A Decentralised Reputation Management System for Internet of Things Data Marketplace

Subhasis Thakur
National University of Ireland, Galway
Galway, Ireland
email: subhasis.thakur@nuigalway.ie

John Breslin
john.breslin@nuigalway.ie
Galway, Ireland
email: john.breslin@nuigalway.ie

***Abstract*—A correct reputation management system can differentiate between low-quality and high-quality data providers in an Internet of Things (IoT) data marketplace. There are challenges in designing an unbiased and secure reputation management system that can not be manipulated by wrong feedbacks or wrong aggregation of feedbacks. In this paper, we develop a decentralised reputation management system for the IoT data marketplace that prevents biased selection and aggregation of reputation feedback. The proposed reputation management system uses blockchain offline channels, which makes the solution secure, unbiased, scalable, and least costly. We prove the security and correctness of the proposed reputation management system and present its experimental evaluation using simulation of data marketplace and blockchains.**

***Index Terms*—IoT, Data marketplace; Reputation management; Bitcoin; Lightning Network; Blockchain Offline channels.**

I. Introduction

In an Internet of Things (IoT) data marketplace there are three entities (1) data providers, (2) data consumers, and (3) data brokers. The data brokers act as match-makers between a data provider and a data consumer. The quality of data in a data marketplace is a big concern. A correct reputation management system can identify bad data providers. However, malicious behaviour of data consumers and data brokers may also affect the correctness of a reputation management system. In this paper, we propose a reputation management system that considers all such malicious entities.

Blockchains can be a useful platform to host a decentralised IoT data marketplace. Smart contracts are commonly used to act as a data broker in such a decentralised IoT data marketplace. However, executing data trade operations via smart contracts may be costly. Also, public blockchains such as Ethereum, Bitcoin have a scalability problem. In this paper, we develop a decentralised reputation management system for the IoT data marketplace. We advance the state of the art in reputation management for IoT data marketplace as follows:

- Correlated reputation: We proposed a reputation management system that correlates reputations of data providers, data brokers, and data consumers in such a way that if one entity had given negative feedback about another entity but the reputation of the other entity is eventually increased then the entity who had provided negative feedback loses its reputation.
- Economical feasibility: We used data brokers in this reputation management system. The proposed reputation management system uses a blockchain offline channel network, and these brokers invest to build such a network. In return, they get a financial benefit for executing the reputation management operation.
- Scalability: We execute the proposed reputation management algorithm in blockchain offline channels. It significantly improves the scalability of the solution as the number of transactions needed to be recorded in the blockchain is greatly reduced.
- Low fee: As we execute the reputation management system in blockchain offline channels we reduce the cost of executing the reputation management operations by reducing the number of transactions.
- Competitive reputation score calculation: In the proposed reputation management system, the data brokers act as betting houses where the data buyers place bets on the reputation of the data sellers. The data broker may deploy its own algorithm to find the accurate reputation of the data sellers and announce the betting odds accordingly. The accuracy of the algorithm to predict the reputation of the sellers will determine the revenue for the data brokers. This allows the proposed solution to be extended further by data brokers as they may deploy machine learning-based algorithm to accurately find the reputation of the data sellers.

The paper is organised as follows: in Section 2 we discuss related literature, in Section 3 we describe our solution, in Section 4 we present an analysis of the solution, in Section 5 we present an experimental evaluation of the proposed solution, and we conclude the paper in Section 6.

II. Related Literature

In [1] the authors developed a flexible reputation management model for IoTs, which chooses the best reputation model based on the current environment of the sensor. In [2] the authors developed a reputation model for a peer-to-peer network where one peer provides feedback about service provided by another peer. In [3] the authors developed a decentralised infrastructure for edge computing and IoTs. In [4] the authors proposed group formation among IoTs based on their reputation using blockchains. In [5] the authors developed

 ISBN: 978-1-61208-986-7

proposed a centralised trust management system for IoTs using a centralised trust manager. In [6] the authors developed a trust management system for social IoTs. In [7] the authors developed a social IoT model [8] using trust relations among the sensors. In [9] the authors proposed a trust calculation method where a user may have personal and non-personal trust values. In [10] the authors developed a reputation system for IoT data marketplace using Ethereum. In [11] the authors developed a smart contract-based reputation management method for IoTs. In [12] the authors developed a decentralised IoT data marketplace with blockchain. In [13] the authors developed a smart-contract-based data trade model for IoT. In [14] the authors proposed a payment settlement method in IoT data marketplace using blockchains. In this paper, we used proof of work-based blockchains. Proof of work-based blockchains was proposed in [15]. There are several variations of blockchains in terms of consensus protocols. Offline channels for Bitcoin, i.e., Bitcoin Lightning network was proposed in [16], which allows peers to create and transfer funds among them without frequently updating the blockchain. Similar networks were proposed for Ethereum [17] and credit networks [18].

