

Patent Smart Contract on Ethereum Blockchain Using Solidity

¹Hiresh Chaudhari, ²Rajmeet Arora, ³Saurabh Bachawe, ⁴Swapnil Gharat,

^{1,2,3}UG Student, ⁴Mentor, Rajiv Gandhi Institute of Technology, Mumbai, India.

¹hireshchaudhari1706@gmail.com, ²rajmeetarora1999@gmail.com, ³saurabh4514@gmail.com,

⁴swapnil.gharat@mctrigit.ac.in,

Abstract - In the current scenario, data of individuals is of highest priority. In a lot of organizations, data is fed into a centralized database which can be tampered / altered depending on the security constraints in place. In case of filing patents, instances of fraudulence can occur for malicious intentions. Blockchain makes use of decentralization and cryptographic hashing to make the history of any digital asset transparent and unalterable. The proposal of this paper is to explore the possibilities of a decentralized system based on blockchain technology. It allows individuals to file patents for their inventions using the Ethereum Blockchain. A solution to the aforementioned problem is having decentralized technologies like Blockchain in place. Our proposed software (web application) is made using Smart Contracts. This approach gives the patentee utmost security and reachability to their documents whenever needed. This will eliminate data-leaks / fraud-patent claims since it is impossible to tamper with the data that is written into the blockchain. The parameters to be analyzed are time-stamp (on Blockchain) of patent certificate generation, name of the Patentee, topic of patent invention, etc.

Keywords — *blockchain, data, data privacy, Ethereum, individual preferences, patents, smart contracts*

I. INTRODUCTION

A blockchain is a chain of blocks, but not in the traditional sense of those words. [1] In this context, the words “block” and “chain” point to digital information (the “block”) stored in a public database (ledger). [3] Ethereum is a technology that is public, open-source, blockchain-based distributed computing platform which features smart contract (scripting) functionality. [8] Miners work to earn Ether, a type of crypto token that fuels the network of Ethereum blockchain. Ether is also used by application developers to pay for transaction fees and services, in addition to being a tradeable cryptocurrency. Owing to its immutable nature, Blockchain serves as a permanent record of any transfer of value that has ever taken place in the past, while preserving the privacy of the identity of clients at both ends of any transaction (cryptographically). [5]

Smart contracts are applications that run on a virtual machine called the Ethereum Virtual Machine (EVM). [3] EVM is a decentralized “world computer” which gets its computing power from Ethereum nodes. Any node providing computing power pays for that resource in Ether tokens.

They're named smart contracts because you have the ability to write “contracts” that are automatically executed when the requirements are met. [9]

The rest of the paper is organized as follows. Section II gives a brief overview of Smart Contracts and the programming language Solidity. Section III discusses algorithms for our proposed software system. Section IV shows the implementation of the proposed system with elaborative screenshots. Finally, Section V concludes the paper with further goals and aspirations.

II. BACKGROUND

A. Smart Contracts

Smart contracts can be used for many different things. [3] Developers can create smart contracts that provide features to other smart contracts, similar to how software libraries work. Or smart contracts could simply be used as an application to store information on the Ethereum blockchain.

To actually execute smart contract code, someone has to send enough Ether as a transaction fee—how much depends on the computing resources required. This pays the Ethereum nodes for participating and providing their computing power.

B. Solidity

Solidity is a high-level, object-oriented language for implementation of smart contracts. Solidity was influenced

by Python, C++ and JavaScript. [7] It targets the Ethereum Virtual Machine (EVM). Solidity is typed statically, provides inheritance support, libraries and complex user-defined types along with a variety of other developer-useful features. [3] Voting, crowdfunding, blind auctions, and multi-signature wallets are some of the many applications of Solidity. Generation of wallets is the basis of our system as we shall discuss in further sections.

In the field of Patent registration, there exists a possibility of frauds in case of unauthorized access to the Patentee's application. Also, human errors can result into a similar consequence.

C. Keccak Encryption Algorithm

Keccak is a broad cryptographic primitive family designed by Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche, building upon RadioGatún. It has subsets including popular cryptographic algorithms including SHA-3 (Secured Hash Algorithm).

Keccak makes use of a novel approach called sponge construction. [10] It is based on a wide random function, also called a random permutation, and allows inputting ("absorbing" in sponge terminology) a variable (any) amount of data, and outputting ("squeezing") a variable (any) amount of data. All along, it acts as a pseudorandom function with regard to all previous inputs as well. Hence, this leads to great flexibility.

