Blockchain-Based Proof of Delivery of Physical Assets With Single and Multiple Transporters

Sunil Kushawaha[1], Remya Sivan[2]
Student, Atria Institute of Technology, Visvesvaraya Technological University, Bangalore
Assistant Professor, Atria Institute of Technology, Visvesvaraya Technological University, Bangalore

Abstract- *With the widespread of E-commerce, the need of a trusted system to ensure the delivery of traded items is crucial. Current proof of delivery (PoD) systems lacks transparency, traceability, and credibility. These systems are mostly centralized and rely on trusted third parties (TTPs) to complete the delivery between sellers and buyers. TTPs can be costly, a single point of failure, and subject to hacking, privacy evasion, and compromise. The blockchain is an immutable, trusted, and decentralized ledger with logs and events that can be used for transparency, traceability, and tracking. In this paper, we present a solution and a general framework using the popular permission less Ethereum blockchain to create a trusted, decentralized PoD system that ensures accountability, Auditability, and integrity. The solution uses Ethereum smart contracts to prove the delivery of a shipped item between a seller and a buyer irrespective of the number of intermediate transporters needed. In our proposed solution, all participating entities are incentivized to act honestly by using a double deposit collateral. Automated payment in ether is an integral part of a solution to ensure that every entity gets its intended share of ether upon successful delivery. An arbitration mechanism is also incorporated if a dispute arises during the shipping process. In this paper, we show how we implemented, verified, and tested the proper functionality of our PoD solution. We also provide security analysis and give estimates of the cost consumption in ether gas. We made the full code of the Ethereum smart contracts publicly available at Github.*

Keywords- Blockchain, Ethereum, smart contracts, cyber security, security analysis, decentralized management.

I. INTRODUCTION

Online shopping has become the most convenient way for most people to shop and buy goods these days. Online shop-ping offers consumers the ability to enormously save time,compare prices, check reviews, similar products, or current trends. E-commerce shopping is getting more favored with time especially with the widespread of smart phones and the ease of accessibility to the Internet . According to the UPS, the percentage of smart phone online purchasers has increased to 77% compared to 55% in 2015 [2]. Consequently, in order to meet the increase in demand, delivery services are now offered by vendors to empower the shopper and elevate their experience. Therefore, proof of delivery of a traded physical items and products is immensely needed to facilitate the shipment in a way that is trusted, transparent, and cost-efficient, especially if the the seller, buyer, and trans-porters are located globally in different countries and can not be trusted. Proof of delivery ensures that the shipped item has reached its entitled destination, with the ability of providing evidence to all involved parties of the state of shipment as it moves from the seller, intermediate transporters, and buyer. Current Proof of Delivery (PoD) systems lack transparency, traceability and credibility. For instance, a large number of PoD services depend on signed papers and documents as a way of authentication and hence, proving the delivery to the recipient. Those papers are typically carried along with the transporter. However, there are other PoD systems which rely on hand-held electronic devices for the authentication procedure. Hence, the recipient would provide an electronic signature and a valid identication card (ID).

Then it would depend on the transporter to validate the provided documents and signature and ensure that the item is given to the right intended recipient. Such method relies on the honesty of the transporter and the recipient as the ID can be faked. On the other hand, online retailers may not always have their own shipping services. Some companies would rely on a trusted third party for managing the delivery. For example, Amazon depends on different courier services for their national and regional delivery services. FedEx, UPS and DHL are some of the companies that Amazon relies on for its regional shipments .Furthermore, current systems are mostly centralized, relying on trusted third parties (TTPs) to complete the delivery between a seller and a buyer. Such systems are hard to manage and are costly as they involve TTPs. Not only this, but TTPs can be a single point of failure, and are subject to hacking, privacy evasion and compromise. Thus, making them unreliable and no trustworthy. As a result, there is an immense need for a decentralized solution that provides PoD of physical items as well as traceability in a secure, and trusted method without relying on a third party. Blockchain is an immutable, tamper-proof, decentralized distributed ledger with ample security features that make it possible to create the needed PoD solution. Blockchain uses ordered logs and events which are used to achieve traceability and Auditability. In

addition, using Ethereum makes blockchain programmable. Ethereum smart contracts empowered blockchain by allowing the execution of code .A sound PoD solution for traded physical assets, items, products, or goods must fully the following key requirements. Accountability which is the ability to attribute certain actions to a particular actor. Accountability is similar to non-repudiation where the actor cannot deny a committed transaction. Penalty and Incentivization which ensures that the participating entities have the incentives to act honestly; otherwise, a penalty, will be incurred. Auditability where the System provides a mechanism to trace and track back events and actions, in a way that is completely secure and trusted.

