A ROAD-MAP OF SMART SOCIAL CONTRACT: EVOLUTION OF A SMART CONTRACT-BASED ECONOMIC AND LEGISLATIVE SYSTEM

Pregledni članak

M.Sc. Mehmet Zirek, email: mzirek@umt.edu.al
Metropolitan University of Tirana; Rr. Sotir Kolea & Budi, Qyteti Studenti, Tirana, Albania
Prof. Dr. Özcan Asilkan, email: oasilkan@cit.edu.al
Canadian Institute of Technology; St. Xhanfize Keko, Xhura Complex, No. 12. Tirana, Albania

Abstract: Public perception of modern, electoral liberal democracy is distorted by rapidly changing technology and the internet, undermining the effectiveness and even legitimacy of elected officials who are unable to cope with growing governance issues. Resolution of some of these problems such as the effective communication of decision making processes and the economic and social results of decisions in an open and transparent way requires a fundamental change in the implementation of the foundational philosophy of Social Contract in a society. In this paper, a roadmap of technology-based progress is proposed to redesign the roles of the citizens and the representatives in the process of public decision-making. The side questions of election systems, universal basic income, tax collection, open and transparent communication of the public projects as well as compliance with global and environmental constraints are discussed and findings based on block-chain technology are proposed, drawing a roadmap to Smart Contract based transparent society.
Keywords: Social Contract, Smart Contract, Block Chain, Liberal Democracy, Economy, Legislation

1. Introduction

The economic and legislative systems of most of the 21st century democratic countries are based on the 18th century developments in the USA and France, mainly on the human rights declaration and constitutional studies at the focal point of these two political and economic changes. The philosophy behind these changes is called Social Contract theory, and Hobbes (1651), Locke (1660-1662), Rousseau (1762) base their important works and lives on this theory. Many European states followed suit, declaring their independence from monarchies and empires.

Since then, three major waves of change have occurred that have changed the world's political and economic environment. These waves can be listed as follows:

- The industrial revolution that brought a huge increase in railroads, mass production, and international trade and banking
- The microelectronics and computer revolution of the mid-20th century
- Communication and internet revolution in the late 20th century

Currently, social media and mobile technologies are shaping and deepening the internet revolution. The amount of data in business and social life is increasing exponentially. The accelerating pace of change in the economy, education, health and communications fields

requires more effective and detailed policies that are both higher volume and becoming more complex to address and tackle problems.

However, in much of the world, the representative systems of democracies still rely on representatives of parliaments, congresses and senates, who are re-elected within an average of 4-5 years, forming and controlling governments. Election mechanisms for representatives are not public and transparent, and interpretations of the law regarding the powers of representatives are often decided by governments. This shadowing of the legislature (parliament/senate) by the executive branch (government) extends to the judiciary alike in many countries. The constitutional rights of the people are so abstract and it is difficult to impose a transparent and open system, because the economic decision-making role of governments gives them so much power that they even take control of the press, which is the 4th force with the role of overseeing the balance and separation of the three main estates.

In the 21st century, governments are confronted with increasingly sensitive and complex domestic, international and even global problems at an unprecedented rate. Gender inequality, global warming, energy security, unequal distribution of wealth and resources threaten the peace and stability of economies not only in underdeveloped countries but also in developed countries of the world.

The use of technology, particularly the Internet and mobile communications, to solve some of these global-scale problems has been suboptimal at best. In fact, the international companies behind these technologies are causing additional data privacy and information security issues for people.

The centralization of power, whether it’s financial or technological, results in loss of freedom of the individual. Decentralized nature of blockchain technology with smart contracts can be the remedy of this issue. In this paper, a transformation of the economic and legislative system is proposed, aiming at an ideal system where all legal, economic and social decisions as well as pre-existing legislation are converted into smart contracts and publicly verified on an open blockchain. Voting power for verification and verification is equally distributed among citizens, including children of all ages. The use of voting rights is continuous, that is, public projects can be stopped, changed, re-voted if enough changes in public opinion accumulate. The role and responsibility of the agents is the preparation of smart contracts with the help of technically trained public officials for this purpose.

2. Literature Review

Lee's (2014) working paper describes how the integration of citizens and public interest groups into the European democratic decision-making process has failed and gives the example of the Eurozone crisis, where national rulers, heads of international organizations and EU institutions systematically excluded national legislators from negotiation processes and subsequent responses. The vertical transformation of democracy in the EU with a top-down approach undermined the inclusion of National institutions in the EU integration process and played a major role in increasing economic and political inequality in the EU.

