International Journal of Advanced Science and Technology
Vol. 29, No. 6, (2020), pp. 01-06

A Performance Comparison of Different Security Hashing in a Blockchain Based System that Enables a More Reliable and SWIFT Registration of Land

Ranjith Kumar MV, Sathyajith R, Naveen Kumar U, Pushpalatha M
Department of Computer Science Engineering
SRM Institute of Science and Technology, Kattankulathur, Chennai, India
drmvranjithkumar@gmail.com, sathyasat98@gmail.com, naveenkmr2310@gmail.com, pushpalatha.m@ktr.srmuniv.ac.in

Abstract

The core value proposition of this paper is to put the entire land industry onto the same blockchain network, creating a digital network for parties involved in the real estate, using blockchain and smart contracts technology. The land's unique physical properties and transactions are hashed and maintained in the digital ledger. The land's history like place of origin and chain of custody are traceable. The blockchain empowers the transparency of the property network. By storing the records on a distributed ledger which is then impossible to alter or tamper, hence implementing land related businesses like registry and selling in blockchain will be a revolution. Different hashing combination is implemented in blockchain to secure the data by simulating randomness. Hash functions keccak256() and ripemd() are combined in the contract and their performances are compared by hash length, time taken and few others.

Keywords: *Land registry, Blockchain, Smart contract, keccak256( ), ripemd160( )*

Introduction

Land registration and real estate is a system whereby authority control (ownership) and land rights are taped by a government establishment. The recorded records provide information of title, ease transactions, and forbid fraud. Outdated land registry systems introduce delays in ownership verification, slow down legitimate transactions, and in the worst-case scenario, could enable land misappropriation. For Indian citizens, the economic opportunities can be improved by providing land related rights. For government entity, land ownership records are primary to provide services, collect taxes, and establish its territorial authority. Bestowed the value of land registration for economic devolution, the World Bank has been spearheading efforts to improve land registration in several countries. The paper-based method is not only unwieldy to access and maintain but also open to natural or man-made disasters. The involvement of multiple stakeholders such as government entity, and financial institutions make land registration process a complex one. By developing this system with blockchain technology, we have a potential to fix many of existing problems. With the blockchain practice we are incorporating many key benefits of the technology, such as: an unchangeable history of transaction data, doubt of authenticity is removed; records are linked to the system permanently, so no one can ever tamper, alter or forge a record and these records or data can be seen by anyone, any time. The blockchain technology implementation in land registry has the potential to solve many problems that characterize typical centralized recording of titles. Blockchain technology is a decentralized peer-to-peer network system in which each user act as a node and hold a copy of the shared ledgervia a consensus protocol. Digitalization of land records removes redundancy and concurrency, also improves consistency of the records or data in database systems. Moreover, land registration system todayispaper based which are not updated oftenleading to innumerabledisputes like tampering of recorded data. Recordsstored in a decentralized ledger or distributed ledger areinfeasible to alter, creating a revolution in land registry system. Existing land database is typically centralized ledgers that provides a system of record of a nation's land transactions. Usage of decentralized databases through blockchain technology can prevent replication and duplication. Smart contracts enables self-execution where the transactions could be completed faster when certain conditions are satisfied. The usage of these contracts

ISSN: 2005-4238 IJAST

would double up the registration process by automatically updating the ledger, instead of the conventional method of transferring the ownership through an application form.[7]

Issues in current system

Manual/Physicaldata entry**:** Process in current system in not digitized, it is a manual paper driven process where the probability of the records getting tampered or altered is higher.
Long Process: Current procedure is very slow to catalogue a property and too much corruption is involved.
Accessibility ofrecords: Land documents undergoes several mutations over generations which are not always properly reflected on the public records. The records are maintained in some government entity and accessing those data is a time intensive and cost incentive procedure at the end.
Establishment of ownership: Indian courts have several pending cases dealing with land related disputes especially regarding with establishment of one's ownership.
Land encroachment: In India lands are more vulnerable to encroachment, particularly of older people having no primary support or of NRIbecomes soft target and legal way of eviction is also time consuming.
Double registration:There are few case filled against double registration of single land by different people which are realized several years after.
Human error**:** In paperbased land registry system the accuracy of documentation depends upon the particular individual who is responsible for updating the records.
Broker: Brokerage system or involvement of middlemen results in additional cost to the buyer becausehe needs to pay for the land and also to the broker.
Transparency: They face practical issues during document presentation because of fewer documentation and improper registration of land.[8]
Corruption: There is too much corruption involved in real estate industry and registration process. The paper based system is more prone to bribery and illegal ownership of land.

