Adoption Of Pets In Distributed Network Using Blockchain Technology

Article *in* International Journal of Blockchains and Cryptocurrencies · January 2019

DOI: 10.1504/IJBC.2019.10024984

5 authors, including:

Gururaj H L
Manipal Institute of Technology
103 PUBLICATIONS **300** CITATIONS

SEE PROFILE

Adoption of pets in distributed network using blockchain technology

H.L. Gururaj*, Athreya A. Manoj, Ashwin A. Kumar, S.M. Nagarajath and V. Ravi Kumar

Computer Science and Engineering Department,
Vidyavardhaka College of Engineering,
Mysuru, India
Email: gururaj1711@vvce.ac.in
Email: manojathreya.cs@vvce.ac.in
Email: ashwinkumar.cs@gmail.com
Email: nagarajath.cs@vvce.ac.in
Email: ravikumarv@vvce.ac.in
*Corresponding author

Abstract: As the whole world is moving towards digital payments, ethers and the transaction methods with quick payment features are stored in a blockchain in a distributed network. To adopt pet animals, this technology provides security and flexibility to users. The distributed network is a network system through which data, software and computer programming are spread across on more than one node(computers) and these nodes are dependent on each other. It is nothing but a peer-to-peer network which eliminates a single point of failure. The blockchain is a growing list of records called blocks, that are linked using cryptography. It is a decentralised, distributed and an immutable ledger to store digital transactions. Its databases are managed using a peer-to-peer network where all the nodes in a network are equal and are the major concern in the types of network architecture. The consensus protocol is used for transacting and communicating between the nodes. In this paper, a unique way of adopting pets is proposed where the transaction details are stored in a blockchain whereby using hash value returns further details of the transaction. It provides users more convenient access in adopting pets and provides a better approach to the existing centralised system.

Keywords: blockchain; decentralised; distributed; peer-to-peer network; smart contracts.

Reference to this paper should be made as follows: Gururaj, H.L., Manoj, A.A., Kumar, A.A., Nagarajath, S.M. and Ravi Kumar, V. (2020) 'Adoption of pets in distributed network using blockchain technology', *Int. J. Blockchains and Cryptocurrencies*, Vol. 1, No. 2, pp.107–120.

Biographical notes: H.L. Gururaj is working as an Assistant Professor in the Department of Computer Science and Engineering at Vidyavardhaka College of Engineering, Mysuru, India. He received Young Scientist Award for International travel Grants from ITS-SERB, DST, Government of India. He is an ACM Professional member and Faculty Sponsor of VVCE ACM Student Chapter. His main research interests include QoS aware network congestion control, network security, cloud computing and machine learning.

Athreya A. Manoj is currently pursuing Bachelor of Engineering in Computer Science at Vidyavardhaka College of Engineering, Mysuru, India. He is the Chair of VVCE ACM Chapter and his research interests include blockchain technology, machine learning and IoT.

Ashwin A. Kumar is currently pursuing Bachelor of Engineering in Computer Science at Vidyavardhaka College of Engineering, Mysuru, India. He is the Treasurer of VVCE ACM Chapter and his main research interest includes cyber security and blockchain technology.

S.M. Nagarajath is currently pursuing a Bachelor of Engineering in Computer Science and Engineering at Vidyavardhaka College of Engineering, Mysuru, India. His main research interests include blockchain technology, decentralized storage and machine learning.

V. Ravi Kumar completed his BE in Electrical and Electronics from VTU University, Karnataka, India in 1998 and MTech in Computer Science from VTU University, Karnataka, India in 2001 and PhD from VTU University in 2015. He is currently serving as a Professor and Head in the Department of Computer Science and Engineering at Vidyavardhaka College of Engineering, Mysuru, India. His main research interests include data science, cloud computing, internet of things and artificial intelligence.

1 Introduction

Each and every human being in this world has an affection towards animals, who take cares and nurture them everyday. Pet animals are the integral part of human life and there exist some organisations which feeds them and take care of such animals, if a person needs to adopt them, they can make use of distributed network to do so which provides them secured transaction of money between the two parties. Peer-to-peer (P2P) networks has no central point of failure, as they lack single centralise points of vulnerability that hackers can exploit. P2P protocols provides distribution of high data capacity to users, which are scalable (Wichtlhuber et al., 2013). Blockchain technology can be used to create a constant, transparent, public ledger for organising sales records, which tracks digital payments between users (Ehmke et al., 2018). For storing the transaction details, Blockchain Technology is used as it is decentralised, distributed and public digital ledger. Decentralisation means storing data in different nodes across P2P network, thus eliminating the risks when the data is centrally stored in client-server architecture.

