Democratic Aftermarket for Domain Names

Hrishabh Sharma, Ujjwal Kumar, Amruta Mulay, Rishabh Kumar, and Sankita J. Patel

1 Introduction

With the development of Blockchain Technology, we observe that the world is considerably shifting toward decentralization. The users demand actual control over their data and information. Therefore, efforts are being taken to eliminate the brokers/mediators and the centralized entities present in different use cases. The Secondary Market of Domain Names is one of such areas that demands decentralization for precluding the idea of a broker system. The rapid increase in the growth of Internet users has attributed to an exponential growth in the ownership of domain names. Domainers belonging to different categories have recognized the importance of unique and appealing domain names, engendering a competitive secondary marketplace for domain names. This provides an incentive for the proposed model to focus on the rapidly growing secondary market of domain names along with the entities involved and implement a Blockchain-based system over this legacy system to permit the potential sellers who own a domain and their respective buyers to communicate directly without the need of a broker as a mediator. The overall objective lies in making the system more reliable, transparent, independent, and reducing the commission rates, thus providing a smooth service to the domain buyers/sellers.

In the present-day market of Domain Names, the middlemen are responsible for providing the services for buying and selling these domain names. The middlemen act as the centralized entities that play the role of trading the ownership of domain names and the monetary worth associated with it between the buyers and sellers. Consequently, the buyers are given access to the domain name they pay for, while the sellers settle down with the agreed price. The main concern here is that the brokers charge a commission rate for the service they provide to both these parties. In this paper, we propose a novel decentralized service for domain buyers and sellers using

H. Sharma (✉) · U. Kumar · A. Mulay · R. Kumar · S. J. Patel
Sardar Vallabhbhai National Institute of Technology, Surat 395007, Gujarat, India
e-mail: sjp@coed.svnit.ac.in

U. P. Rao et al. (eds.), *Security, Privacy and Data Analytics*, Lecture Notes in Electrical Engineering 848, https://doi.org/10.1007/978-981-16-9089-1_4

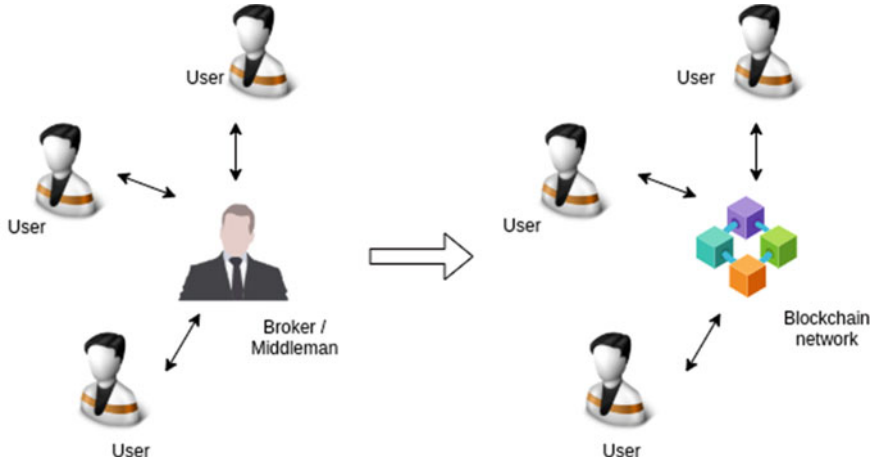

Fig. 1 Moving from centralized to a decentralized system

Blockchain technology. In the proposed system, the brokers are eliminated, allowing the buyers and sellers to communicate directly. This system provides transparency as well as reduced commission rates, thus giving benefits to both parties.

The main aim is to provide the decentralized service based on Blockchain Technology, as depicted in Fig. 1. This recommended system is safer as compared to the centralized domain name market, and avoids various attacks caused due to the broker's existence like phishing attacks, click-baits, masquerade attacks, overpricing, etc. If economically feasible, this proposed service can supplant other domain escrow services that the domain name registrars provide. The scope for applying this service is not circumscribed only to companies or organizations but can be broadened to almost everyone on the Internet.

