Towards partial fulfillment for Undergraduate Degree Level Programme
Bachelor of Technology in Computer Engineering

A First Stage Project Evaluation Report on:

Decentralized Domain Name Broker Service

Prepared by :

Admission No.	Student Name
U17CO094	Hrishabh Sharma
U17CO089	Ujjwal Kumar
U17CO003	Amruta Mulay
U17CO052	Rishabh Kumar

Class : B.TECH. IV (Computer Engineering) 7th Semester

Year : 2020-2021

Guided by : Dr. Sankita J. Patel

DEPARTMENT OF COMPUTER ENGINEERING
SARDAR VALLABHBHAI NATIONAL INSTITUTE OF TECHNOLOGY,
SURAT - 395 007 (GUJARAT, INDIA)

Student Declaration

This is to certify that the work described in this project report has been actually carried out and implemented by our project team consisting of

Sr.	Admission No.	Student Name
1	U17CO094	Hrishabh Sharma
2	U17CO089	Ujjwal Kumar
3	U17CO003	Amruta Mulay
4	U17CO052	Rishabh Kumar

Neither the source code there in, nor the content of the project report have been copied or downloaded from any other source. We understand that our result grades would be revoked if later it is found to be so.

Signature of the Students:

Sr.	Student Name	Signature of the Student
1	Hrishabh Sharma	HSharma
2	Ujjwal Kumar	
3	Amruta Mulay	
4	Rishabh Kumar	

Certificate

This is to certify that the project report entitled Decentralized Domain Name Broker Service *is prepared and presented by*

Sr.	Admission No.	Student Name
1	U17CO094	Hrishabh Sharma
2	U17CO089	Ujjwal Kumar
3	U17CO003	Amruta Mulay
4	U17CO052	Rishabh Kumar

Final Year of Computer Engineering and their work is satisfactory.

SIGNATURE :

GUIDE JURY HEAD OF DEPARTMENT

Abstract

In this growing age of the internet, people want to have a domain name that is relevant to their work. In many cases, it might not be possible to have a domain name and they might want to purchase it from someone. We aim to provide a platform that is secure, decentralized, and cheaper than the currently available options. The project focuses on a growing secondary market of domains and entities involved with legacy DNS architecture but shares nothing with Blockchain-based DNS architecture. With that said, the idea is to implement a Blockchain-based service on top of the legacy system to allow Domain owners (potential sellers) and their Buyers to interact directly without any middle-man in between the two parties involved.

Keywords: *Domain name transfer - Blockchain - Decentralised model.*

Contents

List of Figures

List of Tables

List of Acronyms

DNS	Domain Name System
SEO	Search Engine Optimization
TPS	Transactions Per Second
CA	Certificate Authority
PKI	Public Key Infrastructure
TLD	Top Level Domain

1 Introduction

In the current market of Domain Names, the domain brokers provide the service of buying/selling domain names. Domain name brokers are centralized entities, who act like a middle-men in exchanging the ownership of domains and the value associated with it between the buyer and seller. These brokers charge a commission to provide the service to both the parties. At the end of the process, the buyer gets the domain name access and the agreed price is settled with the seller.

Our goal is to provide a service based on blockchain to make the process transparent and reduce the commission charges to minimal. In the proposed service there is no scope of scams which is a very big concern with the current scenario of the market. The service (if economically feasible) has the potential to create a competitive marketplace for domain selling and completely replace other domain escrow services provided by the domain name registrars themselves.

1.1 Applications

A meaningful and appropriate domain name can increase the traffic on the website by improving SEO ranking. People might want to sell their domain names which are no longer active, and thus it will help them also get some amount of monetary benefits. The model aims to connect potential buyers and sellers to transfer domain name ownership.

The application scope of the model is not limited to only companies or organizations, but it can be used by almost everyone on the internet.

