

Developing an integrative framework of Artificial Intelligence and Blockchain for augmenting smart governance

Venkatesh R, Aayush Kumar, Yadhukrishna S Pai and Projjal Gupta

Abstract—Government systems are often slow, opaque and prone to corruption. The public benefits system, in general, suffers from slowness and bureaucracy. In this paper, we propose a system that utilizes blockchain and artificial intelligence techniques for governance, that enables the government to function more efficiently and with more transparency, thus increasing the level of trust the people have in their government and in democracy.

Public Distributed-Ledger Ethereum (MainNet) is the backbone of this proposed system. SHA-256 of Elliptic-Curve cryptography generates a Public-Private keypair. Each transaction is validated by P2SH and the consensus is achieved through Proof-of-Work Algorithm. A smart contract encodes the algorithm and enforces constraints on users activity. Artificial Intelligence is used to analyze the data wherever necessary and the output of the network is used as a trigger for activating the smart contract, which can be connected via IoT services and automation devices. This can be used for making government contracts more transparent.

Some use cases are automatic payments based on achieved deadlines and allowing public consensus on government policies. Other applications include a better functioning public benefits system that allows the government to directly provide the public with incentives rather than relying on middlemen. Decentralization via blockchain is a complete end-to-end solution for democratizing the current systems.

I. INTRODUCTION

Government is an organization or a group of people given authority to govern a particular state or country. It is the largest administrative and executive body of any country and is responsible for its management, which also includes judiciary and legislation. Each and every minute decision was taken by a government affects the life of its citizens. So ideally a government should be open and incorruptible.

Modern technology can be used to re-enforce governmental policies. Introducing Artificial intelligence to identify and analyze human behaviour can yield beneficial data, which in turn can be used for the proliferation of the standards of living. Usage of secure and immutable data storages such as blockchains can eliminate redundancy and can be used for logging accurate data, which cannot be altered. Internet-of-things devices and technology can be used for sampling data and be used as a trigger to call preventive functions and maintain order.

This paper discusses the vision of smart government propelled by the use of modern technology and machines. The fundamental idea of a smart government pushes forward a set of rules and protocols which ensures no fractures in the foundation of a governing body.

II. OVERVIEW

A. Blockchains

Ethereum is a distributed database that keeps a permanent record of digital transactions. This database doesn't require any central authority to maintain and secure it. Instead it operates as a trustless transaction based framework in which individuals can make peer-to-peer transactions without needing to trust a third party or one another.

A blockchain is a cryptographically secure transactional singleton machine with shared-state. Every state of Ethereum has countless of transactions. These transactions are grouped into blocks. A block contains a series of transactions, and each block is chained together with its previous block.

To cause a transition from one state to another, the transactions must be valid. For a transaction to be considered valid, it must go through a validation process known as mining. Mining is process done by a node in which it attempts to solve a cryptographic puzzle by expending its computational resource. A miner who validates a new block is rewarded with a certain amount of value for doing this work.

In Ethereum, the state is made up of objects called "accounts", with each account having a 20-byte address and state transitions being direct transfers of value and information between accounts. An Ethereum account contains four fields:

- The account's current ether balance.
- The account's contract code.
- The account's storage.

The nonce, a counter used to make sure each transaction can only be processed once.

```
{ "hash": "0000000000e37 ...",  
  "prev_block": "000000000000a5d ...",  
  "time": 135410800,  
  "difficulty": 436527338,  
  "nonce": 282060624,  
  "tx": [ { "hash": "5c1 ...",  
            "in": [ { "prev_out":  
                    { "hash": "000...", },  
                  }  
            ], "out": [  
              { "value": "50.53620000",  
                "scriptPubKey": "152a1..."  
            } ] } ] }
```

Listing 1. A schematic representation of block in the blockchain, in form of JavaScript Object Notation (JSON).

B. Artificial Intelligence

In the most trivial terms, an artificial intelligence is a system that can learn how to learn, or in other words a series of instructions (an algorithm) that allows computers to write their own algorithms without being explicitly programmed for. Unlike blockchain technology, artificial intelligence is not something new and has been around since the 1950s. AI as an interdisciplinary field, which covers (and requires) the study of manifold sub-disciplines, such as natural language processes, computer vision, as well as the Internet of things and robotics.