The major contributions of our work are as follows:

- We eliminate the unfairness involved in the present domain aftermarket to develop a competitive and fair market of domain selling and buying through a Decentralized Ethereum application.
- We present the detailed system architecture in the form of algorithms, sequence, and entity diagrams.
- We discuss the economic feasibility and the reduction of commissions through the proposed approach.

2 Background

In this section, we discuss the background of how domain transfer takes place with a centralized entity involved. This will create a clear image to understand where and what entities should be replaced to transform into a decentralized model. The promi-

nent members who are actively participating in the centralized model of Domain Name Transfer are as follows [1]:

- **Registry/Domain Name Registry:** It maintains a database of the domain names and corresponding registrant details. It also enables third-party entities to get administrative control on a domain name.
- **Registrar/Domain Name Registrar:** It is the agency responsible for managing the reservation of domain names.
- **Registrant:** This entity holds a registered domain name.
- **Buyer:** Refers to the person or party that is willing to buy a domain name presently owned by someone else.
- **Seller:** Refers to the person or party that owns a particular domain name and is interested in selling it to someone else.
- **Domain Broker Service:** Concerned with the service of transferring the domain ownership between two interested parties. They act as mediators and charge commission rates for the service they provide.

Having discussed the above main terms, the domain transfer from one registrant to another occurs in the following manner.

Initially, the domain name owner, i.e. seller, requests a change of registrant by contacting the present registrar. This registrar will request for owner's confirmation via some secured means like email verification. Once the verification process has been done, the owner initiates the transfer of the domain name to the registrar. The registrar contains the updated list of all the domain names that are available for selling. Meanwhile, the broker negotiates the price for selling that particular domain name with the owner and finds an appropriate buyer. Once both the parties have settled down with the negotiated price for buying and selling, the funds are transferred, and the domain ownership is handed over to the buyer. Here, the broker adds extra commission charges for its service, thus causing the buyer to pay more and the seller to earn less.

The current approach of the centralized model contains flaws related to the veracity between the parties involved. There may arise issues such as the broker denying fund transfer to the seller even though the buyer has made the payment and the seller has already transferred the ownership of the domain name. Another issue may be that the buyer has successfully transferred the money to the broker. In contrast, the seller has not yet completed the ownership transfer of the domain name, allowing the broker to scam with the money received from the buyer. Moreover, due to the non-transparency in the model, there is a high possibility of overpricing from the broker's side to maximize their profits. Thus, the buyer has to pay higher price money than required. In the use case that is being considered, trust needs to be established between the buyer and seller where the transaction will take place through digital currency, which the smart contract will govern. This eliminates the involvement of any centralized fiat currency.

2.1 Accessing Registry Data

The registrant data (information shared at the registration) is stored with the registrar and shared with the registry. Till May 2018, one could find the contact information (name, email address, contact number, postal address) associated with a domain name using WHOIS [2] protocol service [3]. However, this service has now been modified to bring it in line with the General Data Protection Regulation (GDPR) [4] policies (enforced in May 2018). So, at its present state, WHOIS does not provide the contact details of the registrants (postal address, email address, contact number); hence, we cannot use WHOIS for our verification process.

Nevertheless, WHOIS has now been accompanied with another service, namely Registration Data Access Protocol (RDAP) [5] which provides many features over the previous WHOIS protocol. RDAP provides differentiated access, meaning one can query RDAP service either anonymously or with some authentication.

2.2 Blockchain

Blockchain is a popular distributed database of records such that the records are stored in the form of blocks, and each block is connected to the previous block by storing its block hash. Thus, it is a chain-like linked structure formed of immutable blocks. Depending on the different architectures of the Blockchain Network, the degree of decentralization may vary; this is primarily due to the conspicuous trade-offs that will arise due to the various characteristics of Blockchain [6].