III. Decentralised Reputation Management

A. Blockchain and IoT networks

An IoT data marketplace will consist of a set of data buyers, data sellers, and a set of betting houses that will manage the reputation of the buyers and the sellers. In this paper, we will use Bitcoin or proof of work-based public blockchain as the blockchain. The buyers in this IoT data marketplace, are the devices or applications seeking IoT data and the sellers are IoT devices providing sensing data. We will denote the buyers as the set $B = (B_1, \ldots, B_n)$ and the sellers as the set $S = (S_1, \ldots, S_m)$. The betting houses will allow the buyers to bet on the reputation of the sellers and they will maintain the betting odds of the sellers. The betting odds of the sellers will denote the reputation of the sellers. The reputation of the buyers will be their investments, i.e., the bets they have placed. All actors of this IoT data marketplace will establish uni-directional channels with each other to place bets on the reputation of the sellers.

B. Unidirectional Offline Channel

Blockchain offline channels [16] uses multi-signature addresses to open an offline channel among peers of the blockchain. This offline channel [16] is bidirectional and potentially infinite, i.e., it can execute the infinite number of transfers between two peers provided they do not close the channel and each of them has sufficient funds. We construct an offline channel for proof of work-based public blockchain with the following properties:

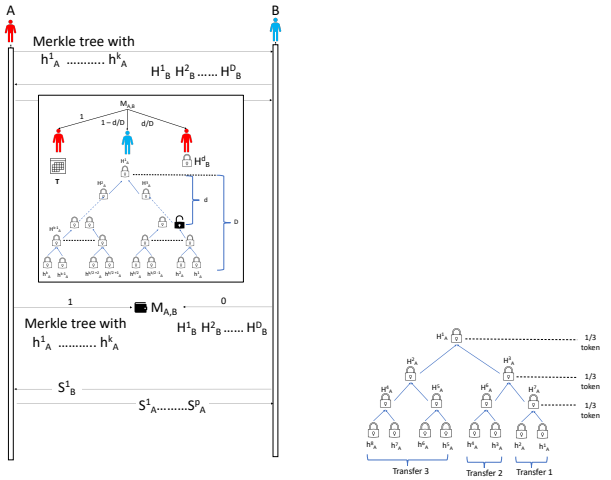
- We construct a uni-directional channel between two peers, i.e., only one peer can send funds to another peer of this channel.
- We construct a uni-directional channel that can be used for a finite number of transfers from a designated peer to another peer.

The procedure for creating the uni-directional channel from A to B (A transfers token to B)is as follows: Let A and B are two peers of the channel network H. $M_{A,B}$ is a multi-signature address between A and B. This is a unidirectional channel from A to B.

1) A creates a set of k (k is a positive even integer) random strings $S_A^1, \ldots, S_A^k$. Using these random strings A creates a set of Hashes $h_A^1 = Hash(S_A^1)$, $h_A^2 = Hash(S_A^2)$, $\ldots$, $h_A^k = Hash(S_A^k)$ where $Hash$ is Hash function (using SHA256). A creates a Merkle tree height $D = Log_2 k$ using these Hashes. In this tree there are k leaf nodes and $k-1$ non-leaf nodes of this Merkle tree. We denote the non-leaf nodes as $H_A^1, \ldots, H^(k-1)_A$.
2) B creates a set of $D-1$ random strings and corresponding Hashes $H_B^1, \ldots, H_B^{D-1}$ such that there is a lexicographic order among these Hashes with $H_B^i \leq H_B^{i+1}$. We will call H_B^x is ranked more than H_B^y if the lexicographic order of H_B^x is more than H_B^y.
3) A will create a Hashed time locked contract as follows:
   a) Let A wants to transfer $1-d/D$ tokens to B where $d \leq D$.
   b) From the multi-signature address $M_{A,B}$ 1 token will be given to A after time T(will be measured as the number of new blocks to be created from the current block in the blockchain) if B does not claim these tokens by producing the key to any non-leaf node H_A^x of the Merkle tree created by A, which is at a distance d from the root of the Merkle tree.
   c) If B produces the key to such a Hash H_A^x at depth d then $(1-d/D)$ tokens will be given to B and remaining d/D tokens will be given to A if it can produce the key to a hash H_B^x in the set $H_B^1, \ldots, H_B^{D-1}$, which is ranked more than d hashes in this set.
4) A will sign this Hashed Time Locked Contract (HTLC) and send it to B.
5) Now A will send a transaction to $M_{A,B}$ of amount $1+\epsilon$ token with the Merkle tree mentioned in the transaction. B will send ϵ tokens to $M_{A,B}$ with $H_B^1, \ldots, H_B^D$ in the transaction data field where ϵ is the transaction processing fee. More than 1 token can be transferred by A. We are using 1 token as an example.
6) Before the next transfer from A to B, A will send the keys to the subset of Hashes $h_A^1, \ldots, h_A^k$, which can generate the Hash H_A^x. Fig. 1b(b) shows the sequence of subsets of non-leaf nodes of the Merkle tree, which A should reveal before each transfer of amount $1/D-1$. It will be possible for A to transfer multiples of $1/D-1$ tokens to B, in such a case multiple subsets of non-leaf Hashes of the Merkle tree will be revealed by A.