Integrity where all transactions, logs and events are time-stamped and tamper-proof. Authentication and Authorization which ensure that certain functions and operations can only be carried out by specific actors. Time bound which ensures that the item reaches its l destination within a specific time frame. Furthermore, another important requirement is Off-chain Arbitration which allows for a judging entity to settle any dispute in case of false claims by any actor. The chosen arbitrator has full access control to assembled funds which can be dispersed by the arbitrator after examining the evidence on the ledger.

II. RELATED WORK

In this section, we review and summarize work related to proof of delivery algorithms and techniques that make use of blockchain. We also survey decentralized blockchain-based marketplaces. The authors in proposed a simple scheme based on Ethereum blockchain which involves transporting a product between two parties. The scheme depends on a single key that is given to the transporter by the seller [9]. The transported along with the item and is handed over to the receiver who is the buyer. The buyer then needs to enter the key for verification. The key hash would already be available in the smart contract which acts as an escrow and holds the the buyer's Ether. The Ether would only be placed in the seller's account if the hash of the key entered by the buyer matches the existing hash in the smart contract. A successful verification leads to the transfer of the Ether to the seller . This solution is easy to implement as it is simple and depends on only one key. The method however, depends on trusting the transporter completely that no manipulation of the key would take place before reaching the buyer. It also lacks incentives to keep all parties involved honest, although this approach fails with a malicious act from any participating entity especially the transporter.

A solution that utilizes the blockchain technology to create an online decentralized peer to peer marketplace for trading Ether is called `localEthereum'. LocalEthereum does not depend on the contract to act as an escrow. There technique relies on a trusted third party which is a funded escrow agreed upon by both the seller and the buyer. This method requires trusting the third party and costs more as it requires paying the escrow. Furthermore, the seller places the Ether with the funded escrow and the buyer provides the payment directly to the seller. If the seller confirms the payment, the trade is complete and the seller would release the escrow. However, if a dispute arises, an arbitrator (which is localEthereum) is setup to settle the dispute. Clearly, this solution is costly as it depends on a TTP to act as an escrow, also it does not give the buyer and the seller, the ability to choose their trusted arbitrator in the case of any dispute. It also does not show ways of incentivizing the participating entities and the transporter is not involved in any on the chain logs.

All of these existing blockchain decentralized approaches have clear limitations that need improvement to have a more efficient and complete system that includes a PoD solution.

Firstly, in there is no incentive to any of the participating entities to act honest. The seller, buyer and transporter are all trusted completely. Secondly and depend on a trusted TTP or arbitrator to act as an escrow and hold all the funds from the beginning of the selling process till its end. Having a TTP that holds the funds can be a single centralized point of failure and is also costly. Furthermore and do not have a mechanism to resolve VOLUME 6, 2018 46783 H. R. Hasan, K. Salah: Blockchain-Based PoD of Physical Assets disputes if any occur. Hence, there will be a lost to the seller, buyer or both for any act of dishonesty. Additionally, all of the above solutions with the exception of the rest one [9] are decentralized markets that do not provide decentralized PoD solutions. References keep the transporter off chain and do not involve the transporter in any incentives or logs that take place on the chain. Hence, this makes tracing and tracking more complex and does not utilize the blockchain to prove the delivery of the goods. In our solution, we create a decentralized PoD solution that not only involves arbitration in the case of disputes and incentivizes all the participating parties to act honest without the use of a TTP, but also involves single and multiple transporters to be on the chain to ease tracing and tracking as well as the resolving of disputes.

III. PROPOSED BLOCKCHAIN SOLUTION

In this section, we present our Ethereum blockchain solution that utilizes the security features of the technology to

create a solution for PoD between a seller and a buyer involving a single or multiple transporters. The seller and buyer could be located a few miles apart or in different countries. Our solution can be extended to as many transporters (or courier services) as required and works in an adequate, reliable and secure way similar to working with only one transporter. Our solution incentivizes all the parties to act honest by ensuring a collateral is deposited by each participating entity. Also unlike other solutions, the transporters are part of the on chain system and play a role in the PoD solution proposed. This increases trust and security and helps in resolving disputes accurately.

