“Proof of Work” generation using Blockchain

Dr.M.Senthil Kumar[1], Ashwin R[2], Likith Podalakuru[3], Bala Subramanyam M[4]

[1]*Associate Professor, Department of Computer Science & Engineering,*
SRM Valliammai Engineering College, Tamil Nadu, India
[2]*UG Students, Department of Computer Science & Engineering,*
SRM Valliammai Engineering College, Tamil Nadu, India
[3]*UG Students, Department of Computer Science & Engineering,*
SRM Valliammai Engineering College, Tamil Nadu, India
[4]*UG Students, Department of Computer Science & Engineering,*
SRM Valliammai Engineering College, Tamil Nadu, India

ABSTRACT

Ever since the occurrence of NAPSTER issue in 1999, the Need to secure a content had increased drastcically for a User (or) Organization. Now, Blockchain plays an important role in resolving this issue since any content uploaded over the Blockchain network is immutable and permanent. With the addition of “Timestamp” factor, users can trace back to the time when they had the content and claim their novelty over it. IPFS & Blockchain are made for each other, large amount of data can be addressed through IPFS & it is immutable, permanent link can be placed into Blockchain transaction. This will timestamp & secure the content, without having to upload the data on the chain itself. Now, the users can have the undisputable proof that their content existed at that time when it was uploaded

Keyword: - *Blockchain, copyrights, proof of work, IPFS, Smart Contract.*

1. INTRODUCTION:

A Blockchain is known as Distributed Open Ledger containing blocks of transactions executed in a network, maintained by node itself. A Block is added to chain & hash of block is included in the next block - chronological chain of data guaranteed by sequential nested blocks. Now, the data cannot be changed without changing its block fist and all its following blocks, thus making the content immutable.

The header of block's hash denotes it’s parent block & it’s body part has batches of valid transactions that are hashed & encoded. In addition , Timestamp & Nonce value (Random integer that's repeatedly discovered until the hash of the block will contain a leading zeroes that makes the block qualified to be added in the blockchain) are added to the block. In this paper, a prototype is proposed where this timestamp factor is used to resolve the novelty issue of a content . Moreover, the probability of an attacker being able to change the entire database system by recalculating the hash value is resolved by applying a keyed hash algorithm with a unique private key to individual blocks.

1.1 Content to Hashcode conversion

Any content before being uploaded in a block must be converted into its respective hash code. Hashing is a process of converting a string of characters or data in any format into a fixed length value, it serves the process of indexing and retrieval in a database – since its faster to search a content by its hash value rather than its original value.

IPFS- InterPlanetary File System – it’s a peer-to-peer network for storing and retrieving data in a distributed environment. It uses content addressing to uniquely identify each file in a global namespace connecting all computing devices as nodes. To support content addressing, fingerprint (i.e) hash code (message digest) is generated from the content when passed through the hash function.

SHA256 is recommended by SHA256 by Microsoft due to the collision problem with SHA1.

```
//Convert the content into an array of bytes.
    byte[] messageBytes = ue.GetBytes(messageString);

//Create a new instance of the SHA1Managed class to create the hash value.
    SHA1Managed shHash = new SHA1Managed();

//Create the hash value from the array of bytes.
    hashValue = shHash.ComputeHash(messageBytes);

//Display the hash value to the console.
    For each (byte b in hashValue)
    {
      Console.Write("{0} ", b);
           }
```

IPLD – Object. It has 2 parts

- Data- blob of unstructured binary data of size < 256 kB.
- Links- array of Link structures. These are links to other IPFS objects.
  Every Link structure has 3 data fields – Name, Hash, Size.

1.2 Multihashing in ipfs

Every ipfs hash starts with Qm, (i.e) hash itself specifies which hash function is used, & length of resultant hash is in the 1st 2 bytes of multihash. Content is chunked up into smaller parts (about 256k each), each part is hashed, CID (Configuration Identification) is created for each chunk, and they are combined into hierarchical data structure, for which a single, base CID is computed. This data structure is essentially called- merkle DAG (Directed Acyclic Graph)

2. SMART CONTRACT – PROPOSED SYSTEM

It's a self- executable protocol designed to verify, allow , enforce a contract online without any 3rd party involvement. These transactions of smart contract are irreversible and can be tracked. They are applied in system where there needs to be lot of 3rd parties and verification process. Due to the "Lack of trust among the users", this protocol serves the purpose of 3rd party – exhibiting a trusted contract between users, bank, or any organization. Users are identified by smart contract with their unique ID – mapping the user node system to protocol.