AI may be broadly classified into three types-

- Application specific AI - This is the type of artificial intelligence that is built to solve a particular task by being trained on the data required to solve the task. An example of this would be IBM's deep blue ^[1].
- Artificial General Intelligence - This is the type of AI that can generalize its intelligence to a range of task. It is not trained to for specific application but rather can apply its knowledge to a range of tasks. Although we are far from reaching this the closest example would be Googles' Deep Mind ^[2].
- Artificial Super Intelligence - This is the type of artificial intelligence whose ability far exceeds those of humans and is capable of scientific and creative thinking. This is the kind of AI which will have emotions and ability to interact with humans and other AI.

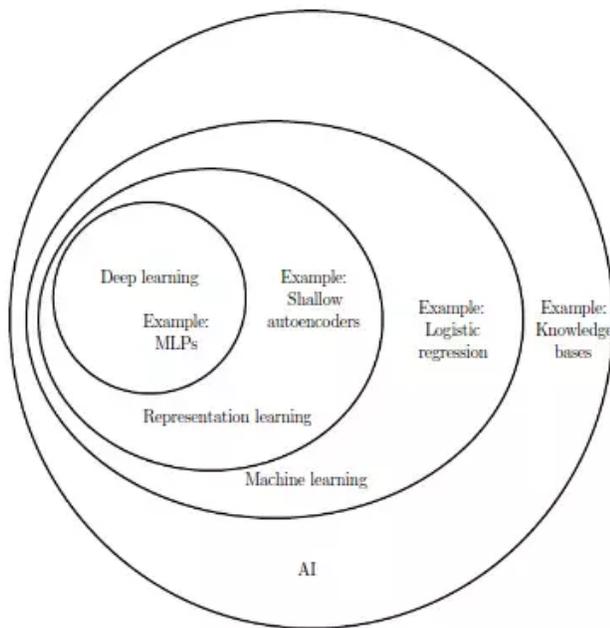


Fig. 1. Constituents of Artificial Intelligence

C. Internet of Things

Internet-of-things is an ecosystem based on interconnected machines and platforms. At a higher level, IoT facilitates the communication amongst multiple devices, ranging from handheld devices to server farms. The philosophy behind

the IoT was proposed in 1990's and it is a broad-spectrum term used for all forms of communication protocols, both hardware and software.

IoT is an essential middleware when being used in a smart government model. All the data required by an AI model for processing is provided for by an IoT device or service. IoT devices are also used as a trigger for mechanical outputs. In case of a trigger event, IoT communications can enable the preventive measures required.

III. ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN

It is undeniable that AI and blockchain are two of the major technologies that are catalyzing the pace of innovation and introducing radical shifts in every industry. Although extremely powerful, a blockchain has its own limitations as well. Some are tech-related while others are due to economic inefficiency, Artificial Intelligence can help solve them.

- Energy Consumption : As of the date of writing this paper, the energy consumption of bitcoin mining is 49 TWh. The country closest to this amount of energy consumption is Singapore. The mining centres generate a lot of heat that must be removed to keep the servers running. This cooling is typically accomplished via large industrial equipment such as pumps, chillers and cooling towers. Researchers at Googles Deep Mind have addressed this issue by using machine learning to solve this issue by dynamic adjustment of cooling equipment.
- Scalability : The average block size of 1MB for a block interval of 10 minutes leads to the size of blockchain to cross 200GB. Unnecessary data on blockchain like fully spent transactions on a single device could be removed. Federated Learning could be used on blockchain or better sharding techniques could be applied to solve this problem.
- Reduce Monopoly: Currently conglomerates like Google , Microsoft and Alibaba have a huge advantage when it comes to access to user data. And as we know data is the new currency this puts small companies at a huge disadvantage. Also these companies are free to do whatever they want with our data without anyone to question them. Blockchain technology can allows us to auction our data without revealing sensitive information.
- Anonymity & Privacy: Ever Since the silk road got compromised the question of actual anonymity and privacy is in question. Methods like homomorphic encryption^[3] and projects like Enigma^[4] provide possible solutions. Ring Signatures implemented on Monero^[5] and Zk-Snark on ZCash^[6] are possible solutions to anonymity.

