ChatGPT

Blockchain and the State: Functions, Opportunities, and Constraints

Introduction

Modern governments fulfill several core functions that underpin societal trust and order. These include maintaining authoritative records (e.g. land titles, identity registries), coordinating collective decision-making (e.g. elections and lawmaking), and allocating or regulating scarce privileges (e.g. issuing money, granting spectrum licenses, managing carbon quotas). As blockchain technology promises **tamper-evident ledgers, decentralized consensus, and programmable transactions**, a critical question is how these **affordances** might **replicate, complement, or constrain** traditional state roles. This report analyzes the primary functions of government in theory and practice, and evaluates blockchain's potential to **replace**, **augment**, or **limit** the state's monopoly in each domain. We draw on case studies from the US, EU, and UK – from **land registries in Sweden and Georgia** to **digital identity under EU eIDAS**, **CBDC pilots**, **Wyoming's DAO law**, and **supply-chain platforms like TradeLens** – to illustrate real-world experiments. We also compare major blockchain platforms (Ethereum, Hyperledger Fabric, Cosmos, etc.) and their suitability for "civic" applications. The analysis takes a globally comparative perspective (with emphasis on US, EU, and UK) and provides a realistic appraisal of where blockchains could credibly substitute for governmental roles in the near- to medium-term.

Government's Core Functional Domains and Blockchain Affordances

1. Notarization of Facts: Records, Registries, and Proof of Ownership

One foundational role of government is to **notarize facts** – certifying and storing authoritative records of identity, property, contracts, vital statistics, and other legal rights. Public registries (land cadastres, corporate registries, birth certificates, etc.) provide a **single source of truth** backed by the state's authority. The government, in effect, serves as a trusted notary and record-keeper, ensuring records are accurate and protecting them from tampering or fraud. This centralized system has strengths (legal finality, clear custody) but also weaknesses: records may be siloed, prone to bureaucratic delay or corruption, and rely on fallible human procedures.

Blockchain's Affordances – Auditability & Immutability: Blockchain ledgers offer **immutable, append-only record-keeping** where each entry is time-stamped and cryptographically secured. This creates a **tamper-evident log** of transactions or data updates, potentially providing the same assurance of authenticity that a government notary would. As one blockchain expert noted, *"the best way to think about this technology is that it's like a global notary"* [1]. A blockchain-based registry can be **audited by any participant** – every change is transparent and verifiable – which could reduce fraud and errors. In theory, once a property deed or birth record is recorded on an immutable ledger, it cannot be altered or back-dated without detection. This inherent integrity is especially attractive in contexts where **trust in government is**

low or corruption is a problem, since an immutable public ledger can **embed trust in technology rather than in fallible institutions**.

Replace, Complement, or Constrain? To what extent can blockchain replace the state's notary function? In a *replacement* scenario, a decentralized ledger could serve as the primary record of, say, land ownership – independent of a central authority. In practice, full replacement is rare and challenging: while a blockchain can record **proof of ownership**, enforcement of those rights (ejecting a squatter, adjudicating disputes) still requires state power (police, courts). **Complementary** models are more common: governments can **leverage blockchain for added security and efficiency** in their registries, while still providing the legal and institutional framework around the data. For example, a government land office might record title transfers on a distributed ledger to create an indelible audit trail (complementing the official registry). In doing so, the state remains the ultimate guarantor of property rights, but blockchain acts as a **technological check** – constraining officials from altering records unilaterally or **increasing transparency** to deter corruption. In this sense, blockchain can **constrain** malfeasance by **locking in an immutable history** of official records. However, the state's monopoly is only partially constrained: a dishonest official cannot secretly erase a title if the blockchain is public, but the legal system still governs how that record is used or when it's considered valid.

Real-world Examples: Several governments have piloted blockchain in notary/registry functions, especially for **land records**. **Sweden's land registry (Lantmäteriet)** conducted a multi-year pilot (2016–2018) using a private blockchain to record property transactions [2] [3]. In this system, **authorized parties (land authority, banks, buyers/sellers)** ran nodes on a blockchain network; each step of a property sale (from signing a contract to registering title) was logged and visible to all participants in near-real time [3]. The pilot showed that blockchain **can drastically speed up property deals** – reducing the time from signing to registration **from months to days** by automating verification and eliminating paper-based processes [4]. Lantmäteriet estimated such a system could save Swedish taxpayers over €100 million annually, thanks to faster transactions, better data redundancy, and enhanced security [4]. Notably, Sweden's implementation used a **permissioned blockchain** (access restricted to vetted entities) rather than a fully public chain – reflecting a design choice to balance openness with privacy and control. While successful as a proof of concept, officials acknowledged that scaling to nationwide use would require resolving **governance and legal questions** (e.g. how to legally recognize the digital ledger records) [5] [6]. As of the pilot's conclusion, the technology was promising but not yet a replacement for the official land register.

Perhaps the most cited success in this domain is **Georgia's land registry**. In 2016–2017, the Republic of Georgia partnered with Bitfury to **integrate blockchain into its national land titling system** [7] [8]. The approach Georgia took is instructive: they used a **hybrid model** where a **private permissioned blockchain** manages the land registry's internal records, and **cryptographic hashes of those records are anchored to the Bitcoin public blockchain** [8]. This means that while the Georgian government still controls the primary database of land titles, every title deed or transaction is hashed and the hash is stored in a Bitcoin transaction – providing an immutable, timestamped proof of the record's existence that **no one (not even the government) can falsify**. By 2017, Georgia had recorded over **100,000 land title documents** to the blockchain in this way [9] [10]. The benefit is twofold: Georgian citizens gain confidence that their property records are **secure and verifiable** (no bureaucrat can back-date a sale or alter the ledger without detection [8]), and the land agency gains a robust backup and audit trail. This **complements** the government's role – the state still handles registrations and disputes, but blockchain provides **independent verification**, effectively **constraining any insider tampering**. Georgia's example has been hailed as a model for other countries with historical issues in land administration: *"A secure property registry built on blockchain can*

secure billions of dollars in assets… by addressing the rapidly growing demand for transparency and accountability," Bitfury noted of the project [11]. Indeed, the initiative was partly inspired by economist Hernando de Soto's push to strengthen property rights in emerging economies [7] [12]. It illustrates that **blockchain can substitute for some functions of a notary (providing proof of integrity) while still relying on the state for legal enforcement**.

Beyond land, governments have explored blockchain for **notarizing myriad records**: birth and death certificates, business licenses, educational certificates, and more. For instance, **academic credentials** can be issued as verifiable digital records on a blockchain, making it easier for employers or other schools to trust their authenticity. In this vein, the **European Union** via its *European Blockchain Services Infrastructure (EBSI)* is developing a **verifiable credentials framework** aligned with the upcoming eIDAS 2.0 regulation. In this model, universities or governments issue tamper-proof digital diplomas or ID attributes to citizens, which are then **cryptographically signed and registered on a blockchain for verification** [13]. The **blockchain acts as an immutable registry of trusted issuers (e.g. accredited universities or civil registries)** and their public keys, so that anyone verifying a credential can check the issuer's signature against the ledger [13]. Importantly, the EU's design does *not* put personal data on-chain (to comply with privacy laws); only **proofs and issuer attestations are recorded** [13]. This **complements government digital ID systems** by adding a layer of cryptographic trust and cross-border interoperability – effectively **extending the notary function of the state into the digital realm** with greater auditability. Under the new eIDAS framework, EU member states will likely act as **"Qualified Trust Service Providers"** issuing verifiable credentials (e.g. a government could issue a digital ID credential or a driving license credential), and the blockchain-based system will **ensure these credentials are universally verifiable across jurisdictions**. This can be seen as blockchain *augmenting* the state's notary role (making it more robust and cross-compatible) rather than replacing it. It also shows how blockchains can *constrain* states indirectly: once a credential is issued and anchored on a public ledger, it's much harder for any authority to retroactively invalidate or doctor it without leaving evidence.

Limitations: Despite these successes, blockchain is not a cure-all for registries. **Garbage in, garbage out** still applies: a blockchain can prove a document hasn't been altered, but it cannot guarantee the document was correct or honestly issued in the first place. Human error or fraud at the input stage (e.g. registering a fake land deed) will be perpetually memorialized. Moreover, the **"oracle problem"** means that linking real-world assets to blockchains is tricky – you always need a trusted source to confirm ground truth (for example, a surveyor or registrar must confirm that Person A indeed sold Parcel X to Person B). Blockchains also introduce new costs and complexities (node infrastructure, digital key management for users, etc.). Governments have to decide on **governance of the ledger** (who runs the nodes, how updates to code are handled, how to recover from mistakes). These issues have slowed full adoption. In the **Swedish pilot**, officials noted the need to resolve governance questions before going live [5]. In short, blockchains can **enhance the integrity and efficiency of public records** and even substitute for some notary functions, but they work best in tandem with legal systems. The state's role as **guarantor of last resort** (backing the data with force of law) remains crucial, although the technology can **lock in honesty** and **shine a light on malfeasance**, thereby *constraining* any abuse of the state's custodial power over important records.

2. Synchronization of Collective Decisions: Elections and Legislative Processes

Another core domain of government is to **facilitate collective decision-making** – that is, to aggregate the will of the people or their representatives into actionable decisions. This includes **conducting elections** (from national votes to local referenda) and managing legislative or deliberative processes in councils and

parliaments. These processes require **fairness, transparency, and acceptance of outcomes**, which traditionally rests on trusted procedures (e.g. secret ballots, supervised vote counts, official gazettes for publishing laws). The state monopolizes this coordination role to ensure a single, legitimate result (e.g. who won an election, what law is in effect). Failures in this domain – whether fraud in voting or lack of transparency in lawmaking – can undermine democratic legitimacy.

Blockchain's Affordances – Decentralized Consensus & Transparency: Blockchains inherently achieve **consensus** among distributed participants on the state of a ledger. Applied to voting or decision records, this could mean that **no single authority can falsify the outcome** – a majority of the network must agree on the result. A blockchain-based voting system, for instance, can provide an **open, auditable trail of votes** without revealing individual votes (if designed with cryptographic anonymization). The immutability of blockchain can ensure that once a vote is cast, it cannot be altered or deleted, and results are **verifiable end-to-end**. Blockchain can also enable new forms of "digital governance" such as **smart contracts** that automatically execute a collective decision (for example, releasing funds if a quorum approves a proposal). The idea of a **"decentralized autonomous organization" (DAO)** exemplifies an attempt to synchronize collective decisions via code: stakeholders vote with tokens, and the outcome (encoded in a smart contract) directly triggers changes, with no central intermediary. In theory, this could be applied in civic contexts – e.g. a local community DAO voting on budget allocations, where funds are automatically disbursed according to the blockchain vote result.