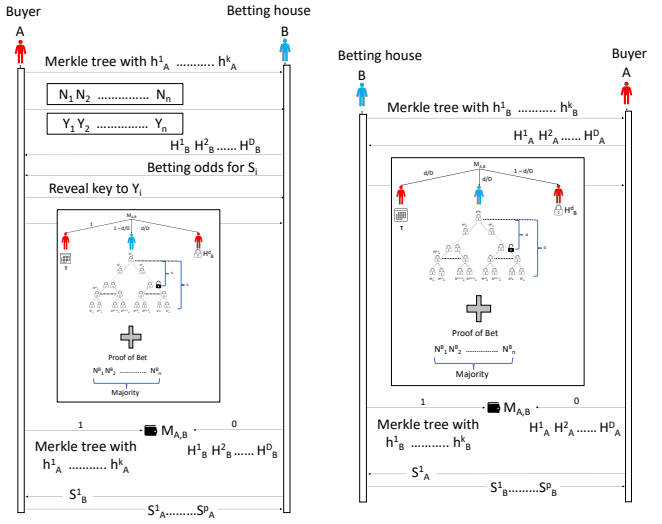
Note that,

- B signs and publishes the HTLC to claim the tokens. It gets the most number of tokens by using the last known



(a) (b)

Fig. 1: (a) Procedure of creating unidirectional offline channels, (b) sequence of keys given by A to transfer fund to B .



(a) (b)

Fig. 3: (a) Channel creation from a buyer to a betting house, (b)Channel creation from a betting house to a buyer.

keys of the Merkle tree leaf nodes. Thus, B will always use the last known keys of this Merkle tree leaf node.

- The channel is secure as A can not transfer to B more than the current balance of the channel as B will know the current balance by finding the non-leaf nodes from the keys supplied by A and depth of such a non-leaf node.
- All peers of the blockchain will know the existence of this channel and Hashes used in creating the channel as transactions to $M_{A,B}$ are visible to all peers.

C. Channel network formation

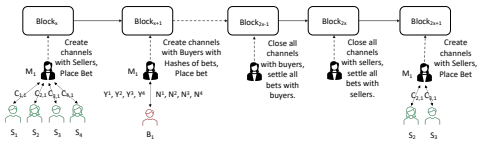


Fig. 2: Sequence of channel network creation in the IoT data marketplace

The channel network among the data buyers, sellers, and brokers (betting houses) will be constructed as follows:

1) The unidirectional channels with the betting houses will have a life span of x new blocks.
2) A betting house at the block $Block_{x-1}$ will settle all bets and close all channels. Channels can be closed by publishing HTLCs to the blockchain.
3) A betting house will create channels with all sellers and these channels will be created in the block $Block_x$. No further channels with the sellers will be created after the creation of the block $Block_x$. A betting house will create two channels 'to' and 'from' each seller.
4) Each betting house can open channels with all sellers.
5) From block $Block_{x+1}$ to $Block_{2x}$ any buyer can establish a channel with a betting house and place a bet on the reputation of a seller.
6) At the block $Block_{2x}$ all channels to and from the betting house will be closed.
7) The betting house can again facilitate betting on the reputation of the sellers by repeating the above steps.

D. Channel between a buyer and a betting house

The procedure to open a channel between a buyer and a betting house is as follows:

1) The procedure is the same as opening a uni-directional channel with these additional steps.
2) The buyer can check the set of sellers who established a channel with the betting house as the sellers should establish channels with the betting house before any buyer can do the same. The buyer can check the previous blockchain head for the existence of such channels.
3) Let there are n sellers who have established channels with the betting house.
4) The buyer will create two sets of n Hashes $(N_1, \ldots, N_n)$ and $(Y_1, \ldots, Y_n)$. If it reveals the key to the Hash N_i then it will mean it is betting against the reputation of seller S_i and if it reveals the key to the Hash Y_i then it will mean it is betting for the reputation of seller S_i.
5) A buyer who has betted against the reputation of a seller will win the bet if the majority of buyers have placed bets against the reputation of the same seller at the same betting house otherwise it will lose.
6) A buyer who has betted for the reputation of a seller will win the bet if the majority of buyers have placed