1.2 Motivation

The exponential growth of the secondary market of domain that motivates us to work on this idea are :–

- With the exponential growth in internet users, domain ownership has grown exponentially too. Thus, creating a huge demand for domain names.
- Different categories of domainers (individuals, organizations, etc.) have realized the value of attractive and unique domain names, thus creating a competitive secondary marketplace for domain names.
- There lies a paucity of the good and appealing domain names. It even becomes infrequent for these domain names to return to the public domain. Even if it turns out to be so, it is regarded as a casualty or carelessness from the registrant's side.

- With the growth of the secondary market, it has also marked the advent of mediators or negotiators who play a vital role as third parties building favorable situations for transactions. The third parties also stand a chance to scam the buyer/seller involved to make extra profit.

1.3 Objectives

The proposed work focuses on a growing secondary market of domains and entities involved with legacy DNS architecture and implements a Blockchain based service on top of the legacy system to allow domain owners (potential sellers) and their Buyers to interact directly without any middle-man in between the two parties involved.

The aim is to make the process reliable, transparent, and reduce the commission charges to minimal thereby offering hassle-free service to domain buyers/sellers. In the proposed service there is no scope of scams which is a very big concern with the current scenario of the market. The proposed service is economically feasible and has the potential to create a competitive marketplace for domain selling. The proposed system is transparent, reliable, cost-effective, and has the prospective to completely replace other domain escrow services provided by the domain name registrars themselves.

1.4 Organization of project report

Chapter 1 covers the introduction to the project, including its application, motivation behind choosing this project, and objectives of the project. Chapter 2 contains the literature survey, it includes previous works done in this field. It also provides a theoretical background of all the topics covered to help in understanding the project properly. Chapter 3 contains a detailed report about the proposed implementation methods needed to carry out this project. Chapter 4 covers the conclusion of this report.

2 Literature Survey

This Chapter covers the theoretical background needed to understand this project report. It includes a detailed explanation of all the terms of a blockchain-based system and it also highlights the terms related to the domain name and its transfer.

2.1 Blockchain

Blockchain is a distributed database in which data is store in the form of blocks and each block(except the first block, known as genesis block) contains the cryptographic hash of the previous block, thus giving it a chain like structure. The linked structure makes the Blockchain an immutable data structure. The another important property of the Blockchain Network architecture is the 'Decentralisation'. However the degree of decentralisation varies from one blockchain platform to other, due to obvious trade-offs among characteristics of blockchain. [4]

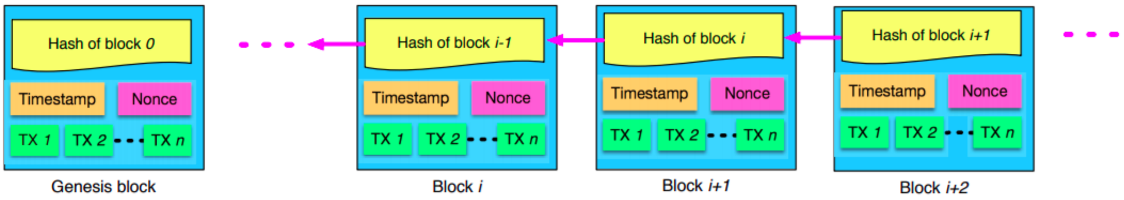

Figure 1: Illustration of Blockchain [9]

2.1.1 Advantages of Blockchain

- The main aspect of blockchain is that it is a decentralised system. This eliminates the central server. The decentralised system distributes the copy of the database to each of it's participants on the network, thus making it almost unfeasible to hack into the system. (except for the "attack 51%")

- Every participant on the blockchain network holds the information of complete chain of blocks in encrypted form. These distributed copies are continuously and periodically synchronized.

- The beauty of blockchain is the transparency that it provides in the system which makes almost any operation to be easily traceable.

- Each time a new information is added into the database, it gets added in the form of new blocks. This new data is collectively agreed upon by each of the other registered nodes on the network, thus becoming a part of the chain parmanently.