Replace, Complement, or Constrain? *Replacing* core democratic processes with blockchain is ambitious and controversial. One could imagine a **fully blockchain-based election** where votes are cast on a public ledger rather than via government-run ballot boxes – in effect, the *network* counts the votes, not a government agency. This has appeal in terms of **removing single points of failure or trust**: no election commission official or corrupt insider could secretly manipulate the count, because the tally is computed by decentralized nodes and is fully transparent. However, practical and security challenges abound (discussed below). More plausible in the near term are *complementary* uses: blockchain can **complement election infrastructure** by providing an added layer of verifiability. For example, after a traditional paper-ballot election, the results from each polling station could be hashed and posted to a public blockchain. This would **audit-proof the results** – any later change in the official results could be detected by comparing to the blockchain record (which is timestamped and immutable). Such approaches have been piloted in some locales to increase trust in announced outcomes. Another complementary use is in **proxy voting or smaller-scale decision processes**: e.g. a city could use a permissioned ledger to let citizens vote on local issues online, with each vote recorded immutably, while still having the city clerks verify eligibility off-chain.

Blockchain can also **constrain governments** by enabling *parallel* methods of decision-making outside state control. The rise of online communities or activist DAOs illustrates this – groups can organize votes among themselves (say, on funding public goods or coordinating protests) using blockchain tools, which the government cannot easily censor or manipulate. In authoritarian contexts, this could potentially constrain the state by creating a **tamper-resistant record of collective sentiment** (though such use is nascent). Additionally, if a government knows that citizens can verify results via an independent blockchain record, it is constrained from misreporting or altering those results without detection.

Real-world Examples: The most direct experiments with blockchain in collective decision-making have been in **voting systems**. In 2018, **West Virginia (USA)** ran a landmark pilot allowing overseas military voters from several counties to **vote in a midterm election via a blockchain-based mobile app** [14]. The app, provided by Voatz, recorded encrypted ballots and then **anchored the votes on a blockchain ledger**

for the state to count. Only a small number of voters participated (dozens), but it was the first federal election test of blockchain voting in the US [14] [15]. Voters used biometrics on their phone to authenticate, cast their ballot, and could later verify that their vote was recorded on the blockchain [16]. From the user's perspective, this promised greater accessibility (they could vote from anywhere via phone) and confidence that their vote wasn't lost in the mail or miscounted [17]. Indeed, deployed military often have to sacrifice ballot secrecy by emailing or faxing ballots – the blockchain system restored secrecy while also providing a real-time digital receipt [18]. West Virginia's Secretary of State noted the goal was to see if the tech could improve participation for those who can't easily vote in person [19] [20]. In terms of results, the pilot was considered successful in usability – *"pretty slick!"* was the first soldier-voter's verdict [21] – and it modestly increased turnout among eligible overseas voters in the trial counties [22].

However, this experiment also highlighted concerns. Security researchers later identified vulnerabilities in the Voatz app, and **expert opinion remains sharply skeptical of internet voting via blockchain** [23]. Renowned cryptographers argue that while blockchain can make vote tallying transparent, it does not solve problems of **malware on voters' devices, server penetration, or voter coercion**, and that the addition of blockchain might introduce new attack surfaces. The **synchronization of collective choice is uniquely sensitive**: anonymity must be preserved (to prevent coercion) while ensuring one-person-one-vote and resisting cyberattacks – a very high bar. In West Virginia's case, after security audits, the state paused further blockchain voting deployments. This underscores that **fully replacing state-run elections with a decentralized system is not yet practical** given security and trust issues. That said, smaller-scale uses continue. For example, the **Swiss city of Zug** (known for its "Crypto Valley") conducted a test of a blockchain-based municipal vote in 2018 (for a consultative poll), and **Estonia** – famed for digital governance – has explored blockchain for *maintaining integrity* of its already-digital voting system (Estonia's i-voting logs are hashed to a ledger for audit). These cases treat blockchain as a **complementary safeguard** rather than the primary voting mechanism.

Beyond elections, consider **legislation and public administration**. Blockchain could enable novel forms of **"smart legislation"** – laws or regulations encoded as smart contracts that execute automatically. For instance, a environmental regulation could be implemented as a smart contract that automatically fines factories (by deducting tokens) if pollution sensors report emissions above a limit. This kind of *programmable law* could **constrain discretionary enforcement** (everyone knows the rule will trigger objectively) and improve compliance. However, real legal systems are too complex and value human judgment, so this remains largely theoretical or limited to narrow cases (like **algorithmic allocation of budgets or benefits** under pre-defined rules). There is also an emerging concept of **"GovTech"** platforms where citizen input is recorded via blockchain for policy-making (e.g. **liquid democracy** platforms that track delegate votes on-chain). These aim to make the legislative process more transparent or participatory, but they are experimental.

One tangible development is how governments respond to **DAOs** – decentralized autonomous organizations that operate by member votes on blockchain, often managing real assets or funds. DAOs represent a **new mode of collective governance** that exists independently of nation-states (some call it *"borderless governance"*). While not a replacement for public government, the rise of DAOs has prompted jurisdictions like the US state of Wyoming to integrate them legally (discussed in the case studies below). By recognizing DAOs as legal entities, governments are effectively acknowledging an alternative form of organizing collective decisions (for co-ops, companies, communities) that is mediated by blockchain consensus rather than by state law alone. In the long run, widespread use of such structures could

constrain traditional governance by offering people new ways to coordinate and self-govern (for example, community DAOs managing local resources with limited state oversight).

Limitations: The **limits of blockchain in collective decisions** are as much social and political as technical. Even if one solves the cryptography of a secure voting ledger, the **trust in the system's setup** (who wrote the code? who runs the nodes?) and the **final mile** (proving a voter's identity, preventing vote buying, etc.) are non-trivial. Also, a blockchain cannot compel losers of a vote to accept the outcome – that still requires institutional legitimacy. In legislatures, while blockchain could record votes of lawmakers immutably, the negotiation and deliberation processes aren't easily captured on a ledger. For now, blockchain's main contribution is likely in **increasing transparency and auditability** (e.g. immutable logs of proceedings, public identities of decision-makers recorded, smart contracts for enforcing procedural rules). These help **complement** governance by shining light on processes and potentially **constrain** behind-the-scenes alterations, but they do not remove the need for trust in actors and institutions. As one report noted, despite interest in blockchain for voting, *"considerable skepticism [persists] about whether blockchain is the right technology to accomplish online voting — or whether online voting is the right way to go at all"* [23]. Thus, in the near term we expect to see **blockchain as a tool for transparency in decisions (audit trails, open data)** more than as a wholesale platform for conducting large-scale public votes or passing laws autonomously.

3. Allocation of Scarce Privileges: Money, Licenses, and Quotas

A third critical function of governments is the **allocation of scarce resources or privileges** that are subject to public policy. This includes **monetary issuance** (central banks issuing fiat currency and controlling the money supply), distributing spectrum licenses for wireless communications, permits for resource extraction, quotas for carbon emissions or fisheries, and more. Such allocations often have **economic value and require authority** – the government's role is to ensure fairness, prevent conflict, and align distribution with policy goals (e.g. auctioning spectrum for efficient use, issuing currency to stabilize the economy). The state's monopoly in these areas is sometimes explicit (only the central bank can create legal tender) or effectively so (only regulators can grant broadcast licenses or pollution credits). Mismanagement or abuse (over-issuing money leading to inflation, corrupt license awards) can have large societal costs, so there is perennial interest in mechanisms that impose discipline or transparency on these allocation processes.

Blockchain's Affordances – Decentralization, Tokenization & Programmability: Blockchain technology directly emerged in this domain with **Bitcoin's invention (2009)** – a decentralized currency not issued by any state. Cryptocurrencies demonstrated that a network of nodes could enforce **scarcity of a digital token** through consensus rules, without needing a central issuer. This directly challenges the monopoly of governments over money. Beyond currency, blockchains enable **tokenization of assets or rights** – creating digital tokens that represent ownership or usage rights (which could correspond to licenses or quotas). These tokens can be **programmed with rules** (smart contracts) and traded in transparent markets. For example, a blockchain could host a **spectrum license exchange** where rights to radio frequencies are represented as tokens that can be auctioned or traded in real-time, with all transactions logged immutably. Similarly, **carbon credits** or **fishing quotas** could be issued as tokens that are traceable and have built-in compliance checks (e.g. automatically retiring a token when used). The **auditability** of blockchain means every issuance and transfer of a privilege can be tracked, reducing corruption or double-allocations. **Decentralized consensus** means the rules (like a cap on total tokens) can be enforced by code, preventing any single actor from unilaterally changing the supply or giving someone special favor – in other words, **immutability and consensus can enforce scarcity and rules** even against government wishes.

Replace, Complement, or Constrain? In the monetary realm, blockchain-based cryptocurrencies like Bitcoin and Ethereum are often framed as *replacements* or alternatives to sovereign money. In practice, while crypto adoption is growing, no major economy has replaced its national currency with a blockchain currency (El Salvador's adoption of Bitcoin as legal tender in 2021 is a notable experiment, though the US dollar remains in parallel use). Where blockchain has arguably *constrained* governments is by **creating competitive pressures**: central banks see the popularity of Bitcoin, stablecoins, and other crypto assets as pushing them to innovate (hence the rush to explore Central Bank Digital Currencies, or CBDCs). Cryptocurrencies, being **non-state money**, also constrain monetary authorities by offering an escape valve – if a government inflates its currency or imposes capital controls, citizens can potentially turn to crypto as an alternative store of value or means of transfer. Indeed, the motivation behind some CBDC projects is explicitly to *"fend off the threat to [central banks'] money-printing powers from Bitcoin and Big Tech firms"* [24]. In that sense, blockchain has already curtailed the absolute monopoly governments had on digital money by proving a viable alternative channel.

