International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

Bit-Contracts: Smart Contracts for Cars

Ashish J. Roy[1], Alay Parekh[2], Priti B. Negi[3], Dr. Vinayak D. Shinde[4]

[1,2,3]Department of Computer Engineering, Shree L. R. Tiwari College of Engineering, Maharashtra, India
[4]Head of Department, Department of Computer Engineering, Shree L. R. Tiwari College of Engineering, Maharashtra, India

---

Abstract - *Security and Legitimacy are two most vital factors on which a trade is conducted. Usually a third party is involved who acts as a mediator to verify trade between two parties. As a result, the confidentiality and integrity of trade is compromised. Moreover, these transactions have valuable information of the two parties that are stored on traditional database systems which could be jeopardised.*

We propose an efficient solution for providing a smart contract between the functionality of a car buying and selling system that allows individuals to sell or buy their personal, underused cars in a completely decentralized manner; annulling the necessity of an intermediary. Our answer, named Bit-Contracts, leverages smart contracts and uses them to carry out secure and personal car booking and payments.

Key Words: **Blockchain, Cryptocurrency, Smart Contracts, Ethereum, Cryptocurrency Exchange, Ether, Distributed System, Security, Ledger**

1. INTRODUCTION

Blockchain is a digitized, decentralized, public ledger of all crypto currency transactions [1] [2] [3]. Perpetually growing as 'completed' blocks (the most up-to-date transactions) are recorded and side to that in written account order; it permits market participants to stay track of digital currency transactions while not central recordkeeping. Every node (a laptop connected to the network) gets a replica of the block chain, which is downloaded automatically.

Originally developed as the accounting method for the virtual currency Bitcoin, blockchains – that use what is referred to as distributed ledger technology (DLT) [4], are appearing in a variety of commercial applications today. Although it is possible to digitize code and insert practically any document into the blockchain, currently the technology is primarily used to verify transactions, within digital currencies. Doing so creates a permanent record that cannot be changed; moreover, the record's legitimacy can be verified by the whole community using the blockchain rather than a single centralized authority. The project 'Bit-Contracts' has been developed for World User. The project is mainly focused on selling and buying vehicles based service on the website, this website helps to maintain the users account and its various details.

The main advantage of using this website is Bit-Contracts merely track and store orders and deliveries, with providing features as transparency, traceability and auditability. In this domain, so as to keep up with trust and dependability along the whole supply chain, it is essential for the database to be tamper-proof, while the best case would be if each actor issuing transactions could do that without relying on any centralized third-party intermediary. The Project Coding relies on several tools, which are used to develop this website and are so well connected that the project resembles the computerization of the Web services operation of the firm.

The database design and coding techniques have been highly enhanced and optimized. This makes the website an overall user friendly and easy for naive users. The website is surprisingly simple: just load it up, and it starts saving all details saved from user details. Any device that has access to the internet should be able to run the website with the help of a web browser.

2. SMART CONTRACTS IN ETHEREUM

Ethereum is a cryptocurrency which has the second largest market capitalization [5]. Aiming at realizing a "world computer", Ethereum allows users to program smart contracts with a Turing complete language and guarantees the correct execution of these contracts and the integrity of the system with its underlying blockchain [3].

Smart contracts are special accounts on Ethereum blockchain, which contain code and persistent storage along with an address and balance like normal accounts [6]. They are computerised protocols, which process without relying on any mediators, satisfy contractual conditions and minimize attacks by adversaries. As in any other computer program, the code of smart contracts also manipulates variables, and it can be invoked by sending a transaction to its address along with the required payment for its execution and parameters.

CryptoMiners are entities who perform computational work to embed transactions into the blockchain, and are compensated by transaction fees in ether, the native currency of Ethereum, from the transaction initiators [7]. The transaction fee is calculated as the total amount of gas consumed by the transaction execution, multiplied by the gasPrice, while the gas-ether exchange rate is specified in the transaction. Gas is calculated by accumulating the

consumption of all instructions of the execution. Each instruction has predefined gas consumption. To prevent denial of service attacks, each transaction also specifies a startGas. A transaction execution that exceeds that startGas cannot be carried out; however, the transaction fee still goes to the miner.

