of Findings

The analysis of Layer 1 of the Pyramid of Power demonstrates that the Immutable Civic Bedrock is no longer a theoretical concept but an empirically validated and technologically feasible foundation for a new social contract. Global deployments, from Estonia's comprehensive digital nation to Georgia's targeted anti-corruption registry and the EU's ambitious transnational wallet, prove that core civic functions can be secured with cryptography at scale. These initiatives, while diverse in their governance models and technical architectures, all point toward a future where the fundamental facts of civic life—who we are and what we can claim—are anchored in verifiable, tamper-evident records. This bedrock is the necessary precondition for rebuilding public trust and rebalancing power in an era of digital transformation and institutional decay.

The Transition from Trust to Verification

The most profound shift represented by this foundational layer is the transition from a social contract based on fallible, opaque trust in human institutions to one grounded in the verifiable, mathematical certainty of cryptography. This does not eliminate the need for good governance, ethical leadership, or just laws. Instead, it provides a powerful new set of tools to enforce them. When government actions are recorded on an immutable ledger, "trust" is augmented by "verification." The ethos of governance can shift from "trust us, we are the authority" to "verify for yourself, the record is public and cannot be changed." This move toward provable accountability has the potential to fundamentally alter the relationship between citizens and the state, fostering a more transparent, participatory, and resilient civic order.

Future Trajectory and Policy Recommendations

The global momentum toward implementing digital identity and securing public records is undeniable. As policymakers and technologists navigate this transition, several core principles should guide their efforts to ensure the bedrock empowers citizens rather than the state or the market alone.

1. **Prioritize Open Standards and Interoperability**: To avoid creating new digital silos, systems should be built on open, global standards like those developed by the W3C for DIDs and VCs. This ensures that an individual's identity and credentials are portable and not locked into a single proprietary ecosystem.
2. **Design for Radical Inclusion**: The digital divide is the single greatest threat to the equity of these new systems. From the outset, design must account for those with limited

access, low digital literacy, or no foundational documents. This requires providing robust offline alternatives, investing in public education, and creating multiple, accessible pathways for enrollment.

3. **Establish Robust Legal Frameworks Before Deployment**: Technology must not outpace the law. Comprehensive data protection legislation, clear rules on liability and due process, and strong, independent oversight bodies are not afterthoughts but essential prerequisites for deploying any digital identity system. These legal safeguards must be in place *before* a system is rolled out to the public.
4. **Foster Public Debate and Democratic Governance**: The architecture of a nation's identity system is a constitutional-level decision with profound implications for freedom, privacy, and power. These decisions must not be made solely by technocrats or government agencies. They require broad public debate and the establishment of democratic governance structures that allow citizens to have a meaningful voice in shaping the rules of their own digital existence.

Ultimately, the goal is to construct an immutable civic bedrock that serves as a true public good—a foundation that secures the rights and enhances the agency of every individual, ensuring that the digital future is one of empowerment, not control.

Works cited

1. The Pyramid of Power - A Modular Framework for a New Digital Social Contract.pdf
2. The Governance of Digital Public Infrastructure: Case Studies - International Center for Law & Economics, accessed September 6, 2025, https://laweconcenter.org/resources/the-governance-of-digital-public-infrastructure-case-studies/
3. Why Legal Digital ID Matters - Digital Legal ID Governance, accessed September 6, 2025, https://www.governance4id.org/why
4. How governments can deliver on the promise of digital ID | McKinsey, accessed September 6, 2025, https://www.mckinsey.com/industries/public-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id
5. Public private partnership models for national identity programs - Thales, accessed September 6, 2025, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/public-private-partnerships
6. Digital Identity Ecosystems: Unlocking New Value - World Economic Forum, accessed September 6, 2025, https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf
7. e-Estonia - We have built a digital society & we can show you how, accessed September 6, 2025, https://e-estonia.com/
8. e-Estonia: The power and potential of digital identity - Thomson Reuters Institute,

