Governance in the Blockchain Era: The Smart Social Contract

***Abstract*— Since the emergence of bitcoin, 14 years ago, cryptocurrencies and the blockchain technology that underpins these virtual currencies have experienced a rapid growth, with a plethora of applications emerging. While most popular applications of blockchain technology are in the business field, its main features – such as decentralization or enhanced security – make it suitable to redesign social, cultural and political realities such as the social contract that regulates the relationship between states and citizens. Blockchain-based applications have the potential to change social values and the social contract itself. This paper aims to discover if smart contracts and blockchain technology can bind the social contract between the state and its citizens in such a way as to reduce corruption and increase efficiency of service delivery. Further, the emergence of a new type of social contract will be investigated: the smart social contract. This new concept aspires to enhance Jean Jacques Rousseau's social contract with the benefits inherent in blockchain technology. It involves an automatic execution of the obligations that a government assumes through a certain program, determined by consensus by all the members of society. In case of non-fulfillment of the obligations, the persons /institutions responsible are sanctioned appropriate penalties. We implement and evaluate a prototype of a smart social contract in Solidity, finding that the contract is capable of automatic execution upon the achievement of predetermined conditions, such as the fulfillment of an obligation by a local government official.**

Keywords—blockchain, smart contract, social contract, e-government, smart social contract

I. Introduction

The advent of blockchain technology has opened up possibilities for innovative solutions in diverse domains, including contract management. Smart contracts, which are decentralized, self-executing programs that enforce the terms of an agreement automatically, have garnered substantial interest in recent years. However, the application of smart contracts has been confined to conventional contractual relationships, predominantly in the financial and legal sectors. On the other hand, the social contract, a philosophical notion that characterizes the association between individuals and society, has served as a fundamental principle for governance over the course of history. In modern-day democracies, the social contract refers to the implicit agreement between citizens and the state, in which individuals' hand over some of their personal freedoms in return for the security and protection provided by the government. The premise of this notion is based on the assumption that individuals are better off in a society with a robust government, rather than in a state of nature where there is no safeguard from external dangers. Pursuant to this agreement, citizens possess certain liberties and rights, such as freedom of expression and worship, while the government has the obligation to defend and preserve these rights. In exchange, citizens commit to participating in the democratic process through voting, paying taxes, and adhering to the laws and regulations established by the government.

In this paper, we introduce the concept of a smart social contract, which combines the benefits of smart contracts with the fundamental principles of the social contract. Our motivation is to create a decentralized, trust-minimized, and transparent framework that can enhance the social contract's governance and enforcement mechanisms. We contribute by providing an analysis of the existing literature on smart and social contracts, identifying the gaps and challenges in their implementation, and proposing both a theoretical as well as a technical framework for a smart social contract. Furthermore, we present a potential application of the smart social contract in an example of a mayor-led community. Overall, this paper offers a novel perspective on the integration of smart and social contracts, providing insights into the future of contractual relationships in a decentralized world.

The remainder of the paper is organized as follows: Section 2 presents a brief introduction to the concept of the social contract, showing insights of all major works related to the subject starting with Plato and Aristotle and finishing with modern schools of thought as well as short considerations about the blockchain technology and the smart contracts, in context of the social contract. In Section 3, we introduce and explain the novel concept of smart social contract, a concept that unifies the social contract and smart contract, resulting in a digital instrument for overseeing the convention between a government and its citizens. Section 4 contains an evaluation that aims to assess the effectiveness, efficiency and usability of the proposed theoretical framework, Section 5 contains challenges and limitations of the new concept and Section 6, concludes the paper.

II. Background

A. A brief introduction to the concept of social contract

The ideology behind the state as we know it today has its foundations on the philosophical concept of the "social contract". The relationship between the state, its citizens and the law has been intriguing since ancient times: among the first mentions of a "social contract" are found in Plato's "*Criton*" Dialogue and *"The Republic"* (Neu, 2012) and Aristotle's works, like "*Politics*" or "*Nicomachean Ethics*". In Plato's work, the concept of a social contract was seen as a necessity for providing common good and securing order in society. The central idea in *"The Republic"* was that individuals had natural abilities based on which the society was divided into classes, and the social contract accommodated this division. The central role in society was played by the rulers or "philosopher-kings", which, as the name states, were supposed to have a philosophical education in order to be able to assure a just and beneficial governance. However, Plato's view included a paternalistic element, granting philosopher-kings the power to control and regulate citizens' behavior and thoughts. In conclusion, Plato saw the social contract as a necessary means to ensure the stability and well-being of society (Chroust, 1968). Plato's student, Aristotle, had a different view on the social contract consisting of the fact that it was not a deliberate agreement between individuals and the state, but rather a natural consequence of relationships between individuals and social cooperation with the ultimate goal of ensuring well-being as well as survival. His thesis stated that individuals clustered in communities and nation states in order to consolidate and effectively use resources and protect from external threats. A highlight in Aristotle's work was the linkage between justice and the social contract: the ideal form of government, in his view, was a mixed constitution which incorporated elements of democracy, aristocracy, and monarchy, where each component served as a restraint on the power of the others (Das, 1975; Knop, 2008).

The modern social contract theory and the best description of the relationship between the state, its citizens and the laws began to emerge in the Renaissance period and is found in the works of Thomas Hobbes, John Locke or Jean-Jacques Rousseau. (Donaldson, 1978).

Thomas Hobbes's[1] 1651 original work, "Leviathan," stands as a pivotal example of social contract theory. Hobbes advances the idea that in a "state of nature," where no common authority exists to create a balance of respect and fear, people inherently live in a "bellum omnium contra omnes" or a war of all against all. This metaphorical "state of war" signifies not constant battle, but a persistent readiness to fight, leading to a life of fear and making productive labor ineffective. Hobbes outlines three options for humanity: persist in this natural state, unite under a government with limited power, or establish a civil society ruled by a sovereign with absolute authority. He dismisses the second choice as illusory, advocating for an absolute sovereign. This leads to his theory of a hypothetical social contract, where individuals collectively give up their rights to a central authority in exchange for security from the chaos of the natural state. In Hobbes's view, this contract justifies the sovereign's absolute power and the subjects' moral duty to obey, marking a transition from anarchy to a structured society. (Kavka, 1998).

John Locke's[2] theory of the social contract can be found in his 1689 work "*Two Treatises on Government: In the Former, The False Principles, and Foundation of Sir Robert Filmer, and His Followers, Are Detected and Overthrown. The Latter Is an Essay Concerning the True Original, Extent, and End of Civil Government"*. Although Locke's theory starts from the same "natural state" point as Hobbes describes, yet in his sense, this term has quite another meaning, having nothing to do with a state of a general "war". "The natural state means a state of nature where humans are not subject to a common legitimate authority with the power to legislate or adjudicate disputes. From this natural state of freedom and independence, Locke stresses individual consent as the mechanism by which political societies are created and individuals join those societies. While there are of course some general obligations and rights that all people have from the law of nature, special obligations come about only when they are voluntarily undertaken. Locke clearly states that one can only become a full member of society by an act of express consent" (Tuckness, 2018). Just like Hobbes, Locke concluded that the exclusive right to defend in the "state of nature" was not sufficient, so people created a civil society in order to resolve conflicts, with the aid from a government in a state of society. In conclusion, according to Locke, the social contract is a means of preserving individual freedom and promoting the common good, and citizens have the right to overthrow the state if it failed to fulfill its obligations.