3. SYSTEM MODEL

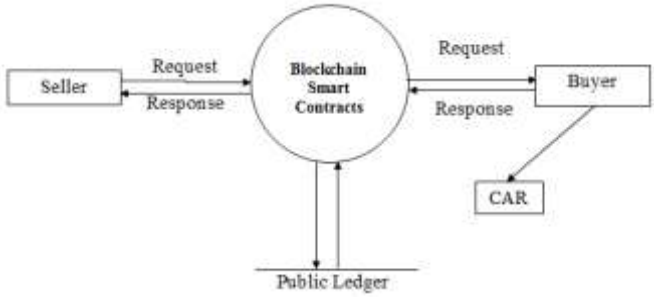


Figure 1: System Model of Bit-Contracts.

As illustrated in Figure 1, our system model consists of following entities:

- Seller: An individual with the intent to sell his/her car.
- Buyer: An individual in need of a car.
- Car: A car that is available for trade. Car's access provision could be handled by any robust access provision protocols like SePCAR [8].
- Public Ledger: A record where all transaction details have been stored that maintains participant's identities in secure and anonymous form with their respective cryptocurrency balances.
- Smart Contract: This smart contract is accountable for receiving a booking request, ensuring that acceptable deposits are created by the buyer, handling cancellation requests, dealing with fraudulent activities, and a smooth procedure in general.

4. THREAT MODEL AND ASSUMPTIONS

The following threat model is used in Bit-Contracts. There is no trust between the seller and the buyer to carry out all transactions honestly. The integrity and proper execution of the smart contract is guaranteed by the underlying public ledger, in our case the Ethereum blockchain. Due to the blockchain's public nature, any private information embedded in the blockchain is considered leaked [9].

For our system to work, we also make the following assumptions. The buyer has agreed upon the initial booking details that are listed on the website by the seller. We also assume that the owner and the consumer have a public/private-key pair along with their digital certificates. Lastly, the communication channels are used by the seller and the buyer are private and authentic.

5. BIT-CONTRACTS

This section provides an overview of how Bit-Contracts handle a car trading scenario.

5.1 System Flow

Figure 2 illustrates the system flow of Bit-Contracts.

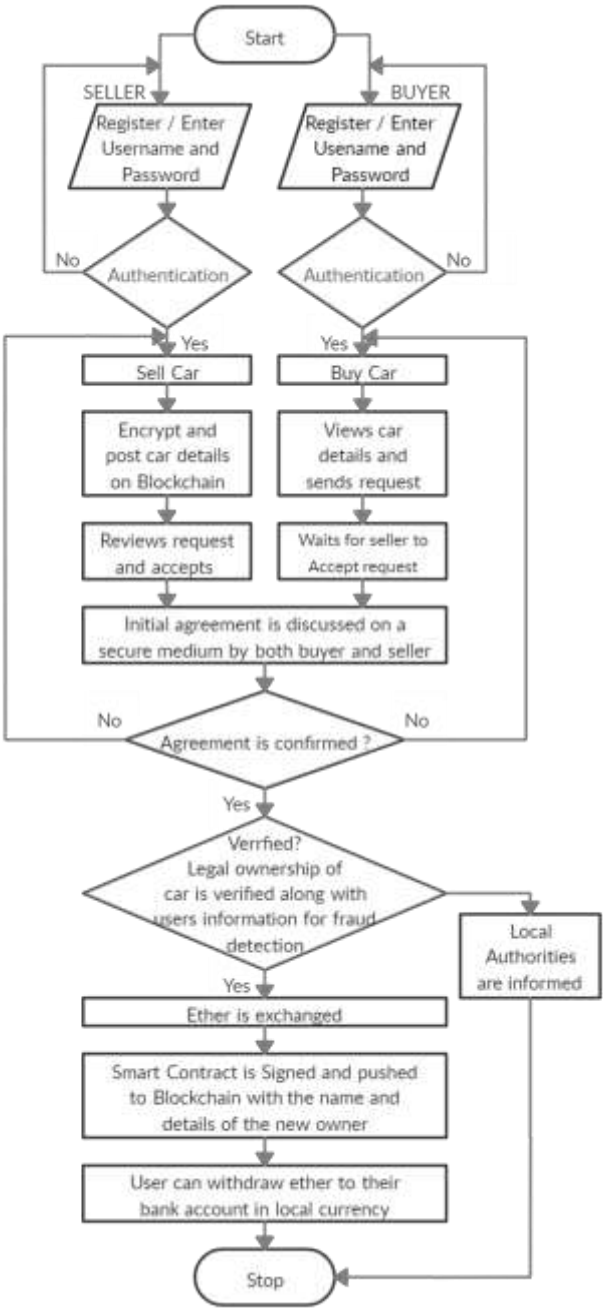
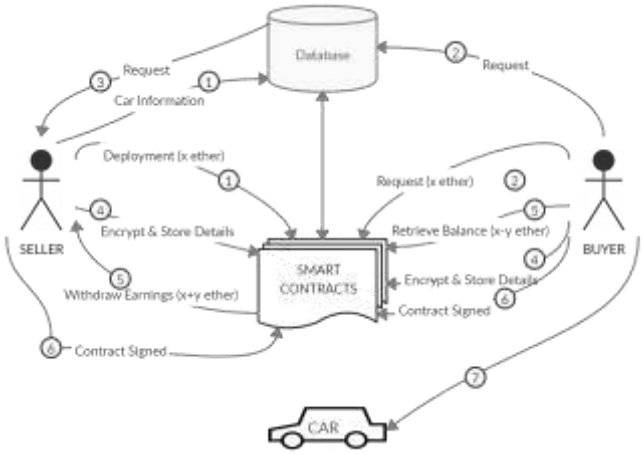