2.3 Smart Contract

Smart contracts are code stored on the blockchain which serves as a type of agreement, and contain business logic. It gets executed when certain pre-written conditions are met. Smart contracts eliminate the risk of any fraudulent activity from the participants [7].

2.4 Auction

The definition of an auction is a public sale of the property to the highest bidder. The ultimate goal of an auction sale is to obtain the best financial returns for the property owner and allow free and fair competition among bidders. The most common types of auctions are (i) Increasing price auction (English auction), (ii) Sealed-bid auction,

(iii) Decreasing price auction (Dutch auction), and (iv) Second-price auction. This paper uses English auction in its implementation [8].

According to a study, the following features of a deal help one determine if auction is the right choice to go with—

- **Buyer Profile:** The number of potential buyers should be large and familiar.
- **Process Setter's Profile:** An auction is quicker than a negotiation making it a finer mechanism when the speed is critical.
- **Contextual Factors:** Auction should always be preferred in cases where transparency and secrecy are significant factors to consider.

3 Related Work

Although there have been many pioneers for establishing aftermarket deals, all are centralized. Many domain registrars, e.g. GoDaddy, provide their domain broker service. But this comes at a fee for hiring a personal Agent ("Domain Buy Agent", as GoDaddy calls it). The "Broker Service Fee", as mentioned, there is around >8000 INR, and this cost has been doubled in the last 6 months. Once users buy their service, the negotiation with the current registrant of a domain (who may or may not be interested in selling) proceeds. If the negotiation is finalized, the buyer will have to pay the final settled price for the domain plus any commission charged by the Service Provider. GoDaddy's commission for the same is 20% of the settled price [9].

Apart from the registrar's provided domain broker services, there have been attempts to provide the aftermarket through escrow methods. "Escrow.com" [10] is one such example. Sedo.com [11] is another popular online web platform that provides services like domain acquisition and auctions for aftermarket domain selling.

To the best of our knowledge, there has not been any attempt in the literature to make the domain name aftermarket decentralized. On the other hand, this is not the case with Blockchain-based domain names. These domain names are established and managed on the Blockchain itself and use the DNS running on the Blockchain network. For example, the Ethereum Naming Service (ENS) is one of the Blockchain-based domain names which allows managing and transferring the ownership on the network itself (Ethereum Blockchain Network). Since ENS exists on Blockchain, the execution of an aftermarket is achieved natively and easily. But when we talk about domain names that exist on the existing DNS architecture, the execution requires some engineering workaround and no existing solutions exist.

4 System Architecture

In the concerned use case, the end goal is to bring trust between the buyers and sellers for the transactions in digital currency, governed by smart contracts, without any need for centralized fiat currency.

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. Then, interested buyers can put on their bids on the domains which they want to buy. A separate smart contract will wholly govern the auction process. During bidding, the visitors will have to transfer the bid amount to the contract address. The amount paid by the auction winner will be transferred to the seller's account after the ownership transfer of the domain. Another smart contract will govern all the data related to the listing of the domains.

4.1 Valuation of Domain Name via Auction

Association française pour le nommage Internet en coopération (AFNIC), an association that operates on French country code top-level domains (ccTLD), has suggested in one of their Issue Paper [12] that the value of a domain name is determined chiefly by factors like search engine rankings, the meaning of the name, public perception, keyword competition, and traffic analysis (and many more). Unfortunately, these factors cannot be formulated easily (at least they have not been formulated to date). Moreover, an individual/organization may prioritize these factors differently (based on their opinion), making the valuation even more difficult. Hence in our opinion, a bidding platform is the most suitable way to determine the value associated with a domain name. We have decided on an English auction type for the scenario at hand to keep the bidding process intuitive to the bidders. Furthermore, the bidding will be public (i.e. all the bidding made will be publicly visible as the bidding continues).