A. SYSTEM OVERVIEW

The proposed blockchain solution focuses on the proof of delivery of traded physical assets between two parties. Figure 1 shows the main participating entities of the system, the seller, buyer, courier service(s), arbitrator and the smart contract attestation authority (SCAA). Each of the entities has an Ethereum address and interacts with the smart contracts created throughout the process based on permissions.

As the item gets handed over between two entities a chain of contracts is created based on the number of courier services.

However, at least two contracts are required between a seller and a buyer. Moreover, the terms and conditions of the agreement between the seller, buyer and courier service(s) should be signed and agreed upon before starting the transaction.

Therefore, the Interplanetary File System (IPFS) hash of the terms and conditions agreement is part of the contracts created. If all entities agree, the transaction starts and the agreed upon collateral is withdrawn from the main entities i.e. the seller, buyer and the transporter. The roles of the participants can be summarized as follows:

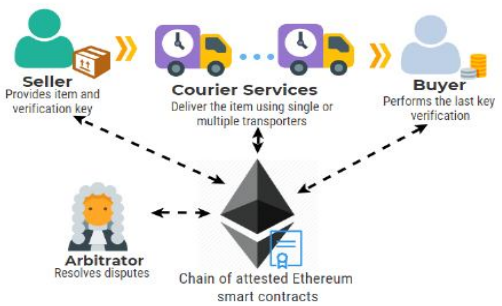


FIGURE 1. The different participating entities and their interaction with the attested smart contracts in the chain.

Seller: The seller has the item to be packaged for transfer to the interested buyer. The seller creates the first contract in the chain. Therefore, the seller is the owner of the first contract created.

Buyer: The buyer would like to spend Ether and buy the item from the seller.

Courier Service(s): Multiple couriers are available to deliver the item from the seller to the buyer if needed based on the geo-location of the seller and buyer. The transporter creates the next contract in the chain.

Arbitrator: The arbitrator is a trusted entity by the seller, courier services and buyer. Its main task is to ensure that the rights of each participating entity are preserved in the case of dispute. The blockchain-solution is completely arbitrator independent during normal transactions. The arbitrator involvement is minimal, and is not involved in every transaction under normal behavior. Furthermore, the arbitrator has no ability to reverse, alter or fake the order and actions of the buyer sellers, or transporters. Any Ether that was deposited to the contract(s) gets transferred to the arbitrator only if the transaction fails and will be then redistributed based on the results of the off-chain arbitration.

Smart Contract Attestation Authority (SCAA):

SCAA attests each contract in the chain to ensure that the code satisfies the agreed upon terms and conditions. If a contract is attested by the SCAA, the contract address would be part of the SCAAs contract and the SCAAs address would be included in the contract. Therefore the attested contract and the SCAAs contract are pointing to each other.

B. SYSTEM DESIGN

In order to deliver the item between he seller and the buyer and to create a solution that adapts to the number of courier services required, three types of contracts are designed. The contracts are created based on the need, and together they make a chain of contracts. Each contract points to the next contract. Therefore, every parent contract has the address of its child contract and every child has the address of its parent contract. In addition, all contracts have the address of the first main contract that started the chain. The main contract has an additional address as well, which is the address of the last contract in the chain. The chain should have at least two contracts. Therefore, this indicates that if only one transporter is needed, two contracts will be created. However, if more than one transporters are needed, then at least 3 contracts are created. It also always starts with a contract of

the type Proof of Delivery (PoD) and ends with a contract of the type Buyer Transporter (BT).Therefore, PoD is the main contract and BT is the end of chain contract. In the middle, if the number of transporters is greater than one then contracts of the type Courier Service (CS) are created as needed.

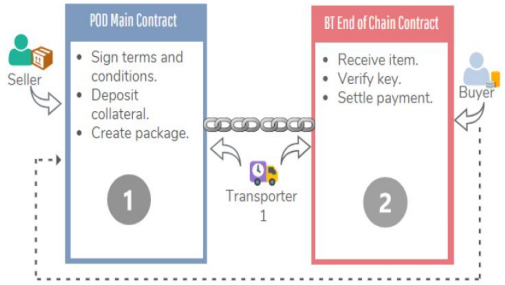


FIGURE 2. A chain of two contracts showing the interaction among actors involving a single transporter.

