ChatGPT

Blockchain and the New Civic Contract in a Post-Labor Economy

Introduction

The advance of artificial intelligence and robotics is rapidly approaching a point where **human labor may become economically obsolete**. In such a scenario, the traditional system of labor rights – which for over a century has been a cornerstone of civic power for the working majority – faces an existential challenge. If machines and algorithms produce all goods and services, **how will society balance power and distribute wealth when people are no longer needed as workers?** This report explores that question through a comprehensive lens, examining historical theories of power, the looming disruption of a post-labor society, and whether **blockchain and related cryptographic technologies could form the basis of a new "laborless" social contract**.

We begin by reviewing the history and **systems-theoretical underpinnings of labor rights as a pillar of civic equilibrium**, highlighting how collective bargaining and labor power have traditionally kept wealth concentration and elite dominance in check. We then analyze the destabilizing effects of **losing labor as a bargaining tool** – how the erosion of labor's leverage could lead to extreme inequality and "elite capture" of institutions.

Against this backdrop, the report investigates emerging **blockchain-based mechanisms for public agency** that might compensate for the loss of labor power. These include **radical transparency**, **decentralized participatory governance** (via DAOs and on-chain voting), **data sovereignty** through self-sovereign identity, and **unstoppable code-based enforcement of rules** via smart contracts. We present case studies of these concepts in practice – from Ethereum's decentralized infrastructure and Gitcoin's quadratic funding of public goods, to Worldcoin's proof-of-personhood initiative and Sovrin's self-sovereign identity network – illustrating how each addresses aspects of civic life once buttressed by labor.

Crucially, we evaluate the **limitations, risks, and technical barriers** that come with relying on blockchain systems in lieu of labor rights. Issues like governance token inequality, security vulnerabilities, regulatory uncertainty, privacy trade-offs, and the digital divide could all undermine a blockchain-based civic paradigm if left unaddressed.

Finally, the report offers **normative proposals and frameworks for a blockchain-based civic contract**. We discuss heuristics like quadratic voting, **universal basic income (UBI)** distributions via smart contracts, decentralized "ownership" of productive AI via tokens, and policy ideas for integrating blockchain governance into public institutions. Throughout, the tone remains academic and policy-oriented, acknowledging that **technology alone is no panacea** – but if designed with care, it can be a powerful tool to **restore social equilibrium and democratic agency in a world beyond labor**.

Power, Labor, and the Historical Role of Labor Rights

Labor rights have long been a core pillar of power balance in modern societies. From a historical perspective, the ability of workers to organize and bargain collectively – through unions, strikes, and political movements – became a primary means by which the broad majority could exercise power over economic and civic life. In the late 19th and 20th centuries, labor movements fought for rights like the eight-hour workday, safe working conditions, fair wages, and social safety nets. These struggles were not just about workplace conditions, but fundamentally about **shaping a more equitable distribution of power and wealth in society**. As political economist Adam Dean and colleagues note, the decline of labor unions since the 1970s in the U.S. was "a major cause" of stagnating wages and rising inequality – evidence that when labor's power erodes, economic disparities widen. Conversely, where labor was strong, societies saw **lower inequality, higher wages, and more robust democracies**. In short, labor rights historically served as a **check-and-balance against the concentration of wealth and authority**.

From a **systems theory** perspective, one can view the economy and polity as an interconnected system of forces and feedback loops. Labor's bargaining power functioned as a *negative feedback mechanism* that kept the system stable. If corporate profits grew too large at the expense of wages, strong labor unions would push back – negotiating higher pay or benefits – thus redistributing resources and preventing runaway inequality. This feedback loop helped maintain what we might call **civic equilibrium**, preventing the societal "engine" from overheating due to extreme concentration of power. In political scientist Karl Polanyi's terms, the labor movement was part of society's "double movement" to re-embed the market in social constraints, countering the excesses of unfettered capitalism. **Game theory** also illuminates labor's role: In the classic employer-employee "game," an individual worker is at a disadvantage (easy to replace), but by forming coalitions (unions) and threatening collective action (strikes), workers changed the payoffs. They introduced credible commitments to withdraw labor, which forced employers to share more gains or face costly shutdowns. In effect, **collective bargaining solved a coordination problem among workers** (preventing the race-to-the-bottom of individuals competing for jobs) and created a more balanced power dynamic – a kind of negotiated equilibrium in the game of production.

Labor rights thus became enshrined not only in laws (like minimum wage, the right to organize, and labor standards) but also in the **governance design of many democracies and corporations**. For instance, some countries implemented co-determination laws requiring worker representation on company boards, integrating labor's voice into governance. Unions also became major political actors, mobilizing voter turnout and advocating policies for the working class. This had broad civic impacts: union density correlates with higher voter participation and pro-democratic policies. It is telling that labor leaders often frame their role as **defending democracy itself**. A Harvard Law School project on labor and democracy observes that labor organizations have been critical in legitimizing and defending democratic governance. In sum, **labor rights have functioned as a cornerstone of the social contract**, ensuring that the majority who depend on selling their labor had a say in how society is run, both economically and politically.

However, these historical achievements were predicated on the assumption that human labor was essential for production – giving workers **leverage**. That leverage underpinned what one might term the "labor bargain": workers contribute to economic output, and in return claim a fair share of the gains and a voice in decisions. The next section explores what happens when that assumption no longer holds – when human labor is no longer needed or valued in the production process.

The End of Labor Leverage: AI, Automation and Elite Capture

Accelerating advances in automation raise the prospect that we are entering a **post-labor society** in which human workers can be largely replaced by machines and algorithms. In such a scenario, labor's traditional leverage evaporates: if capital owners (the "elite") no longer *need* human labor to create wealth, the bargaining power of workers approaches zero. The implications for civic equilibrium are dire. As historian Yuval Noah Harari warns, we may see the emergence of a "**useless class**" – billions of people pushed out of employment by AI, essentially "useless" from the perspective of the economy. Harari ranks this **rise of the useless class** as one of the 21st century's greatest threats. It's not simply an economic problem of unemployment, but a **political problem of disenfranchisement**: historically, even elites had to pay heed to the masses because they depended on their labor or at least their consumer demand. But in a future where AI and robots generate abundance, **elites could perceive the non-working masses as largely irrelevant** – or worse, a nuisance.

Indeed, thinkers are actively speculating about futures where labor's disappearance leads to radically different social outcomes. Sociologist Peter Frase's **"Four Futures"** scenario exercise is instructive. In a best-case scenario of "Communism" (post-scarcity *and* equality), advanced automation makes human labor obsolete and abundance is shared broadly, resulting in a classless society of equals. However, Frase notes this outcome would require not just technology but a **"radical shift in human values and governance structures"** to ensure egalitarian distribution. A more dystopian scenario is "Rentism": here technology abolishes the need for labor but **wealth remains concentrated** in the hands of those who own the robots, AI, and intellectual property rights. In Frase's Rentism, "the privileged few who control intellectual property secure perpetual income without significant contributions to productive labor, exacerbating societal divisions". This is a portrait of **extreme elite capture**: a small minority monopolizes the productive assets (intelligent machines, patents, data) and, since they don't need workers, can extract wealth without sharing or accountability. It fundamentally "alters our understanding of work and value," potentially stifling innovation and mobility due to monopoly control of knowledge. Crucially, it **breaks the post-war social contract** where productivity gains were shared (however imperfectly) with labor – instead, all gains flow to the owners of capital.

In such a world, the traditional channels through which the majority exert influence – striking for higher wages, or leveraging labor scarcity – simply vanish. **Civic equilibrium could quickly degrade into oligarchy or worse**. Some analysts even contemplate a scenario Frase terms "Exterminism," where scarcity and inequality persist together: a rich elite, freed from reliance on labor, might fortify themselves and oppress or even eliminate surplus populations to secure resources. While extreme, this scenario underscores the risk of violent **de-coupling of elites from the masses**. When asked what holds elites back from simply ignoring or abusing the majority, historically the answer was: they needed the masses (as workers, soldiers, consumers). Remove that need, and the **incentive for elite restraint diminishes**. We already see early warning signs – as labor union influence wanes, wealth inequality has skyrocketed and political power tilts toward the wealthy. A recent Economic Policy Institute report points out that the decline of unions since the late 20th century directly contributed not only to wage stagnation but also to a more *vulnerable democracy* in the U.S.. Without organized labor countering corporate political influence, policies favoring the wealthy multiply, and voter suppression efforts face weaker opposition.

Thus, **the loss of labor as a bargaining tool threatens a self-reinforcing cycle of elite capture**. The rich few, owning the AI and robot-driven means of production, accumulate even more wealth, which they can use to influence politics and entrench their position – further excluding the many from wealth or voice.

Traditional redistributive tools (progressive taxation, welfare programs) rely on political power that historically depended on labor-backed mass movements. If those movements lose their leverage, can progressive policies be sustained? This feedback loop of **power begetting more power for the elite**, and conversely disempowerment begetting more disempowerment for the masses, is the fundamental challenge of a post-labor world.

Yet, even as this dark horizon comes into view, **new forms of technology offer a potential counterweight**. The very advances that render labor obsolete – global networks, automation, cryptography – also enable new modes of organization. The key question is whether **blockchain and similar technologies can substitute for labor's role in the social contract**. In other words, can we engineer alternative mechanisms of *public agency, economic solidarity, and accountability* that don't depend on one's value as a worker? The next sections delve into this possibility, starting with the specific capabilities of blockchains and cryptographic systems that might empower individuals and communities in novel ways.

New Mechanisms for Public Agency: What Blockchain Technology Enables

Blockchain technology, alongside related cryptographic tools (such as distributed ledgers, smart contracts, decentralized identifiers, and zero-knowledge proofs), offers **a toolkit for reimagining civic empowerment and governance** in a post-labor context. These tools fundamentally change how trust, value, and organization can be managed at scale – *potentially* allowing society to replace some functions that labor-based institutions used to serve. We focus on four key capabilities of blockchain systems that could underpin a new civic architecture:

- **Radical Transparency** – Open, tamper-proof ledgers that make economic and political processes visible and auditable to all.
- **Participatory Decentralized Governance** – Decision-making systems (like DAOs) that enable broad, direct stakeholder participation without centralized gatekeepers.
- **Data Sovereignty and Decentralized Identity** – Frameworks (like self-sovereign identity) that return control of personal data and identity to individuals rather than corporate or state authorities.
- **Unstoppable Protocol Enforcement** – Smart contracts and decentralized networks that *automatically enforce rules* and agreements, reducing reliance on centralized authorities for upholding rights.

Each of these mechanisms addresses dimensions of civic life traditionally buttressed by labor power (such as accountability of elites, representation of the majority's interests, control over one's economic identity, and enforcement of fair play). Below, we examine each capability in turn, noting how it works and why it matters for a society where human labor can no longer be the leverage it once was.

Radical Transparency and Accountability

Blockchain's most immediate contribution is radical transparency: the ability to have a **public, immutable ledger** of transactions, decisions, or other records that anyone can inspect. Unlike conventional institutional record-keeping (which might be siloed, opaque, or alterable behind closed doors), a blockchain by design **openly exposes the flow of information and value**. Perianne Boring, of the Chamber of Digital Commerce, explains: *"We are talking about radical transparency. Anyone can look into the blockchain and look into every transaction that ever happened… and you can use it for any type of provable fact."*. In practice, this

means that **important civic data could be made** permanently auditable **by the public** – budgets, election results, supply chain records, legislative changes, and more. For instance, a city government could record its procurement contracts or spending on a blockchain; citizens and oversight bodies would then have real-time access to tamper-proof records of how public funds are used.

This level of transparency can compensate for the absence of labor unions and mass political pressure in holding powerful actors accountable. In the past, unions or whistleblowers within a workforce might call out corporate malfeasance or government corruption. In a future with fewer workers, we will rely more on **data visibility** to spot and check abuses. **Blockchain ledgers provide a "perfect audit trail" by design**. Every expenditure, every vote, every transfer of assets can be traced. **Corrupt intermediaries and hidden backroom deals become harder to hide** when "all transactions are visible to every participating node in real-time". For example, one proposal has been to record **land titles and financial records on blockchain** to prevent officials from altering records for personal gain. Similarly, blockchain-based voting systems can enable public verification of vote counts, mitigating fraud (as discussed further below).

It's worth noting that transparency is a double-edged sword – absolute openness can conflict with privacy (a point we'll revisit in limitations). However, the advent of techniques like zero-knowledge proofs can allow **verification without full disclosure** (e.g. proving a transaction or credential is valid without revealing all details). Some jurisdictions and organizations are already pushing for blockchain-enabled transparency in governance. For example, the city of **London had candidates suggesting blockchain ledgers for city finances and land records** to prevent data manipulation. Even environmental and social governance (ESG) efforts see potential: **De Beers uses a blockchain ledger to track diamonds** and ensure none are conflict-sourced, illustrating how transparency can enforce ethical standards in supply chains.

In a post-labor society, **radical transparency can serve as a new form of "social audit"**. Instead of relying on labor unions or journalists embedded in workplaces to surface wrongdoing, a transparent ledger makes oversight collaborative and continuous. Citizens, civic tech developers, NGOs, or AI algorithms can monitor blockchain-recorded data for anomalies or patterns of misuse. If government benefits or UBI payments are on-chain, for instance, any attempt by officials to divert funds would be evident in the ledger. This helps **deter "elite misbehavior" by increasing the likelihood of detection** – much as labor unions increased the costs of exploiting workers. In summary, **blockchain transparency shines a light where labor power used to cast a shadow**, creating a new layer of accountability in the civic system.

Decentralized Participatory Governance (DAOs and On-Chain Voting)

Another promising mechanism is the rise of **decentralized governance through blockchain-based organizations**, often referred to as *Decentralized Autonomous Organizations* or **DAOs**. A DAO is essentially a **collectively-owned, blockchain-governed entity** with decision rules encoded in smart contracts. Participants (who can be globally distributed) hold tokens or credentials that allow them to vote on proposals, allocate resources, and otherwise steer the organization's actions – all **without centralized leadership**. DAOs enable a form of **participatory governance** that is **borderless and peer-to-peer**. Vitalik Buterin describes a DAO as *"a collectively-owned organization working towards a shared mission"* where coordination happens via transparent rules on the blockchain rather than through a traditional hierarchy.

In the context of replacing labor rights, **DAOs offer a way to give individuals voice and agency in decisions that affect them, independent of their status as employees**. Consider how, in the industrial era, labor unions gave workers a seat at the table in corporate decision-making. In a future where fewer

people are employed, one might instead have *stakeholder DAOs* for different facets of society – e.g., a **DAO for gig workers** on a platform, or a **DAO for residents of a city to manage local resources**. Each member can directly vote on proposals (such as how to spend community funds or set rules) using secure digital voting. This is **participatory democracy hard-coded into software**. Notably, blockchain-based voting can be *more* secure and trustworthy than many current voting systems. By leveraging cryptography, **votes can be recorded immutably and even tallied in real-time, while preserving anonymity**. Pilot projects have already demonstrated this potential: **West Virginia, USA, trialed a blockchain voting system for overseas military voters**, and it was successful in providing both security and convenience. In Europe, several political parties and local elections have experimented with crypto-voting to increase verifiability.