Another theorist of the social contract – and perhaps the best known of all – was Jean Jacques Rousseau[3]. His theory of the social contract can be best described with his opening line from the work originally published in 1762 "*The Social Contract*": "Man is born free, and everywhere he is in chains. Those who think themselves the masters of others are indeed greater slaves than they" (Rousseau, 1978 edition). Rousseau is trying to respond to what he considers to be the fundamental issue of politics, namely reconciling individual freedom with state authority. This reconciliation is necessary because human society has evolved to a point where individuals can no longer satisfy their own needs but must depend on the cooperation of other individuals. The social contract aims to establish an alternative to this dystopia, an alternative in which, according to Rousseau, each person will enjoy the protection of a "common force", remaining as free as in the "state of nature". The solution to this reconciliation is the idea of the general will: the collective will of the citizen body taken as a whole. General will is the source of the law and is desired by every citizen. By respecting the law, every citizen is thus subjected to his will and, accordingly, remains free. (Bertram, 2018). In Rousseau's view, the social contract was an agreement between individuals to join together and form a political community for the purpose of protecting their natural rights and promoting the common good.

The differences in the three mentioned visions were shaped by the different view on human nature, role of the state and the government and the intrinsic relations between individuals. While Hobbes' vision of the social contract was that of a transfer of individual sovereignty to the state, with the purpose of providing security and stability in the face of the dangerous and chaotic state of nature, Locke's and Rousseau's visions of the social contract stated that individual freedom and promoting the common good were the core ideas, with a heightened focus on democracy and citizen participation.

After the social contract theory crystallized and the French Revolution had changed the existing paradigm that was into place up to that point in Europe by eliminating absolutist monarchies and replacing them with republics and democracies, the notions of citizen, state, nation-state and law have profoundly changed their meaning, obtaining the modern connotations that we know today. Furthermore, nowadays, the relationship between the state, its citizens and the law is also in a continuous metamorphosis due to external factors – rather than internal factors as thought before, subject to *ceteris paribus* clause.[4]

In modern times, as stated before, the social contract can be synthesized in the following way: citizens of a certain nation-state obey the laws and pay taxes in fiat currencies issued by the governments in order to receive in return the rule of law and an efficient governance. The primary aim of the social contract is to provide a justification for the rules imposed by a governing body. The principles derived from a fundamental social contract should form the basis for the regulations governing the relationship between the political power of the governing body and the agreement of society. In regards to the relationship between individuals and the state, the social contract serves a dual purpose. It must establish criteria that both legitimize the political power of the state and validate the consent of citizens (Allsobrook, 2018). Sometimes compared to Plato or Rousseau of the modern society, John Rawls was the theorist of the 20th century that redefined in an all-encompassing manner the essential features of the social contract and added a few extra features, characteristic of the era in which we live. In his work *"A theory of justice",* Rawls states the concept of the original position is considered a generalized and highly abstract manifestation of social contract theory. This theory asserts that principles of justice can only be deemed legitimate if all individuals, under ideal circumstances, reach a consensus on them. (Allsobrook, 2018) One of the most recent theoreticians of the social contract, Primavera de Filippi, resumes in her work "*Blockchain and the law"* the interplay between blockchain technology, legal systems and social contracts in the Web3 era. The paper argues that blockchain has the potential to change the traditional social contract between individuals and institutions by providing a transparent platform for governance and the legal system. (De Filippi, 2018)

[1] English philosopher, considered to be one of the founders of modern political philosophy; he lived during the most crucial period of early modern England's history: the English Civil War, waged from 1642-1648

[2] English philosopher and physician, widely regarded as one of the most influential of Enlightenment thinkers and commonly known as the "Father of Liberalism"

[3] Genevan philosopher, writer and composer. His political philosophy influenced the progress of the Enlightenment throughout Europe, as well as aspects of the French Revolution and the development of modern political, economic and educational thought

[4] The term "ceteris paribus," meaning "all other things being equal," is used to isolate the effect of one variable in an analysis by assuming that all other relevant factors remain constant.

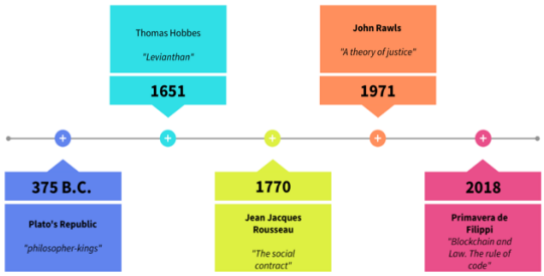

Figure 1: Evolution of the concept of "social contract"

B. *Short considerations on the blockchain technology in the light of the social contract*

Since the emergence of bitcoin, 14 years ago, cryptocurrencies and the blockchain technology that underpins these virtual currencies have experienced a rapid growth. The main features of the new blockchain technology, such as decentralization, distributed ledgers, immutability, consensus or enhanced security (Kim, 2020), have determined the extension of its use from cryptocurrencies to a multitude of other areas such as data privacy, banking, healthcare, business and supply chains (Lee, Kriscenski & Lim, 2019). In the healthcare field, blockchain technology has the potential to improve the security and privacy of health data, as well as enable the secure sharing of patient information. Introducing blockchain technology in this sector, electronic health records (EHRs) have the potential to become one of the most important innovations within the health care sector, as they are expected to significantly improve intersectoral collaboration and reduce health care expenses (Beinke et all., 2019). Regarding the supply chain management sector, blockchain can help enhance transparency and efficiency by enabling secure tracking of goods and transactions. Traditionally, "supply chain activities involve several intermediaries, trust, and performance issues. The potential of blockchain can be leveraged to disrupt supply chain operations for better performance, distributed governance, and process automation". (Chang, Chen, 2021) A field of interest for the present paper is that of e-voting. Electronic voting has become more popular due to its capability to reduce costs and increase voter turnout. However, there are concerns about the security and accuracy of electronic voting systems. Blockchain technology is seen as a potential solution to these issues, as it provides decentralized nodes and end-to-end verification. (Jafar et all, 2021)

Since the technology can be used in any domain that manages data, the use cases for blockchain are practically endless. Although the most popular applications of blockchain technology are in the business field, their main features – such as decentralization or enhanced security – make them suitable to redesign social, cultural and political realities (Reijers, Coeckelbergh, 2018), like the social contract.