More directly, many governments are looking to *complement* or modernize their issuance functions with blockchain. A leading example is the development of **Central Bank Digital Currencies**: these are essentially fiat currencies implemented using digital ledger technology (not always blockchain per se, but often inspired by it). A **CBDC** can be thought of as the central bank issuing a tokenized form of national currency that might circulate on a controlled ledger. The motivations include improving payment efficiency, financial inclusion, and keeping control over digital payments that might otherwise shift to private cryptos. As of 2025, **over 130 countries are exploring CBDCs** and dozens are in pilot or development stages [25] [26]. For instance, the **European Central Bank (ECB)** is on track with a **digital euro pilot**, aiming for a possible launch around 2028 [26]. The **Bank of England** has been researching a "digital pound," which could be introduced later this decade [27]. The United States, while slower on a retail CBDC, has conducted experiments like the MIT-Federal Reserve **Project Hamilton** (which prototyped a high-speed digital dollar ledger) and **Project Cedar** at the New York Fed (which tested a wholesale CBDC for interbank transfers). As of mid-2023, U.S. efforts focus on wholesale use (bank-to-bank settlements), with any consumer-facing digital dollar still in research – one report noted U.S. progress on retail CBDC has "stalled" pending legislative direction [28]. These CBDC projects are *complementary* in the sense that they use blockchain/DLT-inspired designs to **enhance the state's existing role** in money (making it more technologically up-to-date), rather than ceding that role. A CBDC can be built on a **permissioned blockchain run by the central bank and selected nodes** (for example, commercial banks might run validating nodes). This could ensure **auditability** and **programmability** (e.g. money with conditions or automated compliance), but keeps the central bank firmly in control of supply and rules. In short, CBDCs are a case where governments are **borrowing the innovations of blockchain (distributed trust, tokenization)** to **reinforce their monetary sovereignty**, effectively *countering* the potential replacement of fiat by crypto.

Other scarce privileges show a mix of replacement and complement. **Spectrum licenses**: There have been conceptual proposals and some trials for managing spectrum via blockchain – for example, the U.S. Federal Communications Commission and other telecom regulators have discussed dynamic spectrum access systems, where devices could automatically acquire frequency leases via a blockchain-based exchange. This could *complement* the current licensing regime by adding a real-time market and potentially enforce rules like one device cannot double-spend a spectrum token, etc. However, widespread deployment hasn't occurred yet; spectrum auctions remain centrally run (though one could imagine running an auction on a blockchain for transparency).

Environmental and tradeable permits is an area with active pilots. **Carbon credit registries** are being put on blockchains in various initiatives, to improve transparency and prevent double counting of emissions reductions. For example, IBM and other companies launched **blockchain platforms for carbon asset trading**, ensuring each credit (token) is unique and retired once used. Some countries' environmental agencies are experimenting with issuing tokens for renewable energy certificates or carbon offsets, which can then be tracked across borders. This doesn't replace the government's role in setting the cap or validating projects, but it *complements and constrains* by **making the market more transparent** and **automating compliance** (a smart contract can automatically invalidate a credit token after one use, preventing scams).

In the **realm of corporate and financial licenses**, consider that companies traditionally get charters or licenses from governments (for banking, for example). There are now blockchain-native alternatives like **DAO treasuries and DeFi lending platforms** that replicate some functions of licensed banks (taking deposits, making loans) without formal licenses, raising the question of constraint on regulatory regimes. Governments are responding by updating laws (as with Wyoming's DAO law, giving some legal status to such organizations rather than leaving them entirely in gray zone).

Cryptocurrencies & Stablecoins as Constraints: A particularly vivid way blockchain constrains state privilege is via **stablecoins** – privately issued digital tokens pegged to fiat currency (like USD). Stablecoins (e.g. USDC, Tether) now facilitate billions in daily transactions, effectively providing a parallel payments system outside traditional banking, yet denominated in sovereign currency. They grew to fill demand for fast, borderless dollar transactions (especially in crypto markets and emerging economies with volatile currencies). This forced regulators to pay attention – concerns that unregulated stablecoins could undermine financial stability or monetary policy have led to debates on how to oversee or integrate them. In short, **blockchain-based money and tokens have broken the state's exclusive hold on issuing and moving value**, which in turn is *pressuring states to adapt*. As Reuters observed, **all G20 countries (bar one) are now in advanced exploration of CBDC, a dramatic leap from just a few years prior** [25] [26], precisely because no major economy wants to be left without a sovereign footing in the digital currency space.

Real-world Cases: We will delve into specific case studies like **CBDC pilots** (in the next section) and **Wyoming's DAO law**. But to mention a few: **China's e-CNY** (digital yuan) is the world's largest CBDC pilot, reaching over 260 million people in pilot cities, though that's outside our US/EU/UK focus. **Sweden's e-krona** pilot is one of Europe's first – Riksbank built a proof-of-concept DLT system (with R3 Corda) for an e-krona aimed at supplementing cash usage; this is ongoing with tests for retail use [29]. In the UK, while no pilot is live, the Bank of England issued discussion papers and the Chancellor indicated a digital pound (dubbed "Britcoin" in media) is likely needed in coming years [29]. The **European Central Bank** has finished prototyping a digital euro with various technology vendors (some prototypes reportedly based on blockchain or DLT components), and is entering a realization phase [26]. These efforts reflect a *complementary adoption* of blockchain tech under government stewardship. Meanwhile, **Bitcoin adoption** in places like El Salvador or usage of crypto in inflation-hit countries (Argentina, Turkey informally) shows a *replacement or workaround dynamic* – people using blockchain money when they lose faith in state money, thereby **disciplining governments** (El Salvador's dollarized economy now also has Bitcoin ATMs and transactions, for better or worse).

Another interesting "scarce privilege" case is **land/resource rights in developing nations**. For example, some projects propose tokenizing community land rights or water rights to help communities manage them transparently (though these often still need government buy-in). **Supply chain traceability tokens**

can allocate the privilege of saying a product is “authentic” or meets quotas – for instance, **fishing industry pilots** used blockchain to ensure fishing catches don’t exceed quotas by tracking fish from catch to market with tokenized catch certificates.

Limitations: While blockchain can enforce scarcity in the digital realm, tying that to real-world control remains a challenge. A spectrum token is only meaningful if regulators and devices respect it – which requires integration with legal frameworks and hardware. For money, a privately issued crypto will not fully replace fiat unless a whole economy embraces it (which brings volatility and other problems, as seen in El Salvador’s bumpy Bitcoin rollout). Governments also have tools to fight back – they can regulate exchanges, ban transactions, or as in the case of some stablecoins, possibly issue their own to crowd out unregulated ones. Moreover, the **programmability of tokens can be a double-edged sword**: it might enable **fine-grained control (even by governments)** such as programming a CBDC to be non-transferable out of country (capital control) or to expire if not spent (stimulus with expiry). This raises new governance and civil liberty concerns. Blockchain doesn’t inherently decide who sets the rules; it just enforces them rigidly. So, whether blockchain *constrains or enhances state power* in allocations depends on who designs the system. A public cryptocurrency can constrain state monetary power (by limiting their ability to inflate without people fleeing to crypto), whereas a state-run blockchain system might even *expand* state control (through greater surveillance or programmability). The **balance of outcomes** will likely vary by jurisdiction and application.

In summary, blockchain has proven adept at **creating digitally scarce tokens and transparent markets**, which can significantly improve how privileges are tracked and traded (complementing state systems) and in some cases **pose an outside alternative** that forces states to change (constraining their monopoly). The trajectory in the near term is that we’ll see *hybrid models*: government-sanctioned tokens (like CBDCs or tokenized licenses) operating alongside (and learning from) private or decentralized tokens, with careful attention to integrating legal enforceability with the on-chain mechanics.

Case Studies: Blockchain Experiments in Government Functions (US, EU, UK)

To illustrate the above themes in practice, we examine a series of case studies across the United States, European Union (and neighbors), and the United Kingdom. These highlight both **successful pilots and challenges** in implementing blockchain for government-related functions, offering a comparative perspective:

A. Land Registry on Blockchain – Sweden and Georgia

Sweden (EU): Sweden’s *Lantmäteriet* was one of the first European agencies to seriously test blockchain for land title management. Partnering with the startup ChromaWay and other firms, they built a private blockchain system to handle real estate transactions end-to-end [2] [3]. In this 2017 pilot, the buyer, seller, banks, and land registrar would each have a node on the network. Whenever a step occurred (a contract signed, a mortgage issued, a title updated), a **smart contract** on the blockchain recorded it and allowed all participants to verify the status [3]. The blockchain essentially served as a **shared, tamper-proof journal** for the transaction process. The result: they demonstrated cutting the typical time for conveyancing from **months to days**, largely by eliminating the manual paperwork and multi-step verification currently needed [4]. For instance, title registration after a sale could happen almost instantly once conditions (like payment and mortgage registration) were met, instead of waiting months for various parties to send documents.

Mats Snäll, the land registry's head of development, noted that nothing in the pilot indicated the technology wouldn't scale, and that it offered *"a good and secure way to have digital originals"* of property contracts, seemingly **resistant to hacking or corruption** [30]. The projected savings (over €100 million/year) and increased security were strong arguments in its favor [4]. Despite that, Sweden has proceeded cautiously – as of 2025 the land registry has not fully migrated to blockchain, but the pilot informed ongoing digitization efforts. It underscored the need to sort out **network governance (who runs the nodes?)** and **legal alignment** (making sure a blockchain record is legally recognized as the title) before deployment [5]. The Swedish case is a prime example of a *complementary blockchain solution*: it didn't aim to discard the land registry's role, but to **make it more efficient and trustworthy** by sharing the ledger with banks and buyers in real time. It also highlighted a preference for **permissioned chains in government** – control and privacy were maintained by restricting access to known entities, rather than using a public chain.

Georgia (Eurasia): We discussed Georgia's achievement earlier; it's worth reiterating here as a comparative note. Georgia's National Agency of Public Registry, with Bitfury's help, effectively integrated blockchain at scale, reportedly becoming *"the first government to secure land titles on the Bitcoin blockchain"* [7] [31]. By 2017, the Georgian system was operational, meaning any new land transaction would generate a blockchain proof. The Georgian model is often cited in international development circles as a way to **boost trust in property rights in countries with weak institutions** [11]. Indeed, the **Economist** in 2017 noted that experts were eyeing Georgia's experiment *"for proof of whether blockchain technology could alter the infrastructure of government everywhere."* [32] [33] The success in Georgia (a post-Soviet state eager to advance economically) provided momentum for similar efforts in other countries: Honduras had announced plans for a blockchain land registry around 2015 (amid concerns of rampant title fraud), though that faced delays; countries like **Ukraine, Dubai, and others** also engaged in blockchain-for-land projects with varied progress [34] [35]. Notably, **Ukraine** partnered with Bitfury in 2017 to put a range of government data on blockchain, "the largest of its kind anywhere" according to Reuters [36] – including not just land titles but potentially asset registers and more. (Ukraine's plans were disrupted by other events, but some pilots did occur.)