Figure 2 shows the chain of contracts when there is one transporter only. Therefore, the chain is made of only two contracts, the PoD main contract and the BT end of chain contract. Figure 2 also illustrates the entities that interact with each contract. The seller interacts with the PoD contract only, while the transporter and the buyer are part of both the contracts. Moreover, all of them deposit their collateral in the PoD contract. On the other hand, Figure 3 illustrates a chain of three transporters. Hence, there are two other contracts of type Courier Service between the PoD and the BT contracts. The number of Courier Service contracts required is always less than the number of transporters by 1. Figure 3 also shows the entities participating in each contract across the chain. In the PoD contract, the seller, buyer and first transporter sign the terms and conditions and deposit the agreed upon collateral. Later, the seller would create the package and physically hand it over to the transporter along with a key. The transporter would then create the next CS contract and Transporter 2 agrees to the terms and conditions and deposits a collateral which is held by the CS contract. Therefore, every contract acts as an escrow to the Ether deposited to it. Transporter 2 would then receive the packaged item and would notify everyone that Transporter 1 has arrived. This is an important step that will allow Transporter to then confirm that it has reached and that the key is now with Transporter 2. Transporter 2 then enters the key which is hashed and compared to the key hash already available in the contract. If the verification is successful, the next CS contract is created by Transporter 2 and the chain goes on until the destination address is the address of the buyer. When the destination is the same as the buyers address, a BT contractis created, and the final key verification is done.

IV. IMPLEMENTATION DETAILS

The contracts are created and tested using the Remix IDE which provides the necessary tools for testing and debugging.

Hence, making it easier to modify the code as needed while programming. This section focuses on the implementation algorithms used in the smart contracts. The language used for writing the smart contracts is Solidity. Three types of contracts are created as mentioned in the Design section which are the PoD main contract, CS contracts that depend on the number of transporters and the BT end of chain contract. One of the essentials aspects in the implementation is that each contract across the chain has the contract addresses of both the parent and the child contract. This allows the transfer of funds to the intended parties during the automated payment settlement and dispute handling. Moreover, every time the item is handed over in the chain, the receiver would first acknowledge the arrival of the transporter, then the transporter is allowed to confirm the arrival and provide the key verification.

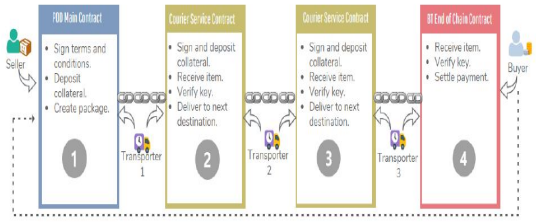
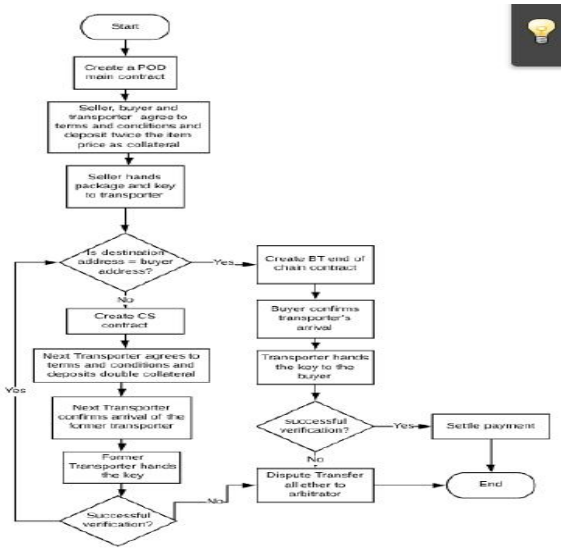


FIGURE 3. A chain of four contracts showing the interaction among actors involving multiple transporters.

This kind of ``handshake" is of great significance as it helps in keeping both parties in need for each other, thus act honestly. Figure 4 illustrates a flowchart that presents the complete logic behind the chain of contracts created using the code.1 The flowchart Shows the full process cycle, commencing with the PoD main contract and ending with the BT end of chain contract. The rest of this section discusses the details of the important

Algorithms used in the code.



IV.CONCLUSION AND FUTURE WORK

In this paper we have presented a blockchain-based solution for the Proof of Delivery (PoD) of traded physical assets. Our solution utilizes the features of the Ethereum blockchain to automate payment and provides tamper-proof logs and events for trusted tractability and transparency. The implemented solution works for multiple transporters as well as single transporter, with a penalty and Incentivization mechanism to force all participants to behave honestly. The solution also eliminates the need of a trusted third party and utilizes the smart contracts as an escrow to automatically settle payments, even under dispute, and give each participants its agreed upon share once the item is successfully delivered to the buyer.

