Blockchain with Artificial Intelligence: Future of Travel

Varsha.C.Bendre, Prabhat Kumar Singh
Dept. of CSE, Sir M Visvesvaraya Institute of Technology
Bangalore, India
Varsha6319@gmail.com, Imprabhat12@gmail.com

Abstract— ***TRAVELBLOIN is the integration of artificial intelligence with blockchain. The new travel agencies are to be registered with the government before it starts functioning. The smart contracts are made between the government and the travel agencies and between the agencies and the customers to validate the Proof-Of-Activity and Proof-Of-Delivery. The digital identification which reduces the verification of the customer every time. It also controls the travel AI market through its distributed open network system of Artificial Neural Network which can interact with the customer and predict the total cost of traveling and also the offers are shown. The ANN algorithm is used to improve the functionalities of the network. This improves the user experience and benefits both the customer and the agency. The Hyperledger Fabric architecture is used to design the network. TRAVELBLOIN reduces the issues caused by fraud due to middle-men.***

***Index Terms*— Blockchain, Artificial Intelligence, Smart Contracts, Artificial Neural Network, Hyperledger Fabric**

I. Introduction

The AI integrated Blockchain has a great potential as the AI consumes as much as datasets as possible to learn better about them. The credibility that the blockchains provide to data makes it a good proposition for all the stakeholders. Integrating the two creates an efficient ecosystem.

The blockchain technology is transformative. The key innovation of blockchain is to access a strict control over privacy in spite of creating a database that is decentralized. Customers could authorize all the stores they patronize to contribute data about their purchases to a blockchain ledger that protects the privacy of both consumers and the travel agencies.

The consortium blockchain is the hybrid between the low trust public blockchain and single highly trusted entity model of private blockchains [1]. The company leveraging a blockchain to distribute the data to their suppliers does not mean that his competitors can see other supplier's data. The buyer can see the data that the suppliers have given the permission to access them.

In spite of making the transactional information public, the distributed ledger only has the amount of transaction and their hash. Hash code is generated by the exercising the cryptographic method on the transaction details. The hash is a code generated by running the actual transaction details through a cryptographic method. Hence, it is not possible to obtain the data other than the transaction

II. Key Elements of the Blockchain

The Distributed Autonomous Organization is one of the emerging blockchain applications and is incorporated on it because the DAO's governance is dependent on the end-users who are the users, owners, and nodes partially on that decentralized network [2]. The key aspects of such applications are that each user is also a worker and by the quality of their work they contribute to the value appreciation of the DAO through the collective participation. The DAO's benefit with User protection, user voice, user governance, transparency, self-regulation, sovereignty.

A. Node Application

In the travel blockchain application, like TRAVELBLOIN the participation is restricted and requires special permissions to join (referred to as consortium blockchains). TRAVEL-BLOCKCHAIN only permits the Travel agencies to run the node application.

Every agency needs to install and run a computer application specific to the ecosystem they wish to participate in. Each system must be running the TRAVELBLOIN application.

In a slight technical parlance, the ecosystem of the blockchain constitutes of a service overlay network (SON) and to be a node in the TRAVELBLOIN the Travel agency should be able to process application-specific messages and the shared state of the SON is affected.

B. Shared Ledger

The distributed or shared ledger is a data structure that is managed inside the node application. Once the node application is running, the respective ledger or blockchain contents of that ecosystem can be viewed.

Any number of node applications can be included and permitted to use, and each of the agencies will participate in the respectively allotted blockchains.

You can run as many node applications as you like and are permitted to use and each will participate in their respective blockchain ecosystems. It is important to note that regardless of how many ecosystems you are a participant in, you will only have one shared ledger for each ecosystem.