A blockchain, also called as a distributed, immutable ledger is essentially an append-only data structure maintained by set of nodes which won't trust each-other fully. Nodes in a blockchain network agree on a set of blocks which are ordered, having multiple transactions. Hence, blockchain is viewed as a log of ordered transactions (Dinh et al., 2017). Blockchain enabled smart contracts employ proof-of-stake validation for transactions, which promises significant performance advantages compared to proof-of-work solutions (Dai et al., 2017). Blockchain technology aims at increasing magnitude of flexible traffic of evolving complexity. The target is to allow complex services which are secure, sustainable and efficient. Therefore, the target is to accelerate/scale blockchain functionality (Wright and Serguieva, 2017). Smart contracts is used such that it act as an agreement that is written to ensure valid agreement. Smart

contracts have become a reality with the boom of blockchain technology, which operates without trusted third parties for settling transactions and disagreements among pseudonymous participates (Buterin, 2013). Ethereum is an essential and an ultimate foundation layer, where a blockchain with in-built Turing-complete programming language. It allows anybody to write smart contracts for building decentralised applications with their own rules of state functions, transactions, and ownership (Buterin, 2013). A distributed ledger in a blockchain is replicated over the nodes in a network. Solidity is a high-level, contract-oriented language which helps in writing smart contracts. It mainly influences Python, C++ and JavaScript and was built for Ethereum Virtual Machine (EVM) (Buterin, 2013).

Wei Dai became the first person to present the paper which introduced the idea of incorporating virtual money through working out cryptographic puzzles as well as decentralised consensus, but his attempt failed as he did not provide adequate details on how decentralised consensus worked. Hal Finney presented a concept of 'Proof of Work', a network which uses idea of solving Hashcash puzzles to create a concept of cryptocurrency, but did not concentrate on issue for trusted computation on backend. Satoshi Nakamoto, in January 2009 set the first blockchain into motion in the name of bitcoin which concurrently introduced two radical and untested concepts, a decentralised P2P online currency and the second is the idea of a proof of work blockchain to allow for public agreement on the order of transactions.

The invention of this idea by Satoshi is simple decentralised consensus protocol, which is based on peers combining transactions into block in regular intervals forming a ever growing blockchain. With proof of work mechanism, peers have the right to participate in the system.

1.1 Characteristics of blockchain technology

1 *Getting trust:* in Ethereum network where the system runs in a fully decentralised manner, consensus mechanism is used to solve problems about guaranteeing truthful service. The facticity of services provided to the network is automatically checked and guaranteed by the consensus. Providers who cheat will be punished or even kicked out from the system. Success of decentralisation depends not only on P2P network but also on being trustless, where an environment needs no trust and no centralisation.

2 *Protecting security:* Blockchain system and a P2P network form the secure backbone of the Ethereum network. Communication operations between devices are embedded in the blockchain and service information is stored and routed by peer nodes and guaranteed by the consensus. The system therefore has no central point which is exposed to attackers and security is guaranteed by the consensus mechanism of distributed miners who are economically motivated to be honest.

3 *Achieving Fairness:* in Ethereum, services are published/subscribed to/from the network. The matching process is performed by a smart contract which cannot be controlled any end-point or a centralised party. The smart contract runs a truthful continuous double auction (TCDA) that prevents cheating and maximises social welfare of the entire community. TCDA is mathematically strategy-proof, where there is no incentive for traders to lie or hide their personal information from other

traders. This is blockchain-based technology to approach to the global fairness of service distribution in system.

4 *Strengthening incentive:* the real-time analysis is carried out for identifying supply and demand, where Ethereum creates new marketplaces built on the foundation established by system and blockchain network for transformation. This enables new P2P model of economies.

The paper is organised as follows: the related terminologies and related work are elaborated in Section 2 and Section 3 respectively. In Section 4, mathematical analysis is depicted. Results are drawn in Section 5. At last, Section 6 is about conclusion of the work.

2 Related terminologies

Blockchain is usually a tech savvy concept which contains a few technical terms. Some of the basic terms which are required to understand blockchain are listed below:

a *Blockchain:* a growing list of records called blocks which are linked together using cryptography. It is a decentralised, distributed and an immutable ledger meant for storing digital transactions.

b *Decentralised Blockchain:* a network wherein nodes interoperate and collaborate with each other to execute consensus algorithms without the need for any central decision-making source.

c *Distributed:* a database held and updated independently by each and every node of the large network. Transactions are not transferred to the nodes by a central authority, rather it is constructed independently by every node.

d *Immutable:* a block of transaction created by consensus among the nodes such that it can never be modified or changed.

e *Ethereum:* it is a platform which enables us to run smart contracts. It is very much similar to Bitcoin with only one major difference between them that is, nodes store the most recent state of each smart contract.

f *dApps:* applications that run on a P2P network rather than a single computer.

g *Transaction:* a small unit of task that is being stored in public records called as blocks.

h *Consensus algorithm:* a set of algorithms meant to achieve reliability in the network. It validates the upcoming block and makes sure that the network is secure.