A major advantage of blockchain governance is **inclusivity at scale**. People from anywhere in the world can coordinate and make collective decisions if they share a common interest, without needing a central authority to organize them. For example, when a group of 17,000+ individuals came together online in 2016 to form "The DAO" venture fund, they **pooled $150 million worth of ether** in a completely decentralized crowd-sale [1]. While The DAO famously had flaws (discussed later), it proved the concept that *large-scale, self-organizing governance is possible on Ethereum*. Today, there are DAOs governing everything from **decentralized finance protocols (e.g. MakerDAO managing a stablecoin)** to **collective media (e.g. a DAO owning NFTs of rare documents)**. Gitcoin, discussed further below, is itself a **community-run DAO distributing grants**. In a post-labor future, one could imagine many public functions handled by DAOs: **municipal services, public media, even regulatory oversight** could be partly governed by token-holding communities rather than bureaucrats. This could mitigate elite capture by ensuring **decision power is distributed among the stakeholders** of a given issue or resource, rather than top-down.

However, it's crucial to design decentralized governance carefully. **Simple token-voting (1 token = 1 vote) can replicate plutocracy** if tokens are concentrated. Indeed, one of the **fundamental challenges in DAO governance is managing power imbalances from unequal token distribution**. In many early DAOs, wealthy early backers or founders held a majority of tokens, giving them outsized influence – a dynamic no better (perhaps worse) than old shareholder capitalism. To truly replace labor's egalitarian influence, new governance models are being tried. For instance, **quadratic voting** or **quadratic funding** mechanisms weight votes such that the **voting power grows sub-linearly with tokens**, elevating the voice of those with fewer tokens. This "**one person, one (or at least more equal) vote**" approach helps level the playing field between whales and average participants. Another model is **reputation-based voting**: platforms like Colony assign voting weight based on contributions to the community, not capital invested. These innovations draw on political science and game theory to create **more democratic governance structures within DAOs**, aligning with the principle that *everyone affected should have a say*, not just those with money. We will discuss these models further in the proposals section, but it's important to note that the **technology allows experimentation with governance at a speed and scale impossible in traditional systems**.

In summary, decentralized participatory governance via blockchain can give the public a **direct voice in decisions** that might otherwise be made solely by technocratic elites or AI owners. By designing these systems to be **inclusive, secure, and resistant to capture**, society can ensure that even when people are not "workers" in the traditional sense, they are still **citizens with agency** in steering economic and social outcomes. This is a potential antidote to the disenfranchisement of the post-labor era – one that shifts the locus of power from employment (where people used to gain influence through unions) to **digital participation** (where people gain influence through networks).

Data Sovereignty and Self-Sovereign Identity

In the age of AI and big data, another arena of power is **personal data and identity**. Today, tech giants monetize our data and identities, often without transparent consent or reward to individuals. In a future where labor income might vanish, **personal data could become one of the most valuable assets individuals have** – whether it's data about your preferences, your health, your genetic code, or your creative content. Ensuring that individuals **retain sovereignty over their data and digital identities** is thus crucial for preventing a new form of exploitation that could replace labor exploitation. Blockchain and cryptographic technologies offer solutions here via **self-sovereign identity (SSI)** and decentralized identity systems.

A **self-sovereign identity** system uses cryptography and distributed ledgers to allow people to *own and control their identity credentials*, rather than relying on centralized authorities (governments, corporations) to manage identity. In practical terms, this means you would have a digital wallet (secured by keys only you hold) containing verifiable credentials – such as proof of citizenship, diplomas, work history, or simply a unique identifier. You could choose to share specific credentials with a service or organization when needed, and these credentials can be **verified via a blockchain without you surrendering the underlying data**. The Sovrin Network is a prominent example of such an SSI metasystem. Sovrin is a public ledger purpose-built for identity, where only *public decentralized identifiers (DIDs)* are recorded on-chain, while personal data stays off-chain under the individual's control. As Sovrin's documentation explains, *"SSI means the individual manages the elements that make up their identity and controls access to those credentials – digitally. The power to control personal data resides with the individual, not a third party"*. In effect, each person becomes the **sovereign of their own identity**, as **"no one can take their identity away"** under this model.

Why is **data sovereignty** so important in a world without labor? One reason is **economic: individuals may need to leverage their data for income or benefits**. If AIs and companies are using your data (say, your social media behavior to train AI, or your medical data for drug research), an SSI framework could allow you to **permission and even sell usage of your data on your terms**, potentially providing an income stream. We already see early attempts at this, such as **data marketplaces on blockchain** that reward users for contributing data. More broadly, retaining control means individuals can **form "data unions"** to collectively bargain the value of their data, analogous to how labor unions bargained the value of work. For example, a group of gig economy drivers might pool driving data and negotiate its sale to an AI mapping company, distributing proceeds among themselves – all facilitated by smart contracts that ensure payment and protect privacy. This flips the current script where corporations simply harvest user data for free.

Another reason is **civic inclusion**. In a society where rights and benefits (like UBI, voting rights, or access to services) might be administered digitally, having a **secure, universally accepted ID** is essential. We cannot rely on traditional employment or national IDs as the basis for identity if people are displaced or globally mobile. Blockchain-based identity can be **portable across borders** and independent of any single government's records, which is powerful for refugees or stateless persons. The Worldcoin project, for instance, is building a **"proof of personhood"** system: using iris biometrics and zero-knowledge proofs, it gives each person a unique World ID so they can prove they are a real, unique human in online interactions [2]. The ID is backed by the blockchain but does not reveal your personal information – it's just a guarantee of *uniqueness* and *human status*. Worldcoin's vision is that such an ID could enable fair global UBI distribution and help distinguish humans from AI bots in digital forums. This speaks directly to the post-labor challenge: if billions will rely on some form of social dividend, **we need a tamper-proof way to ensure each person gets their share exactly once**, and that requires robust digital identity. Blockchains

can achieve this in a decentralized way, avoiding a scenario where a single government or corporation controls the identity system (which could lead to new forms of tyranny or exclusion).

Data sovereignty also has a **political empowerment** angle. Consider that much of modern political discourse and advertising is driven by personal data profiling (think of targeted ads, Cambridge Analytica, etc.). In a future where people have self-sovereign identity, they could **opt out of certain uses of their data** or choose to share data with civic organizations rather than ad networks. They could even verify voting eligibility or petition signatures via zk-proofs of credentials (proving "I am a citizen of X country and over 18" without revealing name or ID number, for example). This would **enable broader participation** (e.g. global digital voting on issues) while **protecting privacy and preventing fake identities** from undermining processes. ZK (zero-knowledge) proofs are key here: they allow someone to **prove a statement about data is true without showing the data itself**. For instance, one could vote on a blockchain voting platform and then produce a ZK-proof that their vote was counted without revealing who they voted for – thus achieving the transparency of count and integrity of one-person-one-vote, *and* the secrecy of the ballot. Experts note that *"ZKPs enable secure and anonymous voting, ensuring appropriate on-chain governance structures"*. This is exactly the kind of cryptographic innovation that aligns with data sovereignty.

In short, **blockchain-based identity frameworks give individuals direct control over their digital selves**. This diminishes the power asymmetry where elites (tech companies or governments) hold all the data and thus all the insight and influence. By decentralizing identity and personal information, and by creating tools for privacy-preserving verification, society can protect people's rights and value in the digital realm – much as labor rights protected people in the industrial realm. An individual might no longer have leverage as a worker, but **as a sovereign data-owner and verified citizen, they gain new leverage**: they can demand value for their data, maintain privacy, and reliably assert their rights to social distributions or participation in governance.

Unstoppable Code: Smart Contracts and Protocol Enforcement

Perhaps the most novel (and controversial) capability of blockchain systems is the idea of **"unstoppable" code-based enforcement of rules** – encapsulated in the phrase "**code is law**." A **smart contract** is a self-executing program on the blockchain that automatically carries out certain actions when predefined conditions are met, without needing further intervention or permission. Once deployed on a decentralized network like Ethereum, a smart contract **cannot be arbitrarily altered or halted by any single party**; it will continue to run as coded, as long as the blockchain itself is operational. This creates a form of **"algorithmic enforcement"** that is **tamper-resistant and credibly neutral**. In a societal context, it means we can encode rights, obligations, and procedures into smart contracts such that *no authority can easily override them for their own benefit*. This property could fill the void left by the weakening of legal and institutional enforcement that labor rights used to bolster.

Consider how many labor rights and social protections depend on **enforcement by institutions**: labor laws require labor inspectors, courts, and sometimes union vigilance to enforce. If political winds shift (due to elite lobbying) or if institutions are corrupt, enforcement can lapse. By contrast, if a rule is embodied in a public smart contract, it is **automatically enforced** by the network consensus. For example, imagine a government implements a **universal basic income policy via a smart contract**: a pool of funds is set aside, and the contract is coded to pay every verified citizen X amount per month. Once launched, *not even the government could divert those funds elsewhere without everyone noticing*, because the rules on-chain would execute payouts as scheduled. It's like a law that executes itself – **an unstoppable UBI distribution**.

Indeed, one of blockchain's earliest promise was "unstoppable money" – the idea that cryptocurrency transactions cannot be censored or halted by banks or governments. This property has been demonstrated; for instance, when certain payment processors blocked donations to WikiLeaks in 2010, Bitcoin provided a censorship-resistant channel for supporters to send funds. In a civic contract context, this **resistance to censorship and intervention** could guarantee that *entitlements or public resources can't be hijacked by powerful interests*.

Another domain is **protocol-based regulation**. We could encode rules like "any factory (IoT-monitored) emitting above X pollution must pay fine Y to a public wallet automatically." If connected to trusted data oracles, such a smart contract would automatically charge companies for emissions, without needing environmental regulatory agencies to sue or prosecute – **the compliance is enforced by code**. There are proposals for "smart regulation" in financial markets using similar logic: e.g., if a bank's leverage exceeds a threshold, a smart contract could automatically freeze certain risky activities. **Blockchain's immutability ensures that these rules cannot be quietly bypassed**; any change requires the transparent consent of the network or stakeholders (much harder than backroom lobbying).

The concept of **"unstoppable protocol enforcement"** is essentially deploying **"freedom as code" at scale**. It removes or reduces reliance on trust in authorities, replacing it with trust in cryptographic protocol. One Facebook engineer was quoted saying of decentralized tech: *"It's a command center — intelligent, fair, unstoppable."* – highlighting that if done right, these protocols execute fairly and relentlessly. A concrete example today is **MakerDAO's stablecoin system**: it enforces financial rules (collateral ratios, liquidations) via smart contracts, with no favors or exceptions, something even regulators acknowledge as a new paradigm of rule enforcement by code rather than human discretion.

Of course, we must acknowledge the flipside: *"unstoppable" code can also rigidly execute bad decisions or contain bugs*. The famous 2016 **DAO hack** exemplifies this danger. The DAO's code had a flaw that an attacker exploited to siphon ~3.6 million ETH (worth about $70 million then) from the fund [3] [4]. The contract did exactly what the code allowed – unfortunately, that included an unintended loophole. The **Ethereum community had to hard-fork the blockchain to reverse the damage**, a controversial intervention that underscored that code is not *always* absolute law when the community deems an override necessary. This taught the lesson that **rigorous audits and safeguards are needed**: today, best practices include formal verification of smart contracts, multi-signature "escape hatches" to pause contracts in emergencies, and other circuit breakers. In the context of a blockchain-based civic system, one must design a balance between *automatic enforcement* and *flexibility to correct or update rules democratically*. We will return to this in proposals (for example, using **time-delayed upgrades** so the public can veto a malicious change).

When well-designed, however, **smart contracts can guarantee consistency and fairness in a way traditional institutions often fail to**. They do not get bribed, they do not discriminate beyond what the code specifies, and they operate 24/7. A poignant small example is how **Gitcoin's grant matching algorithm** (a form of smart contract logic) will allocate matching funds strictly according to quadratic funding formulas, rewarding broad community support – *no behind-the-scenes influence can skew it*. Similarly, **blockchain-based escrow or arbitration services** can ensure that agreements are executed fairly: e.g., gig workers might use a smart contract that automatically pays them once work (verified via oracles) is delivered, preventing platforms from arbitrarily withholding pay.

In a society where people can't threaten to strike or quit en masse to enforce fairness, **having their rights embedded in code provides a new kind of security**. It's like a digital Magna Carta: rights and rules enshrined in algorithms that cannot be unilaterally revoked. However, this is not a panacea; careful governance of the code itself is needed to avoid a tyranny of software. Mechanisms like **multi-stakeholder governance for protocol upgrades** (involving citizens in code changes) will be key. If done correctly, though, **unstoppable protocols could underwrite core aspects of the new social contract** – from guaranteeing an income floor, to preventing manipulation of public assets, to enforcing collective decisions exactly as agreed. This technological pillar complements the others (transparency, participation, identity) to create a robust scaffold for civic life after labor.

Having outlined these four capabilities – transparency, decentralized governance, data self-sovereignty, and autonomous enforcement – we now turn to concrete **case studies and implementations** that demonstrate these principles in the real world. These examples will show both the potential and the current limitations of blockchain-based systems in fulfilling civic functions that once relied on labor power or traditional institutions.

Case Studies: From Theory to Practice in Blockchain Civics

To ground the discussion, we examine several **real-world systems and projects** that illustrate how blockchain and cryptographic technologies are being used (or proposed) to fulfill civic, economic, and governance roles. These case studies provide insight into what is possible today, what challenges have arisen, and how these systems might scale up to form parts of a new civic contract. We will explore:

- **Ethereum and Decentralized Autonomous Organizations (DAOs):** The Ethereum blockchain as a general-purpose platform enabling decentralized governance and "unstoppable" applications, including notable DAO experiments.
- **Gitcoin and Quadratic Funding:** A platform demonstrating decentralized, community-driven funding of public goods, embodying participatory governance and algorithmic resource allocation.
- **Worldcoin and Proof-of-Personhood:** An initiative combining biometrics, blockchain, and UBI aspirations – highlighting innovations and controversies around global identity and income distribution.
- **Sovrin and Self-Sovereign Identity:** A decentralized identity network showcasing how individuals can control their credentials and data in practice, with implications for privacy and agency.
- **Other Emerging Examples:** Brief mentions of additional instances, such as local government pilots or other DAO-governed communities, to illustrate the growing ecosystem of blockchain civic tools.

Each of these cases connects back to the mechanisms discussed and offers lessons for the viability of blockchain as a replacement or supplement for labor-based structures.

Ethereum: A Global Platform for Decentralized Governance and Unstoppable Code

Ethereum is the second-largest public blockchain network (after Bitcoin) and the leading platform for smart contracts and decentralized applications. Launched in 2015, Ethereum was explicitly designed to be a **"world computer"** – a distributed virtual machine that anyone can use to run code that is **transparent, immutable, and censorship-resistant**. In the context of our discussion, Ethereum is important as the *infrastructure that has enabled most of the decentralized governance and civic experiments to date*. Many of the technologies and examples in this report (DAOs, tokens, decentralized identity, quadratic funding) either

run on Ethereum or were pioneered there. Ethereum thus serves as a **proof of concept that critical services can operate without centralized institutions**: financial transactions, contracts, even organizational governance can all be handled by Ethereum-based protocols.