III. PROPOSED SYSTEM

The following section explains the methodology and algorithms of operation for our proposed system. Broadly classified into 2 sections: Google Sign In and Patent Generation Process.

A. Google Sign In

The sign-in process for our proposed system is as follows:

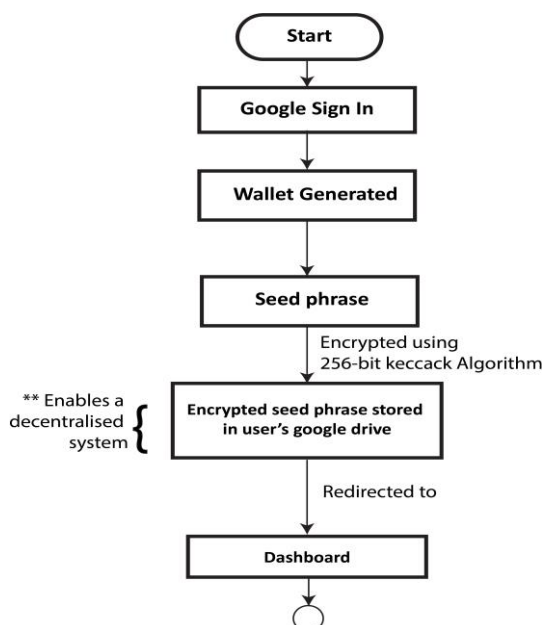


Figure 1: Google Sign-In

Step 1: The system allows the user to log in through Google Sign in to avail the patent filing service.

Step 2: The user's sign-in is accompanied by generation of a unique digital wallet for the user. [4]

Step 3: This generated wallet consists of a "Seed phrase" which encrypts user's credentials using a 256-bit Keccak algorithm. As explained in section II above, Keccak is a broad cryptographic primitive family and a superset of SHA-3 (Secure Hash Algorithm 3). [10]

Step 4: The encrypted seed phrase is stored in the user's Google Drive. This aspect of the system makes it decentralized in nature.

Then, the user is redirected to the system dashboard.

B. Patent Generation Process

The actual patent generation process is illustrated in Figure 2 below.

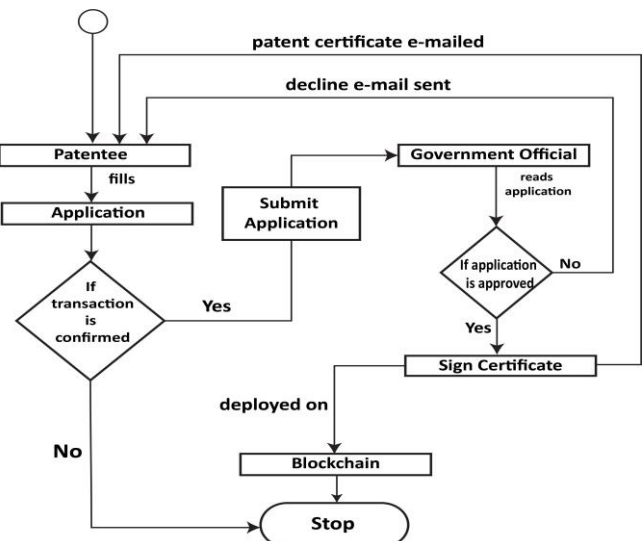


Figure 2: Patent Generation Process

Step 1: The system dashboard allows the user a choice to file a Patent for their respective invention. An application form is provided to the user to fill-in the required details.

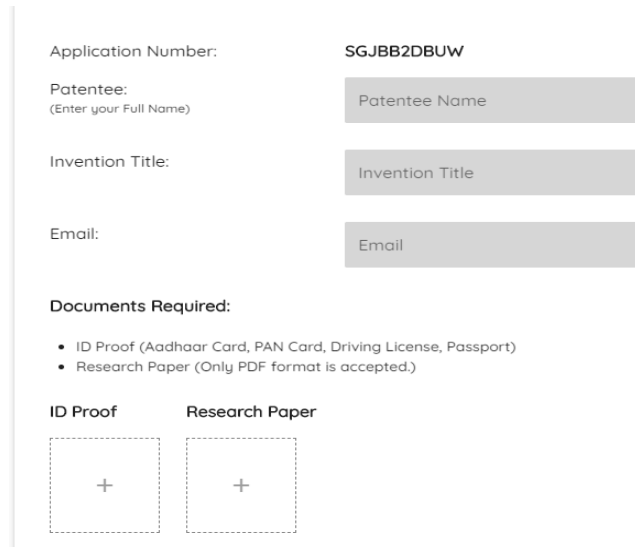
Step 2: After completing online transaction (using Ethereum Blockchain) [2], the patentee's application is submitted to a government official's dashboard. This is done to make sure that the details are validated by a trusted third-party with utmost security of the patentee's application details.