accessed September 6, 2025, https://www.thomsonreuters.com/en-us/posts/news-and-media/e-estonia-power-potential-digital-identity/
9. ID-card - e-Estonia, accessed September 6, 2025, https://e-estonia.com/solutions/estonian-e-identity/id-card/
10. Mobile ID - e-Estonia, accessed September 6, 2025, https://e-estonia.com/solutions/estonian-e-identity/mobile-id/
11. Digital identity in practice – Estonia and the e-state | GBG, accessed September 6, 2025, https://www.gbg.com/en/blog/digital-identity-in-practice-estonia/
12. e-Residency - e-Estonia, accessed September 6, 2025, https://e-estonia.com/solutions/estonian-e-identity/e-residency/
13. Lessons from National Digital ID Systems for Privacy, Security, and Trust in the AI Age, accessed September 6, 2025, https://www.techpolicy.press/lessons-from-national-digital-id-systems-for-privacy-security-and-trust-in-the-ai-age/
14. eIDAS 2.0 | Updates, Compliance, Training, accessed September 6, 2025, https://www.european-digital-identity-regulation.com/
15. eIDAS 2.0: A Beginner's Guide - Dock Labs, accessed September 6, 2025, https://www.dock.io/post/eidas-2
16. The EU Digital Identity Wallet: A Beginner's Guide - Dock Labs, accessed September 6, 2025, https://www.dock.io/post/eu-digital-identity-wallet
17. The European Council has approved the eIDAS Regulation, accessed September 6, 2025, https://www.twobirds.com/en/insights/2024/global/the-european-council-has-approved-the-eidas-regulation
18. Worldcoin price today, WLD to USD live price, marketcap and chart | CoinMarketCap, accessed September 6, 2025, https://coinmarketcap.com/currencies/worldcoin-org/
19. World (blockchain) - Wikipedia, accessed September 6, 2025, https://en.wikipedia.org/wiki/World_(blockchain)
20. World - The real human network., accessed September 6, 2025, https://world.org/
21. blog.kleros.io, accessed September 6, 2025, https://blog.kleros.io/introducing-ubi-universal-basic-income-for-humans/#:~:text=The%20ability%20to%20develop%20a,can%20reach%20everyone%20on%20Earth.
22. UK Data Regulator Joins Scrutiny of WorldCoin - Dechert LLP, accessed September 6, 2025, https://www.dechert.com/knowledge/onpoint/2023/8/uk-data-regulator-joins-scrutiny-of-worldcoin.html
23. Eye Scans and Legal Lines: How Worldcoin's Global Expansion ..., accessed September 6, 2025, https://medium.com/@j.razo7869/eye-scans-and-legal-lines-how-worldcoins-global-expansion-sparked-a-data-privacy-backlash-b37ede357317
24. Sybil Resistance Identity Layer - Humanity Protocol, accessed September 6, 2025, https://www.humanity.org/web3-verticals/sybil-resistance