One salient example is the aforementioned **The DAO**, which was launched on Ethereum in 2016. The DAO was effectively a **decentralized venture capital fund**: individuals invested ether (ETH) and received DAO tokens, which entitled them to vote on proposals for projects to fund and to share in returns. In less than a month, The DAO raised ~**$150 million in ETH from over 11,000 participants** around the world [5]. This was unprecedented – it demonstrated that **a massive number of strangers could coordinate financially without a traditional corporate structure**. Although The DAO fell victim to a hack, as described earlier, it was a watershed moment that spawned the ongoing "DAO movement." Today, **Ethereum hosts thousands of DAOs** of varying sizes – some with treasuries in the billions of dollars (like certain protocol DAOs in decentralized finance), others small and local. The **governance token model**, where people hold tokens that allow voting on governance proposals, is now common. For instance, **MakerDAO** (on Ethereum) manages the DAI stablecoin (a cryptocurrency pegged to the dollar) through a global community of token holders who vote on risk parameters, fee rates, and upgrades. This is essentially a **central bank run by citizens (token holders) rather than government bankers**, all made possible by Ethereum's infrastructure.

Ethereum itself has also undergone governance challenges that illustrate the interaction of code and community. After The DAO hack, Ethereum's community (via informal off-chain governance) decided to implement a **hard fork** to reverse the theft, effectively restoring the stolen funds. This was controversial – it went against the notion of strict immutability – and led to a minority splitting off to continue the old chain (Ethereum Classic). The episode is instructive: it shows that *even in decentralized systems, human governance remains in the loop*, but also that blockchain communities can organize and make tough decisions in a relatively transparent, decentralized fashion. Since then, Ethereum's core development (like the recent switch to Proof of Stake in 2022) has been guided by open proposals (EIPs) and broad discussion, if not direct on-chain voting. Newer blockchain projects like **Tezos and Polkadot** have built-in on-chain governance, where coin holders can vote on protocol upgrades – giving a taste of how perhaps a *future digital democracy might amend its "constitution" via token votes*.

From a civic standpoint, Ethereum's biggest contribution is showing that *critical economic functions can be decentralized*. People can **save, lend, send money (via DeFi)**, **fund projects (via ICOs or DAOs)**, **organize collective action (via DAO tooling)**, **establish identity or reputation (via DIDs and attestations on Ethereum)** – all without traditional banks, companies or governments at the center. This disintermediation is powerful. It means that if we want to implement a new social contract (say UBI or participatory budgeting), we *do not necessarily need to route it through a central state or giant corporation; we could implement it on a public blockchain like Ethereum*, ensuring global accessibility and neutrality.

Of course, Ethereum's open ecosystem has also seen **pitfalls**: scams, speculative bubbles, hacks, and governance failures have occurred. These serve as lessons: for instance, the **2017 boom in ICOs (initial coin offerings)** raised billions in an unregulated way, some of which ended in fraud or failure. This highlighted the need for **better governance and checks even in decentralized finance**. It is analogous to early capital markets in the 19th century – eventually, norms and regulations (or self-regulations by code) needed to catch up to prevent abuse. Ethereum's ongoing development (with initiatives for more secure contract languages, auditing standards, and identity standards) is addressing some of these issues. The **energy consumption** issue, once a huge criticism, was largely solved by Ethereum's switch from proof-of-

work (like Bitcoin) to **proof-of-stake consensus**, reducing energy use by ~99%. This illustrates that the technology can evolve to become more sustainable and politically acceptable.

In summary, **Ethereum provides the backbone for implementing many blockchain-based civic solutions**. It has proven the viability of decentralized networks at scale (settling billions of dollars in transactions daily) and the concept of **autonomous organizations and agreements that operate without centralized control**. Its existence and resilience give confidence that if we encode parts of our new civic contract in blockchain applications, the underlying platform can carry them out. As we look to specific solutions like Gitcoin, Worldcoin, and Sovrin, it's worth remembering that **Ethereum (and similar networks) are the public infrastructure making them possible**, much as roads and utilities made industrial society's institutions possible.

Gitcoin: Quadratic Funding and the Decentralized Funding of Public Goods

One of the compelling case studies in how blockchain can replicate civic functions is **Gitcoin**, a platform that uses decentralized methods to **fund public goods and open-source projects**. Gitcoin emerged from the Ethereum community in 2017 with a mission to support the development of open-source software – something traditionally underfunded (since it's a public good) but vital to the digital economy. **Gitcoin's innovation is to use a** quadratic funding **mechanism, executed via smart contracts, to allocate matching funds based on broad community support**. This is essentially a new **funding model for the commons**, one that aims to be more democratic and efficient than either centralized grant committees or pure market funding.

Here's how it works: Gitcoin runs periodic **grants rounds** where many projects (not only software now, but also climate initiatives, educational programs, etc.) invite contributions. Alongside individual donations from the crowd, there is a **matching pool** of funds provided by sponsors (often large crypto donors or organizations like the Ethereum Foundation). The allocation of the matching pool to projects is determined by the quadratic funding formula. In quadratic funding (QF), the key principle is that **matching is proportional to the *square* of the sum of square roots of contributions** – which simply means **the number of distinct contributors matters much more than the total amount contributed**. A project that raised $100 from 50 people (each giving $2 on average) will get a much larger match than a project that raised $100 from 1 person. This reflects a democratic ideal: *a project that has many people's support, even with small dollars, is deemed more socially valuable than one rich person's pet project*. In practice, Gitcoin's smart contracts tally all contributions and then compute the optimal matching distribution. This computation is transparent and verifiable on-chain (anyone can inspect the contributions and the resulting match). The result is that **Gitcoin has been able to fund a wide array of public goods in a way that responds to community preferences rather than top-down decisions**.

The impact has been significant. **Since 2019, Gitcoin has provided over $56 million in funding to public goods projects** across open source, Ethereum infrastructure, community, climate tech, and more. Over **6,000 projects have been funded** in its first few years. This makes Gitcoin a substantial financier of global public goods – effectively a decentralized, voluntary counterpart to government R&D grants or philanthropic foundations. Some projects that started with Gitcoin grants (like decentralized developer tools, or COVID relief efforts in some regions) might not have found funding otherwise. Kevin Owocki, Gitcoin's founder, framed the mission as **"funding what matters to your community"** – empowering communities to collectively support the resources they rely on, which traditional markets undervalue. This is a clear parallel to labor unions historically pooling resources for mutual aid or political causes, except

Gitcoin's "union" is open to anyone globally and decisions are made by a distributed crowd's donations rather than union officials.

Gitcoin also exemplifies **participatory governance** in its operations. It evolved into a **DAO (GitcoinDAO)** which now manages the platform. GitcoinDAO has token holders and delegates who propose and vote on changes (for example, decisions like moving to a new blockchain (they launched their own sidechain called Public Goods Network) or modifying matching rules are done through community governance). Interestingly, GitcoinDAO is learning that pure decentralization can be inefficient; recently it decided to simplify and become more "streamlined" (some described it as "going kinda corporate") by granting more decision power to core teams for agility. This highlights a *pragmatic approach*: even within a DAO, some centralization or leadership can help, as long as it's accountable to the community. The **lessons Gitcoin is learning mirror those of traditional civic organizations** – balancing broad participation with effective execution – but in a far shorter timespan and with global stakeholders.

From a systems perspective, Gitcoin demonstrates a **working model of decentralized wealth redistribution and civic investment**. It channels funds from those with resources (crypto donors) to those creating shared value (developers, activists) in an automated, bias-minimized way. It's as if one took the idea of **taxation and public spending** and made it voluntary and algorithmic: individuals "contribute" to projects they like (like earmarking taxes) and the algorithm amplifies the collective signals. This doesn't entirely replace the need for actual taxation or state spending (since Gitcoin relies on voluntary donations), but it suggests a future where **communities around the world self-organize to fund their public goods via blockchain**, reducing reliance on nation-state budgets which may be strained in a post-work economy. In fact, some economists have mused that if automation increases private wealth but erodes the tax base (due to joblessness), *voluntary, global funding mechanisms might be crucial to finance public goods*. Gitcoin's success to date provides a template for that.

The **quadratic funding mechanism** itself, championed by economists like Glen Weyl, is a **heuristic to restore equilibrium in resource allocation**. It ensures broad interests are represented rather than just concentrated capital – echoing how labor unions aimed to give the broad workforce representation against concentrated capital owners. By encoding that principle in a formula, Gitcoin shows one way to **embed fairness into the code**. Other DAO projects are taking note; for instance, cityDAO experiments and some philanthropies are looking at quadratic voting for community decisions.

In conclusion, **Gitcoin showcases blockchain's capacity to fulfill a civic function historically tackled by governments or civil society**: funding the commons. It has created an open, global version of a grants council that is arguably **more attuned to the people's will (as expressed in micro-donations) and more transparent in execution** (every grant and result is public). The limitations are that it currently depends on a somewhat niche crypto community and donors – scaling it to mainstream public goods (like roads or fundamental research) would require much larger pools of capital. Yet, as automation advances, perhaps the very companies benefiting could channel funds into such decentralized public goods funding (indeed, **Optimism, an Ethereum scaling network, directs a portion of its transaction fees to public goods funding via a similar model**). Gitcoin is an early but powerful demonstration that **the loss of labor-organized public good provision (like union-run community programs or worker lobbying for public spending) could be offset by new, blockchain-organized public good provision**.

Worldcoin: Proof-of-Personhood and Universal Basic Income Experiments

Worldcoin is one of the most talked-about – and contentious – projects at the intersection of blockchain and the future of society. Co-founded by Sam Altman (CEO of OpenAI), Worldcoin's aim is to create a **global digital identity and cryptocurrency that could support universal basic income (UBI)**. The project encapsulates several themes: **proof-of-personhood** (ensuring each human can be uniquely identified in the system), **decentralized identity via biometrics** (using iris scans as a unique ID, coupled with zero-knowledge cryptography), and the idea of bootstrapping a **UBI by giving everyone a crypto token**. Given our discussion, Worldcoin can be seen as an ambitious attempt to **directly address the "labor obsolete" scenario**: if AI (like Altman's own OpenAI products) creates tremendous wealth while displacing jobs, Worldcoin is positioning itself as an infrastructure to redistribute wealth to every human on earth, outside the traditional labor market.

The core of Worldcoin is the **World ID**, a **"digital passport" that proves you are a unique human**. The system uses a custom device called the **Orb**, a shiny spherical iris scanner. People who want to join Worldcoin have their iris scanned by an Orb (Worldcoin has had sign-up stations in various cities worldwide). The device converts the iris scan into a unique numerical code (an "iris hash") and checks it against the database to ensure that person hasn't signed up before. Importantly, Worldcoin says the actual iris images are not stored; rather, the hash is and it's *impossible to reverse-engineer the iris from the hash*. Once verified, the person is issued a **World ID** – essentially a decentralized identifier (DID) – and a **cryptographic proof of uniqueness** (using zero-knowledge proofs so that later they can prove they have a World ID without revealing which one or any biometric info). In simpler terms, **Worldcoin creates a global list of real people, each represented by an anonymous ID**. This tackles a huge problem in decentralized governance: *Sybil attacks* (one person pretending to be many). With proof-of-personhood, one human gets one vote or one share of the UBI, preventing exploitation by bots or duplicates.

Upon signing up, users in many countries have been receiving a free allocation of the **Worldcoin token (WLD)** – for example, 25 WLD tokens (around $50–60 value at launch). The idea is that these tokens could increase in value as adoption grows, and one day might be used as a **currency for UBI distributions or a currency within a global economy of humans**. Altman has suggested that **if AI and automation produce immense wealth, a currency like Worldcoin could help distribute it to people universally as a basic income**. Indeed, Altman has long been interested in UBI (he funded trials in Oakland) and sees Worldcoin as a tool to implement UBI globally. The project is still in early stages – as of mid-2023, about 2 million people had signed up during beta, and the official launch spurred more interest (along with pushback from regulators).

Worldcoin demonstrates some **technical possibilities** relevant to replacing labor rights: it shows that it is possible to **create a single global registry of humans without a central government**, using a combination of biometrics and cryptography. This is groundbreaking because one prerequisite for many social policies (like UBI or democratic participation) is to prevent fraud (one person claiming multiple benefits or votes). Historically, nation-states issue identities (passports, SSNs) and manage benefits within their borders. But a post-labor world might demand *global* solutions (as AI's impact is global and people might migrate to where resources are). Worldcoin's approach is one attempt at *globally inclusive identity*, where for example an unemployed person in Nigeria and one in Japan both can prove they are distinct humans and thereby both receive the same crypto stipend if a UBI program were implemented. **It lowers the barrier to inclusion** in the economic system to simply having eyes and being willing to scan them, rather than needing paperwork or bank accounts.

However, the **controversies and risks around Worldcoin are significant**, highlighting issues that any blockchain social contract design must carefully navigate. First is **privacy and surveillance** concerns. Scanning people's irises worldwide rings dystopian alarms for many. Edward Snowden criticized it bluntly: *"Don't catalogue eyeballs"* and *"the human body is not a ticket-punch"*, expressing concern that even if hashed, the biometric data could be misused. Privacy advocates worry about how the biometric data is stored and whether individuals could be de-anonymized. Worldcoin claims to delete raw images and only keep hashes, but trust is a factor; some fear a future where an authoritarian actor could use World IDs to track people if not truly secure. This is a lesson that **technological solutions must be paired with social trust and robust governance**. In absence of labor power, we don't want to create a new tool of control.

Second, **consent and exploitation** issues have arisen. Investigations (e.g. by MIT Technology Review) found troubling practices in early Worldcoin sign-ups: in some developing countries, **people were not given full information (terms only in English, not local language) and were lured by small rewards like ~$20, without clarity on data usage**. There were reports in countries like Sudan and Indonesia of aggressive sign-up drives where participants didn't understand Worldcoin's purpose, effectively treating vulnerable populations as guinea pigs for a global tech experiment. This echoes past labor issues (e.g. exploiting cheap labor in poor countries) now transposed to **exploiting personal data or biometrics** of those in need. It underlines that *without ethical oversight, even "world-saving" tech projects can perpetuate inequalities* – here, informational and power asymmetry between Worldcoin operators and participants.

Additionally, a **black market for World IDs** emerged: people in some places were **selling their biometric credentials for quick cash** to speculators who hoped to collect the free tokens [6]. This both undermines the system's integrity and indicates how economic hardship can push individuals to monetize anything – now even one's identity – if labor income is lacking. In Kenya, authorities suspended Worldcoin in 2023 citing concerns over data privacy and security, as **tens of thousands of Kenyans rushed to get the token money, raising alarms about informed consent** [7]. This scenario suggests that any attempt to implement a large-scale blockchain-based social benefit must involve **local stakeholders and clear regulatory frameworks** to protect participants.

On the positive side, Worldcoin has sparked broader conversation and other initiatives in the **proof-of-personhood space**. Another project, **Proof of Humanity** (mentioned in the Time article), used a web-of-trust and video verification approach to register humans and actually distributed a UBI token called UBI (about $50–100 monthly at peak) to each verified person. That project faced its own issues (the token value crashed in the bear market), but it showcased a different, community-driven model. It's possible that the best solution will combine ideas: e.g., multiple proof-of-person systems (biometric, social attestations, etc.) cross-verified for robustness.

