Rewarding device-to-device content dissemination using Proof-of-Prestige

Michał Król, Sergi Reñé, Arnold Cheung, Ioannis Psaras
University College London, United Kingdom

***Abstract*—This demo shows an implementation of a device-to-device data dissemination system for mobile phones. We develop and Android application allowing users to exchange content and collects rewards for transfers using Proof of Prestige scheme deployed on Ethereum blockchain. To interact with the system, mobile devices require to store uniquely their public and private keys reducing the memory footprint. Our implementation inherits blockchain security features and remains resistant to Sybil and collude attacks. We make our application available on Google Play Store for public use.**

I. Introduction

Following the recent success of Bitcoin [1], a plethora of cryptocurrencies have experienced an increase of popularity [2]. There are over 1,900 cryptocurrencies one can invest in with the total market cap exceeding 280B USD[1]. In contrast to resource-wasting Proof-of-Work (PoW) protocols [1] or Proof-of-Stake (PoS) binding users' minting power to the amount of their coins [3], a recent trend sees cryptocurrencies as an incentive method for users to perform useful work and create a shared economy environment.

In the classic setup, useful work can be performed by a *"contributor"* for a *"beneficiary"*. The beneficiary submits a task and a reward to the blockchain that is used to assure payment for service [4]. When the contributor correctly completes the requested task, the payment is unlocked. However, currently, multiple cloud platforms do not expect their users to pay for the services (*i.e.,* Facebook, Youtube). As a result, in order to attract more users, blockchain-based platforms must keep this featue as well. It means involving a third party in the system to whom we refer to as a *"motivator"*. The motivator benefits from increasing the size and popularity of the network and rewards contributors' useful work, while keeping it free for the end-users.

Such a system presents multiple benefits. Beneficiaries do not have to pay for the content, the system remains open for any contributor to join, perform useful work and be paid according to their performance and contribution; the motivator on the other hand benefits from an open platform avoiding costly contracts, and contributor selection process. However, for that to work, the network must be able to automatically verify tasks. While completion of some tasks can be proven to a third party, in many cases this is impossible. For instance, it is not possible to prove that a file has been successfully transferred between any two untrusted nodes. In such cases, the motivator relies only on beneficiary acknowledgments to reward contributors and can be thus susceptible to Sybil attacks. In order to maximize their reward, contributors can create multiple fake identities claiming usefulness of their work. Moreover, even with access restriction techniques or voting power bounded to stake, users can collude and cross-acknowledge their potentially non-existing work.

In this demo, we implement and deploy a rewarded content dissemination system for mobile devices secured by Proof-of-Prestige (PoP) [5]. PoP allows motivators to securely incentivize file transfers with no risk of Sybil or collude attack. Our platform uses data-centric connectivity allowing to verify integrity of fetched data acquired from untrusted, anonymous peers. We adapt PoP to work with constrained mobile devices and deploy it as a smart contract running on top of Ethereum blockchain. The application is available for Android devices and can be downloaded from Google Play Store[2]. Furthermore, we deploy a visualization module allowing users to view statistics and track their prestige in real time.

II. Background

A. Information-centric networking

Information-centric connectivity (ICN) represents a different approach from the current IP host-centric architecture. Instead of naming endpoints, users name data that they want to acquire. It allows efficient content fetching from any device that has the content instead of predefined distant hosts. ICN does not secure the connection, but rather the content itself. Each data chunk must be signed by its producer and encrypted if required by access control. Such an approach allows to download data from untrusted anonymous peers and reliably verify data integrity. In our demo, we use ICN to realize efficient content dissemination between mobile devices.

B. Proof of Prestige

Proof of Prestige (PoP) [5] is a useful-work reward scheme running on top of Proof of Stake blockchains. In PoP, apart from coins, each user has a certain amount of prestige associated with his account. Prestige is a much more volatile than coins and can be considered as a renewable resource. It is slowly generated over time from coins, but only up to a certain threshold called a static value. The static value is defined by the amount of coins each user has. The more coins, the higher the corresponding static value. Prestige directly defines users' mining power and thus the probability of getting rewarded by the system. However, once a user reaches the static value, the automatic prestige generation process stops. To get more prestige, users have to perform useful work. Each worker is rewarded by a prestige transfer by the beneficiary of the

[1] https://www.investing.com/crypto/currencies

[2] https://play.google.com/store/apps/details?id=network.datahop.localsharing

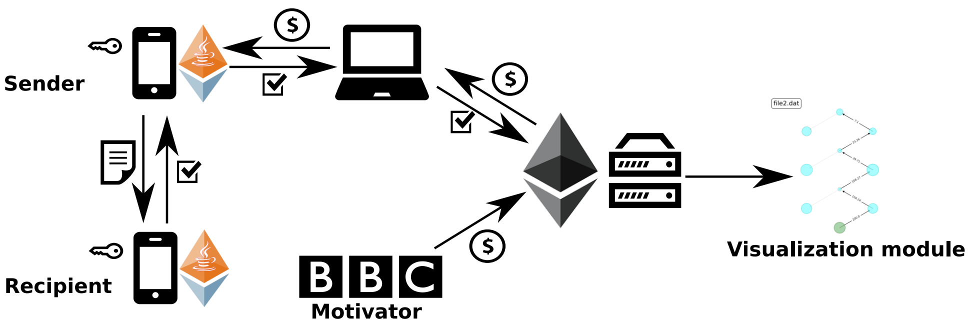

Fig. 1: Demo architecture.