- Ubiquitous Nature - the technology is relevant not only in financial sector, but also in other fields.

2.1.2 Types of Blockchain

- **Public:** Public Blockchain Networks are open anyone can join the network anytime and leave without any permission. In public blockchains, there is no message passing, between the participants for reaching the consensus. So, a single person is elected in some way, and incentivised, to decide the next state, and other participants verify. Therefore, a monetary asset is mostly associated with such blockchains.

- **Private:** In private blockchains, users are able to join or leave if they are authorised to do so. In private networks consensus can be achieved through various classical algorithms, hence no monetary currency is attached to them.

2.1.3 Smart Contract

Smart contracts are basically pieces of code stored inside a blockchain which serves as a type of agreement. It gets executed when certain pre written conditions are met. Smart contracts eliminates the risk of any fraudulent activity from the participants.

2.1.4 Consensus Protocols

In a Blockchain Network, consensus protocols are a way through which untrusted nodes or participants reach to a single agreement about the next block to be added in the Blockchain.

In the case of permissioned and private blockchain networks, participating nodes have a valid identities issued by authorities like CAs and are known to each other. Such blockchain networks use classical consenus protocols like Paxos, Raft, PBFT, RBFT, etc to reach agreement. On the other hand, the participating nodes are anonymous to each other, in case of public blockchain networks. So, in order to reach an agreement, a leader election takes place. The leader election can be done in many ways, and that leads to various existing consensus protocols for such network. The elected leader will be the one to propose a decision for the next block and rest of the participating nodes validate the new proposed block. Some of the consensus protocols involving leader election, in the scope of our project are discussed below:

- **PoW**: Proof of Work(PoW) involves a leader election on the basis of solving a complex mathematical problem directly related to hashing. The selected problem is hard to solve but can be easily verified by the rest of the nodes of the network. A high computation power is required to solve the complex problem first, so the probability of getting elected as leader is directly dependent on the computation power. Bitcoin [7] and Ethereum [8] Network uses PoW to reach consensus. However, Ethereum is constantly making a move to shift towards PoS. [6]

- **PoS**: Proof of Stake(PoS) involves a leader election, in which the probability of being elected directly depends upon the amount of stake(can be the amount of cryptocurrency) the node/participant holds.

- **dPoS**: Delegated Proof of Stake(dPoS) [5] protocol is a variation of PoS mechanism.In the procedure involved, a fixed number of delegates are voted by the network participants. The delegates, also known as "Witnesses" decides the next block.

2.1.5 Comparison of Public Blockchain Networks

1. **Bitcoin -** It is a peer to peer(P2P) electronic cash system, backed on a widely spread Bitcoin Network. All the transactions are made in terms of its cryptocurrency transfer viz. Bitcoin. It ensures the classical problem of double spending using a peer to peer network and using a powerful consensus algorithm 'Proof of Work'. It uses special scripts called 'Bitcoin Scripts' to govern the transactional activities like sending bitcoins, claiming bitcoins, etc.

2. **Ethereum -** It is an open-source public blockchain network, which along with a cryptocurrency associated with it, also is able to carry other assets on its backbone blockchain. The state changes of Ethereum can be easily governed by the Smart Contracts which are executed on Ethereum Virtual Machine(EVM). The transaction on the Ethereum Transactions requires a fee, called Gas in order to be successfully executed. The higher the gas amount a person is willing to pay for a transaction, the more early his/her transaction is executed on the Ethereum Network.

3. **EOS -** It is a public blockchain network, which allows building decentralised applications on the top of it. It also uses the Smart Contracts to govern the transaction. But it differs from the existing public blockchain platforms, in a way that the transactions on EOS are completely free. It uses a hybrid version of Proof of Stake, called Delegated Proof of Stake(DPOS) to eliminate the transactional fee in the network. But this comes at the cost of a little amount of decentralisation.