In parallel with the increasing bottom-up approach of advanced democratic processes, we observe the terms blockchain and decentralization in the literature. The official portal for European data*:* <data.europa.eu > cites the blockchain pilot in the government of Vienna,

Austria as an example of Open Data Blockchains. In this portal, Blockchain is described as a distributed database technology that can be used by individuals who want to complete transactions involving multiple parties without the need for a trusted third party and have the potential to be the next innovation to realize open, transparent and participatory government.

Other examples are found in the literature with different attempts to incorporate blockchains into the management of businesses, cities, towns and other practices of democracy and decentralization. The Public Sector Innovation Observatory (2018) published a statement, mapping the blockchain startups in the world categorizing them in three stages of development in Figure 1.

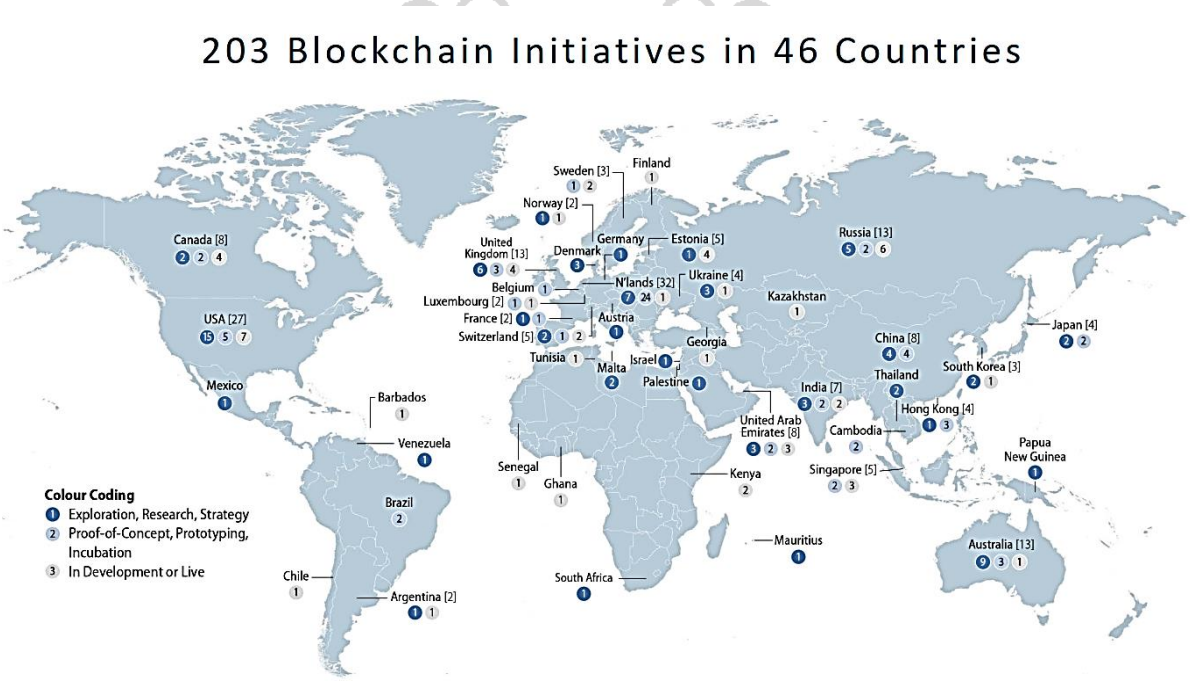

Fig. 1. Country Distribution of the Blockchain Initiatives. Source:Observatory for Public Sector Innovation (2018)

Srinivasan (2017), motivated by the well-known Gini coefficient and Lorenz curve, proposes the minimum Nakamoto coefficient as a simple, quantitative measure of the decentralization of a system. This coefficient is calculated as at least two numbers: first, the basic subsystems of a decentralized system must be enumerated, and secondly, the number of entities to control each subsystem must be compromised. The higher the value of this minimum Nakamoto coefficient, the more decentralized the system is. Srinivasan (2017) gives the following graphic interpretation (in Figure 2) of how the Gini coefficient and Lorenz curve reflect the income equality.