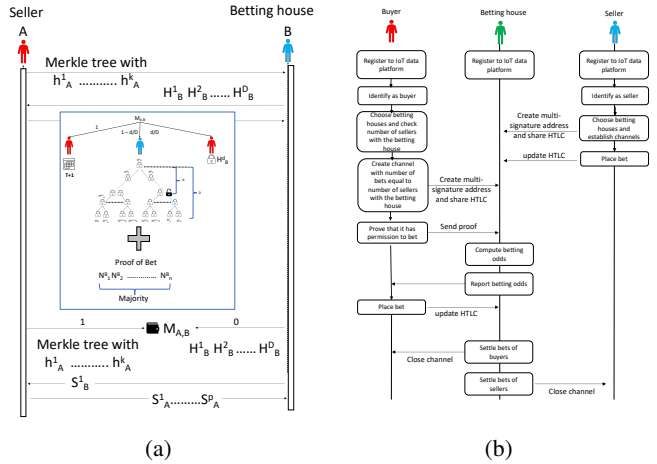
 ISBN: 978-1-61208-986-7

bets for the reputation of the same seller at the same betting house otherwise it will lose.

7) A buyer can place bets of amounts multiples of $1/D-1$ where D is the depth of the Merkle tree from the buyer to the betting house. As shown in Fig. 3(a), the buyer A created the modified unidirectional channel with betting house B.
8) After sharing the set of hashes $\{N_i\}$ and $\{Y_i\}$ with B, A will place the bet for any seller $\{S_i\}$ who has a channel with B.
9) B will inform A about the betting odds of the reputation of a seller S_i. A will reveal its bid by revealing the key to either N_i or Y_i. As shown in Fig. 3(a), buyer A is betting for the reputation of the seller S_i.
10) Next, A will record its bet by creating an HTLC which states the following:
    a) A will get 1 token after time T (equivalent to the creation of x new blocks from the current head of the blockchain) if B does not claim $1 - d/D$ of these tokens by presenting the key to H^c_A of the Merkle tree created by which is at the depth d and by presenting the 'proof of bet' which will show that A lost its bet. In this example, Fig. 3(a) A betted for the reputation of seller S_i. Thus to prove that A has lost its bet, B needs to prove that majority of buyers have betted against the reputation of S_i. The remaining tokens will be given to A if it can reveal the key to H^d_B.
11) After creating the above HTLC A will sign it and share it with B. They will exchange keys to hash H^d_B and $H^1_A, \ldots, H^p_A$ (which can reveal the key to H^c_A in the Merkle tree).
12) This will complete A's bet against seller S_i at betting house B. This bet will be settled after time T (after x new blocks) when the betting house closes its channels with the buyers.

Next, the betting house will open a complementary unidirectional channel from itself to the buyer. The description of this channel is similar to the channel from the buyer to the betting house except, in this case, the betting house (shown in Fig. 3(b)) will send an HTLC to the buyer. If the buyer has betted for the reputation of the seller then the HTLC will be as follows:

1) The buyer will get d/D tokens after time T if the betting house does not claim these tokens by proving that the buyer has lost the bet by presenting keys to a negative feedbacks ($\{N^i_j\}$), which is a majority (in terms of the number of buyers who have channels with this betting house).
2) If the buyer had betted against the reputation of the seller then this HTLC will require proof of bet which should show that majority of buyers have placed bets against the seller's reputation at this betting house.



(a) (b)

Fig. 4: (a) channel creation between a seller and a betting house, (b) sequence of events in the decentralised reputation management systems.

E. Channel between a seller and a betting house

The procedure to create a channel between a seller A and a betting house B (shown in Fig. 4(a)) is as follows: It is the same as the creation of a uni-directional offline channel except in the HTLC from A to B, B can claim the tokens betted by A if it can prove that A have lost the bet. In this case, the seller A can only bet for its own reputation. Hence to prove that A has lost the bet, B needs to prove that majority of buyers have betted against S_i's reputation. It can do so by presenting a set of keys corresponding to a subset of the set $N^1_i, \ldots, N^m_i$, which is a majority, i.e., more size of this subset is more than 50%. The betting house will close the channels with the seller will be closed after all channels among the buyers and the betting house is closed. Similar to the channel from a betting house to a buyer, a complementary channel will be opened from the betting house to the seller. Its description is similar to the channel shown in Fig. 3(b).

F. Computing betting odds

A betting house needs to compute the betting odds about the reputation of a seller. It can deploy various algorithms to do so including machine learning-based algorithms to predict betting odds. A simple betting odd algorithm will use the history of bets on a seller's reputation. At any time, there are x bets for the reputation of the seller and y bets against the reputation of the seller. If $x > y$ then betting odds are $0:1$ (indicating that the betting house considers the seller as a reputable seller) and it will present proof of bet as a collection of bets for the seller. Otherwise betting odd will be $1:0$ indicating that the betting house considers the seller a less reputable seller and it will present proof of bet as a collection of bets against the seller.