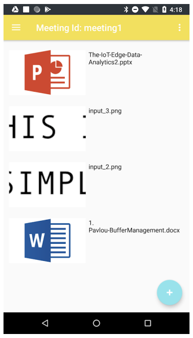
4:18
Meeting Id: meeting1
The-IoT-Edge-Data-Analytics2.pptx
input_3.png
input_2.png
1. Pavlou-BufferManagement.docx

Fig. 2: Main screen of the mobile application.

service. However, the total amount of prestige of the worker and the beneficiary remains constant making PoP resistant against Sybil and collude attacks. The scheme introduces two different types of prestige transfers (simple and progressive minig) allowing its use in various use-cases.

III. Overview

As an intermediary step for future deployment on a native PoS blockchain, we deploy PoP as a smart contract on Ethereum Ropsten testnet. We are thus unable to collect transaction fees and newly minted coins, but our scheme can distribute rewards submitted by motivators (Figure 1).

a) Mobile Application: We develop a device-to-device file sharing application[3] for Android phones(Figure 2) and connect it with PoP. Contributor devices advertise their content using a Bloom filter encoded into Bluetooth Low Energy beacons. When a beneficiary user discovers a file they are interested in, they send a request, and the file is transferred between devices using WiFi direct. Once the beneficiary finishes downloading data, they verify its integrity by checking its digital signature. If the signature is correct, the beneficiary transmits a signed acknowledgment to the contributor. The contributor device collects acknowledgments and can submit them later to a full node.

Due to limited amount of memory, mobile devices are unable to keep blockchain data in their storage. We thus adapt our scheme so that Mobile devices requires to store only the account credentials (public and private key) as well as the contract interface in a form of a lightweight Application Binary Interface (ABI) file. The mobile application uses web3j[4] library for interacting with the contract, credentials generation and signing acknowledgments with the private key.

b) Smart Contract: The smart contract acts as an intermediary between users and PoP server (described below). It enables users to deploy ether into PoP. Each 1000wei translates into 1 PoP coin. The smart contract generate events when a user deploys or withdraws funds or registers a transfers between devices. Furthermore, beneficiaries can use contract methods to register their file transfers by sending signed acknowledgments. If the signature is correct, the contract also generates a corresponding event. Finally, the contract allows motivators to register their rewards for specific file distributions. However, how the rewards ae distributed is decided by the contract owner (in our case PoP server). In such as setup fair reward distribution is not guaranteed by the blockchain, however users cannot loose any coins and can withdraw their funds at any point.

A. PoP Server

a) PoP Server: By default, Ethereum does not allow to automatically invoke functions with new blocks[5]. To reduce the cost of calculating users prestige on-chain, we outsource this operation to an external server. The servers is connected to a full Ethereum node using web3py[6] and listens for events generated by the blockchain such as a new block, new file transfer or money deployed into the smart contract. The server, as the contract owner, performs cyclic (every 1000 blocks) payments proportional to prestige of each user.

Furthermore, the server implements a visualization module displaying graphs and statistic about the scheme. Users can easily verify the current amount of their coins, acquired prestige and registered transfers and their evolution over time.

IV. Conclusion

In our demo, we have successfully showcased a practical example of how to incentivize content dissemination by mobile devices. The rewards are distributed by a smart contract and calculated by an external server to reduce the operational cost. The demo allows participants to download the application and distribute the content and gain prestige and new coins themselves. The mobile devices use only minimum amount of their storage while the whole scheme inherits blockchain security guarantees.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, "Consensus in the age of blockchains," *arXiv preprint arXiv:1711.03936*, 2017.

[3] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Annual International Cryptology Conference*, pp. 357–388, Springer, 2017.

[4] M. Al-Bassam, A. Sonnino, M. Król, and I. Psaras, "Airtnt: Fair exchange payment for outsourced secure enclave computations," *arXiv preprint arXiv:1805.06411*, 2018.

[5] M. Król, A. Sonnino, M. Al-Bassam, A. Tasiopoulos, and I. Psaras, "Proof-of-prestige a useful work reward system for unverifiable tasks," in *Proceedings of the 1st International Conference on Blockchain and Cryptocurrency*, IEEE, 2019.

[3] https://play.google.com/store/apps/details?id=network.datahop.localsharing

[4] https://github.com/web3j/

[5] such functionality is offered by several external services(*i.e.,* https://github.com/ethereum-alarm-clock), but requires paying a fee with every new block

[6] https://github.com/ethereum/web3.py