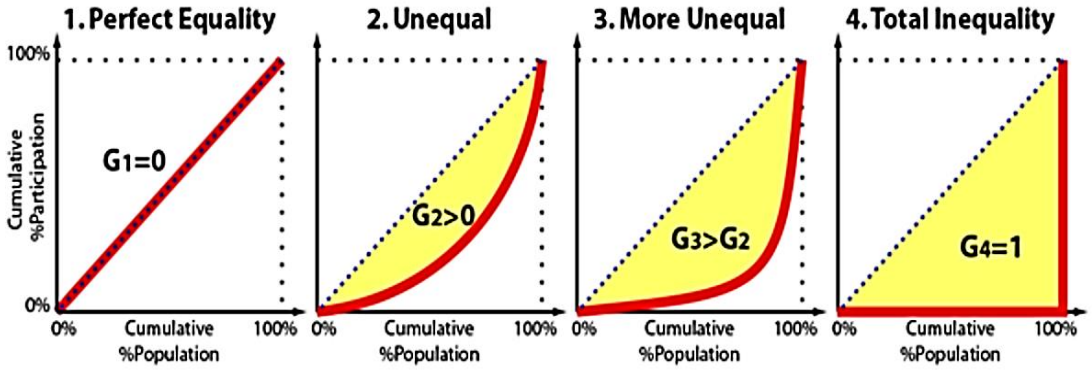

Fig.2. Gini coefficient and Lorenz curve visualization as a measure of Income Equality.Source: Srinivasan, (2017)

Similarly, the aforementioned Nakamoto coefficient, along with the Gini coefficient and Lorenz curve, has the potential to reflect decentralization and income equality in Blockchain-based democracies.

An open source report from Democracy Earth <github.com/DemocracyEarth/paper> argues that centralization is the only point of failure in elections and is incompatible with democracy. When centralized digital voting is applied to Partido de la Red decisions, it has been found that if an election is high-stakes (all or most members have a biased interest in the outcome), the probability of system disruption increases.

In Austria, Vienna's Open Government program is implementing one of the first public sector blockchains. The Open Government Data (OGD) portal in Vienna, < open.wien.gv.at >, defines its own task as making administrative data publicly available for any use.

Of course OGD programs in the EU are a good step forward towards an Open and Transparent democracy, while the data quality in these programs is an important issue. To address this issue, Raça, Velinov, Cico and Kon-Popovska (2021) describe in their recent paper, an application-based framework developed for analysis, monitoring and evaluation of National Open Data Portals. Following figure reflects results of six countries measured by their approach. As seen from this example, the main role of academia in reaching an open government is to be the oracle, defined above, of the governance data to inform the public in an unbiased way to support the transformation steps mentioned here.

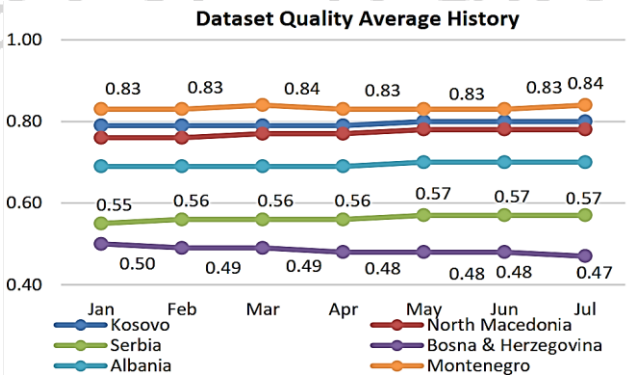

Fig.3. Dataset Quality Average history 2021 Jan-Jul. Raça, Velinov, Cico and Kon-Popovska (2021)