The Proposal aims to build a blockchain network, where users can upload their content in any format & receive a "Proof of Work" signature , also identifies in case of any other user trying to use or claim the uploaded content. Objective requires an Ethereum Decentralized Application (dApp) using React, Redux, React Router & Bootstrap.

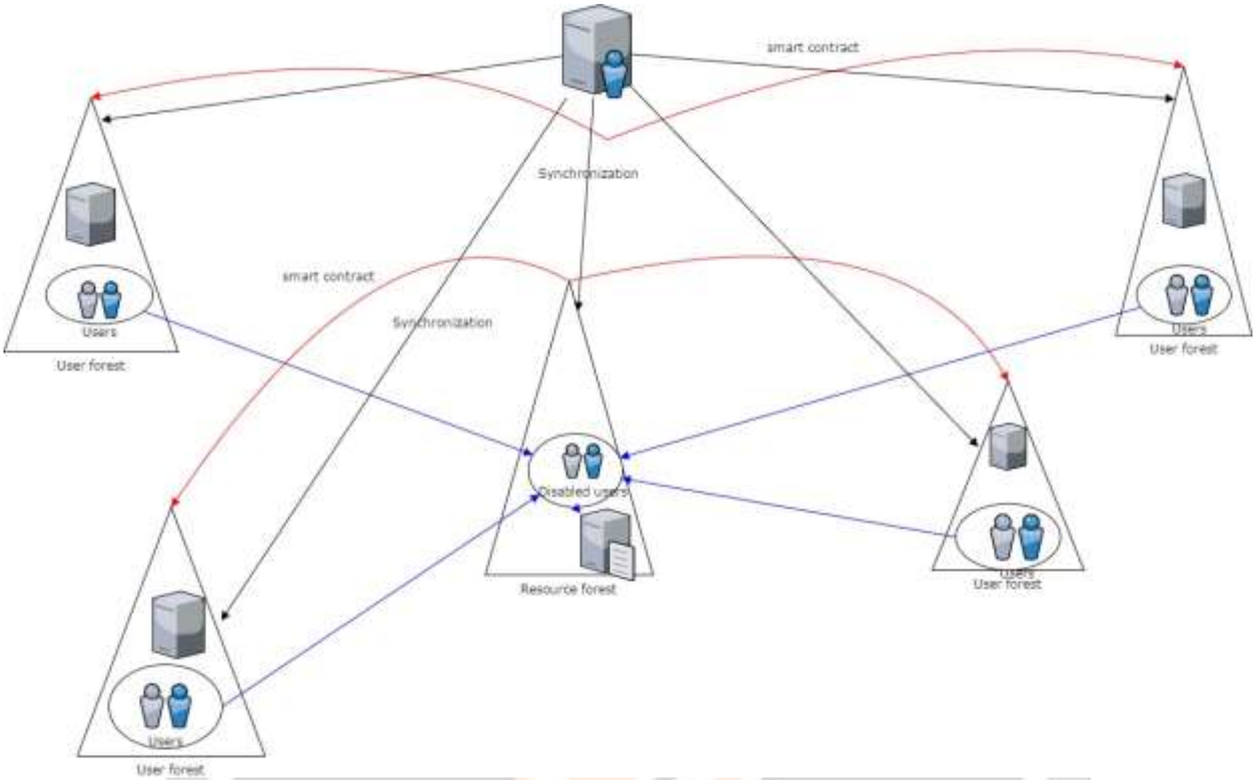


Fig -1: smart contract between all nodes – user system

2.1 WORKING

Smart contracts work by a basic procedure of (IF, WHILE, ELSE IF , THEN) conditional statements implemented in the code of blockchain – builds the network protocol as management system. The actions involves sending notifications and alerts.

2.2 BENEFITS

- Speed and accuracy – time efficient , automated
- Trust – predetermined rules and open transaction process
- Security – records are encrypted, difficult to hack or decode.
- Savings – no need of 3rd party.