Step 3: The Government official checks the application request. If approved, the Government's signature is provided. The patent for the patentee's invention is generated and sent to their e-mail (provided by user in the application form). However, if the application is not approved, the user receives an e-mail of the same with the reason for rejection mentioned in the e-mail.

Step 4: Finally, the patent is deployed on to Blockchain so that it cannot be tampered by any un-authorized intruder.

IV. WORKING OF THE SYSTEM

In this section, we explain the working of our proposed system illustrated with the help of screenshots shown below.



Application Number: SGJBB2DBUW

Patentee: (Enter your Full Name) Patentee Name

Invention Title: Invention Title

Email: Email

Documents Required:

- ID Proof (Aadhaar Card, PAN Card, Driving License, Passport)
- Research Paper (Only PDF format is accepted.)

ID Proof Research Paper

+ +

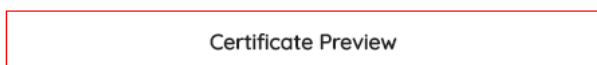
Figure 3: Application Form

A. Application Form

The Patentee fills out details on the application form such as Full name, Invention title and e-mail address (where the patentee wishes to receive the Patent certificate after generation). Also, the user is required to provide identification details and the research paper in PDF Format.

B. Patent Certificate Preview (Real-time)

A Patent Certificate Preview is generated on the screen in real-time as the Patentee fills out the application form. This makes sure that the patentee gets a good idea of how his/her details will show up on the final patent certificate. [6]



Certificate Preview

Patent Certificate

Sl. No. SGJBB2DBUW

Patent No. Available upon issuance.

Date Of Filling: DD/MM/YYYY

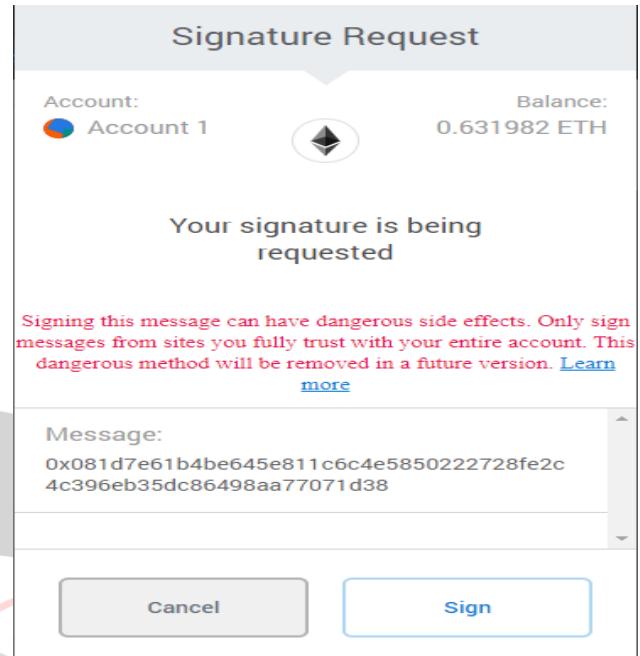
Patentee:

It is hereby certified that a patent has been granted to the patentee for an invention titled "" as disclosed in the above mentioned application for the term of 20 years from DD/MM/YYYY in accordance with the provisions of the Patent Act, 1970.

Figure 4: Patent Certificate Preview (Real-time)

C. Signature Request & Hash Generation

This is a very crucial step in the process. The system prompts a Signature Request to the user. It displays the transaction fees that will be deducted from the user's Ethereum wallet. Also, it generates a unique hash value for the transaction that can help uniquely recognize the user's request.