Smart Contracts: The TRAVELBLOIN has smart contracts between the government and the travel agencies and also between the travel agencies and their customers. The agencies register under the government with the terms and conditions that make them legal and also put them in contact with the embassy which makes it more efficient to know the status Indians in the respective country. The customers are allowed to look into the kind of services and offers provided by all the travel agencies registered under the network of TRAVELBLOIN, compare them and continue with their choice of interest. After a particular agency is being chosen a contract is made between the agency and the customer for every detail including the insurance. In case any accidents the details of insurance are sent to the respective companies and the insurance is claimed with the help of Proof–Of–Delivery.

The cryptocurrencies can also be used for the transactions in the smart contracts and it has a certain amount of benefits such as Irreversibility of the transactions, the transactions remain Pseudonymous as neither the transactions nor the accounts are being connected to the real-world entities, the transactions are fast, global and remains secure as the cryptocurrency funds are locked in a public key cryptography system.

C. Consensus Algorithm

This can also be addressed as the "Rules of the Game" for how the ecosystem will arrive at a single view of the ledger. Every ecosystem has its own methods of attaining the consensus depending on the desired features of the ecosystem needs. Let us consider the example of Bitcoin; it arrives at the consensus of the ledger in a few minutes.[3] The TRAVELBLOIN which is I the development stage takes a couple of minutes to arrive at the consensus of the ledger.

There are a number of different schemes that are being vested in the method for determining the "world state" for the participation in the consensus building process and each of them qualifies the nodes as honest with their algorithms.

Proof of Activity (Proof of Work+ Proof of Stake): The Proof of Work and Proof of Stake is being replaced with the Proof of Authority where the number of pre-approved authority nodes I.e. the sealers. The new node that has been added to the block has to be voted on by the currently approved set of authority nodes and this gives control over which nodes can seal blocks that is mine on the particular network.[4] In order to make sure that a malicious signer should not do much harm to the network any signer can sign at most one of a number of consecutive blocks (floor (SIGNER_COUNT / 2) + 1). The same algorithm is being applied when an authority node is being removed from a network [5].

Proof of Delivery: The Proof of Delivery is used when there is an occurrence of a disaster related to the customer and the insurance has to be claimed.[6] The paper documents and the delivery address will be identified and the recipient to endorse the delivery with a signature. A receipt is defined as an acknowledgment of having received or taken into one's possession. They universally confirm for the proof of purchase.

D. Virtual Machine

The final logical component of the blockchain ecosystem that acts as a container for the remaining logical components to rest, act and also interact with each other. This is a representation of a machine created by the computer program and is operated with the instructions. It is just an abstraction of a machine inside a given machine.

III. Hyperledger Fabric Architecture

The Hyperledger Fabric architecture delivers the advantages as follows Chaincode trust flexibility, Scalability, Confidentiality and Consensus modularity.

[7] The two parts of Hyperledger Fabric architecture are "Elements of the architecture relevant to Hyperledger Fabric v1" and "Post-v1 elements of the architecture"

A. Elements of the Architecture relevant to Hyperledger Fabric v1

The elements of the architecture can be divided into three components, namely

System architecture: The architecture of the system is the blockchain that is the distributed system made of a number of nodes that communicate with each other. The system chaincodes is made up of one or more special chaincodes for managing the functions and their parameters. Only the endorsed transactions are committed and have an effect on the state of the nodes.

The basic workflow of transaction endorsement: The transactions are executed in four steps.

a. The transaction is created by the client and is sent to the endorsing peers of its choice.
b. The endorsement signature is produced and the transaction is simulated by the endorsing peer.
c. The submitting client collects the transaction that is endorsed and broadcasts it through ordering service.
d. The transactions are delivered to the peers by the ordering service.

Endorsement policies: The Endorsement policies are specified and the transaction is evaluated against the endorsement policy.

B. Post-v1 elements of the Architecture

Ledger checkpointing: The abstraction of the ledger contains only the valid and committed transactions, peers may in addition state a ledger maintain the validated ledger. The hashchain is derived from the ledger by filtering out the invalid transactions. A Validated Block is defined as a block without any invalid transactions that have been filtered out from the block. Such Blocks are inherently dynamic in size and may be empty.