Property	Bitcoin	Ethereum	EOS
Consensus	PoW	PoW	dPoS
Transaction fee	Yes	Yes	No
Smart Comtract	No	Yes	Yes
TPS	7-8	15-20	50000
Decentralisation level	High	High	Low

Table 1: Comparison of Public blockchain Networks

2.2 DNS

Referred from: [3]

- **Domain Name**
  Domain Name is the address where Internet users can access a website. It is used for finding and identifying computers on the Internet. Domain names were developed and used to identify entities on the Internet rather than using IP addresses.

- **DNS**
  DNS (or Domain Name System) refers to the legacy DNS system which is hierarchical, centralised and controlled by a trusted organisation, which provides service to resolve Domain Names (or Uniform Resource Locators) to an Internet Protocol Address (IP Address).

- **CA**
  CAs (or Certificate Authorities) are trusted entities in the centralised and hierarchical PKI (Public Key Infrastructure) which are responsible for approving other certificates on the Internet.

- **Registry Operators**
  Registry Operators are entities that manage the registry (database) of a particular TLD (categorised as gTLD and ccTLD) such as VeriSign which operates the .com and .net (both are gTLDs) registries.

2.3 Domain Name Transfer

- **Registrar or Domain Name Registrar**
  Registrar or Domain Name Registrar is a company that manages the reservation of Internet domain names.

- **Registrant**
  A registrant is an entity owning a registered domain name.

- **Buyer**

  Buyer in this document refers to an entity who is interested in buying a domain name that is currently owned by a different entity.

- **Seller**

  Seller refers to an entity that currently owns a particular domain name and is interested in selling that domain name to some other entity.

- **Domain Broker Service**

  Domain Broker Service refers to the service provided by various entities for domain ownership transfer between two interested parties. These are the entities that are in business for their own profit and act as a mediator between buyers and sellers. An entity providing this service is called Domain Broker.

3 Proposed Work

3.1 Current System

The current system to transfer domain names consists of a broker which acts as a middle man between the participants. Domain name brokers are centralised entities. [1]

3.1.1 Domain Brokers

There are different entities that provide broker service such as Hosting providers, a registrar may also provide a service, third-party services to serve as domain broker. But the mandatory entity that is involved is a Domain Name Registrar where the final ownership records are modified to complete the ownership transfer process.
Let's take the case of GoDaddy (an organisation that provides Hosting Service, Domain Broker Service, and is a Domain Name Registrar itself). Here you can buy a new domain. But let's say we search for "paytm.com" (which is already owned by an entity), GoDaddy's interface provides us with an option to take their Domain Broker Service. The "Broker Service Fee" as mentioned there is around > 4000 INR. Now, this fee is for hiring a personal Agent ("Domain Buy Agent" as GoDaddy calls it). Once an entity buys their service, then the negotiation with the current Registrant of "paytm.com" (which may or may not be interested in selling). If the negotiation is finalised, then the Buyer will have to pay the final settled price for the domain plus any commission charged by the Service Provider. The GoDaddy's commission for the same is 20% of the settled price. So in total, the Buyer pays (4000 + 1.2 * (Price of Domain)) INR to GoDaddy and the original owner of "paytm.com" gets (price of domain) INR.

3.1.2 Domain transfer from one Registrant to another

To transfer a domain name to another registrant, the owner can initiate a change of registrant by contacting the current registrar. The registrar will then ask for the owner's confirmation via a secure mechanism (which typically will take the form of an email to the registered name [3] [2]

holder). The owner must provide their confirmation within the number of days set by the registrar (not to exceed 60 days) or the transfer will not proceed. Once the registrar receives confirmation from the owner, they will process the transfer and notify the owner and the new registrant once the transfer is completed.

Going through the domain transfer process, it is evident that there is no extra charge involved in ownership transfer between registrants. But the current Domain Broker Services charge a lot.