Nick Szabo, a computer scientist known as being the creator of BitGold – a predecessor of bitcoin, sums up on his blog "*Unenumerated*" thus: "the secret to Bitcoin's success is that its prolific resource consumption and poor computational scalability is buying something even more valuable: social scalability. Social scalability is the ability of an institution – a relationship or shared endeavor, in which multiple people repeatedly participate, and featuring customs, rules, or other features which constrain or motivate participants' behaviors – to overcome shortcomings in human minds and in the motivating or constraining aspects of said institution that limit who or how many can successfully participate. Social scalability is about the ways and extents to which participants can think about and respond to institutions and fellow participants as the variety and numbers of participants in those institutions or relationships grow. It's about human limitations, not about technological limitations or physical resource constraints. There are separate engineering disciplines, such as computer science, for assessing the physical limitations of a technology itself, including the resource capacities needed for a technology to handle a greater number of users or a greater rate of use." (Szabo; Tikhomirov, 2018)

The social aspect of cryptocurrencies and blockchain-based technology is not a recent development. The Cypherpunks movement, an enthusiastic group of cryptographers that included Nick Szabo and where the concept of bitcoin was first introduced, emphasized this social dimension (Amsyar et al., 2020). The key ideas behind the Cypherpunk movement can be found in "A Cypherpunk's Manifesto" written by Eric Hughes in 1993. The primary principle highlighted in the manifesto is the significance of privacy (Craig, 2021). Many of the ideas expressed in the manifesto and other works associated with the Cypherpunk movement are evident in the underlying principles of cryptocurrencies that exist today (Basson, 2018).

The Bitcoin White Paper, written by Satoshi Nakamoto in 2008, outlines the need for an electronic payment system based on cryptographic proof instead of trust. This idea, similar to Tim May's Cyphernomicon, highlights the importance of privacy, achieved through technology, encryption, and decentralization (Flood, Robb, 2017). In 2009, Satoshi Nakamoto emphasized the need for a payment system that did not require trust in intermediaries, as conventional currency was problematic in this regard. The central bank and banks needed to be trusted not to abuse their power, but the history of fiat currencies showed that this trust was often breached.

The ideology behind cryptocurrencies, including Bitcoin, is rooted in the anarchist idea of "an-cap": it doesn't categorically view the state as an adversary but as a potential challenge to individual autonomy, advocating for a system where laws and social contracts are underpinned by mathematical and code-based principles. (Swartz, 2018). This view is a response to the social contract theory, which states that individuals form a society and government through a contract in which they agree to obey the laws and pay taxes in exchange for the rule of law and efficient governance (Brittanica Encyclopedia, Skyrms, 2014, Mouritz, 2010). When a decentralized currency like Bitcoin appears, it challenges the part of the social contract that requires individuals to pay taxes and obey the laws. Additionally, it can be suggested that smart social contracts could be instrumental in transitioning towards more decentralized forms of governance, resonating with the ideas of minimizing state overreach while maximizing individual liberty and privacy. This perspective offers a compelling framework for rethinking the role of the state in an era increasingly dominated by digital and decentralized solutions.

Blockchain technology, with its decentralized and enhanced security features, holds the potential to transform various aspects of society, culture, and politics, even redefining the social contract. Cryptocurrencies, for instance, could revolutionize the financial system by addressing issues faced by the unbanked and underbanked. Similarly, blockchain-enabled voting systems could significantly influence the development of new democracies. The impact of blockchain extends well beyond business, offering possibilities for altering social values and reshaping the social contract.

C. *Short considerations on the smart contracts in the light of the social contract*

Smart contracts have gained significant popularity since the emergence of blockchain technology, as they offer a high degree of customization to transactions. As a result, a wide range of smart contract applications has emerged in diverse areas, including financial services, life sciences, healthcare, energy resources, and voting. (Macrinici, Cartofeanu, Gao, 2018)

A universally accepted definition of the term *smart contract* does not currently exist, because of the novelty of this concept and its complex technological basis. At its simplest, a smart contract can be defined as an agreement that is executed automatically. Nick Szabo,

a pioneer in the analysis of automated self-performed agreements, defines smart contracts as computerized transaction algorithms that enforce the terms of the contract. However, this definition may not clearly differentiate smart contracts from other well-known contractual constructs that also implement automated performance. (Savalyev, 2017)

Smart contracts are pieces of computer code that operate on an If/Then basis. However, they differ from other programs that utilize this concept for automation by running on a distributed ledger, which grants them the same properties as the ledger itself, such as immutability, security, and censorship resistance. While programs running on third-party servers are limited to the functions of those servers, smart contracts are only restricted by the skill of the smart contract developer and the integrated technologies on which they depend (the latter includes, for example, gas restrictions limiting run times, and limits on the expressibility of smart contract languages). Furthermore, because smart contracts are enabled through agreement across a distributed network, they engender more trust than any centralized third-party alternatives (Li, Mohammad, 2021).

Smart contracts take the scalability and potential of decentralized systems to the next level, enabling predefined processes or even real contracts to be executed in full transparency without external influence. These programmed processes can range in complexity from simple transaction forwarding to anchoring values on the blockchain through token (smart) contracts. This allows for the issuance and transfer of digital tokens, such as cryptocurrencies, by users (Lennart, 2021)

III. Blockchain governance: The smart social contract

The issue of transparency in public administrations has become increasingly important in recent public debates. Access to information held by public entities is considered crucial from multiple perspectives, as it can support the democratic process, facilitate citizen participation in public decision-making processes, and serve as a tool for preventing and combating corruption. Blockchain can be utilized to create decentralized public networks, enabling every participant to access the distributed database. This feature can enhance administration transparency by introducing a new radical system for disseminating open data (Benedetta, Carullo, 2021).

The public sector has become a significant area of application for the blockchain technology, with governments and other actors announcing over two hundred use cases worldwide. Several areas are currently testing blockchain technology for public services, including digital currency/payments, land registration, identity management, notarization, supply chain traceability, healthcare, education, corporate registration, data management, auditing, energy market, taxation, voting, and legal entities management (Kozak, 2022). Despite the significant interest in blockchain technology, its implementation in the public sector has been limited. Past studies have identified various adoption challenges, including inadequate regulation, concerns about security and privacy, insufficient and non-interoperable infrastructure, inefficient and energy-intensive transactions, the necessity for value-driven transitions in administrative processes, and, last but not least, the lack of effective governance models (Evrim, Mahua, 2021).

Although Bitcoin, blockchain and smart contracts, on one hand and the nation-state, democracy and smart contracts, on the other hand may seem like polar opposites at first glance, they have become intertwined through the emergence of blockchain technology and its influence on governance, also known as "blockchain governance." While Bitcoin is a virtual currency based on a cyberlibertarian philosophy, the nation-state has a long history dating back to the Sumerian civilization and is typically based on democracy and the social contract. However, blockchain technology has proven to offer advantages in public domains such as voting systems and land registries due to its transparency and security.

The question that emerges is whether a "smart social contract" could be created to transfer the entire social contract to the blockchain, which involves the automatic execution of government obligations through a consensus-based program. This concept does not seek to eliminate the state but rather to leverage the benefits of blockchain technology to create an improved version of government systems. According to Atzori (2015), this would replace centralization, coercion, and hierarchies with mechanisms of distributed consensus. Overall, the term "smart social contract" aims to blend the most effective tools from both blockchain and nation-state to keep up with the technological evolution of our time.

A. The smart social contract: the concept

At a first glance, smart contracts and social contracts have nothing in common because they operate in different spheres. Smart contracts are agreements that are executed automatically, designed to facilitate or enforce of a contract, that operate on a blockchain network, in a decentralized environment. On the other hand, social contracts are a theoretical concept from philosophy that refer to implicit agreement between citizens and the state, in which individuals give up a part of their personal freedoms in return for the services provided by the government.