Blockchain

Block Chain In Real Estate

Blockchain is a revolutionary idea in the field of real estate industry. Blockchain is developed in this industry which empowering business to link that gap in a secured, protected, authenticated and indisputable method. Property/Land registration refers to a system whereby ownership and land related rights are recorded by a government entity. This has been developed that users and consumers have a very keen interest in the lifetime journey of their land as well as the industry desires to demonstrate authenticity, transparency and provenance. In land industry, users are hunting more information about their property and the assurance of authenticity[9]. The core characteristics of blockchain offer industries with a key solution to satisfy the consumer, bringing profits to both businesses and consumers. It helps the real estate industry retort to the global demand for responsible tracking. It was started off with land provenance tracing, later expanded to include certification authenticity among others. At any step of the chain, the participants can track the story or history of the land more easily and accurately. By Leveraging the trust less and indisputable nature of the blockchain in this way, it is now possible to keep a fraud-proof transaction record that can follow each property as it makes its way through the supply chain. If these records are stored on a decentralized ledger then it will be impossible to tamper, hence instigating blockchain in this industry will be a revolution. Unique knowledge of prevailing industry protocols and verification systems can be premeditated to function as a bolt on service to existing industry.

The following are the properties of real estate with blockchain technology:
Transparency: As the unique identity of each stone is textured and converged on our platform, investors can buy and sell with greater confidence.
*Compliance:*Blockchain solution provides ease tracking of land transactions, enabling easier agreement against increasingly strict measures.

Trust: Through unparalleled collaboration with seller, buyer, certification and land inspector, we provide independent, personalized solution for the industry.
Sustainability: Our platform intensification visibility and control over responsible and ethical sourcing in the chain.
Decentralization: The model will be decentralized to make work easier. Less corruption, transparent, no encroachments are few advantages of distributed database.
Ownership: Most of the cases in Indian courts are about ownership and control rights of the land because people don't have casual access to documents regarding or due to corruption or they lost it.

Methodology

The proposed system uses several different concepts tied in with the field of blockchain and crypto hashes, with the implementation and result of each individual module is noted. The smart contract technology was harnessed to implement all the modules. Ethereum runs with the help of Ethereum virtual machine and it is the first public blockchain platform supporting smart contracts. A smart contract runs on EVM runtime environment and written using high level programming languages like solidity and serpent. The smart contract code is compiled with EVM bytecode. It is used to design various decentralized applications These decentralized applications gain the benefits of cryptocurrency and blockchain technology combined. A smart contract is an agreement between two parties within the blockchain technology, to enforce the parties to abide by the terms as mentioned in the contract, rather than relying on the traditional ways such as trusting a middleman or using laws to handle disputes.Theblockchain technology provides an excellent solution to store the land based records without any disputes.This system act as a digital marketplace where an individual can register, sell and buy one's land.
Register Property: Land registration system records land related rights and offer evidence to property title holders. The land owner adds the property into the marketplace application by providing details like owner name, phone number, land's address and survey number to the smart contract. It also has the added responsibility of aggregating the sale deed to be legally taped. The record of registered land is stored in the decentralized ledger. After registration, the land record is displayed along with other registered lands to user in tabular form. We developed a ReactJS-based web application with a blockchain explorer for users to view within the application.
Sell Property: If a person wants to sell his land, the land needs to be registered. Only after the registration process, the owner is allowed to add his property into the application for selling. Then the person needs to add it to the marketplace by giving all needed personal information and survey number with the price of land in terms of ether to the smart contract. The given survey number needs to match with the register record.Once after adding, the function display property owner details, address, price, survey number and the current owner address but while listing owner information, land's survey number, price of the land and the owner's metamask address will be hashed and displayed in the platform along with the enabled buying button for the buyer to purchase. Again ReactJS-based web application with blockchain explorer is built for users to view.
Buy Property: Initially, the buyer has to register himself as a buyer in the platform. The buyer can look at the table of available lands and can purchase them. The person's identity is verified by matching the Aadhaar number. Buyer makes a search through all the available properties displayed in the list. On clicking the buy button, the buyer buys the land and the specified amount is automatically transacted as ethers to the seller account. Upon successful transaction the fields in the displayed list gets updated with the buyer's information and the previously registered record gets updated with the present owner information corresponding to the land's survey number.