4.2 Choosing the Suitable Blockchain

Due to the considerable increase in the adoption of Blockchain in various use cases, it has taken different forms comprising different characteristics. Therefore, according to the use case, one must understand the different characteristics and decide on a suitable Blockchain platform. We are now surrounded by hundreds of Blockchains that differ in various characteristics. For example, they can be public or private, permissioned or permissionless, with or without Turing-complete smart contracts. So, there is "No one fit design to all" Blockchain platform [13]. After analyzing the use-case requirement, we needed Turing-complete smart contracts to smoothly govern the auction process and enable buyer-seller to use the application without

permission. This narrows down our search for choosing a suitable public Blockchain network with Turing-complete smart contracts. "Ethereum" and "EOS" come into the mind with these characteristics. After performing a detailed survey plus considering the wide adoption and community support in Ethereum Network, we proceeded with our work by choosing the Ethereum Blockchain [14].

4.3 Components

The entire architecture consists of four major components: (i) The registry of domain names accessible via Registration Data Access Protocol (RDAP) [5], (ii) A server that indexes Blockchain data into information presentable to the user, (iii) The Blockchain network and its underlying database (ledger), and (iv) The smart contract where all the logic for auction and fund management resides.

The server (dApp-backend) and the domain names registry interact on the traditional client-server request model to fetch the ownership information. Another task of the dApp server is to present meaningful information fetched from the Blockchain ledger. The logic for handling the auction process and fund management is realized into a smart contract deployed on the blockchain network, which can never be tampered with once deployed. The record of all the events such as the listing of a domain, starting auction for a particular domain, bids made to a particular auction, ending of the auction and lastly, the transfer of funds is handled through the Blockchain network, which gets saved into the underlying database of Blockchain (Fig. 2).

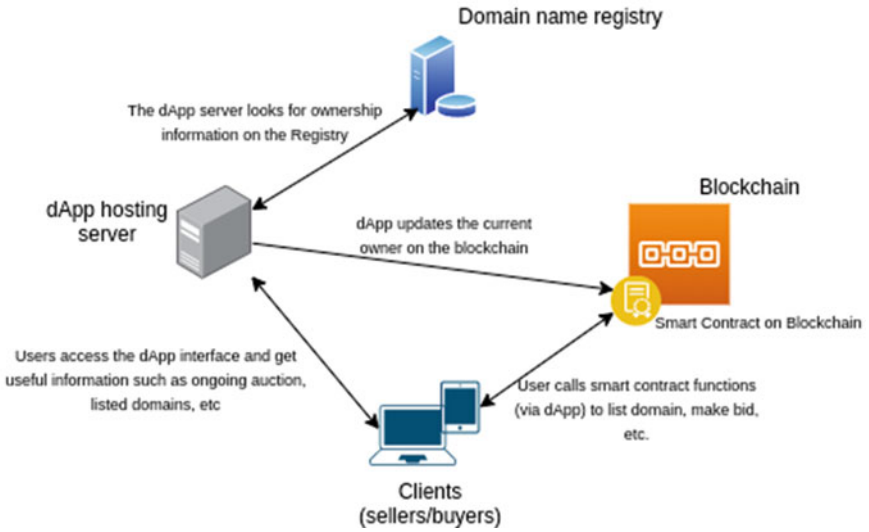

Fig. 2 System architecture—components

4.4 Implementation

This section discusses the step-by-step process that will take place to execute the use case. The activity for domain buying and selling takes place in the following sequence.

4.4.1 Domain Ownership and Email Verification

Initially, the users who are willing to sell their domain names need to fill out a form that verifies the ownership of this domain. Then, email verification can be performed using the One Time Password (OTP) approach. If the verification process is successful, we authorize this user to list their domain for the auction process. As an experimental setup of the architecture and to access the registry of authorized domain owners, the service of RDAP API can be mimicked to match the details while verifying the ownership of domain names.

4.4.2 Domain Listing for Auction

Once the final confirmation is made from the seller's side for domain selling, a Blockchain transaction will be initiated via MetaMask [15] to broadcast it on the Blockchain network. Here, the seller also associates a minimum bidding value for their domain name as the starting price for the auction process, as highlighted in Fig. 3.