In essence, **Worldcoin is a bold attempt to create the plumbing for a post-labor economy (global ID + global currency)**, but it highlights that *technological solutions can't be divorced from ethics and governance*. If labor rights once ensured dignity and consent in the workplace, any new system must ensure dignity and consent in the digital sphere. The outcry from privacy experts and the swift action of some regulators on Worldcoin indicate that **society will demand strong protections in any blockchain-based civic system** – a valuable lesson for our normative proposals later.

Despite the controversies, the core idea of **ensuring every individual has a verifiable digital identity and a share in tech-generated wealth remains powerful**. Worldcoin's ongoing evolution (it has a foundation and is engaging with regulators) will be worth watching. It may or may not succeed as the dominant

platform, but it has already moved the needle on concepts like **self-sovereign biometrics, global UBI distribution, and the need for open discourse on how to implement them**. For our purposes, Worldcoin illustrates both the **potential (global inclusion, AI dividends) and pitfalls (privacy, coercion)** of using blockchain tech to replace labor's role in guaranteeing individuals a share of prosperity.

Sovrin: Self-Sovereign Identity in Action

While Worldcoin represents one approach to global identity (biometric-heavy and controversial), **Sovrin** provides a more understated but fundamentally important case study of **self-sovereign identity (SSI)** implemented via blockchain technology. The **Sovrin Network** is a decentralized, public-permissioned ledger purpose-built to support identity management on a global scale. Unlike Worldcoin, Sovrin doesn't aim to create a new currency or directly address UBI; instead, it focuses purely on **empowering individuals (and organizations) with control over their digital identities and credentials**. This directly ties into the **data sovereignty** mechanism discussed earlier, and Sovrin is arguably one of the most mature examples of that principle in practice.

On Sovrin, every user (or "Identity Owner") can have one or multiple **Decentralized Identifiers (DIDs)** – unique strings that serve as addresses on the network. These DIDs are registered on the Sovrin ledger, which acts as a **global public utility for resolving DIDs to public keys**, enabling trustable interactions. The personal data (actual credentials like "Alice's driver's license" or "Bob's university degree") are *not* stored on-chain; instead, they are held by the user in digital wallets and only shared peer-to-peer when the user chooses. Sovrin's ledger merely anchors the *public* elements needed (like the issuers' public keys, credential schemas, revocation registries, etc.). This design achieves **privacy by architecture**: you don't put private data on the blockchain, you put just enough info to verify authenticity of credentials. For example, the DMV could issue Alice a digital driver's license credential signed with their private key. Alice stores it. When she needs to prove to a bar that she's over 21, she can present a **zero-knowledge proof derived from her license credential** that reveals only "I am older than 21" without revealing her birthdate or license number (Sovrin supports such ZK-proof-capabilities). The verifier (the bar) checks the Sovrin ledger to see that the DID of the issuer (DMV) is legit and that the credential signature is valid and not revoked. This all happens without any central database query – it's decentralized trust.

The governance of Sovrin is also notable. It is run by the **Sovrin Foundation, a non-profit**, and the ledger nodes are operated by **Stewards** – organizations (companies, universities, NGOs) around the world that apply and are approved to run the infrastructure. Over 50 stewards across six continents were involved, including IBM, Deutsche Telekom, universities, etc.. They abide by a common **Sovrin Governance Framework** that sets rules on how the network is used and how privacy is protected. No single entity controls the network – which is crucial for maintaining trust that this identity system isn't another centralized silo. This addresses a piece of the puzzle in a post-labor world: **we need global digital utilities (like identity systems) that aren't owned by any government or tech giant** but are community-governed. Sovrin's model shows how that can work for identity.

In practical use, Sovrin (and the underlying tech like Hyperledger Indy and Aries) has been piloted in various contexts: for example, the government of British Columbia and others formed the **Verifiable Organizations Network** issuing business credentials on Sovrin; some humanitarian organizations have tried Sovrin-based IDs for refugees; and companies use it for single sign-on and credential verification. One oft-cited success is that **Estonia's e-residency and eID system**, while not Sovrin, similarly gives citizens a digital identity to interact with services, boasting high satisfaction. (A blog claims Estonia's blockchain-

supported eID increased satisfaction with gov services from 32% to 99% – though that number seems very high, it underscores the perceived impact of empowering citizens digitally).

For the purposes of replacing labor rights, **Sovrin's approach to identity means individuals could carry their "social reputation" and credentials independently of employers or governments**. Think about labor rights – part of labor power was the ability to **show one's qualifications, organize with others, and have a status in society beyond a single job**. In the gig/AI economy, Sovrin-like identity can allow, for instance, gig workers to hold a verifiable record of all the gigs they've done and ratings they earned, which they control and can present to any platform – preventing lock-in to one company's reputation system. It gives **portability of merit and history**. Also, in interacting with algorithmic systems or claiming benefits, a Sovrin ID could let you prove eligibility without third parties data-mining you. For example, to get a future crypto-UBI, you might prove "I am a unique person and a resident of X country" via credentials in your wallet, without exposing more (avoiding surveillance or discrimination). This preserves **personal agency and privacy** – values core to human dignity that were also central to labor movements (which often fought against intrusive employer practices and for personal privacy off the job).

An important civic aspect of SSI like Sovrin is **reducing dependency on centralized platforms**. Today, losing your job can mean losing your corporate email, your LinkedIn visibility, etc. With self-sovereign identity, your professional and social identity is yours to keep; you just detach from an employer context. In a future where jobs are rare, people might form communities or co-ops that recognize each other's contributions via verifiable credentials (e.g., community service hours, skills learned). This could form the basis of *non-labor social credit* – not in the Big Brother sense, but in a positive, empowering sense of *recording one's contributions to society* even if unpaid, and being recognized for them. For instance, someone might earn credentials for volunteering, for creating digital art, for mentoring others, etc., and these could feed into how governance tokens or UBI distributions are allocated (to reward pro-social activity, something some DAO experiments consider with "proof-of-impact" tokens).

In summary, Sovrin is a quieter revolution compared to Worldcoin, but arguably **a more foundational one for building a fair post-labor society**. It provides the means for **anyone to identify and authenticate themselves in a decentralized way**, which is as fundamental to participating in society as a worker's right to their own personhood and to organize was in the labor era. By eliminating the need to rely on corporate or state intermediaries for identity, SSI ensures that **people's access to economic and civic rights isn't mediated by employment or arbitrary authorities**. However, challenges remain: getting wide adoption (network effect issues), ensuring interoperability (multiple SSI networks need common standards), and dealing with cases where people lose their private keys (Sovrin has mechanisms like social recovery but it's still a UX challenge). These are being actively worked on by an open community.

Together, the above case studies (Ethereum/DAOs, Gitcoin, Worldcoin, Sovrin) paint a picture of a possible new civic landscape: one where **global platforms for collaboration, funding, identity, and exchange exist that are not controlled by traditional power holders**. They are **tools that, if used well, could redistribute power to individuals and communities**, even when those individuals no longer have power via labor. But as we've hinted, these systems are not without flaws or risks. In the next section, we explicitly tackle the **limitations, risks, and barriers** of relying on blockchain systems to replace or augment labor rights, both in theory and as evidenced by real experiences like those we just discussed.

Limitations and Risks of Blockchain Systems as a Replacement for Labor Rights

While blockchain and cryptographic technologies offer unprecedented possibilities for empowering individuals and communities, **they are not a cure-all**, and deploying them as the backbone of a new social contract comes with significant challenges. It is critical to **soberly assess the limitations and risks** – technical, social, and political – of these systems, especially if they are to carry out functions previously upheld by labor power and legal protections. Here we break down the major concerns:

- **Power Concentration and Inequality in Decentralized Systems**
- **Security Vulnerabilities and Technical Failures**
- **Scalability and Efficiency Constraints**
- **Privacy Concerns vs. Transparency**
- **Legal and Regulatory Uncertainty**
- **Adoption, Accessibility, and the Digital Divide**
- **New Forms of Exploitation and Abuse**

By examining each, we can understand where blockchain governance might fail or even exacerbate problems, and thus what safeguards or complementary measures are needed.

Power Concentration and Inequality in Decentralized Systems

One might assume that "decentralized" automatically means fair and egalitarian, but **decentralization can still hide power imbalances**. A chief risk is the **emergence of plutocracy within blockchain governance** – effectively replacing one elite (capital owners) with another (token holders, who, often, are capital owners too). As noted earlier, in many DAOs **voting power is tied to token holdings**, and wealth distribution in crypto is highly skewed. This leads to scenarios where **a small number of large token holders can exert disproportionate influence over decisions**. For example, if a social welfare DAO was governed by a token, whales could sway how resources are allocated, possibly against the interests of the majority. This **mirrors the very elite capture we seek to avoid**, just in digital form. Studies and real incidents have shown this: in one case, a single large voter in the Steem blockchain essentially centralized control (leading to a contentious fork). Even **Ethereum's decentralized finance has been criticized** because governance tokens are often concentrated with venture investors or founders.

There are mitigations: we discussed **quadratic voting/funding** and **reputation-based governance** as ways to curb plutocracy. These are promising, but not yet widespread. Additionally, **Sybil resistance** is needed to enforce one-person-one-vote schemes (hence the importance of proof-of-personhood like World ID or Proof of Humanity). Without robust Sybil control, any system trying to give equal voice can be gamed by fake identities. So, **solving identity is a prerequisite to solving governance equality**. Even then, we face the social challenge of **engagement**: just as in democracies a small organized group can dominate if the majority is apathetic, in DAOs often only a small fraction of token holders vote. Low participation can lead to **decision-making by the few who are active**, skewing outcomes. This is reminiscent of low voter turnout issues in public elections (exacerbated when unions or civic orgs that mobilize voters weaken). So, while blockchain lowers barriers to participation (you can vote from your phone, etc.), *it doesn't guarantee participation*. There may need to be incentives or cultural shifts to encourage broad engagement in governance – otherwise power will centralize by default to those with the time, knowledge, and resources.

Information asymmetry is another subtle factor. Even with transparency, understanding complex protocol proposals or funding decisions requires expertise. This could lead to a **technocracy of coders** or those fluent in blockchain jargon. One could argue this is analogous to how, in labor relations, specialized lawyers or economists could dominate negotiations, but at least unions employed their own experts. In decentralized communities, if average people cannot easily grok the issues, they might defer to "core devs" or crypto influencers – again creating a hierarchy. We see hints of this in some crypto projects where a charismatic founder or core team still effectively guides the direction (the community often rubber-stamps). This challenges the ideal of *autonomous grassroots governance*.

In sum, **there is a risk that decentralized systems replicate or even intensify inequality** if design choices aren't carefully made to distribute power. The early crypto wealth distribution, often called the "Bitcoin or Ethereum whales," is a reality: e.g., at one point, ~2% of addresses owned 95% of Bitcoin. If those same distributions apply to tokens that govern our notional future UBI system or public resource DAO, the outcome could be as unequal as the Gilded Age. So, *explicit mechanisms to counterbalance wealth* – akin to how labor unions counterbalanced capital – must be part of system design. We have those mechanisms (quadratic voting, soulbound non-transferable tokens for merit, etc.), but implementing them widely is an ongoing challenge.

Security Vulnerabilities and Technical Failures

Entrusting key civic functions to blockchain systems means **they must be extremely secure and reliable** – otherwise people's rights could vanish with a hack or bug. Unfortunately, the track record shows that **smart contract vulnerabilities and other technical failures are not uncommon**. We've recounted the **DAO hack of 2016** where a single bug led to millions of dollars being stolen. Since then, numerous decentralized finance (DeFi) hacks have occurred (over $3 billion stolen in 2022 alone by exploiting flaws in code or protocol logic). If these systems were only about money, it's bad enough – but imagine if a flaw allowed someone to **falsify identity credentials or siphon a UBI fund**. The consequences would be severe for society's trust in the system.

Security is improving – professional audits, formal verification, and hacker bounties are now standard for serious projects. But the technology is still young, and the complexity increases as we incorporate advanced cryptography (like zero-knowledge circuits) which could have subtle bugs. Even Ethereum's core code has had vulnerabilities (like the inflation bug in 2018 that was discretely patched). The specter of a **51% attack** on a blockchain (where an attacker gains majority mining or validation power to rewrite history) is another risk. Major networks like Bitcoin and Ethereum are likely safe from this due to scale, but smaller blockchains or side-chains could be attacked, undermining the immutability that is promised. For instance, some minor cryptocurrencies have seen 51% attacks that reversed transactions.

Key management is a huge practical security issue for users. In a blockchain world, **"your keys, your coins; no keys, no coins."** If individuals are to hold their own identity keys, vote tokens, etc., then losing one's private key (or having it stolen via phishing or malware) could mean **losing one's digital identity or funds permanently**. Traditional systems have account recovery through customer support; decentralized ones often do not (though social recovery and multi-sig techniques are emerging, they add complexity). The average person might find the responsibility of securing keys daunting – raising the prospect that they will delegate it to custodial services, reintroducing central points of failure. This interplay of usability and security is crucial: a system unusable by non-experts will fail to gain adoption or will ironically centralize as people flock to easier solutions (like keeping funds on a big exchange, or using a single identity provider).

Smart contract immutability is a double-edged sword: bugs are hard to fix on the fly. Ethereum's forced fork after The DAO was an exception; generally, **"code is law" means if something goes wrong, there's no quick remedy**. This rigidity is risky in governance – what if a smart contract implementing a benefit formula has an error? We'd need a robust upgrade mechanism which itself must be secure (e.g., a time delay and multi-party confirmation to patch). We likely need *circuit breakers* in critical contracts – similar to how traditional systems have failsafes.

Another angle: **dependency on oracle inputs and external data**. Many blockchain-based civic apps will rely on real-world data (e.g. IoT sensors for environmental enforcement, or population data for UBI). These **oracles** can be points of failure – they could be corrupted or go offline, causing smart contracts to behave incorrectly (like triggering false penalties or missing payouts). Solutions like decentralized oracle networks (Chainlink, etc.) help, but they add complexity and cost.

Finally, consider **catastrophic scenarios**: if the internet goes down in an area, or if a solar flare or EMP knocks out infrastructure, do people lose access to their "rights" encoded on blockchain? Traditional systems often have offline backups; distributed ledgers are more resilient in some ways (multiple copies), but also require connectivity. Planning for resilience (perhaps local nodes, mesh networks, physical token proofs) would be needed to ensure continuity of the civic functions in disasters.

In summary, **technical risk is non-trivial**. Just as early industrial workers faced safety risks until regulations improved standards, early adopters of crypto have faced security risks. For blockchain to underwrite social rights, it must reach a level of robustness akin to banking or government systems (and ideally better). This will likely require continued maturation of the technology, rigorous testing, and maybe hybrid approaches where critical safety nets exist (for example, a constitutional DAO might have an emergency vote mechanism to freeze a contract if a major bug is found, akin to a recall of a defective product).

Scalability and Efficiency Constraints

Blockchain networks historically face challenges in **scalability (transactions per second, storage capacity) and efficiency (speed, cost of use)**. If we are to migrate large-scale civic processes (like a national voting system or global UBI micropayments for billions) onto blockchains, these networks must handle **high throughput**. Classic Bitcoin can do ~7 transactions per second, Ethereum currently maybe ~15-30 on Layer 1 (with much more on Layer 2 rollups). By comparison, Visa handles thousands per second routinely. Significant progress is being made – e.g. Ethereum's rollups and sharding roadmap, or alternative high-throughput chains – but **the jury is still out on whether decentralized networks can scale to global population levels while maintaining true decentralization**. There is often a *trade-off between scalability and decentralization*: more centralized solutions (like permissioned chains or those with few validators) can be faster, but reintroduce trust in a few actors.