Despite their intrinsic differences, smart contracts and social contracts display some similarities. Firstly, both conceptualizations rely on the fundamental concept of trust in the sense that smart contracts aim to eliminate the requirement for trust between involved parties by providing a tamper-proof mechanism for implementing and enforcing agreements. In a similar manner, social contracts depend on the underlying trust that people have for the organizations that govern the society as a whole. Secondly, both smart contracts and social contracts hold implications for power dynamics in democratic societies. The ability of smart contracts to alter conventional structures by eliminating intermediaries and enabling individuals to directly enter into agreements with each other, can potentially change power dynamics. Social contracts, on the other hand, establish the connection between individuals and the state and have the ability to influence the allocation of resources within contemporary democratic societies. Last but not least, the emergence and development of smart contracts has raised questions about the role of traditional legal systems in regulating agreements between parties. Some researchers (Filippi, 2019) argue that smart contracts have the potential to transform the way we think about contract law, with implications for the legitimacy of traditional legal institutions. This has implications for the social contract, which is based exactly on the idea of a legitimate authority that is responsible for enforcing the rules of society.

The novel concept of the "smart social contract" unifies the social contract and smart contract, resulting in a digital instrument for overseeing the convention between a government and its citizens. The smart social contract is capable of automatic execution upon the achievement of predetermined conditions, such as the fulfillment of an obligation by a local government official. Through this method, the government–citizen agreement can be realized more efficient and transparent, which can result in an elevated level of trust of citizens in public services and a reduction of misconduct.

In the context of a smart social contract, the stipulations and provisions of the arrangement between the government and the citizens (unwritten until so far) take the form of digital data, which permits the automatic and transparent fulfillment of obligations. This intrinsic characteristic eliminates the requirement for intermediaries and manual procedures, thus enhancing the efficacy of the process.

The widespread adoption of a smart social contract has a significant advantage in enhancing transparency and accountability, particularly regarding government representatives. The use of blockchain technology enables all involved parties in the social contract to have equal access to information and track the execution of obligations in an efficient manner. At the same time, the potential

for corruption, fraud, and other forms of abuse is minimized as a result of the fact that all transactions are recorded in a tamper-proof ledger that is publicly available. Furthermore, a smart social contract may include automatic clauses to incentivize elected officials to fulfill their obligations to citizens. (Balcerzak et al., 2022) For instance, if the elected official engages in a promise to invest in an infrastructure project, the project's progress can be monitored through the contract. If the project fails and the commitments are not fulfilled, this shortcoming can be automatically reported to citizens. As agreed, upon in the contract, non-fulfillment of obligations may lead to coercive measures with automatic execution, such as the revocation of the public mandate.

The bond between citizens and government can be enhanced through the implementation of a smart social contract. This new type of contract has the capacity to ensure the government's commitment to its citizens and oversee the compliance with the said commitments.

A key feature in any type of social contract is the notion of "consent". When talking about the smart social contract, the principle of explicit consent extends beyond the traditional notion of governance. It is important to recognize that just as governments must secure consent for their actions and policies, citizens, too, need to explicitly agree to be part of this innovative form of governance. This mutual consent is not a one-time affirmation but an ongoing process, reflecting the nature of societal values. The smart social contract, therefore, must be designed to facilitate continuous engagement and consent, allowing citizens to express their concerns and influence the governance process actively. The use of advanced technologies like blockchain and smart contracts allows governments to establish systems that are both transparent and secure. These systems do more than just monitor governmental actions: they also capture and document the feedback and involvement of citizens. Such a system ensures that the consent given by citizens is informed. To fully appreciate the smart social contract, it's beneficial to compare it with historical governance benchmarks, notably the Magna Carta Libertatum and English Common Law. The Magna Carta, a seminal document in the history of constitutional law, laid the groundwork for the concept of rule by consent. It established that authority should be exercised within the confines of agreed-upon laws and with respect for the rights of subjects. Similarly, English Common Law evolved as a body of law based on judicial decisions and societal customs, emphasizing precedent and continuity, alongside the adaptability to changing societal norms. The smart social contract can be seen as a modern extension of these historical principles. It integrates the foundational idea of governance with consent — as stated by the Magna Carta and perpetuated through English Common Law — into the digital age. By doing so, it not only adheres to these principles but also revitalizes them, offering a framework that is more aligned with the needs and capabilities of contemporary societies. The era of digital governance necessitates a reevaluation of how consent is obtained, interpreted, and maintained. In a smart social contract, consent is not static but a fluid concept, responsive to real-time inputs and changes. The smart social contract, underpinned by the principles of mutual consent and enabled by digital technology, represents a significant evolution in the concept of governance.

As an example of all the above-mentioned elements: an elected official with a defined term may make campaign pledges to undertake infrastructural development, construct new educational institutions, or deliver specific public amenities within their tenure in order to win the elections against his rivals. A smart social contract could automate the monitoring of these commitments and promptly alert citizens if the corresponding official fails to fulfill his or her obligations. This, in turn, could establish an additional mechanism of accountability in contrast to the present scenario where the most efficacious method is exercised once every four years, solely through the casting of votes. Incorporating such a contract could enhance the transparency and accountability of elected officials, thereby strengthening citizens' faith in the democratic system. By promoting a more impartial and fair connection between the citizens and government, the use of a smart social contract may culminate in a more effective and equitable society.

B. The applicability of a smart social contract in contemporary society

A smart social contract refers to a digital agreement between parties, namely citizens and government officials, and preserved instored on the blockchain network. This type of contract is self-executing, eliminating the requirement of intermediaries to enforce the terms of the agreement.

The provisions and stipulations of a smart social contract are encoded and maintained in the blockchain network, ensuring transparency, security, and immutability. The contract operates automatically upon fulfilment of predetermined conditions and can levy penalties or provide incentives based on the agreement's provisions.

For instance, a smart social contract can be utilized to oversee an elected mayor's delivery of electoral pledges within a specified tenure of four years. In doing so, the contract can self-regulate the mayor's duties according to mutually agreed-upon regulations between the mayor and the citizens who elected him, without necessitating any human intervention.

An instance of a smart social contract implementation can be observed in a city that elects its mayor for a four-year term. Citizens can utilize this contract to hold the elected official accountable for his campaign promises through a digitally stored, transparent, and self-executing agreement, enabling real-time monitoring of the mayor's performance.

The contract can feature several provisions, including the mayor's campaign promises, specific objectives and timelines, performance metrics to measure progress, citizen input, real-time monitoring, and penalties and rewards for performance outcomes. For example, if the mayor fails to deliver on promises, salary deductions or suspension of their right to re-election may occur. Conversely, bonuses may be granted for exemplary performance. A smart social contract in the above-mentioned example may include the following types of provisions: mayor's promises, performance metrics, citizen input, real-time monitoring, penalties and rewards transparency and security.