3 Related work

In earlier days, people used to maintain a ledger to store data systematically. When it comes to maintaining financial transactions, it is more important and must be secured. After digitalisation the paper format was eliminated and data was stored in computers by using programs. These ledgers were maintained by a central authority which is bank or government which act as a trusted party. These digital ledgers were stored and

maintained in a central authority through servers. Hence these centralised systems became an attractive point for adversaries' party they experienced single point of failure. These stored data are hackable with the conventional security being provided. Therefore, blockchain technology came into picture to prevent security Vulnerabilities.

3.1 Blockchain

Blockchain technologically means a set of linked-lists where the data stored in it is immutable, which means data is stored it cannot be changed. Decentralisation means storing data in different nodes in P2P network, thus eliminating the risks of single point of failure. Immutable ledger is fundamentally an append-only data structure retained by set of nodes which won't trust each other completely. Nodes accepts chain of blocks which has multiple transactions in a blockchain network.

Blockchain technology intent at gaining magnitude of extensible traffic of emerging complexity. The target is to grant complex services which are secure, sustainable and efficient. Hence, the target is to scale blockchain functionality (Wright and Serguieva, 2017). Some of its limitations like scalability and protocols faults are being solved under constant research and development (Eyal et al., 2016; Kokoris-Kogias et al., 2019). P2P protocols provides distribution of high data capacity to users, which are scalable (Wichtlhuber et al., 2013). P2P blockchain networks has no single point of failure, as they don't have a central point of vulnerability that hackers can exploit. Blockchain technology can be used to create a constant, transparent, public ledger for organising sales records, which tracks digital usage and payments distribution to content creators (Ehmke et al., 2018).

3.2 Decentralised app

As the world is accommodating to regular apps, the full ecosystem is also emerging. dApps or decentralised applications are a peculiar strain of applications that are not dominated or belong to a single jurisdiction, cannot be lock out or cannot have a downtime. A new influx of decentralised applications called DApps has come into presence to solve major use cases like money management & transfer, business process management, decentralised autonomous organisation. Most dApps not only focus on money management and simplifying money transfer but also there are some innovative use cases of dApps.

dApps advertises decentralisation making them tamper-proof and the records immutable. As dApps are based on secure blockchain network, such apps promote a high security and are unalterable from hacks and intervention. Some features are:

- quick payment processing without requiring to integrate payment gateway to accept transaction
- high data security due to smart contracts administered by private keys
- greater anonymity without demanding the users to comply with the lengthy signup process
- legit data records as users can access the public blockchain to verify transaction information.

Scaling problem mentioned are being solved using sharding (*Towards Scaling Blockchain Systems via Sharding*, 2019) and plasma (Poon and Buterin, 2018) which provides a promising solution.

Various tech stacks, frameworks, and languages are accessible to develop an application but developers are not convinced about a single framework that can offer the good Results.

Increasing the popularity of blockchain-based application has also increased the demand for dApps (*An Empirical Study of Blockchain-based Decentralized Applications*, 2019). Describing dApp in one line is difficult because there is no clear-cut definition seeming to fit all the attributes that make an application a decentralised app. As dApps, an application need to have the following characteristics:

- *Open-source:* the primary aspect of dApps is that they should make their core source code available to everyone. As the core characteristic of dApps is self governed and consistent consensus protocol where the changes must be decided by all or the majority of the users. Also, the code should be available for everyone to know what they are trusting (Chang et al., 2018; Chen et al., 2018).
- *Decentralised:* as the name proposes, dApp stores data on a decentralised blockchain to save the app from hazards of centralised jurisdiction and affirm on self governing nature of the app.
- *Integrity:* dApp is based on the decentralised blockchain where the validators of the block on the network must be rewarded with cryptographic tokens or any form of digital asset which keeps them alive on network and serve the purpose (Liu et al., 2017).
- *Algorithm:* decentralised app requires a consensus algorithm that interprets proof of value in the cryptographic system. fundamentally, this empowers value to the cryptographic token and build a consensus protocol that users agree upon to generate valuable cryptographic tokens.