If systems don't scale, the danger is twofold: either they become **slow/expensive**, or they **centralize to scale**. Neither is acceptable for critical public infrastructure. For instance, Ethereum gas fees have spiked to painful levels in the past (e.g. $50+ to do a token transaction during 2021 peaks). Imagine those costs applied to everyday micro-transactions or voting – it would exclude those who can't pay, effectively creating a class barrier. **High fees or slow performance could recreate inequality** (only the affluent efficiently use the system) or simply drive people away to centralized solutions (like using a big tech company's faster sidechain, giving that company power). In recent years, Layer 2 scaling solutions (Optimistic and ZK rollups) have dramatically lowered costs for users while inheriting main-chain security. This is promising: e.g.,

simple transactions on some Layer 2s cost fractions of a cent now. Still, complex operations (like ZK proof verification or privacy-preserving actions) can be computationally heavy, and cost remains a factor.

Storage and bandwidth: If we envision putting a lot of records (like public finance data, or millions of credential attestations) on-chain, that could bloat the blockchain, making it hard for individuals to run nodes (which hurts decentralization). Pruning techniques and distributed storage networks (IPFS, Arweave, etc.) can offload bulk data, but we then rely on their integrity. It's manageable but requires careful architecture.

Another aspect is **energy efficiency**. Proof-of-work blockchains like Bitcoin have been critiqued for high energy use (comparable to a country's electricity consumption). Ethereum's shift to proof-of-stake dramatically cut its footprint, and many newer chains use PoS or other low-energy consensus. So, while energy concern is being addressed, any plan to make blockchain the backbone of society must ensure it's done in an environmentally sustainable way – otherwise it's trading one crisis (inequality) for another (climate impact). Thankfully, it appears most major platforms are moving away from energy-intensive consensus, and some (like Algorand, Tezos) tout carbon neutrality. Still, the computing overhead of cryptography and global consensus is not trivial, meaning a **blockchain-based system might always be somewhat less efficient than a centralized database**. That's the cost of decentralization. We have to judge if the benefits (trust, resilience) justify that cost for each application.

Latency is also a consideration: a Bitcoin transaction might finalize in an hour, Ethereum in a few minutes (depending on confirmations). In governance or daily interactions, some delays are fine (e.g., you don't need instant finality for a monthly UBI payment), but others might need to be faster. New blockchains and rollups are achieving sub-second block times and faster finality, so this is improving. But complex cross-chain interactions (like using identity from one chain on another, or moving funds) can introduce latency or points of failure.

The concept of **"layered architecture"** likely is key: base layers for global consensus (slower but ultra-secure), and second layers for speed (with periodic settlement on base layer). This requires careful design so that the user experience is smooth and the security assumptions are acceptable. We likely will hide complexity under user-friendly apps that abstract whether something happened on a sidechain vs mainnet etc.

Finally, **governance scalability** is an interesting issue: on-chain voting with millions of participants has not been done frequently. We must ensure that the user interfaces, education, and processing of potentially millions of votes are ready. If not, on-chain governance could become unmanageable or suffer from low participation.

In summary, **scalability is a solvable but still pressing issue**. The risk if not solved is that blockchain systems either **fail under load, price out the poor, or resort to centralizing shortcuts** – any of which would undermine the goal of an equitable post-labor system. As a mitigating note, technology tends to improve, and the intense research in blockchain scalability (sharding, rollups, new consensus like DAGs) is encouraging. But any strategy to implement blockchain-based civic systems must include contingency plans and likely a **hybrid approach (using off-chain where appropriate, keeping critical parts on-chain)** until we're confident in full on-chain scaling.

Privacy Concerns vs. Transparency

Earlier, we praised radical transparency as a tool for accountability. However, **privacy is a fundamental right and necessity** for many aspects of civic life. There is an inherent tension: blockchain ledgers are typically transparent (at least pseudonymously), so how do we ensure individuals' privacy and prevent surveillance or discrimination? This is especially pertinent if people's main interactions (economic transactions, voting, receiving benefits) are on a public ledger. In a worst-case scenario, *an overly transparent system could enable new forms of social control*, if, for example, all spending or political donations are traceable and linked to identities.

Labor rights included aspects of privacy – e.g., the right to secrecy of the union ballot, or protections against employer snooping into one's personal life. In a blockchain civic system, we must replicate those protections. **Zero-knowledge proofs (ZKPs)** and **privacy-preserving cryptography** are the primary tools to achieve privacy on public ledgers. These allow verification of statements (like "this person is eligible" or "this vote is valid") without revealing underlying private data. Projects like **Zcash** showed you can have encrypted transactions that still validate against a ledger via ZKPs. In governance, research prototypes allow **secret ballots on Ethereum** using mixnets or ZKPs, though they are complex and not widely deployed yet.

Another approach is **selective transparency**: for example, making aggregate data public but individual data private. Or having hierarchical access – e.g., a watchdog organization can audit detailed data under certain conditions, but the general public only sees summaries. This, however, reintroduces some trust in gatekeepers, so it must be balanced.

The **Worldcoin debate** underscores privacy fears: even if the intentions are good, people worry about a giant biometric database (even if hashed). Similarly, a global UBI ledger that listed all individuals could be a juicy target for misuse (imagine a regime getting hold of it to target dissidents, etc.). Therefore, **decentralization must extend to data minimization**: store only what is necessary, encrypt wherever possible, and give individuals agency over their info. Sovrin's model of **pairwise pseudonymous DIDs** (a unique DID for each relationship, so it's hard to correlate activities across contexts) is one way to protect privacy by design.

Regulatory compliance is another facet: privacy laws like GDPR demand the right to be forgotten, data consent, etc. Blockchains by nature *don't forget* (immutability). This is a conflict. Solutions like not putting personal data on-chain, or using one-way cryptographic commitments that can be "revoked" by losing a key, are considered. But legal challenges remain; European regulators have pondered whether public blockchain nodes are effectively data controllers under GDPR. A balanced approach might involve combination of on-chain and off-chain storage where needed, plus user-controlled encryption keys.

There's also a risk of **de-anonymization** in ostensibly pseudonymous systems. If someone's addresses or behavior can be linked (through analytics or hacks or voluntary disclosure), their entire history might become visible. For example, if a privacy mechanism is weak and someone links your vote to your identity, your voting record could be exposed – a serious breach of democratic secrecy that labor ballots were careful to guard. Therefore, robust privacy tech is not optional; it's essential to prevent *a blockchain Panopticon*.

Social acceptance will depend on privacy guarantees. If people fear that using a blockchain civic system means sacrificing their privacy, they will resist or seek alternatives (maybe even violent ones if they feel

oppressed by surveillance). One could argue many people already give data to private companies with little care (social media etc.), but when it comes to core rights and money, attitudes can change – plus, handing data to Facebook is different from it being irrevocably public on a ledger.

In summary, **any blockchain-based civic contract must build in strong privacy protections** to be legitimate and to mirror the freedoms that labor rights and human rights have fought for. This can be done with technology (ZKPs, differential privacy, etc.) and policy (open governance of what data is collected, with privacy impact assessments). Getting privacy right will likely involve cutting-edge cryptography and perhaps a gradual increase in what is made transparent as techniques improve (e.g., maybe start with higher privacy, then selectively open up data categories that are safe to share and beneficial for accountability).

Legal and Regulatory Uncertainty

The intersection of blockchain systems with existing legal and political frameworks is a complex and evolving area. **Labor rights historically were enshrined in law** – if a company violated them, courts or regulators could intervene. In a decentralized system, **what is the legal status of DAOs, smart contracts, and digital rights?** Currently, much of the world lacks clear legal recognition for things like DAOs or smart contracts (though some jurisdictions are pioneering, e.g., Vermont's blockchain-based LLCs, Wyoming's DAO LLC law).

Uncertainty about liability and enforcement is a major risk. For instance, if a decentralized UBI smart contract fails to pay someone due to a bug, can they sue anyone? Who is responsible – the developers (maybe anonymous), the validators, the DAO token holders? Today's legal system isn't well-equipped to assign liability in such a diffuse context. This could leave individuals without recourse if something goes wrong. Labor law evolved to allow workers to sue or claim compensation for employer misconduct; in a blockchain future, if an algorithm mistreats you, can you take an algorithm to court? Possibly regulators will force there to be some entity that can be held accountable (this is a current debate: making DAOs establish a legal personality so they can be sued or enter contracts).

Regulatory compliance is another facet: financial regulations, identity (KYC/AML) rules, data protection laws – all these apply. Many blockchain initiatives operate in a gray area or deliberately in a decentralized manner to avoid certain regulations (for better or worse). But when scaling to societal functions, they will come under scrutiny. For example, if a blockchain voting system is used in a state election, it must comply with election laws, accessibility requirements, etc. If a decentralized identity is used for legal identity, how does it reconcile with state-issued documents? Some cooperation with governments might be needed, which introduces political risk (e.g., governments might demand backdoors or try to co-opt the system for surveillance).

Governments might also resist ceding power to decentralized systems. Labor unions often faced hostility from governments in early days; similarly, one can envision governments viewing a parallel blockchain social system as undermining their authority. Already, we see varying attitudes: some countries embrace blockchain for governance (like using it for land registries or voting pilots), others ban crypto (e.g., China cracked down on crypto, though interestingly still uses some blockchain tech domestically for tracking). If a government feels threatened – say, people choose a community DAO's decision over a law – there could be conflict. For example, what if a global UBI via crypto reduces people's dependence on a government's patronage? That government might ban it to maintain control.

Jurisdictional issues: Blockchain networks are borderless, but laws are not. A person might have a "right" on-chain that is not recognized off-chain in their country, or vice versa. This gap could cause issues. If someone's on-chain identity says they are a verified person to receive UBI, but their government says that's illegal, they might face penalties for participating. Conversely, if on-chain governance votes to, say, provide funding to an activity illegal in some country, does that put participants at legal risk? These uncertainties can deter participation or fracture the system by geography.

Integration with existing institutions: In reality, we may not fully "replace" labor rights enforcement overnight but rather integrate blockchain solutions into a hybrid model with current institutions. During a transition, clarity is needed on how smart contracts and DAOs interface with courts, law enforcement, etc. For instance, if a court orders the seizure of someone's assets for a crime, and those assets are locked in a smart contract, how is that executed? Without an interface, authorities might attempt to force miners/validators to comply (as seen in cases where governments pressured Bitcoin miners or Ethereum validators to censor certain transactions under sanctions law). This sets up a tension between **the uncensorability of blockchain vs the requirements of law**. Resolving this might entail legislation that gives smart contracts some recognized status – perhaps akin to legal contracts – and also establishing that certain decentralized governance decisions are binding in law.

Encouragingly, some jurisdictions are working on **DAO legal personhood** (e.g., the Marshall Islands passed a law recognizing DAOs as legal entities). The UK Law Commission has studied how English law can accommodate smart contracts and DAOs. These are incremental steps towards a legal framework where, say, a DAO can own property, hire contractors, and be sued if it violates obligations. That might sound counter to pure decentralization, but it can provide accountability. The challenge is doing so without undermining the core benefits – if you centralize a DAO just to make it legible to law, you lose much.

In summary, **legal ambiguity is a big risk factor** for any large-scale blockchain civic project. It could result in litigation, enforcement actions (we've seen the SEC crack down on certain token projects as unregistered securities, for example), or user hesitance. Overcoming this will require engagement between technologists and policymakers to craft new frameworks. The new social contract might not be purely code-based; it will likely be a combination of code and law. Normatively, one could imagine new laws that *enshrine certain blockchain-based rights* (e.g., a law might guarantee the right to a digital identity that you control, or recognize a smart contract-based vote in a cooperative as legally valid). But getting there will take time, and in the interim, **uncertainty itself is a risk** – it may slow adoption or leave early adopters exposed.

Adoption, Accessibility, and the Digital Divide

Even if we build the perfect blockchain systems for a post-labor society, **will people use them?** Will *all* people be able to use them? There is a genuine risk that these innovations could end up accessible primarily to the tech-savvy or the well-resourced, thereby **exacerbating inequality instead of reducing it**. Consider that currently, participating in DeFi or DAOs requires at least a modern smartphone or computer, reliable internet, some education on managing keys, and often knowledge of English (since much documentation/interface is English-centric). Many of the world's poor – who are supposed to benefit the most in a world without jobs – **lack one or more of these prerequisites**.

Digital literacy is a major barrier. Using blockchain wallets, understanding seed phrases, avoiding scams, etc., is non-trivial for newcomers. Millions have fallen for phishing scams in crypto or lost funds by user error. If critical civic rights or income depend on using these tools, those with lower education or tech

exposure might struggle or become victims of fraud. This is analogous to how uneducated workers historically were more easily exploited until labor orgs provided education. We might need robust public education programs in digital finance and security, or design systems so intuitive that even those with minimal literacy can use them (imagine biometrics to recover keys – though that has its own issues). **User experience (UX)** of blockchain apps must dramatically improve to reach a broad population. The average person shouldn't have to know what a "hash" or "gas fee" is to exercise their rights.

Infrastructure access is another issue. Billions still have limited internet access or none at all. If civic systems go online and on-chain, those offline are left out – akin to not having a factory job in the industrial era left one destitute. Expanding internet access (via community networks, satellites like Starlink, etc.) might be considered part of the new social contract (some argue internet access is a human right now). But if that doesn't happen quickly, we must ensure alternative access points. Maybe community centers, local intermediaries or **bridge organizations** (like NGOs helping people access digital services) will play a role. However, involving intermediaries reintroduces trust and potential gatekeepers.

The **elderly and persons with disabilities** might face difficulties with new tech. Labor movements often fought for inclusivity in the workplace; similarly, we must ensure inclusive design – e.g., voice interfaces for the blind, multilingual support, accommodating cognitive impairments with simpler flows. The risk is that early implementations cater to crypto enthusiasts and overlook others.

Cultural barriers: People may not trust a faceless system. Many rely on personal relationships – a local banker, a government caseworker – and might be uncomfortable dealing with a "black box" algorithm for their needs. Trust-building measures, like community demonstrations, user-friendly narratives (not just "it's decentralized trust us" but showing in concrete terms how it benefits them) will be essential. Otherwise, adoption might skew to younger, urban populations, leaving others in legacy systems and potentially worse off if resources shift to the new system.

Transition period complexities: During any changeover, there will be a mix of old and new systems. People might have to juggle both, causing confusion. If not handled carefully, this could lead to some falling through cracks (imagine someone failing to claim their blockchain UBI because they missed some step, similar to how some don't claim benefits they're entitled to due to bureaucracy today).

Another risk is **public perception and backlash**. Blockchain is often associated in media with scams, volatility, or libertarian agendas. Rolling out blockchain-based governance might face skepticism ("Is this just a new Bitcoin scam?") or ideological resistance ("We don't want governance by algorithm"). Effective communication and gradual introduction of these tools in a way that highlights their tangible benefits will be necessary. Otherwise, political pushback could scrap good initiatives (for instance, a city's plan for blockchain budgeting might get derailed by controversy if not explained well).