United Kingdom: While not in the original prompt's list, the UK's experience provides another EU/Western perspective. **HM Land Registry (England & Wales)** embarked on a project called *Digital Street*, investigating blockchain to improve the speed of land transactions. In 2018, it announced a partnership to build a prototype on **R3's Corda DLT platform** [37]. The idea was similar: to test if distributed ledger tech can **"revolutionise the property buy-sell process"** by sharing data among solicitors, banks, and the Land Registry instantly [38]. The head of HM Land Registry spoke of an ambition to be the world's leading land registry for speed and simplicity, and saw blockchain as a tool toward that goal [39]. Corda was chosen for its enterprise features like privacy and the ability to encode complex workflows (smart contract flow framework) [40]. The pilot successfully demonstrated that a property sale could be completed in under 10 minutes in a controlled environment (as opposed to the usual weeks) [41]. The UK pilot is a case of **public-private collaboration**: it engaged blockchain startups, academics, and industry stakeholders to ensure the solution fit real-world needs [42] [43]. Though the UK has not "gone live" with a blockchain land registry yet, the trial informed their broader modernization efforts and indicated that *blockchain could "transform land registry services by improving speed, simplicity and efficiency,"* as R3's CEO put it [44]. The UK's cautious approach – testing in R&D but integrating pieces slowly – contrasts with Georgia's more leapfrog adoption, reflecting differences in legacy system robustness and risk tolerance.

Lessons: Across Sweden, Georgia, and the UK, a few takeaways emerge. First, **permissioned blockchain networks (or hybrid models)** are preferred by governments for land registries – they want known

validators (agencies, banks) rather than unknown miners. Second, **blockchain alone doesn't solve everything**: these projects require legal reforms (e.g. recognizing digital signatures, smart contracts) and administrative buy-in. Third, where implemented, **user experience** can drastically improve (no lost paperwork, quicker transactions), and **transparency** improves (all parties see the same ledger). Finally, these case studies show **global knowledge transfer** – countries are learning from each other's pilots (the mention of *"we will be able to work with blockchain [by] this summer to place real estate extracts in a totally safe system,"* said Georgia's Justice Minister, touting being a leader in e-government [45]). This competition/cooperation is pushing the technology forward in the public sector.

B. Digital Identity and Verifiable Credentials – EU eIDAS and Beyond

Ensuring trusted identity and credentials is another arena of intense activity, especially in the EU. The **European Union's eIDAS regulation** (Electronic Identification, Authentication and Trust Services) sets a framework for cross-border recognition of electronic IDs and signatures. In 2021, the EU proposed an update (sometimes called *eIDAS 2.0*) which includes a concept of a **European Digital Identity Wallet** for all citizens and businesses. In this vision, people will have a mobile app that can store verified digital credentials (national ID, driver's license, diplomas, bank account info, etc.) that can be used across all 27 member states. **Blockchain and decentralized identity technologies play a key role** in this plan.

The EU's approach leverages the idea of **Self-Sovereign Identity (SSI)**, where individuals control their credentials and share them peer-to-peer, with verification happening via decentralized trust registries. The **European Blockchain Services Infrastructure (EBSI)** – a network of distributed nodes operated by EU member state authorities – is being built to support such use cases. Under EBSI, the **Verifiable Credentials** model works as follows: trusted authorities (like a university or government agency) issue a credential to a citizen in digital form and register a proof of that issuance on the EBSI blockchain. When the citizen needs to prove something (say their age, or their degree), they can present the credential from their digital wallet directly to a verifier, and the verifier can check the issuer's signature and status against the blockchain registry, without needing to call up the issuer each time [13]. The blockchain thus serves as a **publicly auditable directory of which entities are accredited issuers and what credentials they can issue** [13]. It also can list revoked credentials or expired keys, etc., in an immutable way. Crucially, **personal data is not stored on-chain** – only metadata and public key info. This design is highly aligned with privacy requirements: the EU specifically wants a system that **"uses blockchain where it makes sense: to support the verification of Verifiable Credentials"** and *not* to expose personal data [13]. In fact, one of the five design principles EBSI highlights is that *"blockchain is used as an immutable registry of trusted legal entities [issuers]… all other information is shared directly between the holder and verifier, without blockchain's involvement."* [13] This is a very interesting marriage of government trust and blockchain trust: the governments still **approve which issuers are trusted** (e.g. by a national scheme), but blockchain ensures that list of trusted issuers is **shared, secure, and in real-time across Europe**. It removes reliance on any single government database when verifying foreign credentials – a French employer can automatically trust a German university diploma if the German government's blockchain node vouches that the university is accredited and the diploma is valid.

This EU digital identity initiative is a **prescriptive case** – the EU is actively **mandating** member states to adopt this approach in coming years, aiming to reach 80% of citizens with a digital wallet by 2030. It's perhaps the most ambitious government-led blockchain-backed identity project in the world. It does not replace government ID systems; rather, it **interlinks them via decentralized tech**, effectively *constraining states from siloing identity data* and giving more control to citizens. For example, instead of dozens of

separate login accounts and document copies, a citizen might just have their certified attributes in their wallet and share what's needed – with the blockchain ensuring the receiving party can instantly verify authenticity. It addresses a classic trust synchronization problem: how to trust foreign documents – solved by a ledger of trust operated collectively by countries.

Outside the EU, **other examples** abound: **Estonia's e-Residency** program issues digital IDs to global entrepreneurs, and while it doesn't use blockchain for the IDs themselves, Estonia has used blockchain (KSI blockchain) to hash the integrity of its government databases (including identity records) since the 2010s, as a security measure. **Ontario, Canada** had a pilot for blockchain-based driver's licenses (using SSI principles) and some U.S. states (like Illinois, circa 2017) explored blockchain for birth certificate and vital record portability. In the UK, there was work on **digital evidence and driving tests** on blockchain (DVLA trials), and the British government-backed **Open Banking** initiative considered blockchain for secure credential sharing in finance.

The **key takeaway** from identity case studies is the emphasis on **hybrid decentralized solutions**: unlike currency, where some push pure decentralization, in identity the trend is *"government-in-the-loop"* but using blockchain to enhance privacy, security, and cross-jurisdiction trust. It's a complement that could gradually change power dynamics – giving individuals more agency (they hold their credentials, not just the issuing agency), and making systems more resilient (no single database to hack and alter, since verification is multi-source and ledger-confirmed). This in turn can constrain misuse: e.g. a corrupt official in one country can't issue a fake passport credential that will pass verification, because it won't be found on the shared ledger of valid issuers.

C. Central Bank Digital Currencies – Comparative (US, EU, UK)

As previously discussed, **CBDC** exploration is in full swing across major economies. Here we compare approaches:

- **European Union (ECB – Digital Euro):** The ECB has completed an investigation phase (2021–2023) and is moving into a realization phase for a **digital euro**. The design is likely a **two-tier model** (the ECB issues the digital currency, but distribution is through private banks/payment providers) and a **permissioned DLT** is under consideration to handle transactions. Security, privacy, and offline capability are key issues. The ECB's president Christine Lagarde stated in 2021 the goal to launch within ~four years [46] – putting it around 2025, but recent reports push a possible launch to **2028** after extensive pilots [26]. Indeed, the Atlantic Council's CBDC tracker noted the digital euro pilot should begin soon (involving testing with consumers and merchants perhaps) [26]. The EU sees this as not just modernization but **strategic autonomy** – ensuring the euro's role in a digital world and not ceding ground to foreign tech or currencies [47] [48]. They emphasize that a digital euro will co-exist with cash, and the blockchain element (if used) will be under high governance – likely using an **enterprise blockchain (maybe based on Hyperledger Fabric or similar)** for the ledger that authorized intermediaries update. Some prototypes by companies (as per ECB reports) included Hyperledger Fabric and R3 Corda implementations, showing a preference for controlled ledgers. Privacy has been debated: one option is to allow small-value transactions offline with no tracing (like digital cash), but larger transactions would be traceable for AML (Anti-Money Laundering). Blockchain's auditability can thus be a double-edged sword for privacy, and central banks are navigating that.

- **United Kingdom (Bank of England – "digital pound"):** The UK, outside the Eurozone, is in a similar position of exploring a retail CBDC. The BoE and HM Treasury issued a joint consultation in early 2023 calling a digital pound "likely needed in the future" and inviting input on design. They envision it primarily for domestic retail use, safeguarding financial stability. The BoE has done experiments (Project Rosalind with BIS, etc.) that build prototypes using APIs and ledgers. The likely approach is also two-tier, permissioned, and not strictly a blockchain but possibly inspired by it. The Bank's latest reports emphasize resilience and performance – whatever tech is chosen must handle high volumes (tens of thousands of TPS) and be secure. They have not committed to blockchain; in fact, the BoE has been open to either DLT or conventional tech that achieves the same ends. However, they did note any system would need to be extremely robust, possibly using a **private implementation of something like Ethereum or a similar smart contract platform** to allow programmability (smart contracts for certain features). The UK is also unique in that it's a major global finance hub, so they coordinate closely with international efforts (like ensuring interoperability with other CBDCs for cross-border payments). We might see the UK leverage existing networks – for example, joining Project mBridge or others for cross-border CBDC trials. **Timeline**: BoE said no earlier than 2025 for a decision to build, and launch could be in later 2020s. A Reuters piece mentioned the digital pound could be in use by later this decade if approved [27].