Every block of a validated ledger contains:

a. The hash of the previous validated Block.
b. Validated Block number.
c. An ordered list of all valid transactions committed by the peers since the last validated Block was computed.
d. The hash of the corresponding block from which the current validated Block is derived.

Peer Ledger Checkpointing: The invalid transactions in the ledger may not be necessarily recorded forever. Hence, those peers can be simply discarded from the Peer-Ledger blocks. The mechanism establishes the validity of the validated Blocks across the peer network and allows checkpointed validated Blocks to replace the discarded Peer-

Ledger blocks. This also reduces the work to reconstruct the state for new peers that join the network.

IV. Identification with the help of Elliptic Curve Digital Signature Algorithm (ECDSA) Authentication System

Key Pair Generation: A random number generator delivers a numeric value that is the private key and the public key is computed using the equation.

$$Q(x, y) = d \times G(x, y)$$

Signature Computation: A digital signature allows the recipient of a message to verify the message's authenticity using the authenticator's public key. The fixed length message is formed from the variable length message using the secure hash algorithm.[8] After the message digest is computed, a random number generator is activated to provide a value k for the elliptic curve computations.

The signature consists of two integer numbers, r, and s. The computation of r from the random number k and the base point G(x, y):

$$(x1, y1) = k \times G (x, y) \bmod p$$

$$r = x1 \bmod n$$

After r is successfully computed, s is computed using scalar operations.

$$s = (k^{-1} (h (m) + d * r) \bmod n$$

To be valid, s must be different from zero. If s is 0, a new random number k must be generated and both r and s need to be computed again.

Signature Verification: The signature computation is a counterpart of signature verification.[9] The purpose of the verification is to verify the authenticity of the message using the public key. Inputs are the message digests h (m), the public key Q(x, y), the signature components r and s, and the base point G(x, y):

$$w = s\text{-}1 \bmod n$$

$$u1 = (h (m) * w) \bmod n$$

$$u2 = (r * w) \bmod n$$

$$(x2, y2) = (u1 \times G (x, y) + u2 \times Q (x, y)) \bmod n$$

V. Interplanetary File System

The content-addressable web uses the IPLD (Interplanetary Linked Data) data, model. It is a data model for interoperable protocols.[10] It treats all the hash-linked data structures as the subsets of an information space by unifying the data models that link the data with the hashes.

The subsystems are built on top of the other subsystems in order to standardize the interface. The areas where the subsystem fit is:

1. Peer Routing – the Mechanism to decide which particular peers to use for routing the respective messages. The peer routing can be done recursively, iteratively and also in a broadcast/multicast mode.
2. Swarm - Handles everything that touches the opening a stream part of libp2p, from protocol muxing, stream muxing, NAT traversal and connection relaying while being multi-transport.
3. Distributed Record Store - A system to store and distribute records. The role is similar to DNS in the broader Internet.
4. Discovery - Identifying other peers in the network.

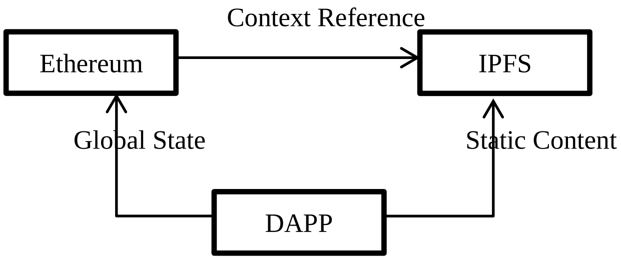

Fig 1: Structure of IPFS

VI. Artificial Intelligence for Blockchain

AI and encryption work very well together: The encryption of the data and Artificial Intelligence work together. The data that is residing in the blockchain is secure. The blockchain provides authenticity without the interference of any other blocks. Data in the blockchain is encrypted hence the security is enhanced. The emerging field of AI is concerned with the algorithms that are capable of processing and operating with the data while it is in the encrypted state [11]. Like any part of a data processor which involves exposing unencrypted data represents a security risk, reducing these incidents could help to make things much safer.