Finally, the **global divide**: adoption may advance faster in some regions than others. If some countries forge ahead with, say, DAO-based governance and others lag, this could create international imbalances. Perhaps in progressive wealthy societies, labor may be obsolete and blockchain systems in place, while in poorer or more traditional economies, labor might still be in use but with weakened rights and no new system to fill the gap – essentially the worst of both worlds locally. This scenario could drive even more migration or brain drain to places where the new social contract is implemented, widening inequality between countries. Ideally, these technologies should be used to uplift the globally marginalized, not just

the already advanced. That will require international cooperation and knowledge transfer, akin to how labor standards were promoted across borders via organizations like the ILO (International Labour Organization).

In summary, **the risk of leaving people behind is real**. It would be a cruel irony if the tools meant to empower the masses in a post-labor world ended up empowering primarily a tech-savvy elite. Avoiding this outcome means investing in education, ensuring intuitive design, bridging digital divides, and phasing changes in a humane way. Essentially, "no person left behind" should be a guiding principle, as it was for labor advocates fighting child labor, sweatshops, etc. If we treat access to the blockchain-based civic infrastructure as we did access to basic education in the 20th century (a necessity for all), and plan accordingly, we can mitigate this risk.

New Forms of Exploitation and Abuse

Every technology can be misused, and blockchain is no exception. We must be vigilant for **novel forms of exploitation** that could arise in a blockchain-governed society, so that preventing them can be part of the design (just as labor law evolved to curb new exploitative practices during industrialization).

One concern is **"economic coercion by protocol"**. For example, imagine a scenario where an entity (could be an AI corporation, or a wealthy individual) accumulates a large share of a governance token and then **bribes or extorts the community** to sway decisions ("I'll dump the token and crash your system unless you pay me or pass this proposal"). This is a sort of hostile takeover akin to company raids, but at a societal scale. Mechanisms like **quadratic voting** help by making buying influence more expensive, but aren't foolproof if someone is resourceful enough. We might need *anti-bribery techniques* (there's blockchain research on vote-privacy to prevent vote-buying, etc.).

Another risk is **digital fraud and scams** targeting individuals. If everyone has a blockchain wallet for their UBI or identity, scammers will target them (phishing for keys, fake support lines, etc.). We already see endless crypto scams – these could proliferate as more regular folks enter the space, potentially wiping out livelihoods. Without an employer or government fallback, a person scammed out of their crypto savings is in trouble. Traditional finance has fraud protections (banks can reverse transactions in some cases, etc.), whereas blockchain typically doesn't. So new protections are needed, perhaps community-run insurance funds or reputational systems to mark malicious addresses.

Data harvesting and profiling could become a new exploitation method. Even with pseudonyms, big data analytics might find patterns linking transactions to individuals, enabling companies or political actors to profile people extensively. For instance, if vote tokens or preferences leak, one could build dossiers to manipulate communities, akin to Cambridge Analytica but with richer data. Labor unions historically protected workers from some employer surveillance; in the future, who protects citizens from blockchain analytics? This ties back to privacy and the importance of ZKPs.

We should also consider **algorithmic bias or errors causing harm**. If more of life is governed by smart contracts or DAOs, a flaw in their logic (or a bias in an AI oracle feeding them) could systematically disadvantage some group. For instance, if an AI decides on resource distribution and has bias in training data, it might allocate less to certain demographics. With labor unions and democracy, those groups could protest; in a fully coded system, the bias might go unaddressed unless consciously monitored. Ensuring **algorithmic accountability** and the ability for humans to correct unfair outcomes is crucial (even if code is

“law”, there must be a legal or governance override when code is unjust – a lesson from The DAO, where humans intervened).

Exploitation of loopholes: savvy actors might find unintended ways to game blockchain systems, similar to regulatory arbitrage in finance. For example, someone might create thousands of Sybil identities that slip past proof-of-personhood if the system isn’t airtight, and claim many UBI shares – depriving the real people of resources. Or malicious validators could collude to censor certain users (imagine a future where a consortium of validators doesn’t like the political leanings of a community and blacklists their transactions). These are exploits of governance and infrastructure that need contingency plans (like diverse validator sets, social slashing where the community forks away from bad actors, etc., but those are drastic and messy remedies).

Criminal misuse: Just as criminals use crypto for money laundering, they could use decentralized identity to mask activities or DAOs to coordinate illicit enterprises out of reach of law (there have been cases like a dark net marketplace considering itself a DAO). If law enforcement finds itself hamstrung by strong encryption and decentralized networks, there could be a backlash or an arms race undermining the stability of the system. Society will have to adapt legal processes (e.g., forensic blockchain analysis is growing, but criminals adapt too, using mixers etc.). The new social contract has to include ways to address crime and disputes – areas where historically the state (and indirectly labor through union-backed political movements for rule of law) played a role.

Loss of human oversight and empathy: One could see as a form of exploitation if people become at the mercy of rigid algorithmic rules with no flexibility. Labor negotiations allowed for human factors (hardship cases, special exceptions). In a purely code-run welfare distribution, someone who loses a key or makes an error might get no recourse – that could feel exploitative or at least inhumane. We may need built-in “circuit breakers” not just for hacks but for mercy: e.g., community moderators who can, by multi-signature consensus, restore someone’s access or grant an exception in edge cases (though that introduces a bit of centralization – always a trade-off).

Finally, **unequal influence through technology**: There’s a risk that those who build and maintain these blockchain systems (developers, large node operators) become a new elite if they are not accountable. In labor terms, this is like the managerial or technical class having power over workers. If open-source communities remain meritocratic but also somewhat dominated by Western developers, the system could inadvertently encode their values and overlook others’. Ensuring diverse participation in protocol development is important to avoid exploitation via cultural bias or neglect of certain communities’ needs.

In summary, **vigilance for new exploitation vectors is essential**. Many of these boil down to **power imbalances re-emerging in different guises** – whether through wealth, technical savvy, or algorithmic control. The design of a blockchain-based civic contract should incorporate checks akin to how labor rights laws had checks on corporate power. This could include: anti-monopoly rules for token holdings, continuous auditing of algorithms for fairness, emergency human governance layers for redress, community insurance and support schemes for those who suffer losses, etc. Just as the early industrial age had to invent regulatory and social innovations to tackle child labor, sweatshops, company towns (where workers were paid in company script usable only at company stores – interestingly analogous to potentially being locked into one platform’s token ecosystem), the blockchain age will need new rules to tackle the issues above.

Having mapped the major limitations and risks, it's clear that *technology alone is not enough* – the social and governance layer around it is equally vital. In the next section, we will shift to a constructive mode: proposing frameworks, norms, and policy ideas for **designing a blockchain-based civic contract** that maximizes the benefits we discussed while mitigating these pitfalls.

Proposals and Frameworks for a Blockchain-Based Civic Contract

Designing a new civic contract for a world beyond labor is a profound challenge – one that demands not only technical innovation but also institutional creativity and ethical grounding. In this section, we outline **normative proposals and frameworks** that could guide the development of a **blockchain-based social contract**. These recommendations synthesize insights from the case studies, attempt to address the risks discussed, and draw inspiration from political economy and systems theory. The goal is to imagine structures that restore equilibrium and fairness in a society where traditional labor leverage is gone, using blockchain and cryptography as foundational tools.

We organize the proposals into key areas:

- **Democratic Governance Models for Decentralized Systems** – ensuring broad, equitable participation and preventing elite capture in blockchain governance (e.g., quadratic voting, soulbound reputation tokens).
- **Economic Security and Public Goods in a Post-Work Economy** – mechanisms like blockchain-based UBI, AI dividends, and decentralized public goods funding to replace the income and social safety functions of labor.
- **Data Dignity and Digital Rights** – policies to guarantee individuals control over their data, identity, and privacy, akin to labor rights for the digital self.
- **Accountability and Rule of Law in Algorithmic Governance** – frameworks for auditing and intervening in smart contract systems to align with human values and legal norms, including integrating with traditional institutions.
- **Bridging the Transition** – strategies for implementation, education, and inclusion to ensure a smooth transition to these new systems without leaving anyone behind.

Throughout, we will use bullet points and structured heuristics where applicable to make the ideas clear. We will also cite analogous ideas from thinkers and related movements. For example, Glen Weyl and colleagues' concept of a **"Decentralized Society (DeSoc)"** and **soulbound tokens (SBTs)** offers a rich vision of embedding trust and cooperation in Web3, which we incorporate. Likewise, concepts of **open cooperativism** and **"radical markets"** inform our proposals for shared ownership and governance.

1. Embrace Pluralistic Governance: Quadratic Voting, DAOs with Soulbound Tokens, and Participatory Polity

To prevent the concentration of power and ensure that **post-labor governance is truly by and for the people**, we propose a **multi-faceted democratic governance framework** for blockchain-based institutions:

- **Adopt Quadratic Voting/Funding as a Standard:** Decision-making in decentralized systems (be it allocating funds, or voting on policies) should use **quadratic mechanisms** to amplify the voice of the many over the money of the few. *In quadratic voting, each additional vote for a choice costs*

exponentially more tokens, so stakeholders with limited tokens can collectively outweigh a wealthy minority. This should be baked into DAO platforms and considered for any collective choice – from budgeting public resources (as Gitcoin does) to electing representatives in a decentralized community. **Quadratic funding** should likewise be the norm for public goods financing, as it "ensures everyone has a voice, no matter the size of their donation". These mechanisms operationalize the principle of political equality that labor unions fought for in the workplace, now applied to the digital commons.

- **Leverage Soulbound Tokens (SBTs) for Merit and Trust:** Introduce **non-transferable "soulbound" tokens** to represent individual credentials, commitments, and reputations in DAO governance. Because SBTs cannot be sold, they serve as proof of **past contributions and trustworthiness** rather than wealth. For example, an environmental DAO could issue SBTs to volunteers who have done community work; those SBTs might grant extra voice on proposals about environmental issues (since those individuals have proven commitment). This idea resonates with giving "one person, one vote" in worker co-ops, but more granular – *one contribution, one unit of earned influence*. In the envisioned **Decentralized Society (DeSoc)**, Souls (individuals) carry a basket of such SBTs that encode their affiliations and achievements, enabling richer, *pluralistic* governance that rewards cooperation and long-term involvement. By using SBTs, we reduce the risk of plutocracy and Sybil attacks: you can't buy reputation or easily fake a history of community service. **Heuristic:** Whenever designing a DAO or tokenized decision system, ask *"Can we replace or augment a transferable token with a soulbound credential that better captures what we value?"*

- **Participatory Budgeting and Policy DAOs:** Create DAOs at various levels (local, sectoral, global) where citizens can directly **vote on budgets and policies**. This draws from the concept of participatory budgeting (successfully tried in cities like Porto Alegre) but executed via smart contracts for transparency. For instance, a city could have a **CityDAO** where residents (verified by decentralized ID) vote on how to allocate a public fund – perhaps using quadratic voting to rank projects. In a world without labor unions negotiating municipal spending or welfare, this gives citizens a new lever to influence resource distribution. Because the voting and funding would be on-chain, results are **enforced automatically** (money goes where the vote decided) and **visible to all**, reducing corruption. **Policy proposal DAOs** could similarly crowdsource and vote on proposals which the elected government is compelled (or at least morally pressured) to consider. Over time, as these prove their reliability, government functions might even be delegated to them by law (for example, a law could stipulate that a certain percentage of budget *must* follow the outcome of a citizen DAO's decision).

- **Multi-Stakeholder Governance Councils:** Not everything can or should be decided by direct mass vote. Borrowing from **co-determination models** (like worker representation on company boards), establish **governance councils for major blockchain networks or public DAOs that include representatives of various stakeholder groups**: developers, users, perhaps randomly selected citizens (a "citizen jury"), and even AI (if representing algorithmic stakeholders). These councils can serve as a check and deliberative body, providing expert input and oversight on code upgrades or emergency situations. Crucially, they should be accountable – e.g., council members could be periodically confirmed or rotated via community vote/SBT merit, and their discussions should be recorded publicly (except where privacy requires otherwise). This introduces a **systems-theoretic feedback loop**: the council can be seen as a moderator subsystem ensuring the overall system

doesn't veer into unstable or unjust states (analogous to how labor arbitration councils resolved disputes, but here proactively guiding protocol evolution).

- **Constitutional DAO and Algorithmic Ombudsman:** At the highest level, consider establishing a **"Constitutional DAO"** which encodes fundamental principles (e.g., privacy rights, non-discrimination, right to appeal) that all other smart contracts and DAOs in the ecosystem must adhere to, somewhat like a digital constitution. This DAO's membership could include broadly trusted figures or entities and perhaps every citizen via an SBT of citizenship. It would have the power to review and veto (or mandate changes to) smart contracts or policies that violate core principles (e.g., a DAO proposal that attempts to exclude a minority group would be struck down for violating the equality clause). Additionally, an **Algorithmic Ombudsman** function can be created – an AI or human-AI committee that continuously audits algorithms for bias or errors and field complaints from users who feel wronged by automated decisions, working with the Constitutional DAO to remedy issues. This ensures that **unstoppable code does not become unaccountable code**. Essentially, this is a *governance layer above code*, something technologists like Vitalik Buterin have suggested in advocating for "explicit social governance" to override code in extreme cases. While it may seem to reintroduce human control, it's humans collectively via transparent processes, not opaque bureaucrats.

These governance proposals align with the idea that **pluralism and broad participation create more resilient and fair systems**. In effect, we're recombining the **civic structures that balanced industrial capital** (unions, democratic legislatures, works councils) into new forms suited for decentralized networks. By doing so, we aim to replicate the bargaining power and voice that labor provided, but in a digitally-mediated, post-work context.

2. Economic Security for All: Blockchain-Based Universal Basic Income and Public Ownership of Productive Capital

One of the core promises to fulfill in a world without labor is that **everyone's basic needs and well-being are ensured**, even when wages are no longer the norm. This was historically addressed through labor wages, union-won benefits, and welfare states funded by labor taxes. We propose a combination of **blockchain-driven economic mechanisms to guarantee economic security and to socialize the gains of AI/robotics**:

- **Implement a Universal Basic Income (UBI) via Smart Contracts:** Establish a **UBI DAO** that regularly disburses a base income to every verified person (using the proof-of-personhood identity system). Funds could come from various sources – for example, a portion of taxes or fees collected from AI companies (see below on AI dividends), voluntary contributions, or even newly minted crypto if managed carefully to avoid inflation. The **payout mechanism** would be a smart contract where, say, every month it checks the list of eligible World IDs (or Sovrin DIDs marked as citizen) and sends each a fixed amount of digital currency. This is done automatically, **without bureaucratic delay or discrimination**, and with **full transparency** of the aggregate outflow (ensuring public oversight that the program isn't being gutted). Some projects like Circles UBI and Proof of Humanity's UBI token have piloted this, but a larger scale implementation might use a stablecoin for predictable value. **Key design elements:**

- Use **tiered UBI** if necessary: e.g., a global minimum and optional supplemental UBI from local communities or nations (where local DAOs can top-up the global amount based on cost of living or policy choices).
- Build in **opt-in community service linking**: not to make UBI conditional (it should remain unconditional to avoid replicating labor coercion), but to encourage contributions, UBI recipients could be nudged to volunteer or take courses, earning additional SBT credentials that might qualify them for bonuses or just to build social capital. This ties into Glen Weyl's notion that *UBI alone is not enough without a productive model around it*; we plug UBI into a larger ecosystem of commons-based production and cooperative work (discussed further below).