Signature Request

Account: Account 1 Balance: 0.631982 ETH

Your signature is being requested

Signing this message can have dangerous side effects. Only sign messages from sites you fully trust with your entire account. This dangerous method will be removed in a future version. [Learn more](#)

Message: 0x081d7e61b4be645e811c6c4e5850222728fe2c4c396eb35dc86498aa77071d38

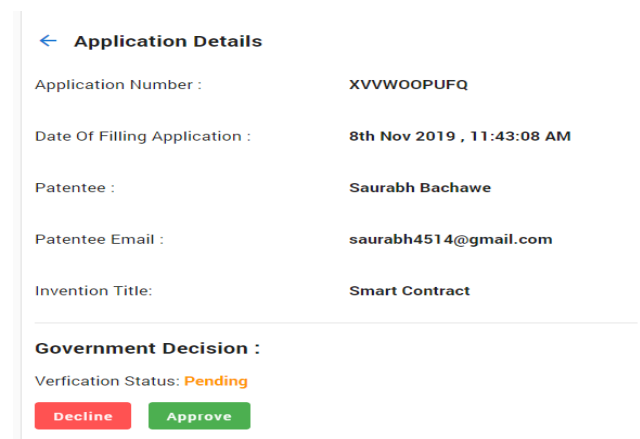
Cancel Sign

Figure 5: Signature Request & Hash Generation

D. Government Decision Verification

As discussed in section III, once the patentee submits his/her patent application, it is sent to a Government authority. The verification status reflects whether the patent request has been verified or not. The user receives an update on their e-mail.

If the patent request is approved by the Government, the patentee receives the patent certificate on their e-mail. However, if the application is not approved, the user receives an e-mail with the reason for application rejection mentioned in the e-mail.



Application Details

Application Number : XVVWOOPUFQ

Date Of Filling Application : 8th Nov 2019 , 11:43:08 AM

Patentee : Saurabh Bachawe

Patentee Email : saurabh4514@gmail.com

Invention Title: Smart Contract

Government Decision :

Verification Status: Pending

Decline Approve

Figure 6: Government Decision Verification

V. CONCLUSION

Blockchain Technology has been catching attention in today's time to a great extent as more and more individuals are getting concerned about their private data online.

The main investigation of this paper was exploring the application of Blockchain in the field of patents generation, assuring individuals that the patents they file for their inventions are secure and free from unauthorized tampering.

Any such system that involves a confidential transaction between two parties could find use of a similar technology. Examples of this could include signing of bonds between major companies, signing of rent and mortgage documents between the officials concerned, etc.

Through the research we have done for this project and our growing fascination with Blockchain technology, we hope to continue diving deeper into the possibilities of a secure but at the same time connected world, powered by this emerging technology.

REFERENCES

- [1] Athina-Styliani Kleinaki, Petros Mytis-Gkometh, George Drosatos, Pavlos S. Efraimidis, Eleni Kaldoudi. A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval. 29 April 2018.
- [2] Mohammad Javed Morshed Chowdhury, Alan Colman, Muhammad Ashad Kabir, Jun Han and Paul Sarda. Blockchain as a Notarization Service for Data Sharing with Personal Data Store. 10 August 2019.
- [3] Karamitsos, I., Papadaki, M. and Al Barghuthi, N.B. (2018) Design of the Blockchain Smart Contract: A Use Case for Real Estate. Journal of Information Security, 9, 177-190. <https://doi.org/10.4236/jis.2018.93013>
- [4] Po-Wei Chen, Bo-Sian Jiang, Chia-Hui Wang "Blockchain-based Payment Collection Supervision System using Pervasive Bitcoin Digital Wallet" Fifth International Workshop on Pervasive and Context-Aware Middleware 2017
- [5] Don Tapscott (Author), Alex Tapscott (Author). Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World. Penguin (14 June 2018).
- [6] IIPRD "Sample Patent Landscape Study – Blockchain." January, 2017
- [7] R. Molecke, "How To Learn Solidity: The Ultimate Ethereum Coding Tutorial", in Blockgeeks, <https://blockgeeks.com/guides/solidity>, 20 Sep 2019.
- [8] A. Rosic, "What is Ethereum? The Most Comprehensive Guide Ever!", in Blockgeeks, <https://blockgeeks.com/guides/ethereum>, 20 Sep 2019.
- [9] Ali Kaan Koç, Emre Yavuz, Umut Can Çabuk, Gökhan Dalkılıç "Towards Secure E-Voting Using Ethereum Blockchain"
- [10] R. Sujatha, M. Ramakrishnan "Keccak MD Hash Algorithm Based Tag Kem for Certificateless Hybrid Signcryption" DOI:10.5829/idosi.mejsr.2014.22.12.21866