IV. APPLICATIONS

A. Payments for public contracts based on smart contracts

The government often outsources its work to private contractors which are privately owned firms. This brings into question the accountability of the company and also the quality and progress of the work done. It is found that the government outsources 51% of its work to contractors. This calls for strict norms in place to ensure that the work

done by these contractors is up to the mark and completed on time. We propose a system which uses a subtle interplay of Artificial Intelligence, Blockchains and Internet of Things to solve this problem.

Convolutional neural networks (CNNs) are a type of deep learning approach that can act directly on the raw inputs. By the recent advances in this learning approach, a novel 3D CNN model^[7] for action recognition^[8] has been developed. This model extracts features from both the spatial and the temporal dimensions by performing 3D convolutions, thereby capturing the motion information encoded in multiple adjacent frames. The developed model generates multiple channels of information from the input frames, and the final feature representation combines information from all channels. This approach can be used to classify the progress of the projects from the construction sites. By taking the surveillance videos and using that as an input for the model, we can evaluate the progress in the completion of work. Using IoT sensors attached to the building, the data collected from the sensors can be sent to a logistic regression model that can classify the quality of the construction work as satisfactory or unsatisfactory without any human intervention. If these two conditions are satisfied, it sends a trigger to call the function in the smart contract.

The external trigger from AI and IoT device will be fed as arguments of a function in Smart Contract, according to the arguments (Progress of Work) the contractors account will be credited with the proportionate amount of assigned fund. The smart contract also keeps track of progress and only transacts the change in progress than the progress as such to prevent relay attacks.

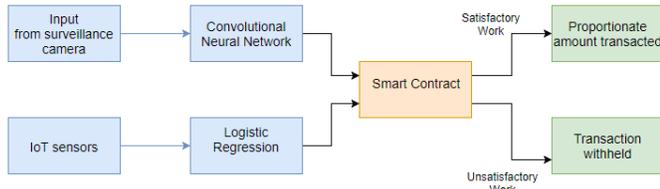


Fig. 2. Workflow of public contracts based on smart contracts.

B. Commodities for the poor at subsidized rates

One of the major problems our country faces is providing financial services, namely banking savings & deposit accounts, remittances, credit, insurance, pension in an affordable manner.

For a country like India with a large population and many people living in the rural areas, this is a huge problem because of -

- Lack of banks and ATMs in remote areas.
- Minimum balance required to open an account.
- Long queues and inefficient operation of banks.
- Corrupt officials at each level of the system.

A public benefit distribution system which is void of such obstacles can be built by exploiting the blockchain

technology with already existing Unique Identity System (UID). A Smart Contract can have an oracle access to the API to get data from identity system. The information analysis tags a person to either Below Poverty Line(BPL) or Above Poverty Line(APL). The below poverty line tag enables access to a subsidised market rate for products like staple food grains, such as wheat, rice, sugar and kerosene, for people purchasing through the vendor contract. If one does not have the BPL tag, that person can purchase at the regular market rate. The person now goes to the distribution centre and provides the transaction (in form of QR-code) which is non-repudiable and gets the product in return. The vendor reads the QR code and marks the transaction as complete and prevents double spending.

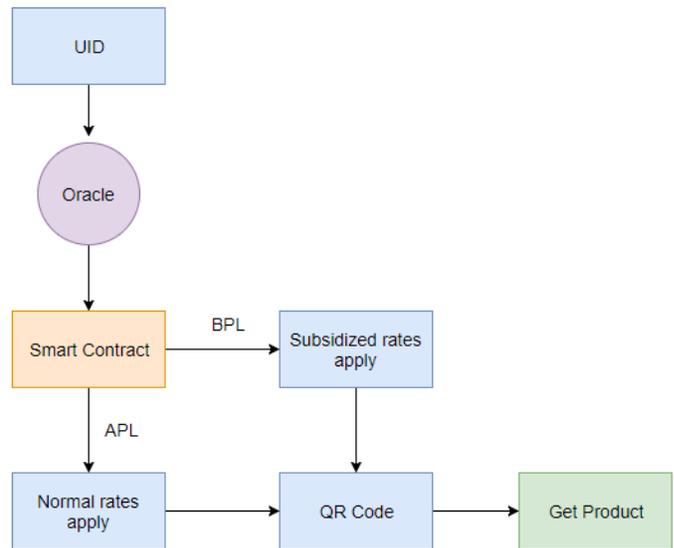


Fig. 3. Workflow of commodities for the poor at subsidized rates.