Just like any new technological concept or programming language, there are different coding options and platforms that developers can take advantage of, while thinking of developing dApps.

dApps are based on backend code in a P2P network when compared to conventional apps. This is a major difference as a regular applications' backend runs on a centralised server. When it comes to the frontend, it can be programmed in any programming language. Using an application programming interface (API), frontend calls the backend in decentralised applications and also frontend can also be hosted on a decentralised storage system such as IPFS (2014) and Storj.

4 Mathematical analysis

4.1 EVM and gas

At a high level, the EVM is the virtual environment in which smart contracts are executed on the blockchain. Each node in the Ethereum network runs the Ethereum blockchain, and all the nodes collectively form the EVM. Within the EVM, smart contracts are

executed. In other words, a transaction on the Ethereum network initiates a smart contract, executed within the EVM.

Gas is a unit of measurement in Ethereum blockchain that measures the work required to run smart contracts within the EVM. The more energy required to run an operation, the more gas is required. Gas price is measured in 'Gwei'. One Gwei is 1 billion Wei, and a Wei is the smallest unit of ether, where 1^{018} Wei represents 1 Ether. Gas limit is the maximum amount of gas one is willing to spend on a particular transaction. With every transaction, a sender sets a gas limit and gas price. The product of gas price and gas limit gives the maximum amount of Wei that the sender pays for executing a transaction.

Figure 1 The usage of gas in the transaction of ethereum blockchain

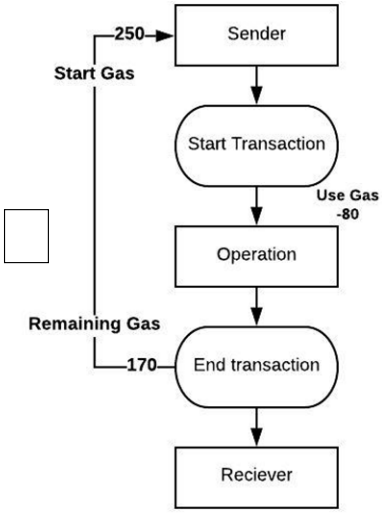
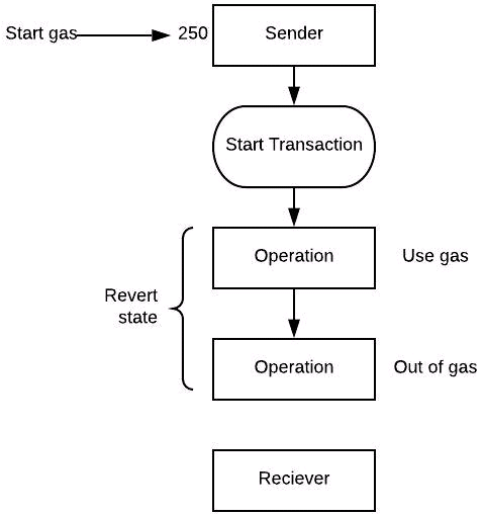


Figure 2 Reversion process of the transaction in case of low gas amount



The maximum gas the sender is willing to spend money on is the gas limit. Figure 1 depicts a scenario where if sender have enough Ether in their account balance to cover this maximum, then the transaction is executed otherwise, the sender is refunded for any unused gas at the end of the transaction which will be exchanged at the original rate.

In the case where the sender does not provide the gas to execute the transaction, the transaction runs out of gas which is considered invalid. This is shown by the figure where, the transaction processing aborts and any state changes that occurred are reversed, such that it comes back at the state of Ethereum before the transaction (Figure 2).

4.2 Transaction execution

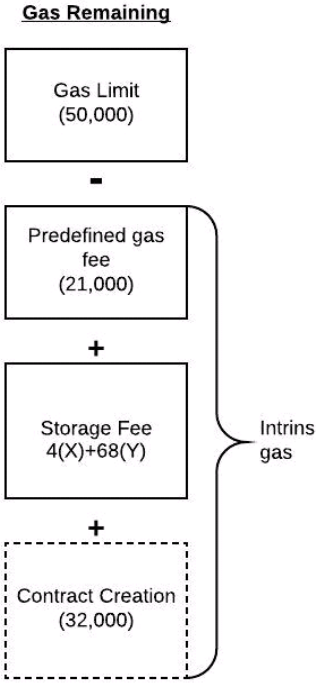
In every transaction, the gas limit must be equal to or greater than the intrinsic gas used by the transaction. The intrinsic gas includes:

1 a previously defined cost of 21,000 gas for executing the transaction

2 a gas fee for data sent to the blockchain with the transaction which includes four gas for every byte of data, and 68 gas for every non-zero byte of data or code

3 an additional 32,000 gas, if the transaction is a contract-creating transaction.