Hashing

Hashing is a data processing method that blockchain uses for authentication and state confirmation. It is a computational function that converts input of any length into a fixed size output. The final result is called

the hash or hash value. Hashes identify, compare against files and then compare the produced value to the original file hash value. The length of the hash value that gets delivered after computation depends on the type of hashing algorithm and it is determined in bits.Example SHA1, SHA256, SHA512. Hash values are definite and deterministic in nature and respond to the given parametric quantity of the algorithm. Every hash value is always unique in nature, so the same hash sequence cannot be reproduced with variable input. So hash is the major functionality of blockchain technology. The resultant hash produced of the input of data is a one-way trap door which means it is irreversible. In Hash function, input of any size can be given and converted into hash value of fixed size. The hash value of the input data will always have the fixed size output and it is impossible to reconstruct the input from the output data. For example, MD5 algorithm produces 128-bit hash, SHA256 produces a 256-bit hash as a result. In land industry, the personal information like aadhar or any other ID number, address are hashed. The details are hashed for protecting the personnel details of the user from others.

Different hashing combination is implemented in blockchain to secure the data by simulating randomness. Hash functions like keccak256(), sha256() and ripemd() are combined in the contract and their performances are compared by hash length, time taken and few others. Our system is combined with different hashes and performance of each system are compared.

Keccak256(): Keccak256() computes Ethereum-SHA-3 hash of the (tightly packed) arguments. Keccak-256() hash of the input and return 32 bytes hash value.

Sha256(): Sha256() computes the SHA-256 hash of the (tightly packed) arguments and returns 32 bytes hash value.

Ripemd(): Ripemd() computes RIPEMD-160 hash of the input and reutrns 20 bytes hash value.

Comparison Of Hash Function

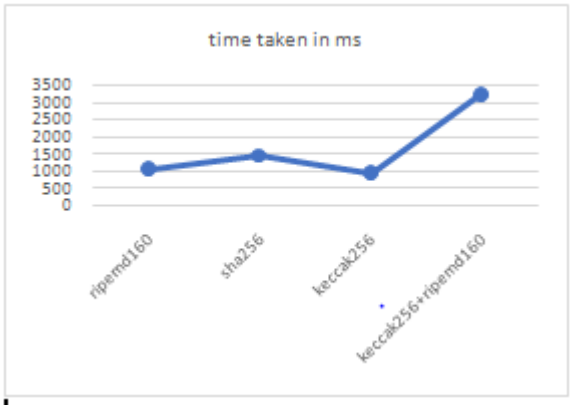
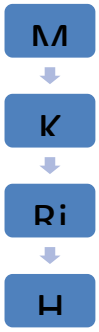


Fig.1.2: Time taken for hash generation

Ripemd 160 generates a 160 bit cryptographic hashes. It provides a secure replacement to 128 bits. Ripemd generates short length hashes which is prone to birthday attacks. SHA3 is a member of secured hash family which generates 256 bit length hash value. Keccak similar to SHA3 hash produces 256 bits. The difference is the additional 1bit appended to the message. Keccak is based on sponge construction – data absorbed into the sponge and the result is squeezed. Keccak hash function is used in Ethereumblockchain. Solidity language also use Keccak 256 as the default hash function.