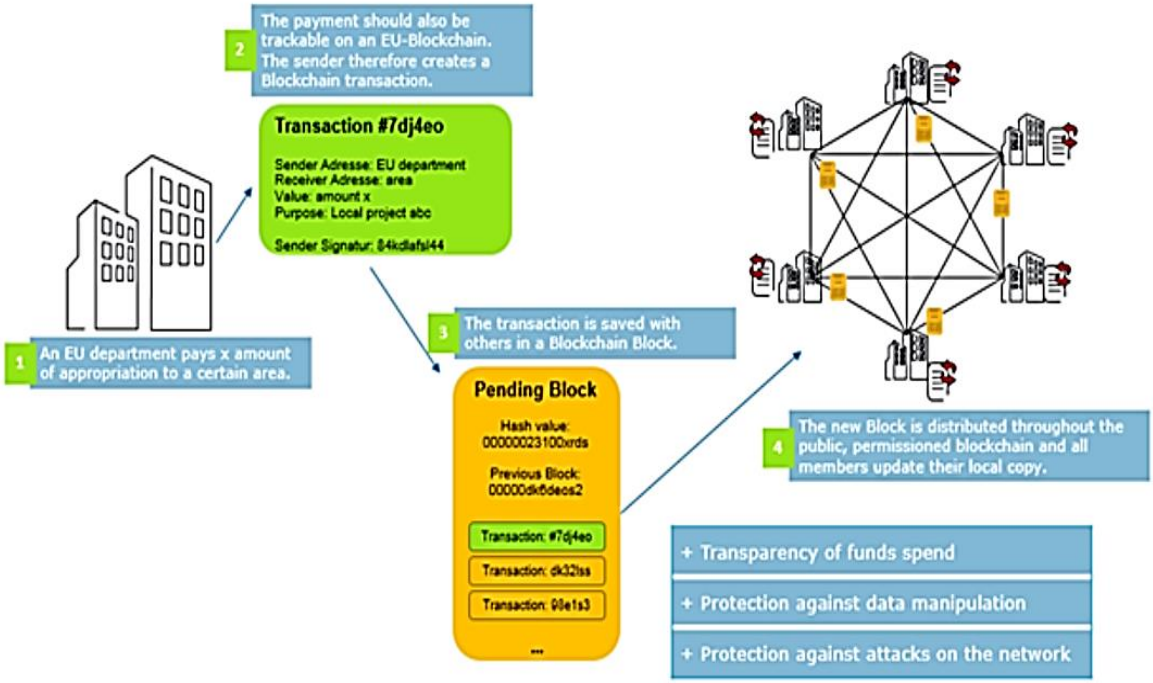

Fig.4. Example of blockchain based financial tracking system. Source: <data.europa.eu/fr/highlights/open-data-and-blockchain-match-made-heaven>

In a recent study on Asset Management of the transportation sector in Albania, Bardhi (2021) argues that public projects can be effectively and timely run if the transportation system assets such as roads, bridges and even road signs and road side commercial areas can be managed effectively. Of course, the main problem in establishing such a system is the lack of coordination of different regional and national institutions involved in projects related to transportation. A smart contract based project management system that will solve the problems of coordination and the smart contract codes can be directly linked to the national database right from the start. Smart contracts can also be extended to other areas and sectors in a bottom-up approach.

3. Smart Social Contract

Any democratic system needs a government formed by the “will of the people" as Rousseau (1762) said, and representative democracies are achieving this to some extent. However in the 21st century, the governments are more and more feeling the tensions and pressure from the changing needs of people due to technology and lifestyles. Increasingly interconnected new generations are more sensitive to global threats and issues and are more aware of the risks and shortcomings of the decisions of representatives and governments, usually behind closed doors. The will of the people needs to be shaped and followed by governments according to the principles of transparency, equality, freedom and human rights. Let’s see how these principles can be realized with current technologies.

3.1 Transparency

The quantity and quality of the open data available in a modern state determines the character of the government, and even the most advanced democracies are suffering from the lack of transparency. On the other hand, the system proposed in this paper contains transparency as an

essential component since every node of the blockchain contains a copy of the block history and is open to the public.

3.2 Freedom and Equality

The simple definition of equality in a democracy can be expressed as: “one man, one vote” However this principle can have a much deeper meaning if you consider this one vote as defined by consensus to be distributed into parts of direct vs. representative percentages. This is a new concept which can be achieved using blockchains and smart contracts as described in the global democracy platform in this paper. Such flexibility in voting has the potential to transform the democracy into a more advanced level and differentiate voting profiles of people more suitable to the level of government, area of voting and voter himself. Currently almost all government levels have similar electoral systems, whereas local governments need to be more direct than national ones and global governments need to be almost always indirect due to the needs of specialization on very complex matters such as global problems such as pandemics and climate change. Smart Contracts give the voters, right to determine the conditions of the voting system and to choose between using the tokens directly, indirectly or in a fraction. Having such a flexibility on the type of voting, will definitely result in the increase in democratic freedom of voters and ability to express the will of people at every level.

3.3 Feasibility

Although blockchains and smart contracts are based on cryptography and coding systems, they are relatively easy to implement due to their decentralised nature. The cost is spread over the individual nodes and open source code to run the chain and smart contracts is shared through a common version management environment such as Github for any enthusiasts to connect, download and install.

3.4 Technical Description

Although blockchains and smart contracts were conceptually defined by Szabo (1997), the real life implementation of them started with cryptocurrencies, especially Bitcoin and Ethereum.

3.4.1 Cryptocurrencies

Nakamoto (2008) has described a peer to peer cash system and created the genesis block, i.e. initial block of the new cryptocurrency, Bitcoin, in 2009. This system used a cryptographic validation and signature system with an open source code to run on a permissionless network of miners and nodes. Transactions are validated and added to blocks using mathematical and cryptographic techniques like hashing and Merkle trees, which in turn are connected to one another according to a consensus mechanism called “proof of work”. Miners who need to use energy to reach consensus on the network are incentivized by a reward mechanism. Thus, the first cryptocurrency was born. Today, Bitcoin’s market cap is around 1 trillion USD, and the total cryptocurrency market cap is over 2 trillion USD.
In Bitcoin and all other cryptocurrencies transactions created, confirmed forming block chains as described in the Figure 5 below.

