BitCar: Curated and vetted Evidence Collection Platform

Anton Mitrokhin
University of Maryland, College Park

Khushali Dalal
University of Maryland, College Park

Darshan Mukund Pandit
University of Maryland, College Park

ABSTRACT

Photographic evidence is increasingly used in investigations pertaining to Auto Insurance claims. Owing to the scope for biased self-reporting by the parties involved, a large number of false reports has to be processed, leading to increased costs of Insurance. In this paper, we propose a solution to address this issue by implementing a decentralized and secure crowd-sourced private information marketplace on the Ethereum blockchain.

We suggest a permission-less, decentralized, incentive-based scheme to report, curate and vet pictorial content submitted by the users on the network. Specifically, we develop a novel multistage incentive mechanism which consists of a Token-Curated market in the initial phase and a crowd-sourced Content-Review market in the second phase to provide quality estimates for the submitted data.

To our knowledge, this is a first such mechanism in existence implemented on a blockchain. In addition, our algorithm is able to discourage falsified and biased reviews for pictorial evidence, thus keeping malicious users astray. We identify possible attacks on our system & thoroughly investigate the threat model and mitigation strategies for these attacks. Our scheme exploits the immutability, transparency and cost-effectiveness provided by Ethereum smart contracts, thus yielding the provably-secure, efficient marketplace.

KEYWORDS

Token Curated Registry; Crowdsourcing; Digital Marketplaces

1 INTRODUCTION

The losses incurred by Auto Insurance providers has been on a steady increase since 2012[4], and was reported to have surpassed over $163 Billion USD for the year 2016. Insurance Research Council reports that during 2012, the excess payments rose from $5.6 Billion to $7.7 Billion USD[3] and represented between 13 to 17% of the total payments. This has led to companies to adopt several strategies to tackle such claims[6], and more often the companies are adopting to follow the optimal strategy of systematic underpayment of claims at the margin as a means to deter loss exaggeration[5]. A side effect of this can be observed in increased cost of Coverage, and unhappy experiences with the Claims processing department, leading to dissatisfaction[7, 8].

With smartphone revolution, increasing adoption of dashcams and other inbuilt sensors within the car, there has been a surge in the quality of Evidences submitted by the claimants. However, several concerns and instances of biased reporting have been reported [1]. In addition, the authenticity of evidences has also been a concern. This becomes critical as companies increasingly incorporate on Automated technologies to evaluate claims. Conventional Investigations while expensive, ensure high quality investigations by domain-experts. Under the after-shock of an accident, a normal person may not be able to perform at his/her optimum and thus may miss out on capturing crucial pieces. An alternative to this option might be to Crowdsource the data pertaining to such events.

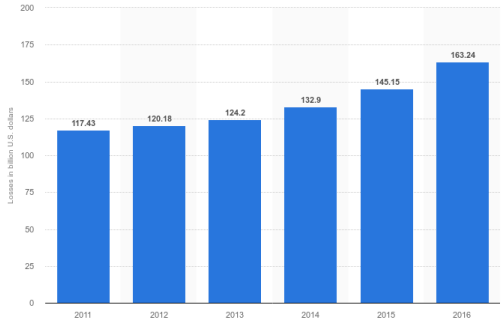


Figure 1: Auto Insurance Claims

First formally recognized by Jeff Howe[2], the phenomena, 'Crowdsourcing' has rightfully gained significant interest and adoption in applications as diverse as raising capital, designing products, to providing services like carpooling amongst; as well as Academic research. Crowdsourcing also constitutes several Computational Architectures, designs and schemes. In some vague fashion, one may even attribute the emergence of consensus amongst Bitcoin miners on transactions as an application of this technique. In it's crudest form, these architectures may have three groups of roles: requester, workers and some co-ordination mechanism. Requester/s submit tasks and provide for the incentives, multiple independent workers compete and submit solutions to these tasks, and the co-ordination mechanism facilitates Information access, incentive distribution and ensure integrity of the solutions.

2 BITCAR OVERVIEW

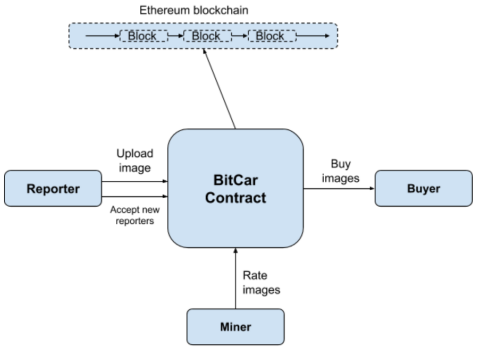
In this section, we provide an overview of the key features of BitCar. We begin by introducing the main components in the BitCar architecture, and then describe the main functions of the system.