C. Transparent Democratized Legislative process with Public Sentiment

The current system of Governance is obtuse in the nature it runs. There is a need to democratize the process of crafting legislation, a hybrid system of immutable, transparent consensus spearheads the way to bring power to the people while not disrupting the current system of Governance by an elected representative. A system where the draft of the bill is proposed on blockchain in form of a Smart Contract entry. The elected representative will vote on the bill and the entire process from proposal to outcome of the bill is recorded and accessible publicly.

The job of the elected representative is to work for and represent the people of that district/state. Often it is seen that many bills are passed in the house of parliament that are unpopular with the public due to lack of communication between the common man and the representatives. This is the leading people losing faith in their elected representatives and the government as whole. Sentiment analysis can be used effectively as a public opinion monitoring system^[9] to better serve the people.

In the condition where the opinion of citizens are necessary like net neutrality, the modifier allows the citizens to participate in the voting process and the outcome is automatically either accepted or rejected. It is impossible to modify the outcome after it is decided.

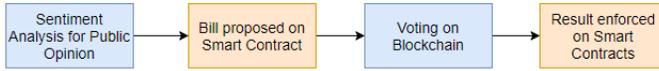


Fig. 4. Workflow of transparent democratized legislative process with public sentiment.

V. CONCLUSION

Artificial Intelligence and Blockchain are by far the most powerful technologies out there. If combined in a symbiotic way, they can be used to help the society in unimaginable ways. This paper covers some of the use cases that these technologies might be used for. The main motivation behind this paper was to create something that can be used for socially impactful causes. Some of the issues that our country faces are-

- In India 43% of the country's population^[10] still don't have bank accounts.
- There are only 18 ATMs' for every 100,000 people^[11].
- The system works on trust and assumes people to behave with honesty.
- Legislative process often is slow and complicated.
- Major technically difficult tasks are outsourced to private firms who may be deceitful.

We hope that the novel methods proposed in this paper can be used to successfully deal with these issues.

ACKNOWLEDGMENT

We would like to thank the Dr. C. Muthamizhchelvan, (Director E&T) for providing us with this opportunity. Also we would like to thank Dr. B. Neppolian and Dr. S. V. Kasmir Raja, (Dean Research) along with their entire team for organizing this event.

We gratefully acknowledge the support of NVIDIA Corporation with their generous donation of the GPUs that were used for this research.

REFERENCES

- [1] Murray Campbell, A. Joseph Hoane Jr., Feng-hsiung Hsu IBM T.J. Watson Research Center (Deep Blue)
- [2] Deep Mind, 6 Pancras Square, London N1C 4AG, UK
- [3] E. H. Miller, (Fully Homomorphic Encryption over the Integers)
- [4] Guy Zyskind Oz Nathan Alex Sandy Pentland (Enigma: Decentralized Computation Platform with Guaranteed Privacy)
- [5] Andrew Miller Malte Moser Kevin Lee Arvind Narayanan (An Empirical Analysis of Linkability in the Monero Blockchain)
- [6] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza (Zerocash: Decentralized Anonymous Payments from Bitcoin)
- [7] Volumetric and Multi-View CNNs for Object Classification on 3D Data, Charles R. Qi, Hao Su, Matthias Niessner, Angela Dai, Mengyuan Yan, Leonidas J. Guibas.
- [8] An Approach of Text Sentiment Analysis for Public Opinion Monitoring System, Min Zeng Email author Yujiu Yang Wenhuang Liu
- [9] 3D Convolutional Neural Networks for Human Action Recognition, Shuiwang Ji, Wei Xu, Ming Yang, Kai Yu

[10] CensusInfo India 2011 Houses, Household Amenities and Assets

[11] Press Information Bureau ,Government of India, Cabinet, 2016