25. A Blockchain-Based Land Titling Project in the Republic of Georgia: Rebuilding Public Trust and Lessons for Future Pilot Projects - ResearchGate, accessed September 6, 2025, https://www.researchgate.net/publication/330069648_A_Blockchain-Based_Land_Titling_Project_in_the_Republic_of_Georgia_Rebuilding_Public_Trust_and_Lessons_for_Future_Pilot_Projects
26. Bitcoin solved land registry in Georgia - Think School, accessed September 6, 2025, https://www.thethinkschool.in/blog/Georgia-CaseStudy
27. BitFury Announces Blockchain Land Titling Project With The Republic Of Georgia And Economist Hernando De Soto - Bitcoin Magazine, accessed September 6, 2025, https://bitcoinmagazine.com/business/bitfury-announces-blockchain-land-titling-project-with-the-republic-of-georgia-and-economist-hernando-de-soto-1461769012
28. Improving the security of a government land registry - Exonum, accessed September 6, 2025, https://exonum.com/story-georgia
29. Bitfury: Blockchain for Government - Case - Faculty & Research - Harvard Business School, accessed September 6, 2025, https://www.hbs.edu/faculty/Pages/item.aspx?num=53445
30. Best crypto license in Georgia in 2025 - LegalBison, accessed September 6, 2025, https://legalbison.com/blog/crypto-license/best-crypto-license-in-georgia-in-2025/
31. Crypto Regulations in Georgia 2025... - CoinStats, accessed September 6, 2025, https://coinstats.app/news/24589942a7cacfb6c9c5dd40fa3ae660e6ff2f917a7460cdda1f206ad6106b9b_Crypto-Regulations-in-Georgia-2025/
32. Georgia Eases into Smart Contracts – Investor.ge, accessed September 6, 2025, https://www.investor.ge/2025/02/10/georgia-eases-into-smart-contracts/
33. The Ultimate Guide to Verifiable Credentials (VC) and DIDs - Gataca, accessed September 6, 2025, https://gataca.io/blog/self-sovereign-identity-ssi-101-decentralized-identifiers-dids-verifiable-credentials-vcs/
34. What are Decentralized Identifiers (DID) | Verifiable Credentials (VC) - Togggle, accessed September 6, 2025, https://www.togggle.io/blog/dids-vcs-explained
35. Decentralized Identifiers (DIDs): The Ultimate Beginner's Guide 2025 - Dock Labs, accessed September 6, 2025, https://www.dock.io/post/decentralized-identifiers
36. Self-Sovereign Identity: The Ultimate Guide 2025 - Dock Labs, accessed September 6, 2025, https://www.dock.io/post/self-sovereign-identity
37. Verifiable Credentials Data Model v2.0 - W3C, accessed September 6, 2025, https://www.w3.org/TR/vc-data-model-2.0/
38. What are Verifiable Credentials? Examples and Use Cases - Gataca, accessed September 6, 2025, https://gataca.io/blog/what-are-verifiable-credentials/
39. Public vs. Permissioned Blockchain: A Quick Look at Pros & Cons - Kaleido, accessed September 6, 2025, https://www.kaleido.io/blockchain-blog/public-vs-permissioned-blockchain
40. Public, Private, and Permissioned Blockchains Compared, accessed September 6,

2025, https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/
41. Permissioned vs. Permissionless Blockchain | Comprehensive Guide - MoonPay, accessed September 6, 2025, https://www.moonpay.com/learn/blockchain/permissioned-vs-permissionless-blockchain
42. Permissioned blockchain - Oracle, accessed September 6, 2025, https://www.oracle.com/developer/permissioned-blockchain/
43. KSI Blockchain Timestamping - Guardtime, accessed September 6, 2025, https://guardtime.com/timestamping
44. Keyless Signature Infrastructure - Guardtime, accessed September 6, 2025, https://m.guardtime.com/files/KSI_data_sheet_201509.pdf
45. Keyless Signature Infrastructure® (KSI™) Technology ... - blockchain, accessed September 6, 2025, https://blockchain.machetemag.com/wp-content/uploads/2017/11/Guardtime_WhitePaper_KSI.pdf
46. WGISS-52 Executive summary – Blockchain KSI Technology, accessed September 6, 2025, https://ceos.org/document_management/Working_Groups/WGISS/Meetings/WGISS-52/2.Wednesday/2021.10.20_12.25_Blockchain%20KSI%20technology.pdf
47. KSI blockchain - e-Estonia, accessed September 6, 2025, https://e-estonia.com/solutions/cyber-security/ksi-blockchain/
48. KSI blockchain provides truth over trust - Invest in Estonia, accessed September 6, 2025, https://investinestonia.com/ksi-blockchain-provides-truth-over-trust/
49. KSI® blockchain in Estonia, accessed September 6, 2025, https://e-estonia.com/wp-content/uploads/faq_ksi_blockchain.pdf
50. An overview of the functioning of the KSI blockchain (source - ResearchGate, accessed September 6, 2025, https://www.researchgate.net/figure/An-overview-of-the-functioning-of-the-KSI-blockchain-source-Guardtime-Extracted-from_fig2_359908026
51. Understanding ISS: VCs and DIDs - Archipels, accessed September 6, 2025, https://en.archipels.io/post/understanding-ssi-verifiable-credentials-vcs-and-decentralized-identifiers-dids
52. Blockchain Technology - SwissTruth, accessed September 6, 2025, https://swisstruth.ch/technology-2/
53. (PDF) Algorithms and digital human rights - ResearchGate, accessed September 6, 2025, https://www.researchgate.net/publication/352062488_Algorithms_and_digital_human_rights
54. Algorithmic Discrimination and Privacy Protection | Falletti, accessed September 6, 2025, https://www.lawjournal.digital/jour/article/view/185
55. Verifiable Credentials: The Foundation of an Ethical AI-Powered Future - Gobekli.io, accessed September 6, 2025, https://gobekli.io/verifiable-credentials-the-foundation-of-an-ethical-ai-powered