Figure 3 Calculation of remaining gas amount



Every sender must pay an amount in ether called upfront cost. The calculation for the upfront gas cost is given by the transaction's gas limit multiplied by the transaction's gas price. The upfront cost is added to the total value being transferred from the sender to recipient.

Figure 4 Calculation of intrinsic gas

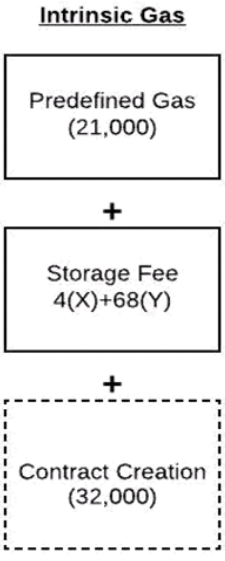
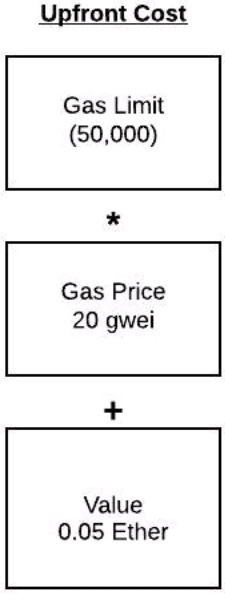


Figure 5 Calculation of upfront gas amount



If the transaction meets all of the requirements then the transaction is proceeded to the next step where deduction of the upfront cost from the sender's balance, and increase the nonce of the sender's account by 1 to account for the current transaction is made. At this point, the remaining gas is calculated which is the total gas limit for the transaction minus the intrinsic gas used.

Figure 6 Home page of the application (see online version for colours)

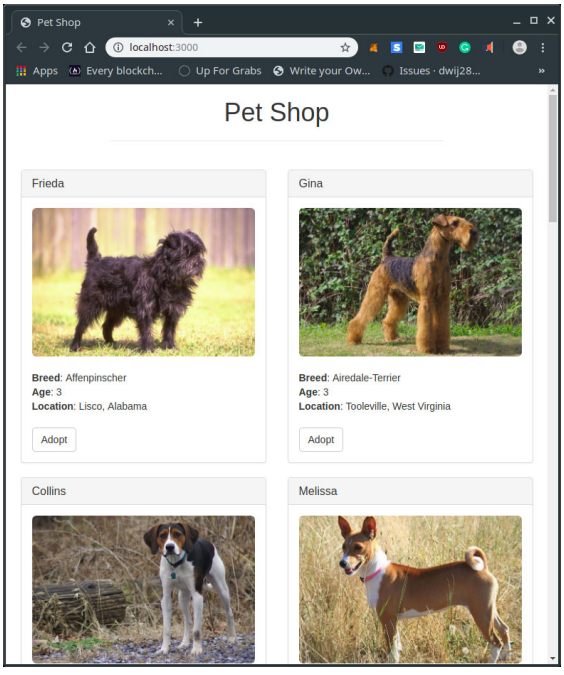
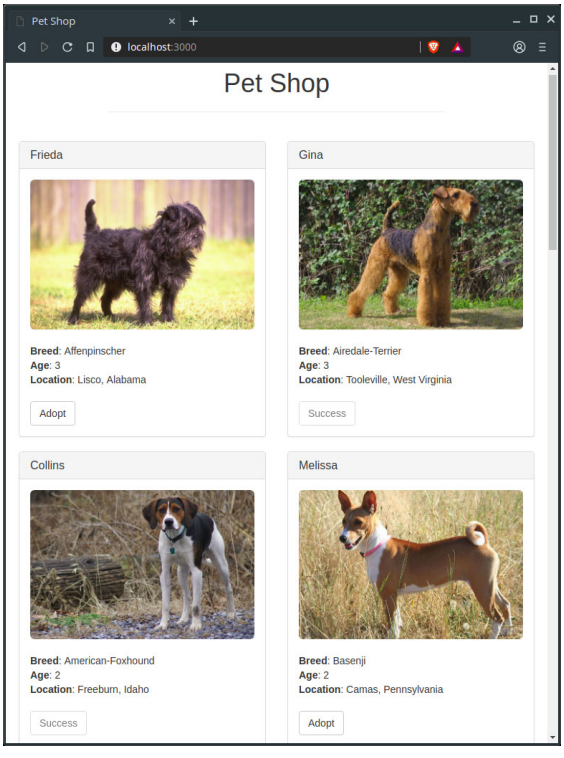