2.1 Architecture

As with any insurance industry, all parties involved are likely to act as malicious agents trying to falsely claim payment for themselves. The evidence is usually needed to circumvent such behaviour. BitCar augments the approach to image-based data collection and trading by adding the decentralized Ethereum marketplace (see high level architecture on Figure 2) for information trading. Such system can be used for a transparent and secure evidence collection and, while there is a great number of uses for such a system, we demonstrate its use case in the domain of the car insurance market.

To summarize, BitCar has four main entities:

2.1.1 ***Reporters.*** There are two main tasks of a Reporter, firstly being to upload a pictures(geotagged and time stamped) and



Overview of the entities in BitCar

Figure 2

second to assist in curation of the new evidences pertaining to the accident. For step one, the application first tries to locate any existing topic with a similar <Geotag,Timestamp> pair, and enlists them. The granularity of these identifiers can be varied depending upon the nature of the event. Reporters can at any time can create/start their own topic and submit their evidence in that Topic using <Geotag,Timestamp, Nonce> pair as an identifier. We do not impose any restrictions on Topic creation, nor do we assume the integrity of <Geotag,Timestamp> identifiers. However, the incentive mechanisms which we discuss in the proceeding sections will heavily discourage from such behaviour.

In it's Evidence Bundle, the reporter submit Proof of Storage for censored version of raw data (To prevent revealing sensitive information and data-theft). This raw-data may also be copyright protected. In addition to this, the reporter also submits Proof of Storage for Uncensored, copyright-protected encrypted evidence, encrypted using Requesters <$Priv_{key}$, Pub_{key}> pair.

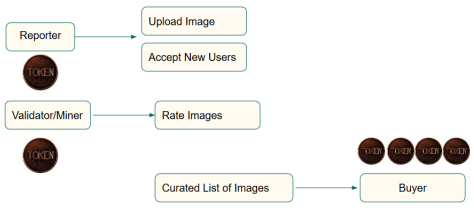
Finally, the bundle also contains two escrows to the topic-list, a fixed-Participation fee and variable Token-purchase amount, depending upon the tokens desired, as a part of the submission bundle to the list. Since these topics are permissionless, at any point all the information, including the raw-censored images are available in the public domain. Upon submission of this Evidence bundle, existing members conduct a Quorom to decide if the evidence-bundle can be accepted. If the Quorom is not formed within a set threshold, the applicaton is accepted by default. Upon acceptance, the both the participation fee and token-purchase amount are held in the smart contract and the Requester is issued Non-Fungible Tokens pertaining to the Topic. We elaborate upon the token issuance in the proceeding section.

2.1.2 ***Miners.*** The second set of entities that can exist in the system are what we call, 'Miners'. Miners participate in the system by evaluating and providing their inputs upon the censored-evidences enlisted in the topic. In context of Bitcar, these miners will provide their ratings on a Likert Scale for each evidence listed. Using Secure Multi-Party Compute Mechanism, the miners reach upon a consensus. The rewards for miners are determined as a function of Stake (#TokensHeld) and their deviation from the thus formulated consensus. In accordance with the permission-less design of our scheme, Anybody can become a miner and participate in the system. The Miner bundle is relatively simplistic, and contains a simple Escrow of a fixed Miner-Participation Fee, and a variable Token Purchase amount. Once registered, the Miner is issued Fungible Tokens corresponding to the Purchase amount submitted. The Miner can then chose to submit a Salted hash of it's Likert Scale rating for one/multiple images. The incentive mechanism will ensure participation of the Miners in the consensus computation mechanism.

2.1.3 ***Buyers.*** The third actor in our system, is the primary consumer of the evidences/data collected. In the context of our application, this would typically be the Insurance companies, however, since the system is permissionless, anybody willing to make the payment, can purchase the data. The buyer bundle typically escrows an amount equivalent to purchasing the entire Fungible Token Market at the prevailing rate, triggering a BUY event. Upon a successful BUY event, typically two events are triggered. First, the Non-Fungible Token holders, ie: Requesters, perform a public reveal of the $Priv_{key}$ for their Uncensored-Encrypted Images. Upon this, the ownership of the Fungible Tokens held by the Non-Fungible Asset Tokens is transferred to the corresponding Requestors. Once a set thershold of Requesters have performed a Public reveal, the Miners enter the Reveal Phase of their Multi-Party Computation and provide their Raw-ratings, and salts for the evidences/data units. Failure to provide these in a set amount of time would simply cause the algorithm to ignore the rating from the Miners, thus imposing a hard-upper bound on time constraint on Consensus resolution.