-future/
56. What Is Verifiable AI? A Guide to Transparency and Trust in AI - Identity.com, accessed September 6, 2025, https://www.identity.com/what-is-verifiable-ai-a-guide-to-transparency-and-trust-in-ai/
57. How Verifiable AI Enables Trust for AI Agent Adoption - cheqd, accessed September 6, 2025, https://cheqd.io/blog/how-verifiable-ai-enables-trust-for-ai-agent-adoption/
58. Assessing the Impact of New Technologies on the Labor Market: Key Constructs, Gaps, and Data Collection Strategies for the Bureau of Labor Statistics, accessed September 6, 2025, https://www.bls.gov/bls/congressional-reports/assessing-the-impact-of-new-technologies-on-the-labor-market.htm
59. When data is capital: Datafication, accumulation, and extraction, accessed September 6, 2025, https://researchmgt.monash.edu/ws/portalfiles/portal/303893944/303893762_oa.pdf
60. Bourdieu revisited: new forms of digital capital – emergence, reproduction, inequality of distribution - Taylor & Francis Online, accessed September 6, 2025, https://www.tandfonline.com/doi/full/10.1080/1369118X.2024.2358170
61. Digital Labour in the Platform Economy: The Case of Facebook - MDPI, accessed September 6, 2025, https://www.mdpi.com/2071-1050/10/6/1757
62. Personal data as a new productive asset - URPP Equality of Opportunity - Universität Zürich, accessed September 6, 2025, https://www.urpp-equality.uzh.ch/en/research/Economic-Change/Personal-data-as-a-new-productive-asset.html
63. Blockchain and sovereignty the beginnings of a digital ID revolution, accessed September 6, 2025, https://ingroupe.com/insights/blockchain-sovereignty-beginnings-digital-identity-revolution/
64. Are We There Yet? A Study of Decentralized Identity Applications - arXiv, accessed September 6, 2025, https://arxiv.org/html/2503.15964v1
65. Can Decentralized Identity make the Internet more democratic? | by Purvi Jain - Medium, accessed September 6, 2025, https://medium.com/@passionatepurvi07/can-decentralized-identity-make-the-internet-more-democratic-604a0f3ce960
66. "The Right to (Digital) Identity" by Sarah M. Snow, accessed September 6, 2025, https://ir.lawnet.fordham.edu/iplj/vol35/iss4/3/
67. POLITICAL DECENTRALIZATION - Boston University, accessed September 6, 2025, https://www.bu.edu/econ/files/2015/04/Mookherjee_PolDecentAREDec14v2.pdf
68. The role of electronic transactions and national digital ID systems in the digital economy, accessed September 6, 2025, https://policyaccelerator.uncdf.org/all/brief-electronic-transactions-digital-id
69. Identified but Unheard. Assessing the Impacts of Digital ID on Civic and Political

Participation of Marginalized Communities, accessed September 6, 2025, https://www.ndi.org/sites/default/files/Identified%20but%20Unheard%20FINAL.pdf
70. Navigating the Risks and Rewards of Digital ID Systems - Open Government Partnership, accessed September 6, 2025, https://www.opengovpartnership.org/stories/navigating-the-risks-and-rewards-of-digital-id-systems/
71. The politics of digital identity: mapping national identity ecosystems for risks and vulnerability analysis | by Dr. Emrys Schoemaker - Medium, accessed September 6, 2025, https://medium.com/caribou-digital/emrys-schoemaker-and-tom-kirk-introduce-caribou-digitals-new-project-to-develop-an-identity-8ec31ba61c9b
72. 8 Countries With the Most Innovative Digital ID Systems - Beyond Encryption, accessed September 6, 2025, https://www.beyondencryption.com/blog/countries-most-innovative-digital-id-systems
73. Publication: Digital IDs for Development: Access to Identity and Services for All - World Bank Open Knowledge Repository, accessed September 6, 2025, https://openknowledge.worldbank.org/entities/publication/305aba36-80d2-5833-9ef7-460de77375c6