Figure 7 Successful Adoption of pet from the website (see online version for colours)



5 Result analysis

The user who wish to adopt a pet must possess a metatmask account, for transaction of money. Then the users choose the pet to adopt from the website and it checks for sufficient amount of ethers and then the transaction process takes place. During the transaction process the ethers are securely sent from the user account to the destination account. The transaction data is been secured in a block. The block contains block-id, nonce, data and previous hash value which decides the hash value. Gas limit and gas price contains the ethers deducted towards transaction. In data part details of the transaction are stored. Then it contains the previous hash value which contains the hash value of the previous block where it has been linked to form a chain of blocks which avoids corruption of data. Then by including all these values a hash value is created for that block. Like this the transaction block is added to the network. Thus, the transaction is securely done and an attacker cannot spoof things as he requires more than half of computational power to change the data which is impossible. The technology assures the security to data.

Figure 6 depicts the process in detail and its process.

Figure 6 depicts the user interface of the project. When the user visits the website, it shows the pictures of dogs so that they select the pets and adopt accordingly.

Figure 7 depicts the payment through Metamask account.

When user selects the pet to adopt it opens the user's metamask account to make the payment.

Figure 8 Adoption complete process (see online version for colours)

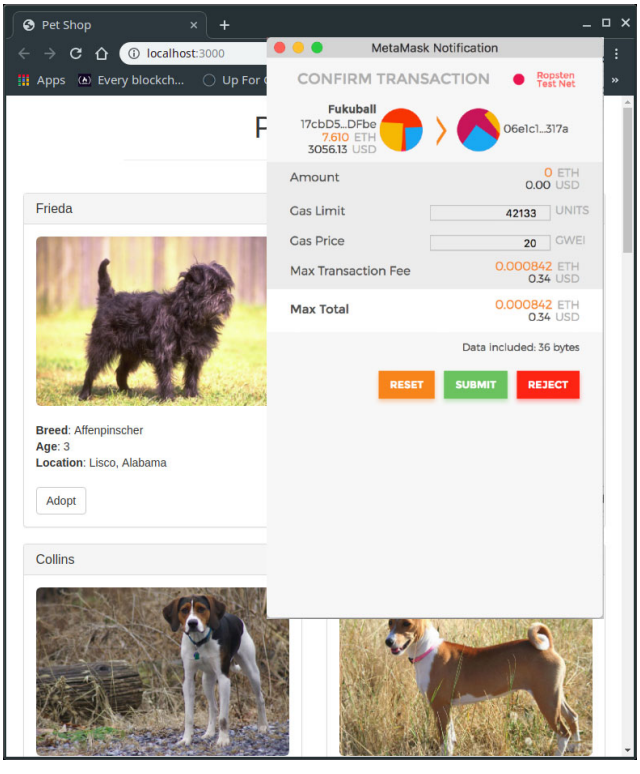


Figure 9 The amount of gas spent on each contact function (see online version for colours)

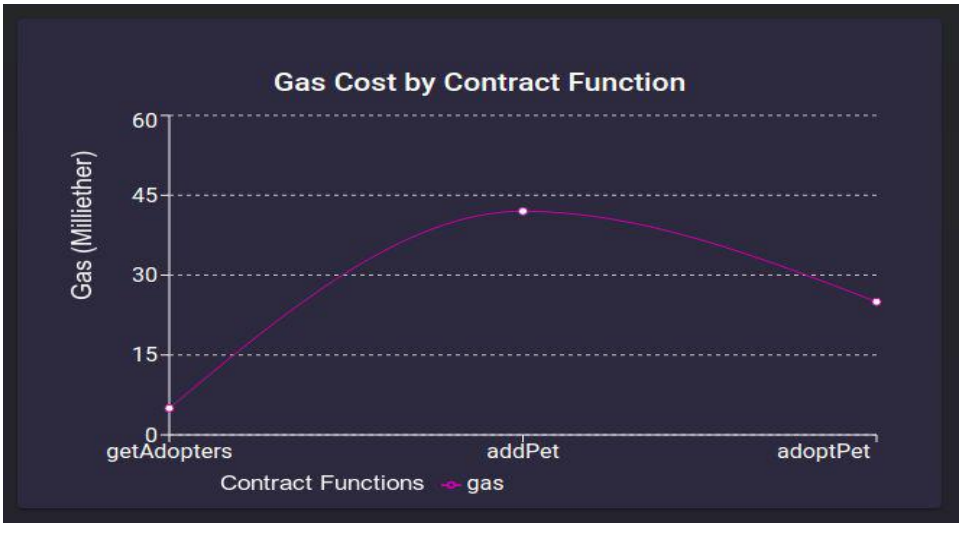


Figure 8 shows the transaction completed and shows that the pet has been adopted by the user and the transaction details are stored in the blockchain. After the transaction is completed the hash value is returned to the user, using that they can check the transaction status. Thus. the pet is adopted and the transaction is done securely..