One of the most important aspects regarding the applicability of the smart social contract in the contemporary society is represented by the penalties and rewards taking into account that they can serve as motivators to encourage the new mayor to act in the best interests of the city and its constituents. The smart social contract can integrate economic incentives and disincentives to motivate the new mayor to fulfill the responsibilities and obligations. One possible economic incentive for the new mayor is a performance-based bonus or salary increase, which is contingent upon the achievement of the objectives defined by the social agreement and the smart contract program. For instance, if the new mayor successfully implements policies that foster economic growth, reduce crime rates, or enhance environmental sustainability, for example, they may be eligible for a monetary reward or bonus. Additionally, an economic reward system could be established to offer tax incentives or subsidies to businesses that invest in the city's economic development or provide employment opportunities for its citizens. The new mayor could promote the city to potential investors by offering financial incentives, such as tax breaks or subsidies, to companies that meet specific criteria, such as creating jobs, advancing sustainable practices, or investing in local infrastructure. Conversely, economic penalties may be imposed on the new mayor for failing to meet their obligations or violating the terms of the smart social contract. For example, if the new mayor fails to implement the campaign promises, (s)he may be subject to a reduction in the salary or penalty fee. Similarly, if the new mayor engages in corrupt or unethical behavior, they may face financial consequences or legal action. The implementation of economic rewards and penalties in the smart social contract can provide a compelling incentive for the new mayor to act in the best interests of the city and its constituents. By aligning

economic incentives with social and environmental objectives, the smart social contract can facilitate a sustainable and equitable economic development model that benefits all stakeholders.

The integration of external data is a key aspect in the operation of smart social contracts, necessitating rigorous verification and consensus mechanisms to safeguard the system's integrity. This is vital, as any compromise in these processes could undermine the distributed ledger's inherent attributes, like transparency and immutability, leading to substantial risks across the system. This aspect becomes particularly critical in the sphere of smart social contracts, where the authenticity and reliability of external data significantly affect governance mechanisms and public confidence. One possible solution is represented by blockchain oracles, a concept increasingly discussed in the literature and emerges as a pivotal solution in this context. The oracles are trusted intermediaries that provides the blockchain systems with external, validated data, thereby linking the blockchain's isolation with the external, dynamic world. This role is indispensable for smart social contracts, which inherently lack the capacity to interact with data beyond their blockchain environment. They provide essential real-world data, ranging from voting outcomes to governance metrics, ensuring that the activities triggered by smart contracts are both pertinent in information. Chainlink stands out as an important example of a decentralized oracle network, offering secure, tamper-proof data feeds for complex smart contracts across various blockchain platforms. Its ability to provide reliable real-world data is key to maintaining the robustness and functionality of smart contracts, especially in scenarios where decisions within smart social contracts are automated and reliant on this external data. In essence, blockchain oracles are indispensable for a smart social contract concept (Cai et al., 2022). By ensuring the secure incorporation of external data, they not only enhance the effectiveness of smart contracts but also reinforce foundational blockchain principles such as security and decentralization.

C. A real-life smart social contract

To illustrate the above concept, we start from the premise that the smart social contract is implemented on the Ethereum blockchain platform using the Solidity programming language. Specifically, in the example case presented in this paper, the contract is created to ensure that an elected mayor upholds his campaign promise to build 20 km of roads within the first year, connecting the city to a nearby cultural centre. As such, the smart social contract sets forth the details of the agreement, including the completion date for the road construction, the distance to be covered, and the consequences that will take effect if the mayor fails to deliver. The contract stipulates that if the mayor does not fulfill his commitment within the specified time frame, certain penalties will be automatically enforced (in this case, a reduction in the mayor's salary). By leveraging the capabilities of the blockchain technology, this new type of contract provides an immutable and transparent mechanism for holding elected officials accountable for their campaign promises. The contract empowers citizens to have a say in the decision-making process and ensures that their elected representatives are held to their word.

From a technical point of view, the steps and details for this smart social contract are the following: 1. Both the elected mayor and the citizens of the city agree to build the smart social contract on the Ethereum blockchain platform, written in the Solidity programming language; 2. The contract specifies the terms of the agreement between the elected mayor and the citizens, including the promise to build 20 km of roads in the first year to connect the city to a nearby cultural centre; 3 The contract includes a deadline for the completion of the road construction project (12 months); 4. The contract specifies the consequences in the event that the mayor does not fulfill his promise (50% reduction of salary for the next 12 months); 5. In the case that the full 20 km of roads are not completed by the end of the 12th month, the contract is self-executing, meaning that it automatically enforces the terms of the agreement without the need for manual intervention; 6. All parties involved can view and verify the terms of the agreement on the Ethereum blockchain, ensuring transparency and accountability.

Regarding the objective verification of the fulfillment of the mayor's task, a neutral third-party (like an independent auditor), may undertake the verification process to determine whether the road has been constructed in accordance with the contract's specifications. This verification process can be automated using smart contract triggers, such as GPS coordinates or satellite imagery, to ensure that the road's construction adheres to the terms. Alternatively, the citizens themselves can be involved in the verification process: for example, a number of citizens can inspect the road and confirm that it has been built in compliance with the contract's specifications before the mayor can receive a bonus or before the penalties are enforced.

In any case, it is essential that the verification process be transparent and tamper-proof. This requirement ensures that the mayor is held accountable for their promise to build the roads, and that the process is not subject to manipulation.

The accessibility of the smart social contract is a crucial aspect to ensure equitable participation and the realization of favorable outcomes for all the parts involved. Typically, the smart social contract should be designed to be accessible through digital platforms which provide efficient communication and interaction channels between the participants. However, it is essential to acknowledge that not all individuals have equal access to digital technologies and the internet, and this may result in certain stakeholders being marginalized and unable to participate fully in the smart social contract. To address this concern, alternative modes of access can be incorporated into the smart social contract, such as phone hotlines.

It is important to note that ensuring accessibility to the smart social contract for all stakeholders is a significant and constant challenge. The design and implementation of the smart social contract should consider the diversity and the unique needs of all the parties involved, including those who are marginalized or disadvantaged. By encouraging inclusive and equitable participation, the smart social contract can promote trust, accountability, and collaboration.

The smart social contract described above has its technical input in Appendix 1.

IV. EVALUATION

This section analyzes the performance of the smart social contract concerning its advantages, limitations, and challenges, along with an evaluation of its potential for future development.

To evaluate the usability and practicality of the smart social contract, a real-world application study (found in Appendix 1) was conducted. The case study included a decentralized system for electing a new mayor and a decentralized governance system. The study conducted provided evidence supporting the notion that smart social contracts have the potential to revolutionize governance. It was demonstrated that these contracts could pave the way for a governance model that is decentralized, trustless, and transparent, marking a significant departure from traditional, centralized systems. Such a shift indicates a possible future where governance is more accessible and accountable to the public. Furthermore, the research highlighted that smart social contracts are not just tools for efficient governance but also potential catalysts for social innovation. By leveraging the features of blockchain technology, these smart social contracts facilitate a level of collaboration and coordination among various stakeholders that was previously hard to achieve. This collaborative framework is particularly beneficial in tackling complex social issues, where diverse approaches are needed.