- **United States (Federal Reserve – Digital Dollar):** The US is a cautious outlier among the big economies. With the dollar's global role, the Fed and U.S. Treasury are carefully studying rather than rushing. In March 2022, President Biden's executive order asked agencies to evaluate CBDC benefits and risks [49]. The Fed issued a report in January 2022 outlining possibilities but taking no stance without Congressional support [50]. **Wholesale vs Retail:** The U.S. is more actively prototyping wholesale uses (e.g., interbank settlement). The New York Fed's **Project Cedar** in 2022 demonstrated a prototype for foreign exchange settlement using a blockchain-based wholesale CBDC – it achieved atomic settlement (simultaneous exchange of currencies) in 10 seconds, showing DLT could improve cross-currency transfers. On retail, the Boston Fed and MIT's **Project Hamilton** (Phase 1 report in 2022) built a high-performance transaction processor that in testing could handle **1.7 million transactions per second** with near-instant finality – indicating technology for a very scalable digital dollar is feasible [51]. Interestingly, that prototype combined some blockchain techniques with novel architectures, but wasn't a traditional blockchain (it was more a processing engine plus a validated transaction history). Currently, U.S. progress on a consumer CBDC is described as "moving forward" only on wholesale, while **"stalled" on retail** absent new laws [28]. There is also political pushback in the U.S. – some in Congress want to prohibit the Fed from issuing a retail CBDC, citing privacy or government overreach concerns [52]. So the fate of a digital dollar is uncertain. In the meantime, the U.S. is observing and participating in cross-border pilots (the Atlantic Council notes the U.S. finally joined a multi-country CBDC test called Project Agora with several other central banks) [52]. This is to ensure the U.S. isn't left out of setting global standards. Another nuance: U.S. regulators are focusing on stablecoin regulation – arguably treating that as an intermediate step to ensure private stablecoins (like USDC) are safe, which could serve many retail needs without an official CBDC, or pave the way for one.

Comparative insights: Across US, EU, UK – the **EU is most driven by policy cohesion and user convenience** (hence the pan-European wallet concept strongly supported by a regulated blockchain infrastructure). The **UK and US are more concerned about financial stability** (they worry how a CBDC might disintermediate banks or shift credit flows). Technologically, **all three are weighing permissioned DLT** versus alternative architectures. None have indicated using a public permissionless blockchain (due to

throughput, control, and privacy reasons). However, they all borrow the innovations of crypto: using cryptographic wallets for users, possibly using blockchain-inspired consensus for resilience, and aiming for some level of programmability (e.g. enabling automated payments or logic on the currency). **Case outcome so far:** No Western major economy CBDC is launched yet (contrasting with smaller ones like Bahamas' Sand Dollar or Nigeria's eNaira which are live). But within a few years, we expect at least the digital euro to be in pilot circulation. These will give insight into how effectively blockchain-tech can modernize money without causing unintended economic side effects. Notably, a **Reuters study in mid-2023** found *"all G20 countries bar one [Argentina] are now in advanced development/pilot of CBDC"* [53] and pointed out *"the push for CBDCs comes as cash use falls and authorities look to ensure they retain control in face of crypto and Big Tech."* [24] This encapsulates the theme: blockchain is being used by states to **complement and safeguard their function in money** even as it initially emerged as a challenge to it.

D. Decentralized Autonomous Organizations (DAOs) – Wyoming's Legal Recognition

The concept of a **DAO** – an organization governed by blockchain-based rules and community voting – directly intersects with government in terms of legal recognition and regulation. In traditional terms, forming an organization (corporation, partnership, co-op) is a privilege granted by the state via incorporation statutes. DAOs present themselves as internet-native organizations that operate by code, often without a clear legal status. This raised questions: can a DAO own assets, enter contracts, or have limited liability for its members, without being incorporated under some jurisdiction's law?

Wyoming, USA has been at the forefront of addressing this. In 2021, Wyoming passed first-of-its-kind legislation (Bill SF38) that **allows DAOs to register as a special type of LLC (Limited Liability Company)**. On July 1, 2021, the law took effect and **the American CryptoFed DAO became the first legally recognized DAO in the US** [54] [55]. Essentially, Wyoming offered a bridge between on-chain governance and off-chain legal personality: a DAO can file for LLC status by providing its smart contract and some information, and then it's treated as an LLC under state law (with members as shareholders, and the smart contract operating as the bylaws/operating agreement to the extent it can). The **American CryptoFed DAO**, which aims to create a token-based digital currency system, seized this opportunity – it filed the required forms, and Wyoming's Secretary of State acknowledged it as a DAO LLC [56]. This was a groundbreaking experiment because it tested how a DAO's on-chain activities would intersect with US securities law and other regulations. In fact, soon after, the CryptoFed DAO tried to register its tokens with the U.S. SEC and that process became contentious (the SEC viewed its filings as deficient, and an administrative battle ensued) [57] [58]. The details are beyond our scope, but suffice to say it's an ongoing story that will set precedents.

Why is Wyoming doing this? The state (which also pioneered other crypto-friendly laws) wants to attract blockchain innovation. By providing legal certainty, it hopes DAOs will base themselves in Wyoming (just like many corporations incorporate in Delaware). Other U.S. states, like Tennessee and Vermont, have also passed laws regarding blockchain-based LLCs or recognition of smart contract governance, though Wyoming's is the most comprehensive. Internationally, other jurisdictions are watching; for example, some Swiss cantons allow associations that are effectively DAO-like, and there's discussion in the EU of how to classify DAOs under existing legal entity forms.

From a government functions perspective, recognizing DAOs is an example of how blockchain is **changing the landscape of organizational governance**, and the government's role shifts from direct oversight to setting frameworks in which algorithm-governed entities can legally operate. One could say Wyoming's law

is **complementing** the state's function of chartering corporations by adding a new tech-enabled category. At the same time, it **constrains** the state in that if DAOs proliferate, some activities that used to be easily regulated (through corporate intermediaries) might occur in more decentralized ways. For instance, a traditional cooperative might be regulated by state co-op laws, but a global DAO co-op might now just register in Wyoming and have global membership operating via tokens – raising questions on how consumer protection, taxation, etc., will be enforced if at all on its activities. Wyoming's bet is that bringing DAOs into a legal fold (even a very light one) is better than leaving them completely "offshore" or in legal limbo.

Cooperative DAOs: The prompt mentioned "cooperative DAOs in Wyoming" – indeed, some DAOs focus on collective ownership of real-world assets or community projects (basically digital co-ops). CityDAO, for example, purchased land in Wyoming collectively as a DAO (it even got a mention by Wyoming's Governor) and registered as an LLC. The idea of **digitally-native cooperatives** managing resources or businesses via member votes on blockchain is powerful. If successful, it could provide an alternative to traditional corporate hierarchies and further demonstrate blockchain's role in **synchronizing collective decisions** and managing shared property (tying back to our earlier sections). Wyoming's framework gives such groups a sandbox to try real projects legally – CityDAO is experimenting with governance of a physical parcel of land by token holders; another one, Krause House DAO, aims to purchase an NBA basketball team collectively someday via a DAO structure (a lofty goal, but they are raising funds via tokens). Each of these tests the boundaries of both blockchain tech (can on-chain governance manage complex real assets?) and law (will regulators accept a token vote as legitimate corporate governance?).

UK/EU perspective on DAOs: Neither the UK nor EU has dedicated DAO laws yet, but discussions are underway. The UK Law Commission in 2022–23 examined how English law might accommodate DAOs, looking at whether they could fit into trust or partnership frameworks. The EU, through its blockchain initiatives, is aware of DAOs but likely to address them indirectly via existing legal structures or through upcoming cryptoasset regulations (MiCA, etc., which focus more on tokens than governance structures). It's possible the EU may eventually harmonize certain aspects (for example, recognizing a DAO organized in one country under some legal form EU-wide).

Outcome so far: Wyoming's experiment is ongoing. By early 2024, only a handful of DAOs had registered as LLCs – it's a niche but growing area. The legal battles (like CryptoFed vs SEC) will determine how attractive it is for others to follow. But even if few formally register, the existence of legally recognized DAOs is symbolic: it shows a government can *adapt its monopoly on granting corporate status* to accommodate blockchain-based governance. It's a case of government not being replaced but adjusting – handing some control to code and communities, while still providing a wrapper of legal legitimacy. For individuals in the crypto world, it's encouraging: they see a path to connect decentralized projects with real-world commerce (like owning real estate, hiring employees, etc., via a DAO LLC).

E. Supply Chain Traceability – IBM/Maersk's TradeLens

Global trade involves many actors – manufacturers, shipping lines, ports, customs, importers – and the **exchange of documents and data** among them. It's notoriously paper-heavy and fragmented, leading to delays, fraud, and opacity. TradeLens, launched by IBM and Maersk in 2018, was a flagship example of using blockchain to tackle this by providing a **shared platform for supply chain data**. The idea was to get all parties onto one **distributed ledger** where shipping events (like container departure, arrival, customs clearance, etc.) and key documents (bills of lading, packing lists, certificates) would be **uploaded and**

digitally signed, creating a single, tamper-proof history for each shipment [59] [60]. Maersk, one of the world's largest shipping carriers, contributed its data and network, and IBM provided the Hyperledger Fabric blockchain technology.

Achievements: TradeLens attracted significant participation – by 2021 it had **94+ organizations** integrated, including major ocean carriers (besides Maersk, they got MSC, CMA-CGM, etc.), port operators, and **Customs authorities in countries like the Netherlands, Saudi Arabia, Singapore, and Australia** [61] [62]. At one point, 20% of global container shipping volume was flowing through TradeLens in terms of data coverage [61]. The platform would capture over a million shipment events per day on the ledger [63] [61]. Customs agencies found it useful as they could get **real-time, trusted data** on incoming shipments well in advance – e.g. knowing what a container is supposed to contain, who packed it, and its journey, which helps target inspections. An IBM trade expert described it as implementing the "data pipeline" vision customs have long wanted [64] – continuous visibility from origin to destination. Blockchain's role was to ensure no single party (not even Maersk or IBM) could unilaterally alter records – all data was **shared via nodes and cryptographically chained**, so participants could trust that what they see is what others saw at the time [65] [66]. **Key features of TradeLens' blockchain** included: a *shared replicated ledger* (each participant runs a node, gets a copy of data relevant to them), *immutability* (once added, data can't be changed, only amended with corrections visible), *permissioning* (data partitioned so only those in a shipment's channel see it), and *selective endorsement* (only relevant parties validate a transaction, avoiding heavy consensus overhead) [67] [68]. These features leveraged Hyperledger Fabric's enterprise-oriented design and meant **TradeLens did not use energy-intensive proof-of-work** (unlike Bitcoin) [69]. Also, *smart contracts* in TradeLens automated workflows (e.g. when a ship arrives in port, a smart contract could trigger a notification to customs and port operators) [70].

In essence, TradeLens aimed to **complement and improve government and industry processes**. It didn't replace customs or port management – instead, it provided a *neutral data highway* where all parties could publish and retrieve the single version of truth for shipments. This potentially *constrained* unethical behavior: e.g. a corrupt actor couldn't slip in a fake manifest late, because every document's timestamp and origin were recorded; discrepancies would be evident to all. It also could reduce inefficiencies – in one oft-cited example, a simple shipment of avocados from Africa to Europe had to go through **30 organizations, 100+ people, and 200 communications** [71]; TradeLens promised to cut that by eliminating redundant re-entry of data and letting each stakeholder access the info as needed from the ledger [72] [73].