- Ensure **funding sustainability**: The UBI DAO should have a clear revenue model (likely through taxing capital or commons revenue) to continuously fund payments. A **normative proposal** is that *a portion of all gains from automation should flow into the UBI DAO*. This can be achieved by smart contract "taxes" on transactions of certain tokens or through agreed profit-sharing (for example, if an AI is deployed commercially, its smart contract could automatically remit X% of revenue to the UBI pool).

- **Create an "AI Dividend" – Common Ownership of Automated Capital**: In line with thinkers like Yanis Varoufakis or tech leaders (Altman) who suggested taxing AI, we propose a more direct approach: **tokenize the ownership of AI/robotics enterprises and distribute those tokens widely to the public**, so that capital income is shared. Concretely:

- For each major AI/robotic project (say a company deploying autonomous vehicles or an advanced AI service), require that a significant share of its equity or revenue is represented by a **token that is held by a public trust** or distributed as **"Citizen Tokens"** to all. These tokens entitle holders to dividends (profits) or usage rights of the service.
- Use smart contracts to **automate the collection and distribution** of these dividends. For instance, if an AI DAO generates profits from selling services, its code could split the profit: reinvest some, and send the rest to a **"Public Wealth Fund"** contract. This public fund then periodically distributes to individuals (possibly feeding into the UBI system). Alternatively, it could fund public goods like education, healthcare – replicating what taxes used to fund, but via protocol.
- Essentially, this treats productive AI and infrastructure as part of the **commons** from which all should benefit, an idea akin to "technological socialism" or "open cooperativism". The blockchain ensures transparency: anyone can see that, say, **the World AI Fund smart contract** received X from company Y this quarter and paid out Z per person or Z to local project grants, etc.

- **Heuristic/Framework:** Implement a **"Commons Contribution Protocol"** where any automated system above a certain productivity threshold must be plugged into a smart contract that enforces contribution to the commons (similar in spirit to carbon credits but for automation). This can be voluntary or mandated by new policies. One can imagine a **policy DAO coalition** lobbying for such integration, making it a social norm or legal requirement.

- **Decentralized Public Goods Provision through DAOs:** Expand on Gitcoin's model to broader public goods: not just open software, but research, environmental restoration, infrastructure. Launch specialized **Public Goods DAOs** (or Quadratic Funding rounds) for areas like healthcare research, local community improvement, journalism, etc. These DAOs use **crowd sentiment and matching funds** to allocate resources. Funding can come from the AI Dividend above, philanthropy, or government budgets rechanneled through these mechanisms. This democratizes how public

resources are used, effectively replacing what was often negotiated in political processes heavily influenced by labor groups, with a more direct participatory process.

- Example: A **Health DAO** receives a pot each year (from a global health token, funded by a Tobin tax on pharma profits or something); citizens vote on which health issues or research to prioritize (perhaps with quadratic voting to ensure broad consensus). Funds are then granted accordingly via smart contract. This introduces *participatory planning* into domains traditionally top-down, guided by collective intelligence.

- **Encourage Platform Cooperatives and Data Unions**: Use blockchain to facilitate **cooperative ownership models** for digital platforms and data. For instance, drivers of a ride-sharing service could form a DAO coop, each with tokens earned by driving, collectively owning the platform. Smart contracts would distribute revenue among drivers based on clear rules, and drivers vote on policies (like price setting or introducing services). This is essentially using blockchain to scale the cooperative movement, which historically gave workers stake and voice (Mondragon etc.), into the era of gig work and digital platforms. The **regulatory proposal** here is to treat algorithmic platforms as utilities that workers can collectively run, or at least ensure any platform using gig labor issues **"labor tokens"** to its workers, representing profit shares.

- Similarly, **Data Unions**: groups of individuals pool their personal data and negotiate its sale to AI firms via smart contracts (ensuring anonymity and fair compensation). Projects like Ocean Protocol and Streamr have piloted aspects of this. The idea is to treat individuals' data contributions as a form of labor/capital that must be paid. Glen Weyl calls this **"data as labor"**, aligned with giving individuals property rights over their data. A normative framework could require AI companies to obtain data through such consensual unions rather than free scraping, enforced by law or by the data providers only releasing through these protocols.

The overarching theme of these proposals is to **institutionalize economic solidarity and shared prosperity through code**. In effect, we are trying to simulate what strong unions and social democracies achieved – wage floors, profit-sharing, public goods – through automated, global and participatory means. This addresses the system-theory insight that without labor's counterweight, wealth concentrates; so we build **feedback loops** (UBI, AI dividends) that automatically redistribute wealth and maintain equilibrium.

It's also aligned with Polanyi's idea of **re-embedding the market in society** – here, we embed markets in smart contract rules that reflect social goals (like universal welfare) instead of pure profit. Importantly, these mechanisms should be **enshrined in a binding way** (like the UBI contract runs autonomously, not at the whim of political cycles), giving individuals predictable security.

A cautionary point: "UBI alone is not enough" – it should be part of a **holistic model including opportunities for meaningful participation in production and community**. Hence, we emphasize cooperatives and public goods work, so people can still find purpose and contribute even if traditional jobs are scarce. Blockchain can support that by lowering coordination costs (co-ops across borders, micro-contributions recognized via tokens, etc.).

3. Self-Sovereign Identity and Data Dignity: A Bill of Digital Rights

Just as labor rights came with a notion of respecting the worker's humanity (no exploitation, right to privacy, freedom of association), a blockchain-based society needs a **Bill of Digital Rights** to protect individuals in the digital realm. Key proposals include:

- **Universal Self-Sovereign Identity (SSI):** Make self-sovereign identity a **public good and a human right**. Concretely, every person from birth (or whenever they come online) should be provisioned – perhaps by a public authority in collaboration with open-source projects – a **sovereign digital identity wallet** that they (or their guardians) control. This wallet holds their credentials (citizenship, education, etc.) as **verifiable credentials (VCs)** signed by issuers, and only the individual can consent to sharing them. Governments and institutions would need to legally recognize these credentials (e.g., recognize a digital diploma or license presented via SSI as legally valid).
- **Policy idea:** Pass "**Right to Identity and Data Ownership**" laws that ensure individuals own their personal data and credentials, similar to property rights. For instance, California's Consumer Privacy Act hints at this, but we can go further: *any organization collecting personal data must issue it back to the individual in a machine-readable, portable format (perhaps as a verifiable credential) for their SSI wallet*. This flips data control.

- **Implementation framework:** Use existing standards (DID, VC) and networks like Sovrin or Ethereum-based identity to roll out national SSI programs. Some countries (Estonia, etc.) are close – they give e-ID with cryptographic keys to citizens. The proposal is to anchor these in decentralized networks rather than government databases where possible, to ensure censorship-resistance and global interoperability.

- **Zero-Knowledge Proof Infrastructure for Privacy:** Invest in and deploy **zero-knowledge proof systems** at scale for everyday interactions. This means:

- Voting systems where you prove you're eligible and have voted, without revealing who you voted for.
- Age/attribute proofs (prove over 18 without giving birthdate, etc.), important for preserving privacy in on-chain KYC or accessing age-limited services without creating databases of personal info.
- Financial transactions where amounts or identities can be shielded unless certain conditions (like a legal warrant) are met – e.g., using Zcash-like shielded transactions for government aid disbursements to protect recipients' financial privacy.
- Essentially, make privacy tech the default in public systems: **"Privacy by design"** should be mandated. Any new social dApp (decentralized app) that handles personal data should integrate ZKPs or privacy layers, and get perhaps certification (like privacy "UL listed").

- **Normative goal:** Achieve **radical transparency for systems and institutions, but radical privacy for individuals** – a principle often voiced by transparency advocates. For example, a public budget DAO's overall flows are transparent, but individuals' personal balances or choices remain private unless they choose to disclose.

- **Decentralized Data Governance and Consent:** Give individuals fine-grained **consent tools** through their identity wallet for how their data is used. This can be done with smart contracts:

- Example: A person's SSI wallet could have a **"data vault"** where third parties can request access to certain data, but the individual's agent sets conditions (maybe even micropayment required, or only

for a limited time, etc.). Solid (Tim Berners-Lee's project) and others envision such personal data pods. Blockchain could facilitate logging all access in an immutable way, so misuse can be traced (like an audit log – "which entities accessed my data and for what purpose").
- Establish **Data Unions** (as mentioned) where people pool and collectively negotiate data sharing – this not only provides compensation but also an additional layer of consent (the union's smart contract might only share aggregate data or only with ethical AI projects, etc., as determined by members).

- **Legal reinforcement:** Expand privacy laws to give teeth to personal data rights – e.g., heavy penalties for companies that take data without a credentialed proof of user consent. Possibly create an international *Data Rights Organization* similar to the ILO for labor, but focused on digital rights, to set standards that tech cos and governments should follow.

- **Right to Algorithmic Explanation and Appeal:** People should have the right to **understand and challenge automated decisions** that affect them (echoing the "right to explanation" in GDPR). In a blockchain context:

- If a smart contract denies someone a benefit or flags them as suspicious, they need a method to inquire "why?" and an avenue to appeal (perhaps to that Algorithmic Ombudsman or Constitutional DAO mentioned).
- *Heuristic:* Design smart contracts with an **"appeal function"** – e.g., funds are not permanently lost or an action not permanently taken until a short window passes where the user can submit an appeal (could be a transaction with evidence to a designated DAO arbitrator). Only after that window, the action finalizes. This introduces a bit of delay (and someone must handle appeals), but it builds trust that the system isn't absolute and unfeeling.

- For less critical things, at least provide transparency of algorithmic rules (if it doesn't compromise security). If an AI is used, perhaps use **open source AI or auditable AI** so that biases can be spotted. A person might not get a personalized explanation from a neural net easily, but they should get an *audit trail* – e.g., "these were the input factors and weights that led to the decision in your case."

- **Guarantee of Digital Access and Education:** Recognize that having digital identity and rights means nothing if one cannot access the digital realm. So a blockchain-era social contract should include:

- **Universal internet access** – consider internet connectivity a public utility. Possibly fund it partly via aforementioned Public Goods DAOs (there are projects like RightMesh or low-orbit satellites for this).
- **Public digital education** – community centers or online curricula to teach individuals how to use their identity wallets, protect themselves from scams, and engage in DAOs. This is analogous to how unions often educated workers, or how public schools prepared citizens – now digital literacy is civic literacy.
- **Inclusive design mandates** – as part of digital rights, require that critical services (like a UBI app or voting app) adhere to accessibility guidelines (for disabled, elderly). This might mean providing alternative interfaces: voice command, translations, etc., likely a role for government or philanthropic funding to ensure no one's identity/rights are inaccessible due to design neglect.

By codifying these rights and mechanisms, we aim for a **digital world that treats personal autonomy and dignity as sacrosanct**, much as the labor movement insisted a worker is not just a cog but a human with

rights. A citizen in the blockchain society should feel **in control of their digital self (identity, data, reputation)**, not controlled by either states or corporations. This fosters trust in the new systems – people will adopt digital governance if they feel their rights are protected, just as workers embraced labor laws once they saw protections.

This "Bill of Digital Rights" could be literally encoded as a set of guiding principles that DAOs pledge to uphold (possibly enforced by the Constitutional DAO across the ecosystem). It aligns with Don Tapscott's call for a new social contract where trust and privacy are fundamental. And in systems terms, it ensures the **feedback loops of trust and legitimacy**: if people see their data isn't misused and their identity isn't hijacked, they'll continue to legitimize and participate in the system, making it stable and resilient.

4. Hybrid Governance: Integrating Code and Institutions for Accountability

While much of this report envisions decentralized protocols doing what institutions used to, a pragmatic approach acknowledges that **existing institutions (governments, courts, NGOs) will still play a role** and that blending the strengths of code and human judgment yields the best outcomes. We propose **hybrid governance frameworks** to ensure accountability, legal compliance, and flexibility:

- **Legal Recognition and Chartering of DAOs:** Encourage a system where important DAOs (ones managing large public funds or critical services) operate under a **"charter"** that is filed in a legal jurisdiction, essentially getting the rights of a legal entity (as in Wyoming's DAO LLC law). The charter would set out the DAO's purpose, governance mechanisms, and include a pledge to uphold the Bill of Digital Rights and other constitutional principles. This provides a bridge between on-chain operations and off-chain law – e.g., a DAO could be sued if it breaches its charter or causes harm, and it can also access legal systems if needed (like owning real-world property or signing contracts through an elected legal representative). This is similar to how labor unions themselves incorporated and had legal standings to negotiate and sue. The key is to do this without undermining decentralization: the charter should largely point to the code/DAO rules as the source of truth, but adds a wrapper for interfacing with legacy systems.

- **Regulatory Nodes and Oracles:** Bring regulators into the loop by having them run **"observer nodes"** on public blockchains (many regulators already do this for monitoring). Additionally, create **regulated oracle services** that supply data like exchange rates, identity validity, or blacklists of known sanctioned entities to smart contracts. This way, compliance (e.g., with anti-money laundering laws or sanctioned entity bans) can be automated, reducing friction between the crypto world and regulators. For instance, a UBI contract for a certain country could use a government-provided oracle that confirms the person is a citizen (without revealing who, by ZKP) so that it doesn't pay non-citizens if it's not supposed to, etc.

- One controversial but potentially necessary area: **digital courts or arbitration for on-chain disputes**. There are projects like Kleros which act as a decentralized jury for smart contract disputes. Promoting such mechanisms means not every on-chain issue needs to go to a state court – we can resolve many with community jurors (whose decisions are then enforced by smart contracts). However, connecting these to state courts for final appeals or enforcement of off-chain actions (like compelling someone to do something physical) is also needed. So perhaps a **network of arbitration DAOs** recognized by international treaty could be an innovation – a modern version of international arbitration but transparent and crowd-sourced.

- **Algorithmic Transparency and Certification:** For algorithms that impact many (like an AI controlling UBI distribution or moderating content on a decentralized network), set up **independent oversight bodies** – akin to how food and drugs get FDA approval, we might have *Algorithm Auditing DAOs* that certify an algorithm meets certain fairness and safety criteria. This could involve security audits (to avoid The DAO bugs), bias audits (ensuring an AI's outcomes don't systematically disadvantage a group), and performance audits (does it do what it claims effectively?). These oversight DAOs could include experts and citizen representatives, blending expertise with legitimacy. Their findings would be published on-chain (e.g., an NFT badge to the algorithm's contract indicating compliance). Policymakers could mandate that critical algorithms have such certification. This echoes how labor laws mandated things like safety inspections; here it's algorithmic safety inspections.

- **Crisis Management Protocols:** One thing human-run systems handle (not always well, but there's structure) is crises – wars, economic collapses, pandemics. In a blockchain-run world, we should prepare protocols for emergencies:

- For instance, incorporate a **"pause switch"** in major contracts that can be invoked if something catastrophic is happening (like a severe hack or a bug causing huge losses). But guard it: require, say, a multi-signature of a diverse group (the constitutional DAO members, maybe plus an automated trigger if funds drain too fast). Make the use of such a switch transparent and temporary, with a clear plan for resolution. This is analogous to how stock markets have circuit breakers to pause trading in a crash.