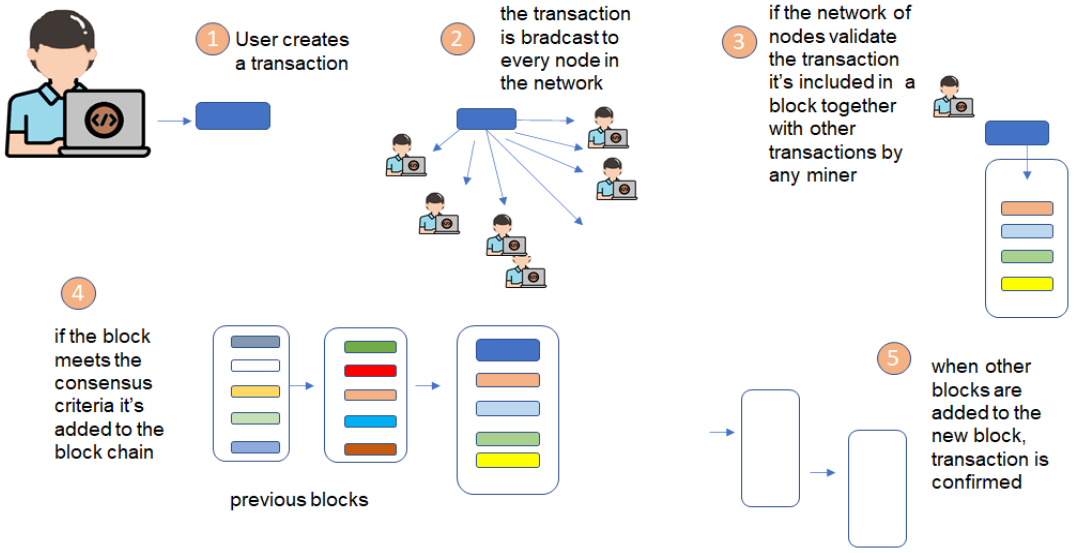

Fig. 5. How cryptocurrency transactions are confirmed.

3.4.1 Blockchains

Blocks of cryptocurrency transactions are immutable and secure due to their decentralized structure having redundant copies of the transaction data all through the network. Data on a blockchain is also very resilient to attacks since any node containing fake or erroneous data can be easily detected and fixed with many other readily available copies of it. Figure 6 below describes the immutability and security of blockchains.

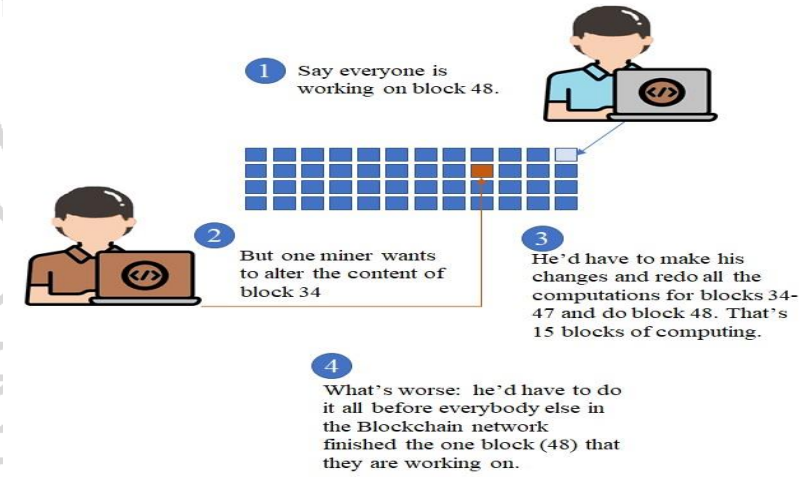

Fig. 6. Why blockchains are secure and immutable?

3.4.3 Consensus

The cryptocurrency rewards are distributed according to the consensus rule that determines the difficulty level at which a block can be mined, so that the alteration of previous blocks is gradually more difficult and computationally infeasible and/or too risky as new blocks are added. Some consensus mechanisms are described below.

3.4.4 Proof of Work

Majority of cryptocurrencies, including Bitcoin, use Proof of Work (POW) as the consensus mechanism. POW can be defined as the usage of hardware, software and energy to provide cryptographic proof of the computational effort required to secure a block chain. The difficulty level of the cryptographic computation can be adjusted in the block chain to achieve a stable cycle of block formation and rewarding of miners.