Challenges and Discontinuation: Despite technical viability, TradeLens encountered adoption hurdles. Shipping is a competitive industry with thin margins. Many companies (and even some governments) were hesitant to join a platform co-owned by *Maersk*, fearing a competitive disadvantage or data ownership issues. Competitors like CMA-CGM initially held out but later joined; however, by late 2022, Maersk announced that **TradeLens would be discontinued** [74]. They stated that *"the need for full global industry collaboration has not been achieved… TradeLens has not reached the level of commercial viability necessary to continue"* [75]. The platform was shut down in early 2023 [76]. This outcome underscores that in multi-stakeholder networks, **technology is only part of the equation** – governance, incentives, and trust among competitors are equally crucial. Maersk and IBM tried to position TradeLens as an "open, neutral platform" (even adjusting the governance model to assuage fears [77] [78]), but ultimately some major carriers invested in a different blockchain consortium (*Global Shipping Business Network, GSBN* led by Chinese carriers), and some governments may have pursued their own solutions.

For governments (customs), the shuttering of TradeLens was a disappointment because many had started integrating with it. However, the knowledge gained isn't lost – it demonstrated what a digitized trade workflow could look like. We might see new international efforts (perhaps through the World Customs Organization or WTO) building on a similar model, but with more neutral governance (e.g. not led by one carrier). In any case, **TradeLens proved the concept** that a *permissioned blockchain can handle global trade data at scale*, and that it can **improve transparency and reduce delays**. For example, the Customs authority of the Netherlands reported improved ability to validate manifests with TradeLens data, and the Saudi Customs did a pilot integrating TradeLens with their systems to get better visibility of incoming cargo.

Comparative angle: The UK and EU had ports involved in TradeLens (Rotterdam, Felixstowe etc.), and UK customs was reportedly exploring it. Post-Brexit, UK customs has big IT changes, and systems like TradeLens were considered for future models. The EU has its own initiatives for digitizing trade documents (the eFTI regulation – electronic Freight Transport Info – which could work with blockchain solutions). The US (CBP – Customs and Border Protection) also piloted TradeLens on select trade lanes. All these show **governments collaborating in consortia led by private sector** – a trend in blockchain for supply chains. Unlike currency or identity, where government might lead, here industry led and tried to bring government along. The failure of TradeLens doesn't mean blockchain isn't useful in supply chain, but it illustrates that **consortium governance** is tricky. In this case, maybe the balance of power wasn't acceptable to enough players.

The learnings likely will inform future platforms: perhaps an international body could host a TradeLens-like ledger where all carriers and customs are truly equal partners (a bit like how SWIFT is cooperative for banks). Or, smaller scale successes might occur in specific supply chains (there have been blockchain pilots in pharmaceuticals for tracking drugs to fight counterfeits, in diamonds tracing origin (Everledger), and in food safety – e.g. **IBM Food Trust** uses a similar Hyperledger system to trace grocery supply chains, and has seen adoption by Walmart and others to quickly pinpoint contamination sources [79] [80]).

In sum, **TradeLens** demonstrated both the **strengths and challenges of enterprise blockchain**. It showed that **auditability, shared ledgers, and smart contracts can greatly modernize inter-organizational processes**, aligning with government's need for better oversight (customs compliance) while benefiting industry with efficiency. Yet, it also taught that unless the **business ecosystem** is fully on board, even the best tech won't survive. The shutdown press release by Maersk emphasized *"full global industry collaboration… not achieved"* [75], highlighting a non-technical failure point. This suggests future efforts must perhaps involve more stakeholders in governance from the start to truly be neutral.

These case studies, spanning different functions and regions, reveal a spectrum of outcomes: some **successes (Georgia's land titles, EU's verifiable credentials pilots, the promise of CBDCs)**, some **ongoing experiments (Wyoming DAOs, UK land registry)**, and some **setbacks (TradeLens)**. Together they provide invaluable lessons for how blockchain can be harnessed by or against government roles.

Comparing Blockchain Technologies for Civic Applications

Different blockchain platforms and architectures vary greatly in their features and suitability for government-related use cases. Here we compare some prominent ones – **Ethereum, Hyperledger Fabric,**

Cosmos – and the general dichotomy of **permissionless vs permissioned** blockchains, in the context of civic or public-sector applications.

Ethereum (Public Permissionless): Ethereum is the largest open blockchain with full smart contract capabilities. As a **permissionless** network, anyone can participate in validating (via proof-of-stake) and anyone can deploy or use applications. Its strengths include a huge developer community, mature tools, and high security (the mainnet has never been compromised at the consensus level and now secures billions in value). For government uses, Ethereum's **auditability and transparency** are a double-edged sword – they provide public trust (anyone can independently verify the ledger's state), but also mean data is visible to all (which is a problem for sensitive information) and **usage costs ("gas" fees)** can be unpredictable. Ethereum is ideal when a use case **requires broad public engagement or neutrality**. For example, if a government wants to prove something to the public in a verifiable way (like publishing a hash of election results or a budget report so it's tamper-evident), using Ethereum or another public chain could be effective. We saw Georgia anchor to Bitcoin's chain; similarly a government could anchor to Ethereum for transparency. Ethereum can also host **decentralized applications (DApps)** relevant to civic life – e.g. decentralized voting systems, petition platforms, or public grant funding DAOs – that *anyone* can inspect. However, **scalability** and **governance** issues make Ethereum less favored for core government databases; it can currently handle ~15 transactions per second on-chain (though Layer 2 solutions greatly expand this), and transaction fees, while much lower post-upgrade, are not negligible. Also, governments cannot easily control or reverse anything on Ethereum if something goes wrong, since it's decentralized by design.

In practice, we see Ethereum being used more by the **private sector or NGOs in civic contexts** than by governments directly. For instance, some municipalities have issued community tokens or NFTs on Ethereum (like "MiamiCoin" was launched on Stacks (Bitcoin sidechain) for Miami, and other cities explored similar). The **European Investment Bank (EIB)** issued a €100m digital bond in 2021 that was registered on Ethereum's blockchain – essentially leveraging the public chain for trust in a financial instrument. This shows a government-related entity using Ethereum's transparency and global verification properties [47]. But most government projects choose permissioned variants for direct service provision.

Hyperledger Fabric (Permissioned Consortium): Hyperledger Fabric, an open-source framework from the Linux Foundation's Hyperledger project, is designed for **enterprise/private blockchains**. It forgoes the concept of cryptocurrency entirely and instead provides a modular platform where a set of known organizations can run a blockchain network with **pluggable consensus (like practical Byzantine fault tolerance algorithms or even simple ordering services)**. Fabric emphasizes **privacy and controlled sharing**: it has features like **channels** (subnets so that only relevant parties see certain transactions) and fine-grained access control. This makes it appealing for use cases like supply chain, records management, etc., where not all data should be public. We saw Fabric used in **TradeLens** and **IBM Food Trust**, and many government pilots. For example, Fabric was used in an **Illinois birth registration pilot** (each hospital and the state health department running nodes, sharing birth records). Also, the **Chinese BSN (Blockchain-based Service Network)** uses Fabric (and others) to offer permissioned chains to businesses and local governments in China for various apps. Fabric's **performance** can be tuned well (hundreds or thousands of TPS in closed environments), and because no mining is needed, it's energy efficient and low-latency (transactions finalize in seconds).

The downside of Hyperledger Fabric is that it is **more centralized by nature** – you must trust the consortium members to some extent. It's not open to public participation, so it sacrifices the censorship-resistance of a public chain. For governments, this is often acceptable or even desired: they *want* control

over who sees or validates data (for legal compliance). Fabric also requires more heavy lifting in setup – there's no existing global network, you have to create a network from scratch for your use case, which involves coordination among participants (and as we saw, that's as much a social challenge as a technical one). In summary, **Fabric is suitable when multiple known stakeholders need to share a ledger for a public service or inter-agency process**, and where **privacy, speed, and customizability** are more important than open decentralization. Use cases: interbank clearing (some central bank experiments used Fabric), supply chains (TradeLens, Food Trust), digital identity consortia (Fabric was used in some national ID pilots), and more. Indeed, as one source notes, **governments are adopting Hyperledger to enhance transparency while maintaining control**, e.g. for sharing public records among agencies securely [81]. Fabric's **smart contract (chaincode)** can be written in general languages like Java, Go, etc., making it flexible for enterprise developers [82].

Cosmos (Interoperable Sovereign Chains): Cosmos is a different beast – more of an **ecosystem or framework than a single blockchain**. It enables the creation of application-specific blockchains (called "zones") that can interconnect via the Inter-Blockchain Communication (IBC) protocol. Each zone has its own validators and rules (it could be permissionless or permissioned, PoS or other consensus, etc.), but thanks to a standard protocol, they can transfer data or tokens to each other through **Cosmos hubs**. The Cosmos SDK has been popular for projects that want more control than just writing smart contracts on someone else's chain; for instance, the **Binance Chain** (for Binance's decentralized exchange) was built on Cosmos tech, as are others like Crypto.org chain, Terra (before its collapse), and **Secret Network** (a privacy-focused chain).

For government applications, Cosmos offers an intriguing middle path: a government (or consortium) can easily spin up its own blockchain, customize it to its needs (governance, token, privacy settings), but still have the ability to **connect with other blockchains** securely if desired. This could be valuable for, say, cross-border interoperability of government blockchains (imagine each country has its own chain for certain records but they can share select data via IBC). Also, Cosmos uses **Tendermint BFT consensus**, which provides fast finality (transactions finalize in a couple seconds) and high throughput, which could meet many public sector demands. It's inherently **modular and sovereign**: each chain's governance is independent, which might appeal to government entities who want full control over their infrastructure (unlike being just one of many dApps on Ethereum). At the same time, it's less battle-tested in hostile open environments than Ethereum.

One example of Cosmos tech in a civic context might be the **European Blockchain Services Infrastructure (EBSI)** itself – EBSI is reportedly using a variant of **Hyperledger Besu and/or Tendermint** for its network (they evaluated various, not sure final pick). Tendermint (Cosmos core) being considered indicates interest in those features. Another example: some cities or regions could launch local Cosmos-based networks for community coins or digital vouchers, which can connect to the wider crypto economy via Cosmos hubs if needed. As of now, we haven't seen a government-run Cosmos chain publicized, but some **public permissioned chains use Tendermint** (e.g. the **CBDC of Thailand** used a Tendermint-based system in Project Inthanon, and **France's CBDC pilot** with Tezos uses a variant of Tendermint). Cosmos's emphasis on **interoperability** aligns with government needs to avoid vendor lock-in – they don't want to be stuck in one platform silo in the future.