Figure 2: System Flow

5.2 Bit-Contracts in Detail

Here is a brief overview of how the system works.

Bit-contracts enable the seller (having an initial currency of x ether) to first feed the information about the car that the seller wishes to sell, in the database. Simultaneously, it also deploys the information into the smart contracts from where the buyer can collect all the necessary details about the car. The buyer (having an initial currency of x ether) retrieves the information about the car from the smart contact and thereby, requests to buy the car of choice to the seller via the database. The seller, on receiving and accepting the request, encrypts and stores his/her confidential credit details, required to complete the transaction between the parties, into the smart contract. The buyer, on the approval of the request, also, enters his/her confidential credit details into the smart contract, thus facilitating the transaction. The buyer then transfers y ether (the price of the car) to the seller, retrieving a balance of x-y ether. The seller, on the other hand, withdraws a balance of x+y ether. The successful transaction leads to the signing of the contract between the parties involved and the buyer receives the ownership of the car.



6. EVALUATION

In this section, we analyze our design and provide a description of how Bit-Contracts fulfills the functional, security and privacy requirements. We also provide the real-world deployment cost of Bit-Contracts on the Ethereum blockchain.

6.1 Functionality Analysis

Bit-Contracts uses the Ethereum blockchain to implement the booking and payment functionalities for car trade platforms. All transactions related to trade of a car are immutable when published on the blockchain. Once a transaction is made using Bit-Contracts, the Seller or the Buyer cannot refute the ownership of it. Moreover, no outsider knows the identities of the Buyer and Seller, and all the sensitive information in booking details is encrypted before being stored on-chain. Even though the system is extremely secure, any possible fraudulent behavior is penalised with a penalty of losing the deposit made within the smart contract.

6.2 Security and Privacy Analysis

The seller's post of selling the car is first encrypted and signed before publishing the details in the blockchain. Bit-Contracts verifies the owner's signature on the booking details before giving access to the buyer to verify if the seller also agrees with the conditions set for the car, thus providing authenticity of booking details. Car access provision protocols such as SePCAR [8] use the encrypted booking details to generate the access token. Bit-Contracts verifies the origin of encrypted details in order to make sure that no one but the owner has signed them. This is achieved by comparing the address of the signer to the address of the owner. This is how we Ensure non-repudiation of access tokens. Smart contracts are auditable by nature, and in case of an incident where the buyer or the seller is involved, the Bit-Contracts is audited to unveil non-public data concerning the ownership guaranteeing the necessity of forensic evidence provision. Bit-Contracts ensure the confidentiality of booking details by enabling only the buyer and the seller to have access to the sensitive information stored in booking details. These details are discussed offline using a secure channel (see assumptions in Section 5) and only stored in the smart contract when encrypted. Bit-Contracts treats the encrypted booking details as the access token and stores them in its internal storage. No one except the consumer and the owner can decipher an access token thus guaranteeing confidentiality of the access token. Anonymity of both the buyer and seller is provided by design in Bit-Contracts. On the blockchain, by using a 20-byte address, the consumer can choose to be anonymous to interact with the contract and not publicise any personal details, while the identity of the car is encrypted alongside the opposite private information by the owner before storing it on-chain.