4.4.3 Auction Bidding

After the seller's list is updated, the buyers can view them on a standard web interface. As shown in Fig. 4, the buyer may show interest in a particular type of domain name and want to buy it. If interested, they may select the "bid" option to initiate a Blockchain transaction creation by MetaMask.

4.4.4 Ending Auction

The sellers have the authority to end the auctions concerning their respective domain names. Once the auction has been ended, the buyers cannot bid for that particular domain name. MetaMask will report an error and restrain the buyer from initiating a transaction. Moreover, once the auction process has terminated, the highest bidder must transfer the bid amount to the smart contract address in a fixed time window. If he/she fails to do so, the auction is discarded; otherwise, the seller is supposed to transfer the ownership of the domain name. After successfully verifying the domain

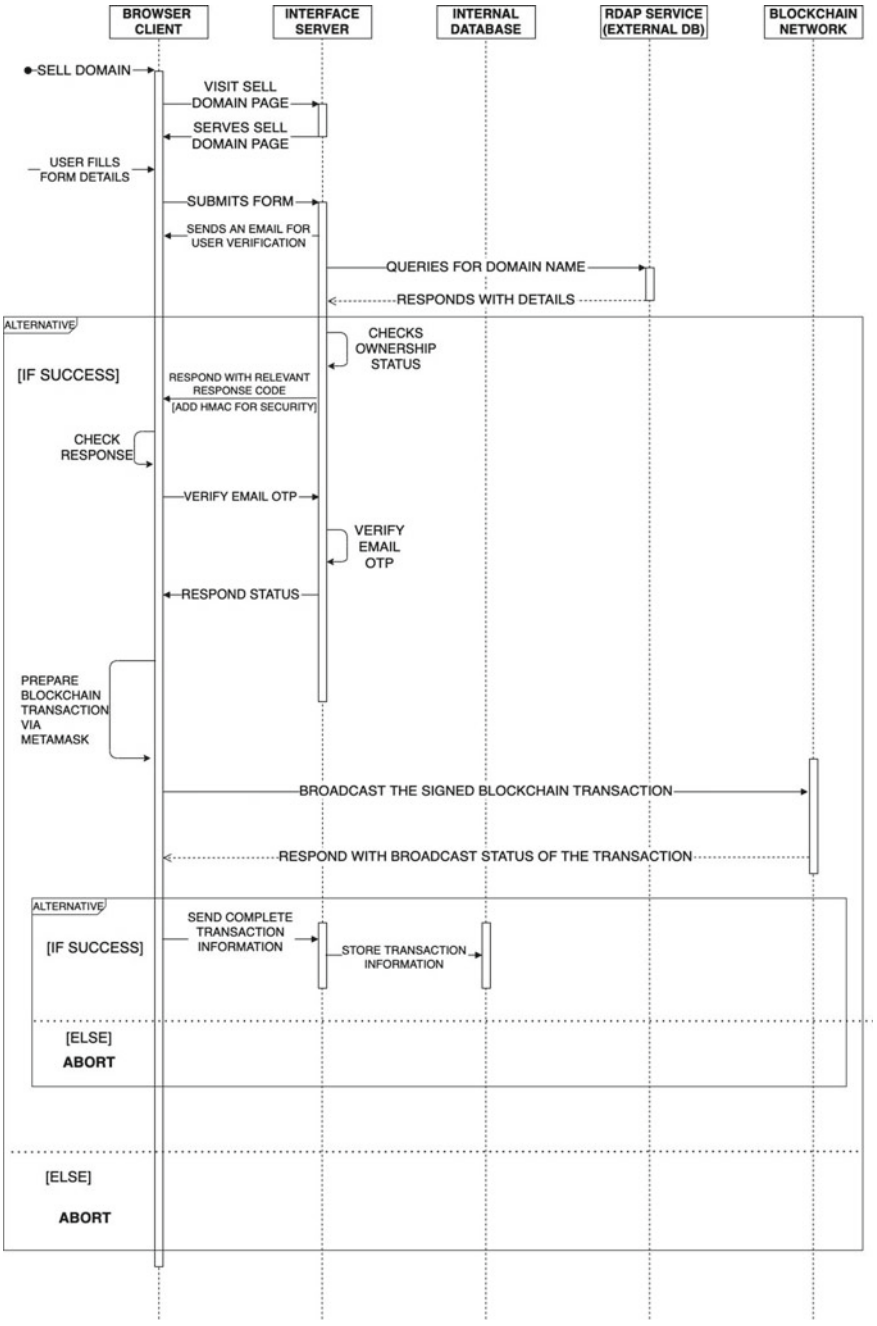

Fig. 3 Sequence diagram of listing a domain

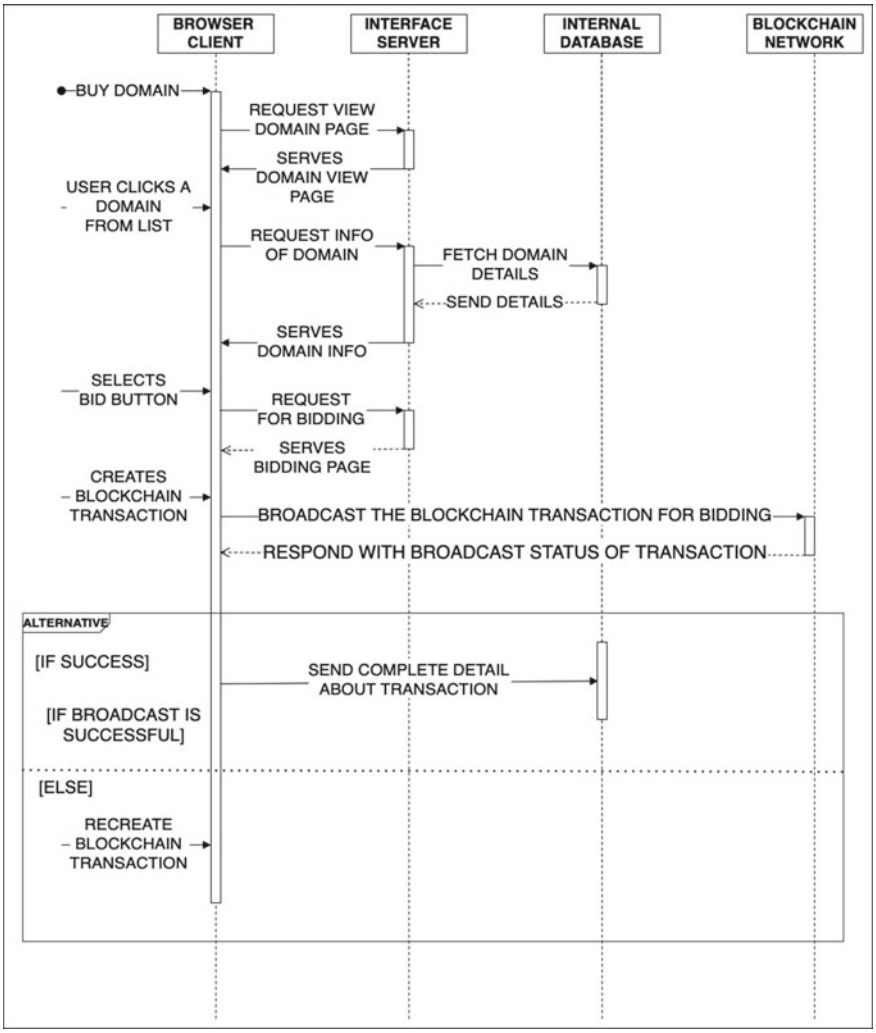

Fig. 4 Sequence diagram of bidding

ownership transfer through the dApp server, the fund settlement is initiated by the smart contract and funds are released to the seller.