Figure 9 depicts the gas cost by the particular function in the contract.

Figure 10 Bar graph of time vs. contract functions (see online version for colours)

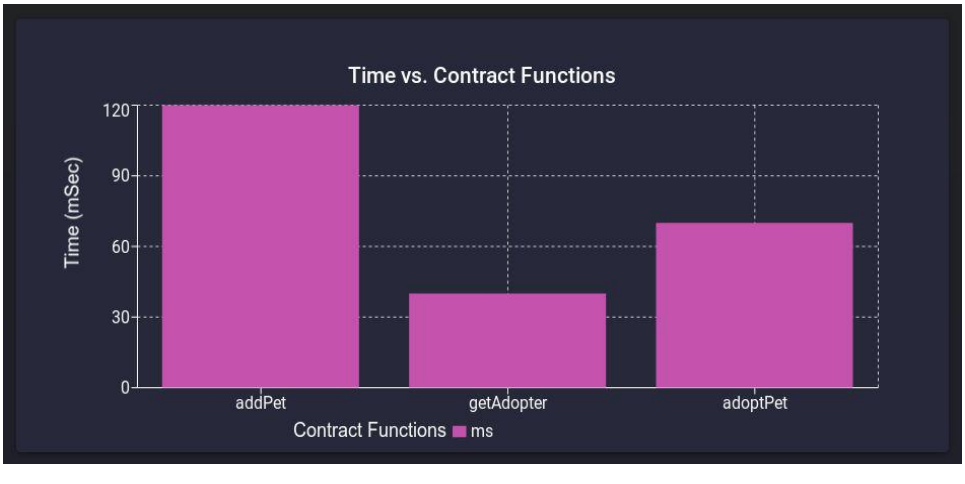
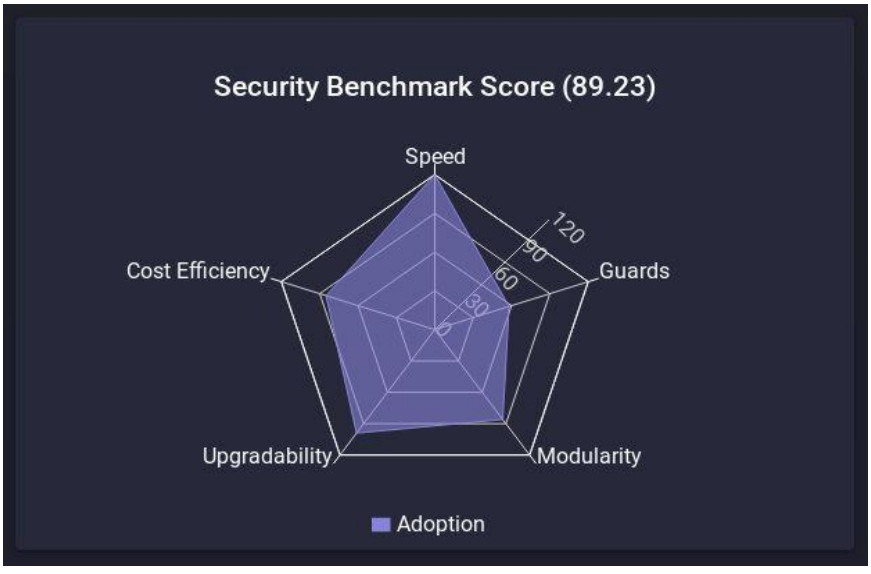


Figure 10 plots a bar graph of time vs. contract functions to show the latency of the called function.

Figure 11 exhibits the total performance of the contract according to the parameters on test blockchain.

Figure 11 Total performance of the contract on test blockchain (see online version for colours)



Blockchain is in its early phase where experiments are performed on existing systems by developers working on reducing the cost and making user activities faster. Their support is limited in terms of computing power and number of nodes within the network are small. The current situation of solutions are usually designed to address where solutions are made by decentralised system. Coin offerings made by blockchain technology implemented using smart contract can deliver high proposition value to the solution over decentralised network where each and every node will have equal importance and control over the decisions made by the system. In future, real power is empowered by smart contract where advanced technologies will enable transactions in faster rate.