G. Decentralised reputation management

In the IoT data marketplace, each actor (buyers or sellers) will identify itself either as a buyer or as a seller as it

participates in the data marketplace. Each actor can open channels with a fixed total value. A seller or a buyer may have channels with multiple betting houses (one channel with one betting house). A seller may place its bet (that it has a good reputation and buyers will not bet against its reputation) by creating channels with the betting houses mentioned in the section III-E. A buyer may place its bet for or against any seller at any betting house with whom both the seller and the buyer have channels. The buyer may choose one such betting house and ask it for the betting odds. If it prefers the betting odds then it may place its bet for or against the seller. The reputation of a seller is its betting odds and the reputation of buyers is the value of its bets. Fig. 2 shows the workflow of the reputation management system, it is as follows:

1) All buyers, sellers, and betting houses will register to the IoT data marketplace by creating an account in the blockchain network used in the IoT data marketplace. All such actors will be identified by their public keys.
2) Betting on the seller's reputation occurs in cycles where each betting cycle is executed for time x (number of new blocks in the blockchain).
3) At the start of each betting cycle, all sellers create or updates their channels with betting houses within a fixed time deadline (marked with the number of new blocks in the blockchain). By creating the channels, the sellers place bets on their reputations.
4) Next, a buyer can create a channel with a betting house to place bets on the reputation of the sellers.
5) A buyer must prove to a betting house that it has permission to place a bet for/against the reputation of a seller. The buyer should prove that it has purchased/used the service of a seller. It can do so by presenting the key to a Hash of a random string created by the seller. The buyer can present the key / Hash pair to a betting house and the betting house can check with the seller about the authenticity of the key/hash pair presented by the buyer.
6) Next, the betting house will reveal its betting odds for the seller and the buyer can place its bet by revealing keys in the set $\{N_i, Y_i\}$ (N_i indicates that it bets against the reputation of the seller i, Y_i indicates that it bets for the reputation of the seller).
7) This process continues for a fixed number of new blocks as buyers place their bets.
8) A betting cycle is closed after x new blocks as the betting houses will reveal the HTLC and proof of bets in the blockchain network to claim tokens from the bets.

IV. Analysis

Theorem 1. *The decentralised reputation management system is secure.*

Proof. There are two ways HTLCs are published as channels are closed after every betting cycle. If a buyer (seller) loses the bet then the betting house will publish the HTLC sent by the buyer (seller) to the betting house with proof of bets. If a buyer (seller) wins a bet then it will publish the HTLC sent by the betting house to the buyer (seller). We have the following security problems:

1) A buyer (seller) may lose the bet and publish the HTLC from the betting house to claim tokens.
2) A betting house may lose the bet and publish the HTLC from the buyer (seller) to claim the tokens.

In the first case, the buyer (seller) will not immediately receive the tokens as it has to wait for time T. By this time the betting will observe the existence of this transaction in the blockchain and claim tokens by presenting correct proof of bets. In the second case, the betting house will not be able to create false proof of bets. This is because:

1) The set of Hashes $(\{N_j^i, Y_j^i\})$ indicating the bets to be placed by the buyers is visible by all peers of the blockchain as it is included in the transaction used to create the channel from the buyer to the betting house. Thus the betting house can not claim correct proof of bet with false pairs of keys and Hashes.
2) A buyer does not reveal its bet for all sellers and the betting house can not know the key to the Hashes $(\{N_j^i, Y_j^i\})$. Thus the betting house can not construct a false but correct proof of bet.

□

Theorem 2. *The decentralised reputation management system is correct if*

$$\frac{k}{k-1} < \frac{1}{(y_1-1)(y_2-1)} \tag{1}$$

where k is the number of buyers, y_1 is the number of rational buyers and y_2 is the number of irrational buyers.

Proof. The reputation management system is correct if reputation (betting odds) of low quality data sellers becomes low, revenue of irrational buyers who provide false feedback (places wrong bets intentionally) becomes low, and revenue of irrational betting houses who provide false betting odds becomes low. Let the demography of this marketplace is as follows:

- Rational betting houses always announce correct betting odds of the sellers. Irrational betting houses announce incorrect betting odds. Initial budget of each betting house is θ_1.
- Rational Buyers place place bets against incorrect data sellers and bets for correct data sellers. Budget of each buyer is θ_2.
- Correct Sellers provide correct data. Budget of each seller is θ_3.

Let there are y_1 rational buyers and y_2 irrational buyers. As mentioned in section 4.3, all sellers arrive before the beginning of each betting cycle and buyers arrive one at a time uniformly at random. Let k buyers arrive in a betting cycle. We assume that each seller has channels with all betting houses and each buyer has channels with all betting houses. The change in funds of a rational betting house is as follows: The probability that a buyer will place a bet at a betting house is $\frac{1}{x}$ where x is

the number of betting houses. The probability that the buyer is rational is $\frac{1}{y_1}$ and irrational is $\frac{1}{y_2}$. The probability that the buyer is placing bets on an incorrect seller is $\frac{1}{z_2}$ and on a correct seller is $\frac{1}{z_1}$.