5 Smart Contracts

In this paper's concerned use case, two Smart contracts will be deployed, i.e. Domain Market and Domain Auction. The Domain Market smart contract will keep track of all the domains available for sale on the blockchain platform and provide the

necessary transaction functions like submitting the new domain for sale and checking the auction's status. Also, an instance of a domain auction smart contract is created and will be associated with each domain available for sale. See Code Listing 1. The domain auction contract will govern the basic auction activities like bidding in the auction, ending the auction, and receiving funds from the highest bidder.

```
struct Domain {
    uint id;
    address payable owner;
    string domainName;
    string contactEmail;
    uint basePrince;
    bool ownerVerified;
    bool succesfullySold;
    DomainAuction auction;
}
```

Listing 1 Structure of a Domain

6 Evaluation

6.1 Improvements over Current Market Scenario

Various advancements are brought by the Blockchain-based service that replaces the current Broker Services offered by various entities. The main objective has been to replace the costly, fraudulent, semi-transparent practices involved in the latter. The brokers' prominent participation in the legacy DNS causes a high probability for unfairness to occur. The Blockchain-based approach eliminates these brokers, therefore assuring no scope for fraud. Moreover, the Blockchain-based model is a decentralized system. It makes sure that the brokers do not gain a monopoly over the system and withdraw an unreasonable amount of money from either party. Since smart contracts are the coded programs implemented in the Blockchain system, this encourages trustful ownership transfer between buyers and sellers. Once any transaction has been settled between a particular buyer and seller, the details concerned with the ownership status remain unchanged and permanent in the system.

6.2 Fees Involved in a Transfer

We designed and deployed the smart contracts on the Ropsten Testnet [16] to estimate the fees incurred in a typical domain name transfer. A domain listing operation used 691,760 gas units and constituted the charges on the seller's end. The cost of listing operation varies for different lengths of domain names because we store the domain names on the Blockchain. Similarly, a long domain name (say 64 characters long)

Table 1 Cost Involved in different operations at gas price of 30 Gwei

Operation	Gas units used	Fee in ETH
Listing a domain	691760	0.0207528
Bidding	48775	0.00146325
Ending an auction	53508	0.00160524

will require 692,528 gas units for the same operation. Similarly, a bidding operation constitutes the major transaction charges from the buyer's end. Single bidding on any domain name took 48,775 gas units on average. Moreover, an explicit termination of auction consumes 53,508 gas units. Table 1 shows the cost discussed above for different operations.

6.3 Reducing the Network Transaction Fee

To make the proposed work more novel, we performed a detailed analysis of the Layer-2 Blockchain solutions based on the Ethereum blockchain. Plasma solutions helped reduce the transaction cost and provide faster transaction speed [17]. We used the Polygon (previously known as Matic) network, an adapted version of Plasma, to perform a detailed comparison in reducing the network transaction fee compared to Ethereum Network. Tables 2 and 3 show the gas used (in ETH) on Ethereum and Polygon Network for seller and buyer, respectively.

Table 2 Seller's fee on ethereum and polygon network

L*	Seller@ETH	Seller@Polygon
27	0.02235768	0.002235768
28	0.02235804	0.002235804
508	0.0332298	0.00332298

Table 3 Buyer's fee on ethereum and polygon network

L*	Buyer@ETH	Buyer@Polygon
27	0.00146326	0.000146326
28	0.00146326	0.000146326
508	0.00146326	0.000146326

*Length of the domain name added with the email address of the owner, in characters
*The Cost is estimated at Average Gas Price of 30 Gwei on Ethereum Network and 3 Gwei on Polygon Network
*All costs are indicated in terms of Ethereum (ETH) cryptocurrency

6.4 Limitations of the Architecture

Most public Blockchains today suffer from the lack of scalability, and hence any solution built using a public Blockchain network will also get a hit on the scalability side. Though the Ethereum platform currently uses the Proof-of-Work consensus mechanism, which offers 15 TPS, it will soon make a complete shift to the Proof-of-Stake consensus mechanism, which will drastically boost the TPS to a few thousand. Another central point that should be noted is that the ownership information of legacy domain names resides on off-chain databases, and Blockchain solutions have the limitation of not being able to access off-chain data directly. Bridging this gap gives the architecture a hybrid design which makes such a solution not full proof as a Blockchain network. Despite this, the proposed design offers significant trust, transparency, and no hassle of negotiation over the legacy aftermarket platforms to handle the auction process and funds.