7. COST OF TRANSACTION AND DEPLOYMENT

Table 1: Cost of Deployment

Deployment Cost in Gas	Deployment Cost in INR
5,36,467	110.06

Table 2: Cost of Transaction

Transaction	Cost in Gas	Cost in INR
Store Encrypted details in Smart Contracts	64,458	13.22
Request for the Car	28,685	5.88
Cancellation	43,752	8.98
Triggering the distribution of earnings	30,874	6.33
Withdraw Money from Ether wallet	25,970	5.33

*These values are an approximate estimation based on the conversion rate of 1 ether = 10,456.52 INR [10] and may vary depending on the exchange rate.

7.1 Gas

Gas is a unit that measures the amount of computational effort that it will take to execute certain operations. Every single operation that takes part in Ethereum, be it a simple transaction, or a smart contract, or even an ICO takes some amount of gas [11] [2]. Gas is what is used to calculate the amount of fees that need to be paid to the network in order to execute an operation. Miners get paid an amount in Ether which is equivalent to the total amount of gas it took them to execute a complete operation.

7.2 Deployment Cost

All transactions in Ethereum cost 21000 gas as a base. Which means that if we are just transferring funds and not signing with a contract, your transaction takes 21000 gas. If you are signing with a contract, your transaction takes 21000 gas plus any gas associated with running the contract.

On combining the following parameters, the main cost of deploying the smart contracts can be calculated [2].

- The costs related to storing the contract code (200 gas per byte).
- Cost of storing additional data on the contract (20,000 gas per 256-bit word).
- 32,000 gas have to be paid to create a new transaction (deployment of a brand new contract) whereas the base cost of each transaction is 21,000 gas.

To calculate the deployment costs of our smart contracts, we have used Remix IDE [12]. The actual deployment cost varies by the size of the smart contract and the total bytes in its storage.

7.3 Transaction Cost

The cost for executing each transaction cost can be calculated as follows [2].

- Minimum cost of each transaction (21,000 gas)
- Cost when 256-bit word is stored on the smart contract (20,000 gas)
- Cost of storing additional data on the contract (5,000 gas)
- Making a decision on transaction having a financial value (9,000 gas)

8. CONCLUSIONS

This paper presented a fully decentralized car booking and payments system known as Bit-Contracts. This system can be incorporated with provision access protocols to provide a secure and private car trading environment without the need of any intermediary. We have shown that Bit-Contracts provides all major functionalities that are required for a car trading platform, and provides security and privacy by design. The sum of the entire cost of deploying and using our system on the Ethereum network is Rs. 27.16 which in comparison is relatively cheaper to the commission fee paid to large organizations. Hence, we conclude that along with being functionally sound, secure and private, Bit-Contracts is also cost effective for its users. As future work we would like to advance our system design and implementation to work with fully encrypted booking details, including renting the car with the price per day of the car, price per extra day and required number of days which are used for calculation of payments. Another potential direction could be to adapt Bit-Contracts so that it supports the use of advanced cryptographic primitives such as zero-knowledge proofs.

REFERENCE

[1] Innovation Hub. (2017, January) Innovation Hub. [Online]. https://maestrolabs.io/blockchain/

[2] Dr. Gavin Wood, Ethereum [Yellow Paper], 2019.

[3] Vitalik Buterin, *Ethereum White Paper - A Next Generation Smart Contract & Decentralized Application Platform*.: Ethereum, 2013.

[4] (2017, August) TechTarget. [Online]. https://searchcio.techtarget.com/definition/distributed-ledger

[5] CoinMarketCap. [Online]. https://coinmarketcap.com/

[6] Leonid Astakhov. (2018, July) Intrachain. [Online]. https://medium.com/intrachain-insights/how-we-revolutionize-accounting-through-smart-contracts-7268c7e87969

[7] Filipe Calvão, "Crypto-miners: Digital labor and the

power," *Economic Anthropology*, vol. 6, no. 1, pp. 123-134, 2019.

[8] Iraklis Symeonidis et al., "SePCAR: A Secure and Privacy-Enhancing Protocol for Car Access Provision," in *Computer Security – ESORICS 2017*. Oslo, Norway: Springer, Cham, August 2017, vol. 10493, pp. 475-493.

[9] Rui Zhang, Rui Xue, and Ling Lui, "Security and Privacy on Blockchain," *ACM Computing Surveys*, vol. 1, no. 1, p. 35, January 2019.

[10] (2020) CoinGecko. [Online]. https://www.coingecko.com/en/coins/ethereum/inr

[11] Ameer Rosic. (2018) Blockgeeks. [Online]. https://blockgeeks.com/guides/ethereum-gas/

[12] Remix-IDE. [Online]. https://remix.ethereum.org/