The rational betting house will lose fund if majority of k buyers ($1 + \frac{k}{2} = k_1$) are are irrational buyers. The probability that there is 1 irrational buyer among a set of k buyers is $\frac{k}{y_2}$. The probability that there are 2 irrational buyers among a set of k buyers is

$$
\begin{aligned}
p_2 = & \overbrace{\frac{1}{y_2}}^{\text{First occurrence}} \times \overbrace{\frac{1}{y_2} + \cdots + \frac{1}{y_2}}^{k-1} \\
& + \frac{1}{y_1} \overbrace{\frac{1}{y_2}}^{\text{First occurrence}} \times \overbrace{\frac{1}{y_2} + \cdots + \frac{1}{y_2}}^{k-2} \\
& + \frac{1}{y_1}^2 \frac{1}{y_2} \times \overbrace{\frac{1}{y_2} + \cdots + \frac{1}{y_2}}^{k-3} \\
& + \ldots \\
& + \frac{1}{y_1}^{k-2} \frac{1}{y_2} \times \overbrace{\frac{1}{y_2} + \cdots + \frac{1}{y_2}}^{1} \\
= & \frac{1}{y_2}^2 [\frac{1}{y_1} \frac{k}{k-1} + \frac{1}{y_1}^2 \frac{k-1}{k-2} + \cdots + \frac{1}{y_1}^{k-2}]
\end{aligned}
$$

The probability that there are 3 irrational buyers among a set of k buyers is

$$
\begin{aligned}
p_3 = & \overbrace{\frac{1}{y_2}}^{\text{First occurrence}} \times \overbrace{p_2}^{\text{occurs 2 times in next k-1}} \\
& + \frac{1}{y_1} \overbrace{\frac{1}{y_2}}^{\text{first occurrence}} \times \overbrace{p_2}^{\text{occurs 2 times in next k-2}} \\
& + \ldots \\
& + \frac{1}{y_1}^{k-2} \frac{1}{y_2} \times \overbrace{p_2}^{\text{occurs 2 times in next 2}}
\end{aligned}
$$

Thus the probability that there are k/2 irrational buyers among a set of k buyers is

$$
\begin{aligned}
p_{k/2} = & \overbrace{\frac{1}{y_2}}^{\text{first occurrence}} \times \overbrace{p_{k/2-1}}^{\text{occurs k/2 -1 times in next k-1}} \\
& + \frac{1}{y_1} \overbrace{\frac{1}{y_2}}^{\text{first occurrence}} \times \overbrace{p_2}^{\text{occurs k/2 -1 times in next k-2}} \\
& + \ldots \\
& + \frac{1}{y_1}^{k/2-1} \overbrace{\frac{1}{y_2}}^{\text{first occurrence}} \times \overbrace{p_{k/2-1}}^{\text{occurs k/2 -1 times in next k/2-1}}
\end{aligned}
$$

Similarly, the probability that there are 2 rational buyers among a set of k buyers is

$$p'_2 = \frac{1}{y_1}^2 [\frac{1}{y_2} \frac{k}{k-1} + \frac{1}{y_2}^2 \frac{k-1}{k-2} + \cdots + \frac{1}{y_2}^{k-2}]$$

The probability that there are k/2 rational buyers among a set of k buyers is

$$
\begin{aligned}
p'_{k/2} = & \overbrace{\frac{1}{y_1}}^{\text{first occurrence}} \times \overbrace{p'_{k/2-1}}^{\text{occurs k/2 -1 times in next k-1}} \\
& + \frac{1}{y_2} \overbrace{\frac{1}{y_1}}^{\text{first occurrence}} \times \overbrace{p'_{k/2-1}}^{\text{occurs k/2 -1 times in next k-2}} \\
& + \ldots \\
& + \frac{1}{y_2}^{k/2-1} \overbrace{\frac{1}{y_1}}^{\text{first occurrence}} \times \overbrace{p'_{k/2-1}}^{\text{occurs k/2 -1 times in next k/2-1}}
\end{aligned}
$$

Following should not hold (we will find the conditions so that it does not hold):

$$
\begin{aligned}
& p_2 > p'_2 \\
& [y_1 \frac{k}{k-1} + \sum (\frac{1}{y_1}^i) + \sum (\frac{1}{y_1}^i \frac{1}{k-i})] \\
& > \\
& [y_2 \frac{k}{k-1} + \sum (\frac{1}{y_2}^i) + \sum (\frac{1}{y_2}^i \frac{1}{k-i})]
\end{aligned}
$$

As $y_1 > y_2$ the above equation is a contradiction if

$$
\begin{aligned}
y_1 \frac{k}{k-1} + \sum (\frac{1}{y_1}^i) & < y_2 \frac{k}{k-1} + \sum (\frac{1}{y_2}^i) \\
\frac{k}{k-1}(y_1 - y_2) & < \frac{y_1 - y_2}{(y_1 - 1)(y_2 - 1)} \\
\frac{k}{k-1} & < \frac{1}{(y_1 - 1)(y_2 - 1)} \qquad (2)
\end{aligned}
$$