The concept of the smart social contract, presented in this paper, highlights an innovative approach to decentralized governance, leveraging the capabilities of blockchain and other digital technologies. This paper has underscored the benefits of such a system, notably its transparency and efficiency. These attributes are important in fostering trust within various sectors, including government, and public administration.

However, the analysis also reveals several limitations and challenges that must be addressed to fully realize the potential of smart social contracts. One of the primary concerns is the legal and regulatory landscape, which, in many jurisdictions, remains underdeveloped in the context of blockchain technology and smart contracts. This current situation poses a significant challenge, as the lack of clear legal frameworks can hinder the adoption and effective operation of smart social contracts. Another notable challenge is the issue of accessibility. While the technology underlying smart social contracts is advanced, there remains a problem concerning technological access and literacy. This divide can lead to unequal opportunities and benefits, potentially exacerbating existing socio-economic disparities. Ensuring general accessibility and understanding of this technology is crucial for its widespread adoption and effectiveness. Furthermore, the risk of cyber-attacks cannot be overlooked. The digital nature of smart social contracts makes them vulnerable to such threats, which could undermine their integrity and trust. Ensuring effective cybersecurity measures is essential to protect these contracts from malicious actors and maintain their reliability.

Despite these challenges, it is important to acknowledge the potential of smart social contracts for future development. Their ability to automate and decentralize governance processes offers a glimpse into a more transparent future. However, realizing this potential requires efforts in research and development. This calls not only for technological advancements but also the creation of a regulatory frameworks, strategies to enhance accessibility, and cybersecurity measures.

While the smart social contract presents a promising framework for decentralized governance, its full implementation and effectiveness depend on overcoming the identified limitations and challenges. This necessitates a multidisciplinary approach, involving tech experts, legal experts, policymakers, and other stakeholders, to work together for refining and advancing this innovative concept.

V. Limitations and Challenges of the Smart Social Contract

In the rapidly evolving landscape of blockchain technology and decentralized systems, the concept of the "smart social contract" emerges as a tool to automate and enforce various social, economic, and governance agreements, potentially altering the dynamics of societal interaction and cooperation. Yet, this innovative potential comes with its own set of obstacles. It is crucial to examine the potential limitations and challenges associated with the application of the smart social contract. These issues include, but are not limited to:

Social Scalability:

The core idea behind the concept of smart social contracts revolves around the objective of social scalability. This necessitates creating a system where an ever-growing community of participants can effortlessly interact with various institutions. Nevertheless, some inquiries concerning the natural constraints of human cognition and the task of guaranteeing that the collective wisdom of the crowd leads to rational and cohesive decision-making emerge. The future phases of developing the smart social contract will investigate the influence of these limitations on the achievement of these types of contracts, especially in scenarios where the intricacy of problems surpasses the cognitive abilities of the participants.

Theoretical Underpinnings:

Another limitation of the smart social contract concept lies in the foundational theories of social choice, namely the Arrow Impossibility Theorem and the Gibbard-Satterthwaite Theorem that both cast a shadow of doubt on the feasibility of constructing infallible smart social contracts. These theorems, known for elucidating the inherent challenges of aggregating individual preferences into collective choices, pose fundamental questions about the practicality of creating a universally acceptable decision-making mechanism.

The Arrow Impossibility Theorem reveals that no voting system can perfectly align individual preferences into a collective decision when dealing with three or more choices, without violating at least one of three key criteria: non-dictatorship, Pareto efficiency, or independence of irrelevant alternatives (Tanaka, 2006). This poses a critical challenge for smart social contracts, which aim to automate and enforce governance agreements based on collective preferences. The theorem suggests that it may be impossible to devise a smart social contract system that is both fair and reflective of all individual preferences, thereby questioning its efficacy in diverse and complex real-world scenarios.

Similarly, the Gibbard-Satterthwaite Theorem points out that any voting system that isn't dictatorial and deals with three or more options is susceptible to strategic voting or manipulation. (Reny, 2001) This vulnerability to manipulation is particularly problematic for smart social contracts, as they rely on the integrity and authenticity of individual preferences to make decisions. The potential for strategic behavior undermines the trust and reliability of these contracts, making it challenging to ensure their decisions are genuinely representative and fair.

As the development of smart social contracts progresses, it is essential to consider these theoretical limitations highlighted by the Arrow Impossibility and Gibbard-Satterthwaite Theorems. Understanding the extent to which these limitations affect the design and implementation of smart social contracts is crucial. It involves acknowledging that while these contracts offer innovative solutions for decentralized governance, their ability to accurately and fairly reflect collective preferences is inherently constrained by these fundamental principles of social choice theory. This recognition necessitates a careful and nuanced approach in developing and applying smart social contracts, ensuring that their design is as inclusive as possible, while being aware of and mitigating their inherent limitations.

Voting Dynamics and Legal and Regulatory Challenges:

The intricacies of the voting process within smart social contracts will also be scrutinized, with an emphasis in ensuring the integrity of the voting process. Furthermore, an in-depth analysis of the substantial issue of fraudulent activities within digital voting systems shall be conducted in the future stages of development. In addition, a comprehensive examination of the legal and regulatory framework enveloping smart social contracts, engaging with concerns relating to their enforceability, adherence by participants, and the intricate challenge of harmonizing technological innovation with established legal constructs will be conducted. This dynamic, characterized by the constant evolution of cutting-edge technology and its interaction with established legal norms, will be subject to meticulous scrutiny and analysis within the scope of this research.

Accessibility and Security Concerns:

One of the challenges of the smart social contract also examines the accessibility side, taking into account factors such as technological literacy, user-friendly interfaces, and digital divide issues. Accessibility barriers can impact the inclusivity and effectiveness of these contracts in diverse social contexts. Additionally, the persistent risk of hacking and cyber-attacks in the blockchain ecosystem will be analyzed in future stages, with a focus on strategies for enhancing the security of smart social contracts and safeguarding sensitive data against malicious actors.

The future development phases will take into account the ethical dilemmas that arise from such a concept and will embark on a comprehensive exploration of the limitations and challenges that address the smart social contract concept. By offering nuanced insights, this research contributes to the understanding of the interplay between technology, governance, legal considerations, societal inclusivity, and cybersecurity in the ever-evolving landscape of blockchain and decentralized systems.

VI. Conclusions

The mixture between the social contract theories and smart contracts has resulted in the emergence of a new concept introduced in this paper: the smart social contract. The new contract aims to blend together the most effective components from both blockchain technology and the social contract philosophy in order to deliver a new and improved pattern of e-government. This incorporation aims to create an enhanced iteration of the existing government systems that aligns with the ongoing technological evolution.

The new type of contract does not advocate for the elimination of the basic institutions of the state, as certain radical philosophies such as anarcho-capitalism may promote. Instead, the new approach seeks to leverage the advantages that this technology has to offer, as evidenced by successful implementation examples, such as those observed in Estonia, where e-government is an acknowledged paradigm.

The novel concept of the "smart social contract" unifies the social contract and smart contract, resulting in a digital instrument for overseeing the convention between a government and its citizens. The smart social contract is capable of automatic execution upon the achievement of predetermined conditions, such as the fulfillment of an obligation by a local government official. Through this method, the government-citizen agreement can be realized more efficient and transparent, which can result in an elevated level of trust of citizens in public services and a reduction of misconduct.