3. CHALLENGES

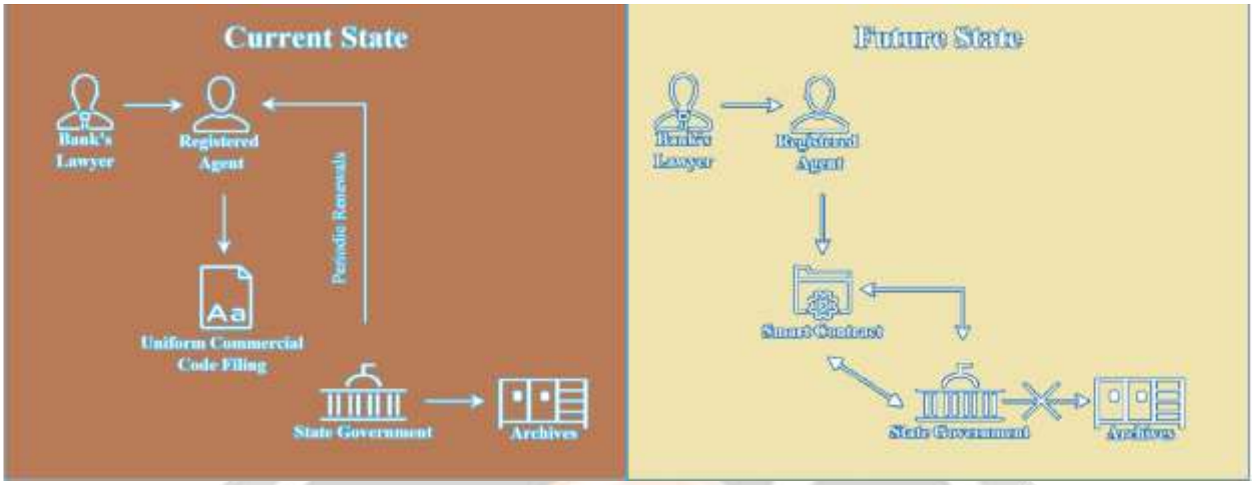
- Peer-to-peer network has to be established in a global level scale.
- Smart contract must trace the hash code that equals the new one to provide non-reputation .

4. BENEFITS

- Users can claim ownership to their content instantly and cheaply.
- There's no involvement of 3rd party to be approached.
- Lack of centralized database overcomes the "central point of failure" problem. .

5. CONCLUSION -FUTURE SCOPE

By implementing this approach to digital rights such as copyrights and patent, then "Proof of Work" can be used as evidence in courts – which will make patent management system , digital rights management system secondary due to it's drawbacks



6. REFERENCES

[1]. C. Lee, J.Lee, Y.Pyo & H.Lee – "Broken Integrity Detection of Video Files in Video Event Data Recorders" KSII Transactions on Internet & Information Systems 2016.

[2]. Xuewang Zhang, Yijun Yin-"Research on digital copyrights based on block chain" , IEEE Conference paper 2019.

[3]. Y. Li, J.K.Huang & R.M.Wang – "DCI control model of digital works based on blockchain" , journal of computer application , vol.37, 2017

[4]. V.Buterin – "next generation smart contract & decentralized application platform", https://ethereum.github.org/bitcoin.pdf, 2018

[5]. Y.Zhang, C.Xu, S.Yu, H.Li & X.Zhang - "SCLPV- Secure certificateless public verification for cloud based cyber-physical system" IEEE Trans. Comput. Social Syst., vol. 5, no.3, Dec, 2018

[6]. D.Zou " A multigranularity forensics & analysis method on privacy leakage in cloud environment" IEEE Internet Things, vol 6, no.2, apr, 2019

[7]. S.Li, S.Zhao, P.Andriotis, L.Xu -"Distributed consensus algorithm for event detection in cyber physical systems" - IEEE Internet things , vol.6, no.2 , apr, 2019.

[8]. M. Singh and S. Kim, "Introduce reward-based intelligent vehicles communication using blockchain," in *2017 International SoC Design Conference (ISOCC)*, 2017, pp. 15–16.

[9]. N. Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2018.

[10]. S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," *Proceedings of the 2016 2nd International Conference on Contemporary Computing and Informatics, IC3I 2016*, pp. 463–467, 2016.

[11]. A. S. Bruyn, "Blockchain an introduction," University AMSTERDAM, Research, 2017.

[12]. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, pp. 25–30, 2016.

[13]. B. Gipp, K. Jagrut, and C. Breitinger, "Securing Video Integrity Using Decentralized Trusted Timestamping on the Blockchain," *10th Mediterranean Conference on Information Systems (MCIS)*, vol. 26, no. 2, pp. 3–17, 2016.

[14]."SHA-1 Broken - Schneier on Security." [Online]. Available: https://www.schneier.com/blog/archives/2005/02/sha1_broken.html. [Accessed: 27-Jul-2018].

[15]. S. Halevi and H. Krawczyk, "Strengthening Digital Signatures Via Randomized Hashing," in *Advances in Cryptology - CRYPTO 2006*, 2006, pp. 41–59.

[16]. R. A. Dobre, R. O. Preda, C. C. Oprea, and I. Pirnog, "Authentication of JPEG Images on the Blockchain," in *2018 International Conference on Control, Artificial Intelligence, Robotics Optimization (ICCAIRO)*, 2018, pp. 211–215.