7 Future Work

There is much scope for improvement concerning off-chain data fetching. Integrating solutions that allow accessing off-chain data more securely and seamlessly will be an ongoing task as improvement in this aspect of Blockchain technology emerges. The weakest part of the proposed architecture is the dApp server, which also fetches domain ownership information. Though the architecture achieves the secure management of funds, it fails to handle cases of breached dApp server, which poses a security threat. This security threat can be handled by allowing the affected party to raise a dispute in scenarios of unfair settlement. It can be achieved using a multi-signature Smart contract design for the Domain Auction. This smart contract will enable the affected party to raise a dispute in a given time frame so that the inaccurate fund settlements do not occur in case of a dApp server breach. The dispute settlement process will again leverage the Blockchain network of independent validators, which will aid the ownership conflict resolution. This model further requires work and analysis for its practicality.

Also, there has been the advent of Blockchain managed domain names. Therefore, the platform can be extended to include those domain names to make it more inclusive. Furthermore, the support of Blockchain-managed domain names will be much more secure and seamless than the auction of legacy domain names as the complete information will be available on-chain, thus reducing the risks of accessing off-chain data.

References

1. ICANN, Resources. https://www.icann.org/resources. Accessed 12 Sep 2021
2. ICANN, WHOIS. https://whois.icann.org/en/about-whois. Accessed 12 Sep 2021
3. Temporary Specification for gTLD Registration Data. https://www.icann.org/en/system/files/files/gtld-registration-data-temp-spec-17may18-en.pdf. Accessed 12 Sep 2021
4. What is GDPR. https://gdpr.eu/what-is-gdpr/. Accessed 12 Sep 2021
5. Registration Data Access Protocol (RDAP). https://www.icann.org/rdap. Accessed 12 Sep 2021
6. Zheng Z, Xie S, Dai H-N, Chen X, Wang H (2018) Blockchain challenges and opportunities: a survey. Int J Web Grid Serv 14:352
7. Mohanta BK, Panda SS, Jena D (2018) An overview of smart contract and use cases in blockchain technology. In: 2018 9th international conference on computing, communication and networking technologies (ICCCNT), 2018, pp 1–4. https://doi.org/10.1109/ICCCNT.2018.8494045
8. Online auction - Wikipedia. https://en.wikipedia.org/wiki/Online_auction. Accessed 12 Sep 2021
9. GoDaddy Broker Service. https://godaddy.com/domains/domain-broker. Accessed 12 Sep 2021
10. About Escrow.com. The Online Escrow service. https://www.escrow.com/why-escrowcom/about-us. Accessed 12 Sep 2021
11. Sedo company details. https://sedo.com/us/about-us/. Accessed 12 Sep 2021
12. AFNIC, The secondary market for domain names (2010) https://www.afnic.fr/medias/documents/afnic-issue-paper-secondary-market-2010-04.pdf. Accessed 12 Sep 2021
13. Kannengießer N, Lins S, Dehling T, Sunyaev A (2020) Trade-offs between distributed ledger technology characteristics. ACM Comput Surv 53(2), Article 42
14. Wood G (2014) Ethereum: a secure decentralised generalised transaction ledger, EIP-150 revision. https://gavwood.com/paper.pdf. Accessed 12 Sep 2021
15. MetaMask About. https://metamask.io/about. Accessed 12 Sep 2021
16. Networks-Ethereum. https://ethereum.org/en/developers/docs/networks/#testnets. Accessed 12 Sep 2021
17. Plasma-EthHub. https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/plasma/. Accessed 12 Sep 2021