Permissioned vs Permissionless – Summary of Trade-offs: The choice often boils down to this fundamental decision.

- *Permissionless (e.g. Ethereum mainnet, Bitcoin, etc.):* These offer **maximal transparency, security through decentralization, and neutrality**. They are good when the goal is public verifiability and inclusion of broad participants (e.g. global communities, or public accountability). However, they have drawbacks of **uncertain governance** (protocol updates decided by open communities, not by government mandate), potential performance issues, and **regulatory challenges** (data on a public chain might conflict with privacy laws like GDPR if not handled properly, for instance). Governments are generally cautious to rely on a permissionless network for core services because they can't control it. But they may use it for anchoring data (for integrity proofs) or for interacting with an existing user base (if many citizens already use a public chain, a service might be deployed there to reach them). One allowed use is **publishing open data to a blockchain to ensure it's not altered**, which some municipalities have done (to increase trust in government data).

- *Permissioned (e.g. Hyperledger, Corda, private Ethereum networks):* These give governments and their partners **full control over participants and protocol rules**. They can ensure compliance (only vetted nodes see data, etc.), and can more easily meet throughput demands by using simpler consensus methods since trust is federated. They integrate better with existing IT and legal processes (you can know who to hold accountable if something goes wrong). The trade-off is **reduced decentralization** – effectively, a permissioned chain is more like a distributed database with cryptographic auditability. It may not garner the same level of trust from an external observer as a public chain ("the government and its friends operate it; can we fully trust them?" one might ask). However, a counterpoint is that even a permissioned blockchain can increase trust **relative to one agency's silo**, because multiple independent parties (maybe different government departments or external auditors) hold copies and must concur, which reduces unilateral tampering risk [13].

For many civic applications, a **hybrid approach** is emerging: use permissioned blockchains for operational needs, but anchor or periodically checkpoint data to a public chain for accountability. This way, you get the best of both – efficiency and privacy for day-to-day, and an immutable public audit trail for oversight. We saw this model in Georgia's land registry (private chain + Bitcoin anchoring) [8], and others are adopting it.

Platform Specifics: A quick comparative note on **R3 Corda** (though not explicitly asked, it's relevant): Corda is another permissioned DLT popular in finance, which the UK Land Registry pilot used [37]. It's tailored to bilaterally shared states (not all nodes see everything, only those in a transaction), aligning with privacy needs of banks or government units. Corda and Hyperledger Fabric often compete in enterprise settings; both forgo mining and have strong permissioning. The **Cosmos vs Polkadot** debate in blockchain interoperability is also notable – Polkadot provides a more structured shared security model (all para-chains rely on a central relay chain), whereas Cosmos is looser (each zone independent). Polkadot has seen some government-related trials too (e.g. in energy grids). The choice depends on whether a government wants a ready-made ecosystem (then build on Ethereum or Polkadot) or more freedom (Cosmos or custom Fabric network).

In conclusion, **Ethereum, Hyperledger, Cosmos** represent three archetypes – public general-purpose, private consortium, and customizable interoperable. In civic contexts:

- Ethereum (and similar public chains like Tezos, Algorand, etc.) might be best for **citizen-facing transparency projects** or where **international interoperability and public trust** are paramount and data can be public (or shielded via cryptography but on a public ledger). For instance, an international aid organization might use Ethereum to distribute relief funds via stablecoins to ensure every transaction is auditable by donors [47] .

- Hyperledger Fabric (and Corda, etc.) shine in **inter-agency or public-private networks** where participants are known and the priority is to streamline processes and cut out paper, but not to expose data to the world. Government adoption so far has largely been here – e.g. **blockchain for tax records sharing among departments**, or a **consortium of hospitals and a health regulator sharing credentials of doctors**.

- Cosmos (and similar like **Hyperledger Besu** for permissioned Ethereum, or frameworks like **Quorum**, **Avalanche subnets**, etc.) are attractive to build **bespoke solutions** that still connect to wider ecosystems. For example, a **national bank might launch a Cosmos-SDK chain for its CBDC** so it can finely tune it, but allow that chain to connect to other national chains for cross-border payments via hubs, rather than each using separate siloed tech.

Finally, when evaluating suitability, one must consider **governance of the platform itself**. Ethereum is governed by a global community (with vitalik & co but also miners/validators, etc.), Hyperledger is maintained by a foundation and you run your own network governance, Cosmos is open-source with many contributors and each chain governed by its operators. Governments may prefer technologies with strong support and known governance: Ethereum and Hyperledger both are backed by large communities and organizations (Ethereum Foundation, Linux Foundation) so they feel “safer” in terms of longevity and support than perhaps a very new platform.

To encapsulate:

- **Ethereum (public)** – Great for *transparency and broad trust*, but **ensure privacy layers if needed**. Not directly controlled by gov, so use for public audit trails or citizen engagement tools; careful with volatile costs and regulatory uncertainties of public chain use.

- **Hyperledger Fabric (permissioned)** – Great for *controlled networks and privacy*, **enterprise-grade**, but relies on consortium trust. Use for back-office optimization, secure data sharing among known entities, etc. Many government pilots show it works well (high throughput, etc.), but success needs strong consortium governance (clear rules among participants).

- **Cosmos (interoperability & custom chains)** – Great for *flexibility and scalability*, **sovereignty of infrastructure** (each chain = full control), and future-proofing with inter-chain communication. Use if you foresee multiple blockchains that need to talk, or if you want to avoid being locked into one network. Requires more technical expertise to launch and maintain your own chain though.

Ultimately, the “best” technology depends on the specific civic application requirements: **privacy vs transparency, scale, legal constraints, and ecosystem maturity**. Often the decision is to start with a

permissioned/private setup (to get stakeholders comfortable and comply with law), and leave an option to migrate or connect to public networks as the technology and regulations evolve. Many projects even use **dual deployment**: e.g. run Hyperledger Fabric for main operations but periodically publish a hash to Ethereum (for public accountability). That hybrid strategy is becoming common as a way to leverage strengths of both worlds.

Conclusion: Toward a Realistic Synthesis of Blockchain and Government

Blockchain technologies have catalyzed a re-examination of how we establish trust in societal functions typically overseen by governments. Through theoretical analysis and practical pilots, we find that **blockchain can indeed reinforce and sometimes redefine core government functions** – but often not in the absolutist "replace the state" manner some early enthusiasts envisioned. Instead, the emerging picture is nuanced:

- **Notarization and Record-Keeping:** Blockchain is highly effective at **securing records against tampering** and providing multi-party transparency. It can **complement state registries** to make them more resilient (as seen in land, identity, and certificate use cases) and in specific niches even *replace* traditional notaries (e.g. using a blockchain timestamp instead of a notarized paper). Yet, the state's role in **enforcing and contextualizing those records remains vital**. The realistic near-term impact is that states which adopt blockchain for registries will likely see **greater efficiency, cost savings, and public trust** in those services [4] [30]. States that don't might face external blockchain alternatives (like people using Bitcoin for property-like claims or organizations like Wikipedia leveraging blockchain for archival) that could challenge their notary monopoly indirectly.

- **Collective Decision-Making:** In areas like voting and governance, blockchain introduces powerful tools for **auditability and direct participation**. However, due to security and social challenges, it's more a **constraint and supplement** on government processes than a wholesale replacement. It pushes governments to improve transparency (knowing that citizens now expect verifiable integrity – e.g. "publish the hashes of vote tallies so we can independently check"). It also provides a sandbox for new governance models (DAOs) that, if successful, might influence how local or even national governance could evolve (for instance, more liquid democracy or participatory budgeting via blockchain voting, once tech matures). In the medium term, we anticipate **incremental adoption**: blockchain-based voting for specific groups (overseas military, shareholder votes, party primaries) will grow as security improves, and **smart contracts might automate certain government decisions** (especially in resource allocations, like automatic disbursements when conditions are met). But broad elections and legislatures will likely only cautiously integrate blockchain (perhaps using it for **result verification** or e-petitions) until/unless solutions to known risks are proven.

- **Allocation of Privileges (Money & Licenses):** This is where blockchain has both the **most direct challenge and the most collaborative response**. Cryptocurrencies opened Pandora's box on who controls money. Governments are responding not by banning the tech (in most cases) but by co-opting it – developing CBDCs and tightening oversight on crypto. We foresee a **coexistence** of sovereign digital currencies and private crypto, with each influencing the other. In stable economies, CBDCs may strengthen the state's hand (enhanced monetary policy tools, more transparent fiscal transfers). In unstable regimes, people may continue turning to Bitcoin or stablecoins as a constraint

on bad policies (hyperinflation, capital freeze). The **monetary monopoly** of states is unlikely to be usurped globally by Bitcoin – but it is already **constrained by it**, evidenced by how seriously central banks take the CBDC race and crypto regulation [24]. In licenses/quotas, blockchain will likely *supplement* processes (with tokenized permits, auctions on-chain for transparency, etc.). For example, we might see a major country's **spectrum auction run on a blockchain system** within the next decade to ensure fairness and maybe even enable secondary markets for spectrum via tokens – a complement that makes the allocation more efficient, while the state still sets rules and adjudicates disputes.

- **Platform Choices:** Governments (US, EU, UK alike) are converging on an understanding that **different use cases demand different blockchain designs**. They'll use **permissioned networks for internal and interagency work** (often leveraging standards from Hyperledger or enterprise Ethereum variants), and consider **public or hybrid networks when citizen trust and engagement are key**. The comparative analysis suggests governments will not "pick one chain to rule them all," but rather adopt a **portfolio approach** – much like they use a variety of databases and IT systems today, they'll use a variety of blockchain networks, possibly bridged. Interoperability frameworks (like Cosmos's IBC, or initiatives to standardize digital identity and asset formats) will be critical so that this patchwork still results in a coherent user experience for citizens across services.