- Develop **disaster recovery DAOs** – essentially mutual aid networks encoded in smart contracts to mobilize funds and help in an emergency. These could be funded by a small tax in good times (like insurance). For example, a Climate Disaster DAO that automatically releases aid to regions hit by disaster (verified by oracles) could complement or even replace slow government aid processes. It's a new-age Red Cross but with funds and volunteers managed by smart contracts and local autonomous chapters. This continues the labor movement tradition of mutual aid societies but at scale and speed.

- **Education and Deliberation Phases:** Borrowing from democratic innovations (like citizens' assemblies), incorporate **deliberative phases** in major decisions. For example, if the global UBI amount or AI dividend rate is to be adjusted, don't just throw it to an immediate vote; have a **discussion period** where experts present arguments, simulations are run (perhaps using AI modeling outcomes), and citizen panels (randomly selected token holders) debate and issue a recommendation. Then token holders vote. This two-step process (deliberation then decision) mitigates rash or uninformed choices that pure direct voting can produce. It's the age-old balancing of direct democracy with considered judgment, now facilitated by online tools and maybe DAOs specifically set up to deliberate (like Pol.is surveys or etc. integrated into DAO governance).

- **Collaboration with Governments on Transitional Policies:** While building blockchain solutions, work with forward-thinking governments to implement **transitional hybrid policies**. For instance, a government might run a pilot where a portion of welfare benefits are delivered via a crypto-UBI to a digital wallet, to test the system under their umbrella (like the city of Seoul's blockchain ID initiatives). Or governments could adopt **Quadratic Voting for participatory budgeting** at municipal levels (as some have started doing with paper, but blockchain can make it easier and more

trustworthy). These not only provide testing ground but also get buy-in from public officials and smooth the regulatory path.

The underlying rationale is that **human institutions and decentralized code should complement rather than supplant each other**. Code can provide consistency, transparency, and efficiency; institutions provide judgment, legitimacy, and adaptability. A systems-theoretical view sees this as creating a resilient socio-technical system with multiple feedback channels: on-chain mechanisms handle routine equilibrium, but off-chain institutions monitor the meta-level and intervene if the system's goals (like fairness or stability) are drifting.

Historically, labor rights emerged from both grassroots pressure and enlightened institutional response; similarly, a fair blockchain order will require both bottom-up community action and top-down legal frameworks. The proposals above aim to embed the new social contract *in both code and law*, so that each reinforces the other. This echoes Tapscott's notion of needing a new social contract among business, government, and civil society in the blockchain era – here business might be largely AI-driven, but still, all sectors must collaborate.

5. Building the New Equilibrium: Education, Inclusion, and Evolution

Finally, beyond structural design, a successful transition to a blockchain-based civic society needs soft infrastructure: **education, inclusive practices, and iterative refinement**. Key proposals:

- **Digital Literacy as a Fundamental Civic Skill:** Launch a massive global initiative to provide **education on digital finance, blockchain use, and civic technology**. This could be like a modern WPA project employing people (since jobs might be scarce) as trainers or content creators for educational materials. Imagine something like **"One Person, One Node"** campaign – teaching people not only how to use a wallet but even how to run a node or participate in network validation if they want. Demystify the tech; use popular education techniques akin to how labor organizers taught workers about economics and law. This is important for equity: without education, early adopters (often already privileged) dominate, so making knowledge accessible equalizes the playing field for influence in the new system.

- **Inclusivity and Co-creation:** Ensure that **diverse communities are involved in designing and governing these systems from the outset**. That means proactively reaching out to marginalized groups (the poor, minorities, those in developing nations) and including them in pilot programs and DAO governance. Use multilingual interfaces and outreach (something often lacking in crypto projects which are English-centric). One could set up **Global Assembly DAOs** – think of it as a digital United Nations – where representatives (perhaps elected via communities or randomly selected citizens) from all over deliberate on cross-border issues of the new economy (like climate, global UBI parameters, etc.). This gives a sense of shared ownership of the new social contract across humanity, not just tech hubs. It also helps prevent the system from encoding biases of a few (the "West Coast" tech ideology, etc.) by bringing in, say, indigenous perspectives on data sovereignty or Global South concerns about currency volatility.

- **Gradual Implementation and Dual Systems:** Recognize that old and new will co-exist for some time (the "hybrid economy"). That suggests strategies like:

- **Pilot programs**: as mentioned, trial UBI or DAO governance in small settings (a city, or one sector) and refine before scaling.
- **Opt-in adoption**: allow people to continue with traditional systems or opt into the new system as they become comfortable. For instance, one could choose whether to receive their benefits via direct deposit (old way) or via crypto wallet (new way). Over time, as the new proves superior, more will switch voluntarily.

- **Safety nets**: ironically, we need safety nets for our safety net. If the blockchain system fails for someone (lost keys, bug, etc.), have an *analogue fallback* – maybe a community organization or government office that can verify identity and restore access (with appropriate checks). This prevents tragedies and builds trust that moving to the new system doesn't mean risking everything. Over time, the goal is to reduce fallback usage as systems become fail-proof, but it's crucial in early phases.

- **Continual Evolution and Learning:** The social contract built now should not be static. We should embed **learning and update mechanisms**. This might involve periodic constitutional conventions via the Constitutional DAO, where every few years citizens can propose amendments to how the system works, based on experience (similar to how laws evolve, but here could be faster and more fluid). Also leverage AI and data to monitor how well outcomes match goals: e.g., track inequality metrics, civic participation rates, etc. If despite UBI and such, inequality is rising, recalibrate with new policies (maybe the AI dividend needs to be bigger, or governance more inclusive, etc.). The aim is to create a *cybernetic governance* in the Stafford Beer sense – constantly self-correcting. In complex systems terms, maintain feedback loops at multiple levels – daily transactions level, policy level, meta-constitutional level – to keep the system in a stable, just equilibrium despite changing conditions (like new tech, population changes, climate events, etc.).

- **Cultural Shift and Narrative:** Encourage a cultural narrative that this new system is *not* a dystopian Skynet control grid, but rather the next logical extension of humanity's fight for freedom and dignity. Emphasize continuity with historical struggles: e.g., "As workers in the 20th century won the weekend and pensions, digital citizens in the 21st century are winning data self-ownership and unconditional income." This framing can rally support. Work with artists, educators, influencers to popularize concepts of decentralization and cooperation (like using fiction, games, etc., to let people "live" the experience virtually and get comfortable). Some movements like **RadicalxChange** have already started pushing these ideas in academic and activist circles, but a broader public campaign akin to environmentalism or civil rights in awareness would help. Possibly institute **Blockchain Civics** courses in schools to train the next generation.

Through these and earlier proposals, we foresee a society where: - Everyone has **financial security** (basic needs met via UBI/dividends) and **a voice** (via DAOs, quadratic voting). - Power is not concentrated in a few hands (because of egalitarian governance and distributed ownership of productive assets). - Transparency keeps institutions honest, while privacy preserves personal freedom. - The system is resilient to shocks and can adapt through collective intelligence and feedback.

It's effectively a **new equilibrium**: no one lever (like labor strikes) dominates, but a network of incentives and rules keeps things balanced. Elites cannot easily capture everything because mechanisms like quadratic funding, SBT-based governance, and commons taxation constantly redistribute both power and wealth. The

civic order would align more with merit, contribution, and need, and less with arbitrary privilege or brute force of capital.

In closing: This is a grand vision, undoubtedly challenging. But as history shows, when one paradigm (labor-based industrial society) reaches its limits, societies undergo **great transformations** (to quote Polanyi) and construct new institutions to safeguard human well-being. Blockchain and cryptographic tech, combined with enlightened governance design, give us the toolkit to do so in our era. It falls on us – policymakers, technologists, citizens alike – to *seize this opportunity* and ensure that the coming post-labor world is not a dystopia of inequality and alienation, but a liberated society where **technology serves the public good, and civic life thrives even without traditional work**.

Conclusion

Humanity stands at a crossroads as profound as the Industrial Revolution. Just as the rise of factories prompted the invention of labor rights to rebalance power, the rise of AI and automation forces us to reinvent our civic foundations. This report has explored how **blockchain and cryptographic technologies – far from being mere financial novelties – can form the backbone of a new social contract in a world where human labor is no longer the key engine of economy**. Through a macro-systems analysis, we examined the destabilization caused by the loss of labor's bargaining power and outlined how decentralized, code-based institutions might restore equilibrium by distributing power, wealth, and information in novel ways.

History and theory remind us that power is never static; it flows into whatever structures we build. In the industrial age, labor rights and democratic institutions were the structures that kept capitalist power in check. In the 21st century, we must build **new structures – digital, decentralized, yet guided by human-centric design – to ensure that the immense wealth and capability generated by AI and robotics are shared broadly rather than captured by a tiny elite**. Blockchain, with its transparency, incorruptible execution, and peer-to-peer ethos, offers tools to encode fairness and accountability at the protocol level. But technology alone is not a panacea; indeed, we identified significant risks – from plutocratic token distributions to privacy perils and regulatory hurdles. The journey to a just post-labor society will require **careful blending of technological innovation with social innovation**: new laws, new norms, and continuous civic engagement to steer these systems.

The case studies of Ethereum, Gitcoin, Worldcoin, and Sovrin illustrate both the potential and the pitfalls. We saw glimpses of a future where: *global public goods are funded by the people for the people*; *each person can prove their uniqueness and claim an equal stake in the digital economy*; and *individuals control their identity and data, immune to corporate or state domination*. At the same time, we confronted sobering lessons – that without deliberate design, **inequalities can reassert themselves in the new medium** (be it token whales or biometric misuse). Our evaluation of limitations underscored that **the values which labor movements fought for – equality, security, dignity – must be intentionally re-engineered into the algorithms and governance of blockchain systems**, or else we risk replicating the old injustices in new forms.

We put forward a comprehensive set of proposals: from **quadratic voting and soulbound reputation tokens** that democratize governance; to **blockchain-based UBI and AI dividends** that ensure everyone benefits from automation; to **self-sovereign identities and zero-knowledge proofs** that protect personal freedom in an age of radical transparency. We suggested how existing institutions – governments, legal systems, educational bodies – can pivot and collaborate in this transformation, providing oversight and

support to purely code-driven processes. Importantly, we stressed **inclusion and education**: a social contract is only legitimate if it is understood and shaped by those whom it governs. The new systems must be accessible to all, not only to technologists, echoing the ethos that "nothing about us without us" – the rallying cry of democratic and labor movements through history.

What emerges is a vision of a society where **public agency is not tied to one's employment status but is a birthright of each person**. In this envisioned world: - A **global basic income** provides material security, administered transparently by code and insulated from political whims. - **Decentralized autonomous organizations** give communities direct say in managing resources and solving collective problems, fulfilling the promise of participatory democracy on a scale never before feasible. - **Data and AI are harnessed as commons**, with their benefits broadly distributed and their governance open and accountable. - People are free to pursue education, creativity, care work, or leisure without fear of destitution – the old dream of "automation liberating us" is realized not through corporate benevolence, but through enforceable, egalitarian protocols instituted by society itself.

Of course, this report is but a starting point. Many questions remain: How do we transition from here to there without social upheaval? How to coordinate globally, given different cultures and governments? And how to guard against new concentrations of power that we cannot yet foresee? These will require ongoing research, experimentation, and dialogue. The solutions will likely be iterative – we will learn by doing, as we did when first implementing labor laws and social security a century ago.

One thing is certain: **standing still is not an option**. If we do nothing, allowing AI and blockchain technologies to develop within the old paradigm, we risk a future of extreme inequality – a "rentism" or "exterminism" scenario where the many are disenfranchised. But if we act with foresight and principle, we can usher in an era that future historians might call the **Age of Digital Commons** or **Civic Web3** – a time when society reinvented its core arrangements to ensure human agency and solidarity survived the end of labor as we knew it.

In closing, the challenge of replacing labor rights is daunting, but as we have argued, blockchain and cryptographic tech give us powerful new leverage. Where once workers brandished the strike and the ballot, tomorrow's citizens will wield the **smart contract and the DAO** – tools of collective action encoded in our very infrastructure. The task before us is to design these tools and the surrounding institutions such that they uphold the timeless values of justice, freedom, and community. It is a rare opportunity to **reimagine what a social contract can be**, with the lessons of history in one hand and the technologies of the future in the other. As we navigate this transition, let us be guided by the foundational insight that has always driven progress: *the legitimacy of any economic system rests on whether it serves the people*. By using blockchain to hard-wire the interests of the many into the operations of our economy and governance, we have a chance to create a society that is **more transparent, more inclusive, and more resilient** than anything that came before – truly a new equilibrium for the post-labor age.

Sources:

- Frase, Peter. *Four Futures: Life After Capitalism*. (Summary: Automation can lead to egalitarian abundance or elite dominance depending on social choices.)
- Economic Policy Institute. *Decline of labor unions weakens American democracy*. (Finding: Union decline since 1970s caused wage stagnation and rising inequality.)

- Young, Joseph. *8 Ways Governments Could Use Blockchain for Radical Transparency*. Cointelegraph, 2015. (Quote: Blockchain allows anyone to audit every transaction – radical transparency.)
- Colony Blog. *Challenges in DAO Governance*. (Observation: Unequal token holdings can concentrate power in DAOs, undermining fairness.)
- Time Magazine. *What to Know About Worldcoin…*. (Noting: Altman hopes Worldcoin's crypto ID could enable global UBI; privacy experts like Snowden warn of biometric "ick factor".)
- RWaltz. *Leveraging Blockchain for E-Governance…*. (Point: On blockchain, all transactions visible in real-time, creating perfect audit trails and accountability.)
- Gitcoin's Crypto Altruism Infographic. (Data: Gitcoin's quadratic funding provided $56M+ to public goods, proving community-driven funding works.)
- Sovrin Foundation FAQs. (Concept: Self-sovereign identity gives individuals control – "no one can take their identity away".)
- Buterin, Weyl et al. *Decentralized Society: Finding Web3's Soul*. (Proposal: Use non-transferable soulbound tokens to encode trust networks, enabling sybil-resistant governance that rewards cooperation.)
- Dean, Adam et al. (EPI). *Union decline and inequality*. (Evidence: The loss of labor's voice correlates with economic inequality and weaker democracy.)
- These and other references in the text support the analysis and proposals made herein.

---

1 What Was the DAO Hack? - Gemini
https://www.gemini.com/cryptopedia/the-dao-hack-makerdao

2 6 7 What to Know About Worldcoin and the Controversy Around It | TIME
https://time.com/6300522/worldcoin-sam-altman/

3 "Hard Fork" Coming to Restore Ethereum Funds to Investors of ...
https://spectrum.ieee.org/hacked-blockchain-fund-the-dao-chooses-a-hard-fork-to-redistribute-funds

4 Exclusive: Austrian Programmer And Ex Crypto CEO Likely Stole ...
https://www.forbes.com/sites/laurashin/2022/02/22/exclusive-austrian-programmer-and-ex-crypto-ceo-likely-stole-11-billion-of-ether/

5 What Was the Famous DAO Heist? - Overview, The Hack
https://corporatefinanceinstitute.com/resources/cryptocurrency/dao-heist/