References

[1] Allsobrook, Christopher, *Universal Human Rights from an African Social Contract,* in *Perspectives* in Social Contract Theory, Cultural heritage and contemporary change. Series II, African philosophical studies; Volume 21, 2018, ISBN 9781565183315

[2] Amsyar, I., Christopher, E., Dithi, A., Khan, A. N., & Maulana, S. The Challenge of Cryptocurrency in the Era of the Digital Revolution: A Review of Systematic Literature. (2020). *Aptisi Transactions on Technopreneurship (ATT)*, *2*(2), 153–159. https://doi.org/10.34306/att.v2i2.96;

[3] Ante, Lennart. "Smart Contracts on the Blockchain – A Bibliometric Analysis and Review." Telematics and informatics 57 (2021): 101519–. Web.

[4] Atzori, Marcella, Blockchain Technology and Decentralized Governance: Is the State Still Necessary? (December 1, 2015). Available at SSRN: https://ssrn.com/abstract=2709713;

[5] Balcerzak AP, Nica E, Rogalska E, Poliak M, Klieštik T, Sabie O-M. Blockchain Technology and Smart Contracts in Decentralized Governance Systems. *Administrative Sciences*. 2022; 12(3):96. https://doi.org/10.3390/admsci12030096

[6] Beinke J, Fitte C, Teuteberg F, *Towards a Stakeholder-Oriented Blockchain-Based Architecture for Electronic Health Records*: Design ScienceResearchStudy2019; 21(10): e13585, doi: 10.2196/13585

[7] Benítez-Martínez, Francisco Luis, et al. "Neural Blockchain Technology for a New Anticorruption Token: Towards a Novel Governance Model." *Journal of Information Technology & Politics*, vol. 20, no. 1, 2023, pp. 1–18, https://doi.org/10.1080/19331681.2022.2027317.

[8] Bertram, Christopher, "Jean Jacques Rousseau", *The Stanford Encyclopedia of Philosophy* (Fall 2018 Edition), Edward N. Zalta (ed.), available at https://plato.stanford.edu/archives/fall2018/entries/rousseau/

[9] C. Christopher Lee, John C. Kriscenski, Hyoun Sook Lim, *An empirical study of behavioral intention to use blockchain technology.* 2019. Journal of International Business Disciplines, Volume 14, Number 1, May 2019, p. 1-21;

[10] Cai, Y., Irtija, N., Tsiropoulou, E. E., & Veneris, A. (2022). Truthful Decentralized Blockchain Oracles. *International Journal of Network Management*, *32*(2). https://doi.org/10.1002/nem.2179

[11] Cappiello, Benedetta., and Gherardo. Carullo. Blockchain, Law and Governance. Ed. Benedetta. Cappiello and Gherardo. Carullo. 1st ed. 2021. Cham: Springer International Publishing, 2021. Web.

[12] Chang S.E. and Chen Y , "When Blockchain Meets Supply Chain: A Systematic Literature Review on Current Development and Potential Applications," in *IEEE Access*, vol. 8, pp. 62478-62494, 2020, doi: 10.1109/ACCESS.2020.2983601.

[13] Chroust, Anton-Hermann. "ARISTOTLE'S CRITICISM OF PLATO'S 'PHILOSOPHER KING.'" *Rheinisches Museum Für Philologie*, vol. 111, no. 1, 1968, pp. 16–22. *JSTOR*, http://www.jstor.org/stable/41244350. Accessed 19 Feb. 2023.

[14] Craig Jarvis, *Cypherpunk ideology: objectives, profiles, and influences (1992–1998),* Internet Histories Journal, 2021, 1—27, https://doi.org/10.1080/24701475.2021.1935547;

[15] Das, Arvind N. "Theories of State: Aristotle to Marx." *Social Scientist*, vol. 3, no. 8, 1975, pp. 63–69. *JSTOR*, https://doi.org/10.2307/3516226.

[16] De Filippi, Primavera *Blockchain and the Law. The rule of Code*, Cambridge, MA and London, England: Harvard University Press, 2018. https://doi.org/10.4159/9780674985933;

[17] Donaldson, Sue Slate, "From the natural to the civil state: the evolutionary process as viewed by Thomas Hobbes, John Locke and Jean Jacques Rousseau" (1978). Master's Theses. Paper 415;

[18] Flood, John A. and Robb, Lachlan, Trust, Anarcho-Capitalism, Blockchain and Initial Coin Offerings (November 20, 2017). Griffith University Law School Research Paper No. 17-23, U. of Westminster School of Law Research Paper, Available at SSRN: https://ssrn.com/abstract=3074263;

[19] Hobbes, Thomas. *Leviathan*. Edited by J. C. A. Gaskin, Oxford University Press, 2008.

[20] Jafar, U.; Aziz, M.J.A.; Shukur, Z. Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors* **2021**, *21*, 5874. https://doi.org/10.3390/s21175874

[21] Jin-whan Kim. *Blockchain Technology and Its Applications: Case Studies*, ISSN 1816-6075 (Print), 1818-0523 (Online) Journal of System and Management Sciences Vol. 10 (2020) No. 1, pp. 83-93 DOI:10.33168/JSMS.2020.0106;

[22] Karen Knop, Citizenship, Public and Private, 71 *Law and Contemporary Problems* 309-342 (Summer 2008) Available at: https://scholarship.law.duke.edu/lcp/vol71/iss3/14;

[23] Kavka S. Greogory, "Hobbes's War of All against All" in the book "The social contract theorists", edited by Christopher W. Morris, Rowman&Littlefield Publishers Inc., Oxford, 1998, ISBN: 978-0-8476-8907-1

[24] Krystyna Kozak. "Algorithmic Governance, Code as Law, and the Blockchain Common: Power Relations in the Blockchain-Based Society." *Frontiers in Blockchain*, vol. 6, 2023, https://doi.org/10.3389/fbloc.2023.1109544.

[25] Li, Jennifer, and Mohamad Kassem. "Applications of Distributed Ledger Technology (DLT) and Blockchain-Enabled Smart Contracts in Construction." Automation in construction 132 (2021): 103955–. Web.

[26] Locke, John et al. Social Contract: Essays by Locke, Hume and Rousseau. London: Oxford University Press, 1978. Print.

[27] Macrinici, Daniel, Cristian Cartofeanu, and Shang Gao. "Smart Contract Applications Within Blockchain Technology: A Systematic Mapping Study." Telematics and informatics 35.8 (2018): 2337–2354. Web.

[28] Neu, J. (2012-05-30). Plato's Analogy of State and Individual: The Republic and the Organic Theory of the State. In On Loving Our Enemies: Essays in Moral Psychology. : Oxford University Press;

[29] Reijers, Wessel and Coeckelbergh, *Mark, The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies.* Philosophy \& Technology 31, 103-130 (2018), https://doi.org/10.1007/s13347-016-0239-x;

[30] Rawls, John, and Samuel Richard. Freeman. *Collected Papers*. Cambridge, Mass: Harvard University Press, 1999.