3.1.3 Current Implementation

1. Broker launches its interface
2. The seller (Current Owner - O1) puts a listing on the broker's list through the interface.
3. The buyer (Final Owner - O3) may visit the interface and see for different listings, showing interests according to the requirement.
4. The actual process -
    - The buyer (O3) pays the decided amount + Broker's commission to the broker (whose status may be viewed by the seller).
    - The seller (O1) transfers the ownership of the domain to the broker (O2).
    - When both of the above steps are done, the next phase starts.
    - The broker starts the transfer process simultaneously. Sends the decided amount to O1 and the domain ownership to O3.

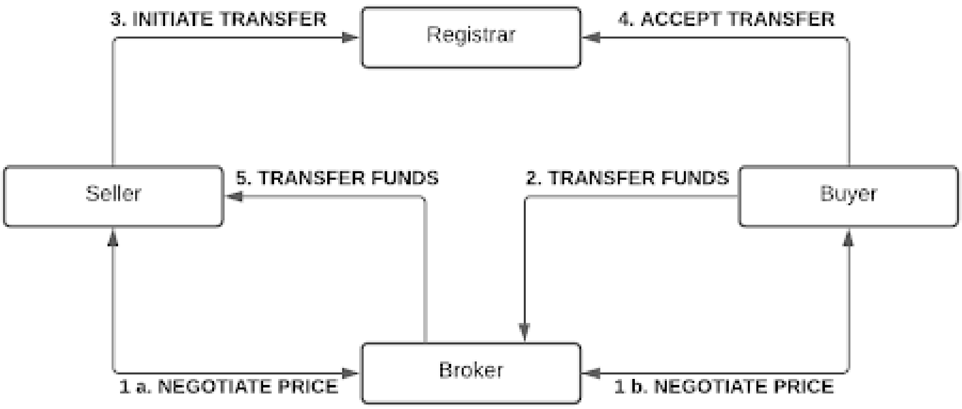

Figure 2: Domain name transfer in a centralised environment

3.2 Blockchain based approach

A Blockchain-based service will replace the current Broker Services offered by various entities. The service will be replacing some of the costly, fraudulent, semi-transparent practices involved in the process.

3.2.1 Advantages

- The middle man plays a vital role in the legacy DNS but there are high possibilities for any scam to take place. In the new blockchain based approach, the elimination of the middle man assures no scope of fraud.
- The blockchain based model is a decentralised system. This approach ensures that the brokers do not have a monopoly over the system and extract unreasonable amount of money from both the ends.
- Implementation of the smart contracts in the system encourages trustful ownership transfer between the buyers and sellers.
- Once a transaction concerning a particular buyer and seller has been settled, the ownership details of the same remains in the system, unchanged and permanent.

3.2.2 Challenges

- To decide the favorable architecture of the Blockchain from the available Public and Private platforms. All the available Blockchain Platforms available in the market have some trade-off between the characteristics.
- Secure procedure for ownership transfer using Blockchain.

3.2.3 Proposed Implementation

In our use case, we want to bring trust between the buyers and sellers for the transactions in the form of digital currency, governed by smart contracts without any need of centralised fiat currency.
Keeping in mind all these points, choosing a public blockchain platform will be more feasible for the selected use-case.

The implementation will include a web-interface where sellers can list the domain for selling. While making an initial request for listing a domain for sale, the seller has to set a base price for auction on the platform. Interested buyers can put on their bids on the domains which they want to buy. The auction process will be completely governed by a separate smart contract. During bidding the visitors will have to transfer the bid amount at the contract address.

The amount paid by the auction winner will be transferred to the seller's account after ownership transfer of domain and rest of the pooled money will be transferred back to the bidders addresses. All the data related to listing of the domains will be governed by another smart contract.