After Satoshi Nakamoto published his paper about *Bitcoin: A Peer-to-Peer Electronic Cash System* in October 2008 and released it in January 2009, sign of disrupting financial and banking sectors was clear. With effective solution but limiting technology, it seemed to unlikely have drawbacks to succeed and implement in full fledge. Excluding financial sectors, healthcare, supply chain and government look forward to implement game-changing results. Companies which are acting as middle man to conduct business can be eliminated using this technology. Thus, they are looking forward to utilise blockchain technology to remove central authority over the network. It enables to achieve transformative change but will take time to solve existing challenges with user scalability and complexity in transaction.

6 Conclusions

In a client-server architecture, users experience single point of failure and even it is prone to attackers to provide better solution the use of distributed network improves the efficiency of the system and allows provides more security to the system. Our work yield fruitful results due to the highlight of the blockchain technology which eliminates the drawbacks of the existing centralised system, it provides significant remarks making the

system efficient compared to the existing one. The advanced way of adopting pets and secured money transactions are the main scope of this paper thus increasing the security, flexibility and ease of use of the technology. In client server architecture, there is a chance of single point of failure and even it is more prone to attackers. Thus, distributed network improves the efficiency of the system and provides more security to it.

The results and future scope indicates the detailed work done on pet adoption project and shows the expansion to the researched work, opening new doors of exploration of the domain and to excavate more informative things on the topic. The algorithms, case diagrams, graphs yield better results which enhances the user interaction with the system and pet animals can be adopted securely, where an animal lover takes care of pet animals by adopting them.

References

Buterin, V. (2013) *A Next Generation Smart Contract & Decentralized Application Platform*, Ethereum White Paper.

Chang, J., Gao, B., Xiao, H., Sun, J. and Yang, Z. (2018) *sCompile: Critical Path Identification and Analysis for Smart Contracts*, White paper, arXiv preprintarXiv:1808.00624.

Chen, W., Zheng, Z., Cui, J., Ngai, E., Zheng, P. and Zhou, Y. (2018) 'Detecting Ponzi schemes on Ethereum: towards healthier blockchain technology', *Proceedings of the 2018 World Wide Web Conference on WorldWide Web. International World Wide Web Conferences Steering Committee*, pp.1409–1418.

Dai, P., Mahi, N., Earls, J. and Norta, A. (2017) *Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform*, IEEE.

Dinh, T.T.A., Liu, R. and Zhang, M. (2017) 'Untangling blockchain: a data processing view of blockchain systems', *IEEE Transactions on Knowledge and Data Engineering*, Vol. 30, No. 7, IEEE.

Ehmke, C., Wessling, F. and Friedrich, C.M. (2018) 'Proof-of-property – a lightweight and scalable blockchain protocol', *2018 ACM/IEEE 1st International Workshop on Emerging Trends in Software Engineering for Blockchain*.

Eyal, I., Gencer, A.E., Sirer, E.G. and Vanrenesse, R. (2016) 'Bitcoin-ng: a scalable blockchain protocol', *NSDI (2016)*.

Koç, A.K., Yavuz, E., Çabuk, U.C. and DalkÕlÕç, G. (2018) *Towards Secure E-Voting Using Ethereum Blockchain*, IEEE.

Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E. and Andford, B. (2019) 'Omniledger: a secure, scale-out,decentralized ledger via sharding', *2018 IEEE Symposium onSecurity and Privacy (SP)*, IEEE.

Liu, B., Yu, X.L., Chen, S., Xu, X. and Zhu, L. (2017) 'Blockchain based data integrity service framework for IoT data', in *Web Ser-vices (ICWS), 2017 IEEE International Conference on*, IEEE, pp.468–475.

Nakamoto, S. (2009) *Bitcoin: A Peer-to-Peer Electronic Cash System*, 24 May.

Poon, J. and Buterin, V. (2018) *Plasma: Scalable Autonomous SmartContracts* [online] http://plasma.io/plasma.pdf.

Sambra, A., Guy, A. and Capadisli, S. (2016) 'Building decentralized applications for the social web', *WWW 2016 Companion*, 11–15 April, Montréal, Québec, Canada, ACM 978-1-4503-4144-8/16/04, http://dx.doi.org/10.1145/2872518.2891060.

Wichtlhuber, M., Heise, P., Scheurich, B. and Hausheer, D. (2013) 'Reciprocity with virtual nodes: supporting mobile peers in peer-to-peer content distribution', *9th CNSM*.

Wright, C. and Serguieva, A. (2017) 'Sustainable blockchain-enabled services: smart contracts', *2017 IEEE International Conference on Big Data (BIGDATA)*.