Blockchain can help us track, understand and explain decisions made by AI: The decisions made by AI are incomprehensible to humans. As the AI systems can access a large number of variables independently of each other and also learning which is important for accomplishing the objectives.

AI can manage blockchains more efficiently than humans: a Large amount of processing power is required to operate with blockchain data which is encrypted. AI is an attempt to move away from the brute force approach and the tasks in an intelligent manner.

An Artificial Neural Network (ANN) is a computational model which imitates the human brain capability of analyzing and processing information. ANN is capable of learning by observing data sets on its own to produce better results.

The costumer interacting with the blockchain can search for the travel cost for any destination. Based on destination location, distance from current location, age, gender, start date and end date we can predict the offers for them. It's not necessary for the customer to provide all the details. The Random Forest Regression is used to predict the NaN (not a number) based on the previous data in the blockchain.

Activation Function: The neuron present in the hidden layer of ANN gets triggered based on the input or set of inputs [12]. The output is calculated according to the activation function used. The ANN is developed by using 3 hidden layers. The Rectifier function is used which is defined as:

F(x) = max (0, x), where x is the input to the neuron.

Stochastic Gradient Descent (SGD): We are using SGD which is an iterative process that takes each row separately to calculate the cost and accordingly adjust the weight using backpropagation to reduce the cost.

VII. CONCLUSION

The time required to get a visa is reduced as the government remains one of the integral parts of the blockchain network. In the particular case that is being developed, the Indian embassy plays a major role. The digital identification can be further improved with the addition of biometric iris recognition. This helps in reducing the boarding time and the verification process time is also reduced. It is also helpful in case the documents are lost. The refugees when they travel from one country to other they will have to issue the documents at the airport. And also, the rest of the certificates which is required for their survival in the country.

VIII. ACKNOWLEDGMENT

Authors are very much thankful to the Head of Department, CSE in Sir MVIT, Bangalore for giving an opportunity to publish this technical paper. Thanks to dear professors whose kind support made this study and design possible.

IX. REFERENCES

[1] G.Foroglou and A.-L.Tsilidou, "Further application of the blockchain," 2015

[2] NRI, "Survey on blockchain technologies and related services," Tech.Rep.,2015.[Online].Available:http://www.meti.go.jp/english/press/ 2016/pdf/0531 01f.pdf

[3] C. Decker, J. Seidel, and R. Wattenhofer, "Bitcoin meets strong consistency," in Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN). Singapore, Singapore: ACM, 2016, p. 13.

[4] D. Kraft, "Difficulty control for blockchain-based consensus systems, "Peer-to-Peer Networking and Applications, vol. 9, no. 2, pp. 397–413,2016.

[5] *Ginni Rometty 'Blockchain: The Beginners Guide To Understanding The Technology Behind Bitcoin &Cryptocurrency(The Future of Money)', IBM CEO*

[6] Y. Sompolinsky and A. Zohar, "Accelerating bitcoin's transaction processing. fast money grows on trees, not chains." IACR Cryptology ePrint Archive, vol. 2013, no. 881, 2013.

[7] V. Buterin, "On public and private blockchains, "2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/ on-public-and-private-blockchains*(PDF) An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*.

[8] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)," International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.

[9] Don Johnson, Alfred Menezes, and Scott Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)",2016

[10] "The biggest mining pools." [Online]. Available: https://bitcoinworldwide.com/mining/pools/ *(PDF) An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*.

[11] J. Kwon, "Blockchain will make AI smarter by feeding better data" v04. pdf, 2014.

[12] C. Miguel and L. Barbar, "Artificial Intelligence And Blockchain: Major Benefits Of Combining These Two Mega Trends" vol. 99, New Orleans, USA, 1999, pp. 173–186.