[31] Reny P., Arrow's theorem and the Gibbard-Satterthwaite theorem: a unified approach, Economics Letters, Volume 70, Issue 1, 2001, Pages 99-105, ISSN 0165-1765, https://doi.org/10.1016/S0165-1765(00)00332-3.

[32] Rennie, Ellie, et al. "Toward a Participatory Digital Ethnography of Blockchain Governance." *Qualitative Inquiry*, vol. 28, no. 7, 2022, pp. 837–47, https://doi.org/10.1177/10778004221097056.

[33] Rousseau, Jean-Jacques. *The Social Contract*. Penguin Books, 2004.

[34] S. Alzahrani and T. U. Daim, "Analysis of the Cryptocurrency Adoption Decision: Literature Review," *2019 Portland International Conference on Management of Engineering and Technology (PICMET)*, 2019, pp. 1-11, doi: 10.23919/PICMET.2019.8893819;

[35] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System, 2008,* available at https://bitcoin.org/bitcoin.pdf;

[36] Savelyev, Alexander. "Contract Law 2.0: 'Smart' Contracts as the Beginning of the End of Classic Contract Law." Information & communications technology law 26.2 (2017): 116–134. Web.

[37] Swartz Lana (2018) *What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology*, Cultural Studies, 32:4, 623-650, DOI: 10.1080/09502386.2017.1416420;

[38] Szabo Nick, Unenumerated blog, *Money, blockchains, and social scalability,* 2017, available at https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html;

[39] Tan, Evrim, Stanislav Mahula, and Joep Crompvoets. "Blockchain Governance in the Public Sector: A Conceptual Framework for Public Management." (2021): n. pag. Web.

[40] Tanaka Y., On the topological equivalence of the Arrow impossibility theorem and Amartya Sen's liberal paradox, Applied Mathematics and Computation, Volume 181, Issue 2, 2006, Pages 1490-1498, ISSN 0096-3003, https://doi.org/10.1016/j.amc.2006.02.035.

[41] Tikhomirov, Sergei, *Ethereum: State of Knowledge and Research Perspectives* (in proceedings); Foundations and Practice of Security; 2018; 206—221; Springer International Publishing; 978-3-319-75650-9;

[42] Tuckness, Alex, "Locke's Political Philosophy", *The Stanford Encyclopedia of Philosophy* (Summer 2018 Edition), Edward N. Zalta (ed.), available at https://plato.stanford.edu/archives/sum2018/entries/locke-political/

Appendix 1

```
pragma solidity 0.8.*;

contract smartCityDAO {

 address addr = {MAYOR_ADR};
 address payable public mayor = payable(addr);

 address adminAddr = {ADMIN_ADR};
 address public aadharAdmin = payable(adminAddr);

 uint8 public population;
 uint8 public totalTaxTxs;
 uint8 public totalActivities;

 function treasury() public view returns(uint) {
  return address(this).balance;
 }

 struct person {
  string name;
  uint8 age;
  uint256 tax;
 }
 mapping(address => person) citizens;

 struct activity {
  string title;
  string description;
  uint32 funds;
  uint8 upvotes;
  uint8 downvotes;
  address[] voters;
  activityStatus status;
  uint256 time;
 }
 mapping(uint8 => activity) activities;

 enum activityStatus{pending, approved, failed}

 event taxPayed(address name, uint256 amount);

 event voted(string activityTitle, address citizen);

 event activityProposedOrApproved(uint8 id);

 event mayorPunished(uint8 id, uint256 amount);

        modifier onlyMayor() {
          require (msg.sender == mayor, "You are not the mayor of this city!");
          _;
        }

        modifier onlyCitizen(address addrs) {
          require (citizens[addrs].age != 0, "You are not a citizen of this city!");
          _;
        }

        modifier onlyAadharAdmin() {
          require (msg.sender == aadharAdmin, "You are not the aadharAdmin
of this city");
          _;
        }

        modifier toVote(uint8 id) {
          bool a = true;
          for(uint8 i=0; i<activities[id].voters.length; i++) {
          if(activities[id].voters[i]==msg.sender) {
          a = false;
          }
          }
          require(a == true, "You have already voted!");
          _;
        }

        modifier approved(uint8 id) {
           require(block.timestamp - activities[id].time > 86400, "The voting
time period hasn't completed");
          require(activities[id].upvotes > activities[id].downvotes, "The activity
has failed due to majority of protesters");
          _;
             if(block.timestamp - activities[id].time > 86400 &&
activities[id].downvotes > activities[id].upvotes) {
          activities[id].status = activityStatus.failed;
          revert("The activity has failed due to majority of protesters");
          }
        }

        /* Functions of aadharAdmin */

        function addCitizen(address payable addrs, string memory name, uint8
age) public onlyAadharAdmin {
          require(citizens[addrs].age == 0);
          require(age != 0);
          citizens[addrs] = person(name, age, 0);
          population = population+1;
        }
```

```
    function readCitizen(address payable addrs) public view onlyAadharAdmin returns(person memory) {
        return citizens[addrs];
    }

    function removeCitizen(address payable addrs) public onlyAadharAdmin {
        delete citizens[addrs];
        population = population-1;
    }

    /* Functions of Mayor */

    function proposeActivity(string memory title, string memory description, uint32 funds) public onlyMayor {
        address[] memory voters;
        totalActivities++;
        activities[totalActivities] = activity(title, description, funds, 0, 0, voters, activityStatus.pending, block.timestamp);
        emit activityProposedOrApproved(totalActivities);
    }

    function getFunds(uint8 id) external approved(id) onlyMayor {
        activities[id].status = activityStatus.approved;
        payable(msg.sender).transfer(activities[id].funds);
    }

    function imposeTax(address citizen,uint256 tax) public onlyMayor {
        citizens[citizen].tax = citizens[citizen].tax + tax;
    }

    /* Functions of Citizens*/

    function payTax() public payable onlyCitizen(msg.sender) {
        require(msg.value <= citizens[msg.sender].tax);
        citizens[msg.sender].tax = citizens[msg.sender].tax - msg.value;
        emit taxPayed(msg.sender, msg.value);
        totalTaxTxs++;
        payable(msg.sender).transfer(msg.value);
    }

    function voteActivity(uint8 id, bool vote) public onlyCitizen(msg.sender) toVote(id) {
        activities[id].voters.push(msg.sender);
        if(vote == true) {
        activities[id].upvotes++;
        } else {
        activities[id].downvotes++;
        }
        emit voted(activities[id].title, msg.sender);
    }

    function myDetails() public view onlyCitizen(msg.sender) returns(person memory) {
        return citizens[msg.sender];
    }

    /* Public Functions */

    function getActivities(uint8 id) public view returns(activity memory) {
        return activities[id];
    }

    function punishMayor(uint8 id) external onlyCitizen(msg.sender) approved(id) {
        require(activities[id].status == activityStatus.failed, "The activity has not failed");
        uint256 balance = mayor.balance;
        uint256 halfTokens = mayorTokens / 2;
        require(halfTokens <= balance, "Mayor balance is not enough to punish");
        mayorTokens = halfTokens;
        mayor.transfer(halfTokens);
        emit mayorPunished(id, halfTokens);
    }

}
```