A combinationof ripemd160 and keccak256 hashes are used to secure the sensible land information. H = ripemd160(keccak256(M)), where M is the input message and H is hash result. Keccak256 is considered as the strong hash till date as it is difficult to attack. Ripemd160 generates relatively shorter hashes than keccak, but they are more vulnerable to crypto attacks. All the sensible messages are first hashed with keccak() and then the output is rehashed with ripemd() converting 256 bits to 160 bits.

ISSN: 2005-4238 IJAST



This scheme works as a belt and brace approach to secure the information. The output of each hash function is given in table 1.1.
Though this scheme takes a longer time to generate, the preimage attacking and collision takes double the amount of steps, time and energy. The time taken for hashing by each function is tabulated below(table 1.2).Birthday attacks takes a longer time as the attacker needs to try $2^{n/2}$ inputs twice once for ripemd160 and second for keccak256 for which the attacks arenot found yet. This scheme has a good amount of avalanche effect by stimulating randomness.

Table 1.1 Hash output for input message "the quick brown fox jumps over lazy dog"

Hash Function	Hash output
ripemd160	ad89d8a898cef7056d2e80fa195bd5f1dc2b6574
sha256	c49d298c2acb8bb6208e18440a7b209dfc5b1a7f92871a4eff6cd7ceed4c92cd
keccak256	06ef655a1601c5c71df059be4662718ad954cec349cc32fba0328465084ffa62
keccak256 +ripemd160	b8853cc21027770b99e374b799c39f6c5c3566db

Table 1.2 Time taken for hash generation

Hash Functions	Time Taken (ms)
ripemd160	1085
sha256	1467
keccak256	959
Keccak256+ripemd160	3231

Conclusion

In summary, blockchain technology can bring a revolution in the real estate industry streamlining all transaction activities under a secure decentralized network. According to performance test of hash functions and their combination, keccak256 seems to outperform its contemporaries with respect to time and combination of keccak256 + ripemd160 prevents collision attack to a greater extent. From Fig 1, though time consumed by the combination is 3 times the keccak256, the strength and complexity of hash generated is enhanced with minimal storage.

References

1. ZibinZheng, ShaonXieHongningDai, Xiangping Chen, Huaimin Wang. "An Overview of Blockchain Technology Architecture, Consensus, and Future Trends" IEEE 2017.
2. Raquel Benbunan-Fich , Arturo Castellanos" Digitalization of land records from paper to blockchain" Research gate 2018.
3. Mechkaroska, VesnaDimitrova and Aleksandra Popovska-Mitrovikj " Analysis of the possibilities for improvement of blockchaintechnology"IEEE 2018.
4. Shuai Wang, Yong Yuan , Xiao Wang , Juanjuan Li , Rui Qin , Fei-Yue Wang "An Overview of Smart Contract: Architecture, Applications, and Future Trends" IEEE 2018.
5. Maxim Ya. Afanasev, Yuri V. Fedosov, Anastasiya A. Krylova, Sergey A. Shorokhov" An application of Blockchain and Smart Contracts for Machine-to-Machine Communications in Cyber-Physical Production System" IEEE 2018.
6. Maria RonaiL. Perez, Dr. Bobby Gerardo" Modified SHA256 for Securing Online Transactions based on Blockchain Mechanism"IEEE 2018.
7. Kumar, MV Ranjith, N. Bhalaji, and Swathi Singh. "An augmented approach for pseudo-free groups in smart cyber-physical system." Cluster Computing 22, no. 1 (2019): 673-692.
8. Narayanan, Varun V., MV Ranjith Kumar, KartikSaxena, P. Madhavan, and N. Bhalaji. "Modern Parking Business Using Blockchain and Internet of Things (IoT)." Artificial Intelligence and Evolutionary Computations in Engineering Systems: 527.
9. Usha, G., P. Madhavan, and MV Ranjith Kumar. "A Novel Design Augmentation of Bio-Inspired Artificial Immune Technique in Securing Internet of Things (IOT)." In Internet of Things for Industry 4.0, pp. 103-114. Springer, Cham, 2020.

ISSN: 2005-4238 IJAST