For example PoW is used in Bitcoin to decide which miner will win the reward and the transaction fees related to a block. It depends on the Hash computation difficulty, the level of which is determined by the network through a negative feedback mechanism dynamically aiming the block formation time to approach 10 minutes, i.e the difficulty is increased if a new block is formed in less than 10 minutes and decreased if the new block requires more time. The competition between the miners requires more computation usage, hence more powerful and advanced hardware which in turn consumes more energy. This energy-hungry mechanism constitutes the foundation of the controversy behind the sustainability issues of the cryptocurrencies.

3.4.5 Sustainability issues

High energy usage in computational difficulty of forming blocks is due to the nature of the POW mechanism of block formation. POW mechanism depends on the energy usage and in case the Ethereum Crypto currency rewards create competition of hardware and resources of miners to form blocks where only one miner can receive reward. Therefore the amount of energy used per transaction is not the energy of a single miner, but the energy used by all mining nodes of the network.

3.4.6 Proof of Stake

However POW isn’t the only consensus algorithm. More energy efficient algorithms, like proof-of-stake (POS), have been in development in recent years. In PoS, owners of a certain level of ETH qualify as validators and are randomly chosen to create blocks rather than miners. Therefore they do not require power-hungry hash machines to beat the competition. Because of this, energy consumption of POS is negligible compared to PoW. Ethereum has already started a gradual transition to this consensus algorithm aimed at significantly improving environmental sustainability. The security of the system comes from the risk of losing the stake when attempted to alter the block data or create invalid transactions.

3.4.6 Proof of Identity

Permissionless blockchain mechanisms of cryptocurrencies described above are transparent, libertarian and censorship resistant, but they have the issues of sustainability and to some extent favoring inequality, similar to the traditional financial systems. Also the need for regulatory power to deal with serious global threats of Climate change and Pandemics such as COVID-19 has not been addressed well enough. Therefore the ideal smart social contract can not be based on cryptocurrencies alone.

The blockchain foundation of the smart social contracts needs to be permissioned and not based on either POW or POS. Instead, the system proposed in this paper depends on the proof of

Identity (POI.) This mechanism gives the initiative to the POI nodes which are run by citizens or members of the blockchain defined in the democratic domain, i.e. the area, region, nation or organization. These citizens or members can benefit from the system to cover hardware and operational costs, and this income can form the basis for the minimum income level to determine different parameters of the relevant domain, such as Basic Income.

3.4.8 Smart Contracts

Szabo (1997) coined the term “smart contract” and defined it as “a set of promises, expressed in digital form, including protocols that the parties perform in other promises”.

Smart contracts are similar to paper-based traditional contracts between parties but written in computer code and automatically executed by the decentralized blockchain network. Some characteristic differences are listed in Table 1. They are immutable, i.e. once deployed, the code of a smart contract cannot change. Unlike with traditional software, the only way to modify a smart contract is to deploy a new instance. They are also deterministic which means the outcome of the execution of a smart contract is the same for everyone who runs it, given the context of the transaction that initiated its execution and the state of the blockchain at the moment of execution.

Table.1 Smart Contracts vs. Traditional Contracts

Traditional contracts	**Smart contracts**
1-3 days	Minutes
Manual remittance	Automatic remittance
Escrow is necessary	Escrow may not be necessary
Expensive	Fraction of the cost
Physical presence (wet signature)	Virtual presence (digital signature)

The main application area of Smart Contracts in a Blockchain-based democracy would be to enable liquidity of the voting processes in the democratic domains within the society. The voters publicly join political groups or vote as individuals, but they may keep the authority and representation rights if the general tendency in the domain changes.
Hierarchy of democratic domains are also established through interacting side chains based on a foundational block chain.

Although Bitcoin can run smart contracts, it doesn’t have a Turing complete mechanism, i.e. has limitations in what can be fed as data and what can be executed in these contracts. However, the second major cryptocurrency, Ethereum, has a block chain algorithm that was especially designed and built for execution of smart contracts. Ethereum block chain is also called decentralized Ethereum Virtual Machine, implying that it can be used as a distributed computational resource to run codes like smart contracts. This cryptocurrency has a potential to be used as a global environment for development and running of a multi-level, flexible, Free Democratic Platform for the World.

3.5 Proposed Democratic Platform

The proposed system contains a dynamic hierarchical network of blockchains, designed, created and run by people of the world to establish and execute smart contracts for each level of government. The electoral systems involve usage of tokens created for specific democratic domains and can be used in a flexible way with a user-determined percentage of direct vs.

representative way. For example, if a voter is using a vote directly in a global domain, he/she can directly use it at the global level and counts as (“1/world population” - hence “one man, one vote”), but another voter can delegate a representative together with the nation/region/district in which the corresponding votes give representative power to the delegate. It is even possible to split one’s vote between multiple cases where each vote would count as a fraction of the original vote. Conceptual diagram is given in the Figure.7 below.