Our decentralized PoD solution uses a chain of contracts, with no cyclic dependencies, to satisfy the need of delivering among multiple transporters. We tested key functionalities, and demonstrated the correct behavior and outcomes con- sidering multiple test case scenarios. We demonstrated and discussed that our solution meets the requirements for a sound PoD system. Moreover, we analyzed the security of our solution and concluded that the solution is resilient to known security attacks and does satisfy cyber security features and objectives. Our cost analysis reveals that the overall system cost is minimal, and increases marginally in the range of $0.1 - $0.2 with the increase in the number of transporters who can be involved in global shipment. The cost of both transactions is proportional to the current value of the gasprice used. However, the expected cost difference between a successful and unsuccessful transaction is expected to be minor. This demonstrates that our solution is cost efficient and can be adopted as a generic solution for the sales and trades of physical assets locally and globally. As for future work, we are currently working on a solution for PoD of the sale of digital assets (such as as those of online books, documents, photos, movies, music, etc.), to ensure decentralized, trusted and secure delivery and automated payment for all types of traded assets whether they are physical or digital.

REFERENCES

[1] Consumers are Now Doing Most of Their Shopping Online. Accessed: Jun. 13, 2018. [Online]. Available: http://fortune.com/2016/06/08/online shopping-increases

[2] UPS Study: Purchases From Marketplaces Nearly Universal Retail now Global as E-Commerce Shoppers Cross Borders. Accessed: Jun. 13, 2018. [Online].Available:https://www.comscore.com/Insights/PressReleases/2018/4/UPS- tudy-Purchases-From-Marketplaces-Nearly-Universal-Retail-/Now-Global-As-E- ommerce-Shoppers-Cross-Borders

[3] About Shipping Carrier Contacts. Accessed: Jun. 13, 2018. [Online]. Available: ttps://www.amazon.com/gp/help/customer/display.html/ref= hp_ss_qs_v3_rt_ci?ie=UTF8&nodeId=201117350

[4] H. R. Hasan and K. Salah, ``Blockchain-based solution for proof of delivery of physical assets," in Proc. Int. Conf. Blockchain, Seattle, WA, USA, 2018, pp. 139_152.

[5] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, ``A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," IEEE Access, vol. 5, pp. 17465_17477, 2017.

[6] K. Biswas and V. Muthukkumarasamy, ``Securing smart cities using blockchain technology," in Proc. IEEE 18th Int. Conf. High Perform. Comput. Commun.; IEEE 14th Int. Conf. Smart City; IEEE 2nd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS), Dec. 2016, pp. 1392_1393.

[7] S. Singh and N. Singh, ``Blockchain: Future of _nancial and cyber secu- rity," in Proc. 2nd Int. Conf. Contemp. Comput. Inform. (IC3I), Dec. 2016, pp. 463_467.

[8] K. Christidis and M. Devetsikiotis, ``Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292_2303, 2016.

[9] Two Party Contracts. Accessed: Jun. 13, 2018. [Online]. Available: https://dappsforbeginners.wordpress.com/tutorials/two-party-contracts/

[10] How Our Escrow Smart Contract Works. Accessed: Jun. 14, 2018. [Online]. Available: tps://blog.localethereum.com/how-our- scrow- smart-contract-works/

[11] Truly Decentralized, Peer-to-Peer Ecommerce Features. Accessed: Jun. 14, 2018. [Online]. Available: https://www.openbazaar.org/features/

[12] Soma the Social Market Place. Accessed: Jun. 14, 2018. [Online]. Avail-able: https://soma.co/documents/
[13] Syscoin 3.0: A Peer-to-Peer Electronic Cash System Built for Business Applications. Accessed: Jun. 14, 2018. [Online]. Available: https://syscoin.org/Syscoin_3.0_Whitepaper___Condensed.pdf
[14] Double Deposit Escrow_Bitbay. Accessed: Jun. 14, 2018. [Online]. Avail- able: https://bitbay.market/double-deposit-escrow/
[15] Eth Gas Station. Accessed: Jun. 14, 2018. [Online]. Available: https://ethgasstation.info/
[16] M. A. Khan and K. Salah, ``Iot security: Review, blockchain solutions, and open challenges," Future Gener. Comput. Syst., vol. 82, pp. 395_411, May 2018. [Online]. Available: http