Once both of these events successfully terminate, the the Buyer is provided with the Raw-Uncensured evidences/data-bundles, and a list of Human-evaluated rating for each of the entry. The Fungible Tokens can also be redeemed for reserve currency by their corresponding holders using their reward function.

2.1.4 ***Token.*** It can be considered as a form of security deposit. Tokens in our scheme are used to pay users for their work. From reporters perspective: maintaining the ledger(voting for new participants) and ranking requires work and the token compensates for that work. Simple analogy, one could think tokens as âĂŸgasâĂŹ for users- which is required at every step of the pipeline. From miners perspective: ranking images is the actual price of the information. Each miner gets paid separately for the amount of work they put in rating images. Simple analogy, the more intense the computational work -higher the chances of solving puzzle.



Sample responsibilities of each entities in BitCar

3 INCENTIVE MECHANICS

The novel contribution of our scheme is the incentive structure that enables our system to behave in two very different mannerism. In particular we employ a pricing curve for the Fungible Tokens based upon a variation of the Logistic Function. As the supply of the Tokens increases, the Price of these tokens increases based upon the value determined by this curve. This phenomena of the variable pricing of the Tokens, based upon supply, is termed as 'Bonding' and the function as 'Bonding Curve'. Our unique implementation of Bonding Curve allows us for the following Behavioural dynamics:

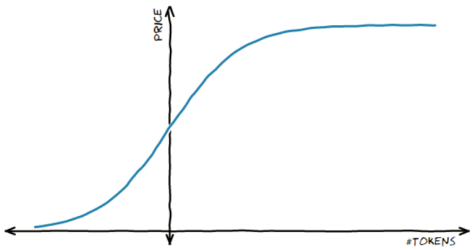


Figure 3: Logistic Bonding Curve

3.1 Token Curated Registry

During the first phase, when the Price increases slowly and then at a rapid phase, this system behaves as 'Token curated Registry(TCR)'. TCR incentives initial entrants into the system by allowing them to enter the system at a relatively cheaper price points. This encourages Data Collection. The Quorom of the members during this phase ensures only quality content is added to the list.

Algorithm 1 BitCar contract event registration

procedure : process event registration
input : reporter paddress , ETH, hImage
Blockchain ← $lookupgeotagginginevent'slist$
if event exists() then
Reporter ← $requesttojoin.$
else
Ledger ← $createnewlist$
endif
end **procedure**

4 BEHAVIOUR AS CROWDSOURCING

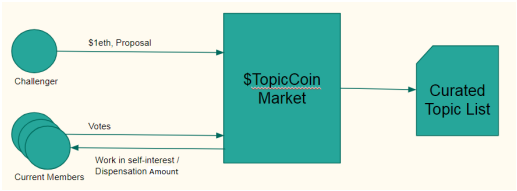
During Second Phase of the system, the period of relatively slower growth in price, the system sheds of the quorom and stops issuing new NFT assets. Miners get active during this phase. A monotonically increasing function ensures that the final BUY event is triggered at a much higher Price point, thus benifiting all the participants in the system, including late entrants.

4.1 Human Miners

As per the saying âĂIJtwo heads are better than oneâĂİ inspired by open and collaborative working handled by the distributed nature of the Internet can challenge traditional interpretations. Our model uses Crowd-voting concept to have a second opinion of the curated list pictures. Though computerâĂŹs nowadays are advanced to do each and every task imaginable, there are certain tasks that produce more reliable output when done by humans. For instance, only a human can really tell âĂIJgoodâĂİ information from âĂIJbadâĂİ. As a form of authorization participants willing to participate in a particular event buys token -votes for the pictures they like -a consensus is created. Miners participate in a Multi-Party lottery by submitting some ETH to purchase token, rates the images and when a buyer wants to buy the curated list of best voted images miners are ranked using a distance measure from the average rating vector aka consensus. The more the hard work the miner would have put into rating good images -the more are the chances to be near consensus and win the lottery. On the other hand, the farther a miner is from the consensus the less they get incentivized and lose the lottery.