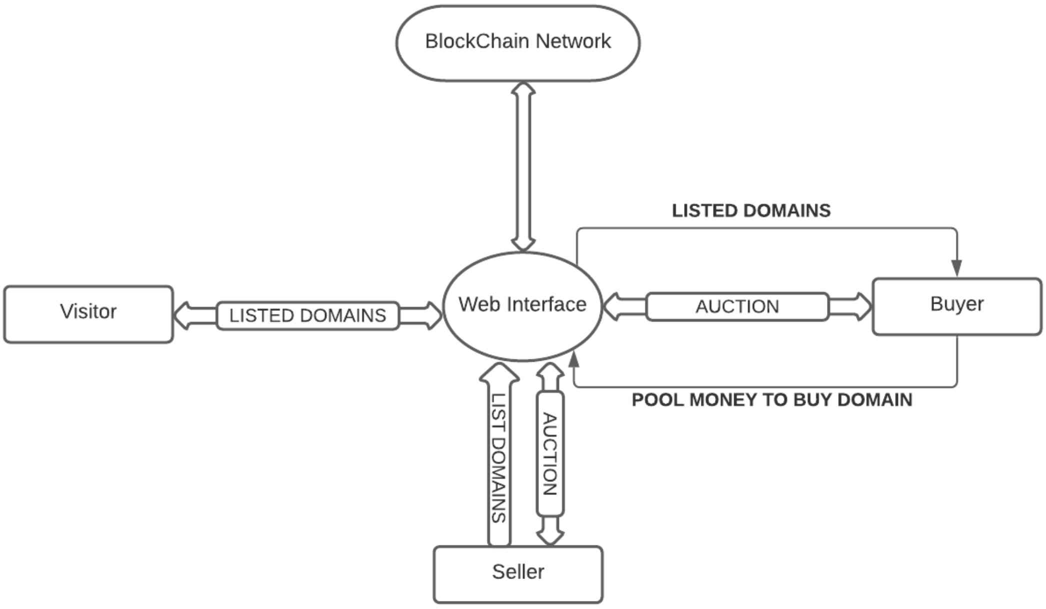

Figure 3: Blockchain-based approach to transfer domain names

4 Conclusion

In this report, we explored the replacement of current central brokers in secondary market of domain names. We have explored how our blockchain-based implementation can be thought of as a replacement for the current market. Alongwith the implementation we discussed our way through what are the best possible choices of architecture for our implementation, various trade-offs made and the enhancements (to the current model) that the new blockchain-based service brings to the table. Our report describes that such a blockchain-based service is feasible to implement using the current technologies.

References

[1] AFNIC. The secondary market for domain names at www.afnic.fr/medias/documents/afnic-issue-paper-secondary-market-2010-04.pdf, 2010.

[2] Escrow.com. How to transfer domain names at www.escrow.com/domains/how-to.

[3] ICANN. Resources at www.icann.org/resources.

[4] Niclas Kannengießer, Sebastian Lins, Tobias Dehling, and Ali Sunyaev. Trade-offs between distributed ledger technology characteristics. *ACM Comput. Surv.*, 53(2), May 2020.

[5] Daniel Larimer. Delegated proof-of-stake (dpos). *Bitshare whitepaper*, 2014.

[6] Olivier Moindrot. Proof of stake made simple with casper. 2017.

[7] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Cryptography Mailing list at https://metzdowd.com*, 03 2009.

[8] Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.

[9] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14:352, 10 2018.

Acknowledgement

We would like to express our deep sense of gratitude and indebtedness to our project guide, Dr. Sankita J. Patel, Associate Professor, Computer Engineering Department, SVNIT Surat for her valuable guidance, useful feedback, and co-operation with kind and encouraging attitude at all stages of experimental work for the successful completion of this work. We would also like to thank our Head of Department - Dr. Mukesh A. Zaveri, Computer Engineering Department for all the support. We extend our sincere gratitude to SVNIT Surat and its staff for providing us with this opportunity which helped us in gaining sufficient knowledge to make our work successful.