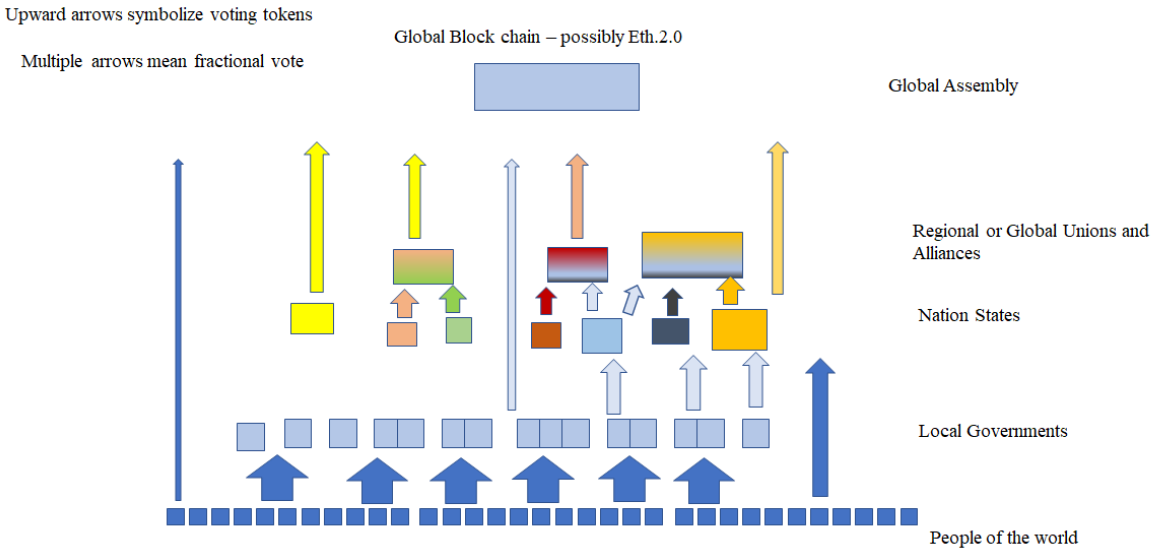

Fig.7: Global Democratic Platform- conceptual diagram.

Main differences between the current democratic systems and the proposed system are summarized in the Table 2 given below.

Table 2: Comparison of Current and Proposed System

	Current System	**Proposed system**
Criteria for election	Votes	Tokens
Voting rights	Citizens above a minimum age	All citizens
Election frequency	Typically every 4-5 years	Continuous
Election scope	Representatives/Presidents/Local governments	Representatives/Public projects/Local and international decisions
Power of elected representative	Limited/highly influenced by the Government	Legally using the tokens given by smart contract
People’s influence on public decisions after election	Very limited through protests and pressure groups	High with the additional tokens distributed over time
Restrictions on the elected representatives	Existing legal framework and judiciary system	Smart contract conditions
Restrictions on the governments	Existing legal framework and judiciary system	Smart contract conditions
Control over public funds spending	Representatives and existing financial controlling bodies	Smart contracts
Transparency of public projects	Low, often resulting in corruption	Public blockchain and tokens = full transparency
Decisions that require consistency and long term decisions	Only controlled by responsible representatives and public vote at the end of the term	Requires public decisions by additional tokens

Budget revisions	Only controlled by responsible representatives and public vote at the end of the term	Requires public decisions by additional tokens
Regional or local votes resolution on specific projects/decisions	Accumulated at the local governments	Can be brought down to citizen level direct democracy depending on the project/decision
Economic incentives and power	Centralised at the government	Can be detailed upto citizen level
Tax collection	In national currency through traditional banking system	In national cryptocurrency through blockchain based banking system
Social security	Traditional social insurance system	Universal basic income
Voting system	Traditional ballot based	Electronic blockchain based
International and global relations	Government foreign affairs administration supported by diplomatic staff	Run by a global regulatory smart contract
Resource management	Run by the government administrative staff on different fields of expertise	Run by smart contracts for each resource and controlled by expert staff

3.5.1 Tax Collection and Public Projects

The greatest barrier against the idea of defining a cryptocurrency as a tax basis is the trans-national character of the cryptocurrencies. The permissionless block chains are perceived as a threat to the national governments and traditional banking systems since governments are reluctant to give up the flexibility in defining monetary policies and taking financial decisions of over-the-budget spending to gain popularity for the elections. Of course, this is not in the best interest of the people in the long run.

Tax collection through permissioned public block chain based cryptocurrencies will make the whole system traceable and auditable since the public accounts used for taxes are included in the block chain in an immutable way. The transactions made from these accounts are also traceable. Therefore ultimate transparency in spending taxpayers' money can be achieved if such a basis is defined.