4.2 Incentives for Miners

Miners have a privilege to choose the list(registry) they wish to mine. Only the good-looking registry have higher chances of getting mined. The reporter of the image tags a small fee aka mining fee to the image while uploading in the registry. This prevents from losing good images or good images being overlooked. In the end, providing poor results will make miner lose hi money. As the consensus lottery is played by bunch of anonymous people who conclude which images are good by rating and a human who would actually perform the task(mine honestly) will stand near the consensus rather than the one not working(selfish) and voting randomly.



5 THREAT MODEL

In Cryptocurrency, tracing a coins history could be used to connect identities to addresses. The pseudo anonymity nature makes it hard to track down activities in blockchain. This has its own advantage of privacy at the same time is one of the most concerned issue as it widens the scope of attack surface.

5.1 Sybil Entries

There is no hard bound in creating a new account. A user has privileges to create n number of accounts for participating in contract. What prevents the user from overtaking the whole contract? In our model, each image is tied with a token. The number of images a reporter wants to upload that many tokens he/she needs to purchase. As discussed in section(??) the price of token relies on bonding curve. Hence, if a malicious user tries to block other participants and

limits the event to only one user(himself), it will ultimately cost the malicious user to invest more. Bonding curve is one of the strategies used to prevent our application from sybil entries attack.

5.2 Registry Poisoning

Denial of Service(DoS) attack, a well known cyber-attack for interrupting availability of services on world wide web is typically achieved by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. Analogy to this attack in registry poisoning, user tries to flood the targeted event/incident list with non-useful information. This will in a way increase the price of token surreptitiously. In defense to this attack, malicious user has to invest some tokens in the contract and if there is no buyer of this junk pictures at the end, malicious user ultimately loses whatever he/she invested.

5.3 P + Epsilon Attack

Precommitment in crytoeconomics is the underlying principle behind smart contracts. Smart contracts relies on "If this then that" conditional statements. Atomic swap of transactions occur when the conditions are satisfied. The idea behind P + Epsilon attack relies on the assumption that the attacker can credibly commit to something quite crazy. The crazy thing is this: paying out 10.01 BTC to all the people who help him in his attack to steal 10 BTC from everyone, but only if the attack fails. This leads to a weird payoff matrix where the dominant strategy is to help him in the attack. The attack succeeds, and no payoff is made. In our model, all the transactions are taking place in the form of token till the buyer buys the information. Possibility of such strategy in BitCar smart contract is highly impossible. Even a malicious user manages to manipulate honest miners in voting for or against a particular picture, there is no guarantee that the miner voted according to the malicious users instruction. Our model is completely self dependent. Every miner has their own choice and no one can manipulate that individual preference.

6 CONCLUSIONS

We have presented a first-of-kind work on private information trading with an application to the auto insurance concept. The thorough threat model analysis was implemented as well as the proof-of-concept implementation. We demonstrate the feasibility of our economic model in the real world application and its security and anonimity features.

REFERENCES

[1] Car insurance companies offering photo claim options | FOX 61. (????). http://fox61.com/2017/06/09/car-insurance-companies-offering-photo-claim-options/

[2] The Rise of Crowdsourcing | WIRED. (????). https://www.wired.com/2006/06/crowds/

[3] 2015. Insurance Research Council Finds That Fraud and Buildup Add Up to $7.7 Billion in Excess Payments for Auto Injury Claims. (2015). http://www.insurancefraud.org/downloads/InsuranceResearchCouncil02-15.pdf

[4] 2018. Facts + Statistics: Auto insurance III. (2018). https://www.iii.org/fact-statistic/facts-statistics-auto-insurance

[5] Keith J Crocker and Sharon Tennyson. 2002. Insurance fraud and optimal claims settlement strategies. *The Journal of Law and Economics* 45, 2 (2002), 469–507.

[6] Richard A Derrig. 2002. Insurance fraud. *Journal of Risk and Insurance* 69, 3 (2002), 271–287.

[7] Sharon Tennyson. 2008. Moral, Social, and Economic Dimensions of Insurance Claims Fraud. *Social Research* 75, 4 (2008), 1181–1204. http://www.jstor.org/stable/40972112

[8] Stijn Viaene and Guido Dedene. 2004. Insurance Fraud: Issues and Challenges. *The Geneva Papers on Risk and Insurance. Issues and Practice* 29, 2 (2004), 313–333. http://www.jstor.org/stable/41953118