If $p'_2 > p_2$ then $p'_3 > p_3$ because $y_1 > y_2$. Following this process we conclude that $p'_{k/2} > p_{k/2}$. As the probability of having a majority of rational buyers in each betting cycle is higher than the opposite, the rational betting houses will lose fewer bets than irrational betting houses. As all actors start with a constant budget irrational betting houses will eventually lose all of their funds. As rational betting houses will persist in this betting system, betting odds for all sellers will be correct. □

We note the following:

- In the proposed reputation management system for data marketplace, betting houses keep the reputation records and the rational betting house will gain revenue from it. This will encourage them to invest and build the reputation management platform by joining the blockchain network.
- As the reputation management operations are executed in the offline channels by exchanging HTLCs, it records

 ISBN: 978-1-61208-986-7

very few transactions in the blockchain. Thus the proposed solution is scalable.

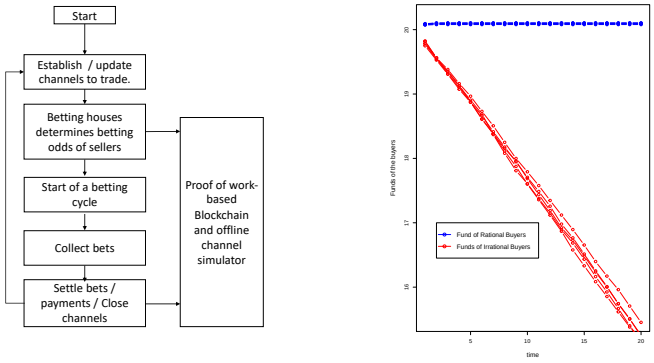
- As very few transactions are recorded in the blockchain the cost of running blockchain operations in terms of blockchain transaction fees is very low.
- Betting houses can develop their own algorithm for predicting betting odds. More precise these algorithms, the more accurate the betting odds. With better algorithms betting houses will have more revenue from bets. This will allow further development of the proposed reputation management solution and its integration with data analytics solutions to predict more accurate betting odds.

V. Evaluation

We evaluate the proposed decentralised reputation management with a simulation of the data marketplace using agent-based modelling of the marketplace and blockchain. We use the blockchain simulator used in [19]. In this evaluation, we use two types of buyers, rational buyers (who bet as per the performance of the data seller) and irrational buyers (who do the opposite of rational buyers). There are two types of data sellers, good data sellers provide correct data and bad data seller sales incorrect data. The buyers arrive (places bet) one at a time and a buyer is chosen uniformly at random. We want to show that, the decentralised reputation management system is correct despite the random arrival of the buyers. We use a set of 10000 buyers with 40% irrational buyers chosen uniformly at random. There are 100 sellers with 40% bad sellers. We used two betting houses one rational and another one irrational. A betting house uses historical betting data to determine the betting odds of a seller. If the majority of bets are against the seller then the betting odd is $0:1$, i.e., if a buyer places a bet for the reputation of the seller and it wins then it will get double the betting amount. Otherwise, the betting house will get double the betting amount. In each bet, a buyer and seller bet the same amount of fund the winner gets all such betted funds. However, it is possible to place different betting odds. As the betting odds are $0:1$ in this example, the reputation of the sellers is either 0 or 1. We use the following model of data marketplace simulation (shown in Fig. 5(a)):

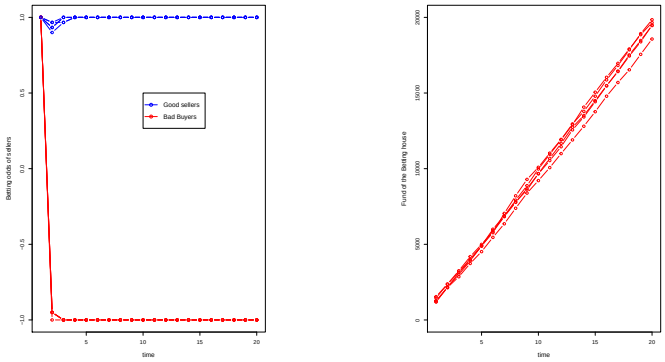
- At the start of each betting cycle channels are established among the actors of the marketplace. We use proof of work-based blockchain and offline channel simulator [19] to simulate such events. The blockchain simulator is built with asynchronous event simulation in Python.
- Next, a betting house determines the current betting odds of each seller and announces it.
- Buyers place their bets by exchanging HTLCs with betting houses.
- At the end of each betting cycle, all bets are settled as each betting house or buyer claims tokens by publishing HTLCs to the blockchain network. This closes or updates their channels.