Public projects are the main source of corruption in many emerging and developing countries. These projects can be traced and decided directly by the people of concern if a smart contract based data sharing and fund transfer mechanism can be established. In the ideal case people can determine the auditing system they want to see in financial controlling and management of the public projects.

3.5.2 Contact with the traditional finance:

One of the important barriers against decentralised finance (DEFI) is lack of reliable contact and conversion mechanism with the traditional finance and economies. If achieved, this gives the opportunity of being a hub for new and valuable DEFI assets to the pioneers of Blockchain based economies. This hub can give diaspora and foreign investors the opportunity to invest in the country through smart contracts developed and supported by the academia and experts.

When the national currencies are attached via stable coins to reliable smart contracts the country will receive free investment from all over the world.

3.5.3 Universal Basic Income

Poverty is the biggest threat to global peace and democracies. Universal Basic Income (UBI) can be defined as a government program that allocates a set amount of money regularly for every citizen. It's an alternative system to the existing social welfare systems. This income can be attached to a special social smart contract which balances the welfare capabilities of democratic domains with the inalienable human rights. It would remove many social problems resulting from lack of financial freedom and gradually replace the current wasteful and unfair social welfare systems. Proposed system in this paper can link this basic income to citizenship and membership rights. This allows for different societies to develop the social contracts suitable for their needs.

4. Conclusions

Proposed blockchain based democratic system in this paper has the potential of actualizing the ideals of social contract theorists with the tools provided by the internet technology, especially blockchains and smart contracts. The system can replace the "chains" of modern states in Rousseau's famous quote[49] with blockchains not only to gain the individual and civil freedom, for the sake of which we enter the civil society but to deal with the global and local problems of the world in a fair, effective, open and transparent way. The technical details of the proposed system is beyond the scope of this work and is requiring further study/studies involving collaboration of fields of finance, law and technology as well as international relations.

5. References

[1] Bardhi, Diana. "Road Asset Management Assessment", European Journal of Engineering and Formal Sciences. July -December 2021Volume 4, Issue 2, pp 28-33
[2] Hobbes, Thomas. Leviathan, or the Matter, Forme, and Power of a Commonwealth, Ecclesiasticall and Civil. 1651, Referenced through Routledge Philosophy GuideBook to Hobbes and Leviathan, 2008, Routledge.
[3] Lee, Dexter (2014). The European Union's Democratic Deficit and Options for EU Democracy in the 21st Century. Working Paper, EU Centre in Singapore.
[4] Locke, John. First and Second Treatises on Government. 1660 & 1662. (Referenced through Routledge Philosophy GuideBook to Locke on Government D.A.Lloyd Thomas., 1995.)
[5] Observatory for Public Sector Innovation (OPSI) proceeding from Meeting of the OECD Global Parliamentary Network, October 10, 2018, https://www.oecd.org/parliamentarians/meetings/gpn-meeting-october-2018/OPSI-Blockchain-Presentation-for-Global-Parliamentary-Network.pdf >, accessed 1.12.2021
[6] Raça, Vigan & Velinov, Goran & Cico, Betim & Kon-Popovska, Margita,(2021). Application-based Framework for Analysis, Monitoring and Evaluation of National

[49] The opening sentence of Rousseau's "The Social Contract" is "Man is born free and everywhere he is in chains."

Open Data Portals. International Journal of Advanced Computer Science and Applications. Vol. 12. 26-36.

[7] Rousseau, Jean Jacques. The Social Contract, or Principles of Political Right (Du contrat social), 1762. (Referenced through Routledge Philosophy GuideBook to Rousseau and The Social Contract, Cristopher Bertam, 2003, Routledge)

[8] Satoshi Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”. White Pap. 2008, 1, 9

[9] Srinivasan, Balaji S. (2017). Quantifying Decentralization, https://news.earn.com/quantifying-decentralization-e39db233c28e >, accessed 1.12.2021

[10] Szabo, Nick. 1997 "View of Formalizing and Securing Relationships on Public Networks | First Monday" < https://doi.org/10.5210/fm.v2i9.548 >

[11] <https://data.europa.eu/en/news/open-data-blockchains-missing-link-opening-governments > accessed 1.12.2021

[12] https://open.wien.gv.at/site/1-blockchain-pilot-ogd-aenderungsprotokoll-und-notarization/ accessed 1.12.2021

[13] < https://github.com/DemocracyEarth/paper >, accessed 1.12.2021

[14] <https://data.europa.eu/fr/highlights/open-data-and-blockchain-match-made-heaven >, accessed 1.12.2021, Open Data and Blockchain: a match made in heaven?