- **Global Collaboration and Competition:** The case studies show a healthy exchange of lessons across borders. The **EU leads in regulatory-framework-backed adoption** (digital identity, possibly digital euro). The **US leads in private sector innovation** (many blockchain startups and protocols) but lags in federal adoption (though some states lead, like Wyoming). The **UK is positioning itself as a pragmatist** – endorsing innovation (e.g. Law Commission on DAOs, fintech sandbox) while being careful on systemic changes. This suggests that **no one country will dominate all aspects**; rather, each will contribute where its strengths lie. International standards bodies (ISO, W3C for credentials, etc.) and consortia will play a big role in ensuring these national or regional solutions can work together. For instance, if the EU's blockchain for diplomas and the U.S.'s eventual approach for digital credentials (should they adopt one) use compatible standards, that would be a win for citizens globally.

- **Constraints and the State's Future Role:** Importantly, even as blockchain can constrain certain state powers (by distributing trust or enabling alternatives), it can also **strengthen the state's capacity** in positive ways – to deliver services more transparently and efficiently. We are likely heading toward a model of the **"augmented state"** – where government leverages decentralizing technologies to augment its services, and citizens enjoy greater **trust without needing to trust** (i.e. they trust the system because it's verifiable [13], not just because the government says "trust us"). The state's monopoly on force and legitimacy is not directly under threat by blockchain (one still needs courts and police, which blockchain doesn't replace), but its monopoly on **trust mediation** *is* eroding. In areas from identity to currency, people have new options to achieve trust (through math and consensus algorithms) rather than through an institution. This is pushing governments to **adopt a more collaborative and transparent posture** – joining networks rather than only commanding them. States that embrace this (like Estonia, or Wyoming at the state level) could boost their digital economies and citizen satisfaction. Those that resist might find shadow systems developing anyway (like parallel crypto economies or unofficial record-keeping via blockchain that bypasses state systems).

Prescriptive Outlook: Governments should approach blockchain neither as panacea nor as threat, but as a **tool in the governance toolbox** – one that is particularly well-suited to problems of **inter-organizational coordination, auditability, and credibility of data**. A realistic path is to start with pilot projects (as many have), share results (to not reinvent wheels), and gradually scale successful pilots into production. Law and regulation need updating alongside: clarifying the legal status of blockchain records, enabling digital signatures, providing oversight for when algorithms make decisions, and protecting citizens (e.g. if a smart contract has a bug, who is liable?).

The comparative lessons suggest a few recommendations:

- **Use blockchain where it adds clear value (transparency, integrity, automation), not just for buzz.** The EU's principle of *"Blockchain where it makes sense, otherwise don't"* [13] is wise. For example, a single-agency database might not need a blockchain, but a cross-border or multi-stakeholder process might benefit greatly.

- **Invest in identity and credential infrastructure now.** This is low-hanging fruit where blockchain can reduce paperwork and fraud (diplomas, licenses, etc.) and pave the way for bigger things. The EU is doing this with EBSI; others should follow or collaborate so that, for instance, a COVID vaccination certificate or a professional license can be universally verified without central silos.

- **Collaborate on governance frameworks for consortia.** TradeLens's fate shows that governance is make-or-break. Governments, as neutral arbiters, could convene industry to create more inclusive governance for shared blockchain platforms (maybe a public-private utility model). If Maersk-led didn't work, perhaps a port authority-led or UN-led trade blockchain might gain trust.

- **Anticipate and legislate for DAOs and crypto assets.** Wyoming's head start might attract talent and capital; other jurisdictions may want to create their own legal pathways for decentralized structures to operate responsibly. The UK and EU should consider how to integrate DAO-like entities into their legal systems, to harness innovation while mitigating risks (e.g. ensure DAOs can be accountable for real-world obligations). Regulatory clarity in things like defining tokens (utility vs security) and tax treatment is also essential to let beneficial projects flourish and bad actors be addressed.

- **Focus on interoperability and open standards.** Each government chain or system should adhere to common standards (for data formats, communication protocols) so that down the line they can connect. Siloed blockchains would be a shameful repeat of siloed databases. Initiatives like the **Blockchain Services Infrastructure in the EU, the Baseline Protocol (for integrating Ethereum with enterprise systems), and global forums (OECD, ISO TC307)** should be actively supported by governments to harmonize efforts.

- **Maintain a human-centric and rights-centric approach.** As governments implement these technologies, they must uphold privacy (GDPR and similar should guide designs), equity (ensuring digital divide issues are addressed so that blockchain solutions don't exclude those without tech access), and recourse (if a smart contract denies a benefit wrongly, a human appeals process must exist). Blockchain can increase transparency **for citizens** into government, but governments should also be transparent about their use of blockchain. Open-source implementations and independent audits can build trust that the government's blockchain systems do what they claim.

In conclusion, blockchain will not render governments obsolete – but it **will change how they operate** and how trust is distributed. Much like the internet forced governments to become more transparent and citizen-centric, the rise of blockchain is forcing governments to become more **platform-like and collaborative**. Those that adapt could see improved governance outcomes: less corruption (since records are immutable [11]), faster service delivery [4], and greater civic engagement (if citizens can directly hold and verify information). Those that don't might see a gradual outsourcing of trust to private or decentralized networks, potentially losing grip on certain functions. The evidence so far points to a middle ground: **blockchains and governments will co-evolve**, each influencing the other. In the near- to medium-term, expect to see blockchain **credibly substituting specific government record-keeping and transactional processes**, while in other areas acting as a **complementary layer of assurance** above government processes, and in yet others as a **constraint that keeps governments honest** in the face of external alternatives.

The path forward is not about *state vs technology*, but about **using technology to build a better state** – one that is more **open, accountable, and effective**. Blockchain can be a powerful ally in that mission if applied with careful consideration of its strengths and limits. The comparative experiences in the US, EU, and UK demonstrate both enthusiasm and caution, innovation and regulation. By learning from each other and from trial and error, governments can harness the "trust machine" that is blockchain to strengthen the social contract, rather than disrupt it. The endgame is a world where **citizens trust the system because they can verify it** – and that could align perfectly with the fundamental purpose of government: to serve the public with integrity.

Sources:

- Land registry pilots and outcomes – Sweden and Georgia [2] [3] [4] [30] [8] [9]
- EU EBSI and verifiable credentials design [13] [83]
- Reuters on global CBDC progress (EU digital euro, US wholesale focus, etc.) [26] [28] [27] [24]
- Wyoming DAO law and first DAO LLC [56]
- TradeLens case (vision and shutdown) [61] [75]
- Hyperledger vs Ethereum differences [84] [85]
- Medium on permissioned blockchains for government uses [86]
- Jamie Smith quote on blockchain as global notary [1]
- West Virginia blockchain voting pilot and expert skepticism [16] [23]
- Bitfury/Georgia land title project details [8] [11]

---

1 9 10 31 34 35 36 News | Bitfury
https://bitfury.com/news/page:8

2 3 4 5 6 30 Sweden trials blockchain for land registry management | Computer Weekly
https://www.computerweekly.com/news/450421958/Sweden-trials-blockchain-for-land-registry-management

7 8 11 12 45 Bitfury, Republic of Georgia Push Ahead With Blockchain Land-Titling Project | Nasdaq
https://www.nasdaq.com/articles/bitfury-republic-of-georgia-push-ahead-with-blockchain-land-titling-project-2017-02-08

13 83 5 reasons why professionals and enthusiasts of Self-Sovereign Information Sharing should look into EBSI this summer - EBSI -
https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/5+reasons+why+professionals+and+enthusiasts+of+Self-Sovereign+Information+Sharing+should+look+into+EBSI+this+summer

14 15 16 17 18 19 20 21 23 West Virginia Becomes First State to Test Mobile Voting by Blockchain in a Federal Election
https://www.govtech.com/biz/west-virginia-becomes-first-state-to-test-mobile-voting-by-blockchain-in-a-federal-election.html

22 West Virginia and Denver say mobile voting pilots increased turnout
https://statescoop.com/west-virginia-denver-mobile-voting-app-voatz-increased-turnout/

24 25 26 27 28 29 49 50 51 53 Study shows 130 countries exploring central bank digital currencies | Reuters
https://www.reuters.com/markets/currencies/study-shows-130-countries-exploring-central-bank-digital-currencies-2023-06-28/

32 33 Governments may be big backers of the blockchain
https://www.economist.com/business/2017/06/01/governments-may-be-big-backers-of-the-blockchain

37 38 39 40 42 43 44 HM Land Registry to explore the benefits of blockchain - GOV.UK
https://www.gov.uk/government/news/hm-land-registry-to-explore-the-benefits-of-blockchain

41 Digging Beneath The Surface Of Blockchain Property Transactions ...
https://todaysconveyancer.co.uk/digging-beneath-surface-blockchain-property-transactions/

46 A ticking clock on central bank digital currencies - Visa
https://corporate.visa.com/en/sites/visa-perspectives/trends-insights/the-clocks-ticking-on-central-bank-digital-currencies.html

47 48 52 Central Bank Digital Currency Tracker - Atlantic Council
https://www.atlanticcouncil.org/cbdctracker/

54 Wyoming Passes DAO Supplement Recognizing Decentralized ...
https://uk.practicallaw.thomsonreuters.com/w-032-5565?transitionType=Default&contextData=(sc.Default)

55 Are DAOs Legal? Exploring DAO Legal Issues and Regulatory ...
https://www.midao.org/blog-posts/are-daos-legal-exploring-dao-legal-issues-and-regulatory-challenges

56 57 58 DAOs vs Nation States: A Wyoming DAO’s Experiment with the U.S. Securities and Exchange Commission | Oxford Law Blogs
https://blogs.law.ox.ac.uk/oblb/blog-post/2024/03/daos-vs-nation-states-wyoming-daos-experiment-us-securities-and-exchange

59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 TradeLens uses blockchain to help Customs authorities facilitate trade and increase compliance – WCO
https://mag.wcoomd.org/magazine/wco-news-87/tradelens/

74 75 76 A.P. Moller - Maersk and IBM to discontinue TradeLens, a blockchain-enabled global trade platform | Maersk
https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens

77 78 94 Companies Join IBM and Maersk's Blockchain Supply Chain
https://www.coindesk.com/markets/2018/08/09/94-companies-join-ibm-and-maersks-blockchain-supply-chain

79 80 86 Permissioned vs. Permissionless Blockchains | by web3author | Medium
https://medium.com/@web3author/breaking-down-the-battle-of-blockchains-permissioned-vs-permissionless-416f9ff85177

81 Hyperledger Architecture: Build Blockchain Networks - Webisoft
https://webisoft.com/articles/hyperledger-architecture/

82 84 85 Hyperledger vs Ethereum in Blockchain - GeeksforGeeks
https://www.geeksforgeeks.org/blockchain-hyperledger-vs-ethereum/