The results of the simulated execution of the data marketplace are shown in the figures below. As shown in the Fig. 5(b) funds of irrational buyers becomes low as they lose bets on the



(a) (b)

Fig. 5: (a)Data marketplace simulator, (b) Funds of the buyers after 20 rounds of betting on the seller's reputation. It shows that funds of rational buyers remain higher than irrational buyers.



(a) (b)

Fig. 6: (a) Betting odds of the data sellers. It shows that betting odds of good sellers remain higher than bad sellers, (b) Funds of rational betting houses increase.

seller's reputation. Fig. 6(a) shows that the reputation (betting odds) of good sellers remains higher than the bad seller. Fig. 6(b) shows that funds of rational betting houses increase over time.

VI. Conclusion

In this paper, we developed a decentralised reputation management system for IoT data marketplace. The proposed reputation management system is secure and correct as it will prevent biased feedbacks and incorrect aggregation of feedbacks to calculate reputation.

References

[1] G. Dólera Tormo, F. Gómez Mármol, and G. Martínez Pérez, "Dynamic and flexible selection of a reputation mechanism for heterogeneous environments," *Future Generation Computer Systems*, vol. 49, pp. 113–124, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X14001289

 ISBN: 978-1-61208-986-7

[2] A. Selcuk, E. Uzun, and M. Pariente, "A reputation-based trust management system for p2p networks," in *IEEE International Symposium on Cluster Computing and the Grid, 2004. CCGrid 2004.*, 2004, pp. 251–258.

[3] I. Psaras, "Decentralised edge-computing and iot through distributed trust," in *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 505–507. [Online]. Available: https://doi.org/10.1145/3210240.3226062

[4] G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarné, "Using blockchain in a reputation-based model for grouping agents in the internet of things," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1231–1243, 2020.

[5] M. D. Alshehri and F. K. Hussain, "A centralized trust management mechanism for the internet of things (ctm-iot)," in *Advances on Broad-Band Wireless Computing, Communication and Applications*, L. Barolli, F. Xhafa, and J. Conesa, Eds. Cham: Springer International Publishing, 2018, pp. 533–543.

[6] O. Ben Abderrahim, M. H. Elhdhili, and L. Saidane, "Tmcoi-siot: A trust management system based on communities of interest for the social internet of things," in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2017, pp. 747–752.

[7] N. S. Nizamkari, "A graph-based trust-enhanced recommender system for service selection in iot," in *2017 International Conference on Inventive Systems and Control (ICISC)*, 2017, pp. 1–5.

[8] L. Atzori, A. Iera, and G. Morabito, "Siot: Giving a social structure to the internet of things," *IEEE Communications Letters*, vol. 15, no. 11, pp. 1193–1195, 2011.

[9] H. Son, N. Kang, B. Gwak, and D. Lee, "An adaptive iot trust estimation scheme combining interaction history and stereotypical reputation," in *2017 14th IEEE Annual Consumer Communications Networking Conference (CCNC)*, 2017, pp. 349–352.

[10] A. Javaid, M. Zahid, I. Ali, R. J. U. H. Khan, Z. Noshad, and N. Javaid, "Reputation system for iot data monetization using blockchain," in *Advances on Broad-Band Wireless Computing, Communication and Applications*, L. Barolli, P. Hellinckx, and T. Enokido, Eds. Cham: Springer International Publishing, 2020, pp. 173–184.

[11] J.-S. Park, T.-Y. Youn, H.-B. Kim, K. Rhee, and S.-U. Shin, "Smart contract-based review system for an iot data marketplace," *Sensors (Basel, Switzerland)*, vol. 18, 2018.

[12] P. Gupta, S. Kanhere, and R. Jurdak, "A decentralized iot data marketplace," 2019.

[13] S. Bajoudah, C. Dong, and P. Missier, "Toward a decentralized, trustless marketplace for brokered iot data trading using blockchain," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 339–346.

[14] W. Lin, X. Yin, S. Wang, and M. Khosravi, "A blockchain-enabled decentralized settlement model for iot data exchange services," *Wireless Networks*, 2020.

[15] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *www.bitcoin.org*, 2008.

[16] J. Poon and T. Dryja, "The Bitcoin Lightning Network:Scalable Off-Chain Instant Payments." [Online]. Available: https://lightning.network/lightning-network-paper.pdf

[17] "Raiden network," http://raiden.network/, accessed 01/06.2022.

[18] G. Malavolta, P. Moreno-Sanchez, A. Kate, and M. Maffei, "Silentwhispers: Enforcing security and privacy in decentralized credit networks," *IACR Cryptology ePrint Archive*, vol. 2016, p. 1054, 2016.

[19] B. Hayes, S. Thakur, and J. Breslin, "Co-simulation of electricity distribution networks and peer to peer energy trading platforms," *International Journal of Electrical Power & Energy Systems*, vol. 115, p. 105419, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0142061519302972

 ISBN: 978-1-61208-986-7