Poster: LocalCoin: An Ad-hoc Payment Scheme for Areas with High Connectivity

Dimitris Chatzopoulos
HKUST
dcab@cse.ust.hk

Sujit Gujar
IIIT Hyderabad
sujit.gujar@iiit.ac.in

Boi Faltings
EPFL
boi.faltings@epfl.ch

Pan Hui
HKUST
panhui@cse.ust.hk

ABSTRACT

The popularity of digital currencies, especially cryptocurrencies, has been continuously growing since the appearance of Bitcoin. Bitcoin is a peer-to-peer (P2P) cryptocurrency protocol enabling transactions between individuals without the need of a trusted authority. Its network is formed from resources contributed by individuals known as *miners*. Users of Bitcoin currency create transactions that are stored in a specialised data structure called a *block chain*. Bitcoin's security lies in a *proof-of-work* scheme, which requires high computational resources at the miners. These miners have to be synchronised with any update in the network, which produces high data traffic rates. Despite advances in mobile technology, no cryptocurrencies have been proposed for mobile devices. This is largely due to the lower processing capabilities of mobile devices when compared with conventional computers and the poorer Internet connectivity to that of the wired networking. In this work, we propose *LocalCoin*, an alternative cryptocurrency that requires minimal computational resources, produces low data traffic and works with off-the-shelf mobile devices. LocalCoin replaces the *computational* hardness that is at the root of Bitcoin's security with the *social* hardness of ensuring that all witnesses to a transaction are colluders. It is based on opportunistic networking rather than relying on infrastructure and incorporates characteristics of mobile networks such as users' locations and their coverage radius in order to employ an alternative proof-of-work scheme. Localcoin features **(i)** a lightweight proof-of-work scheme and **(ii)** a distributed block chain.

1. LOCALCOIN

Decentralised cryptocurrencies have to deal with three main challenges: **(1) Proof of ownership**- users should be able to prove they have the amount of money they claim to have. **(2) Double spending avoidance** - a defense mechanism against double spending. (Users are not able to spend the same money more than once). **(3) Incentives** - for its stakeholders. Mobile devices are unable to partake as peers in any cryptocurrency, because of their lower processing capabilities compared to conventional computers and their unstable connectivity to the Internet compared to ordinary wire-line access protocols. The problem that we address in this work is whether we can develop a cryptocurrency suitable for mobile ad-hoc networks with high connectivity. We propose *LocalCoin*, a scheme that replaces the *computational* hardness that is at the root of Bitcoin's security with the *social* hardness of ensuring that all witnesses to a transaction are colluders (users assisting the malicious user to double spend). Where computational hardness provides a *weakest-link* security guarantee - it suffices to break the scheme once - the social hardness provides a *strongest-link* guarantee: if just one witness to the transaction is not cooperating, the scheme cannot be broken. This makes it possible to apply the same idea in mobile environments without sufficient computation power or internet connectivity, while taking advantage of its distributed nature [4].

(1) We are dealing with the proof of ownership issue by proposing a distributed block chain and demanding users to at least store the blocks containing their transactions. The proposed distributed block chain has a redundancy factor between the users. LocalCoin, similarly to Bitcoin[2], stores transactions into blocks. All the transactions in the same block are collectively verified. In order for one block to be created *a minimum number of users to verify each transaction* is needed The relationship of these variables with the total amount of users affects the time needed to verify one block and prove the ownership of all the users to whom the transactions belong to.

(2) Regarding double spending attacks, we consider the location of each user who verifies the creation of a new block. A block is accepted only when the average euclidean distance of the nodes agreeing for the block to be accepted exceeds a certain threshold. This ensures that the information regarding each transaction is spread sufficiently in the network. In LocalCoin, cheating is made very difficult because a malicious user has to misinform the majority of a set of trusted users. Every user in the LocalCoin protocol selects the users she trusts. LocalCoin avoids double spending in two ways. **(i)** The receiver of one transaction will accept the transaction if and only if she receives the transaction signed by at least *a minimum number of trusted users* of her trusted network. This constraint imposes a useful delay that spreads the transaction message to more users and

ACM MobiHoc 2016 July 5–8, 2016, Paderborn, Germany

DOI: http://dx.doi.org/10.1145/2942358.2947401

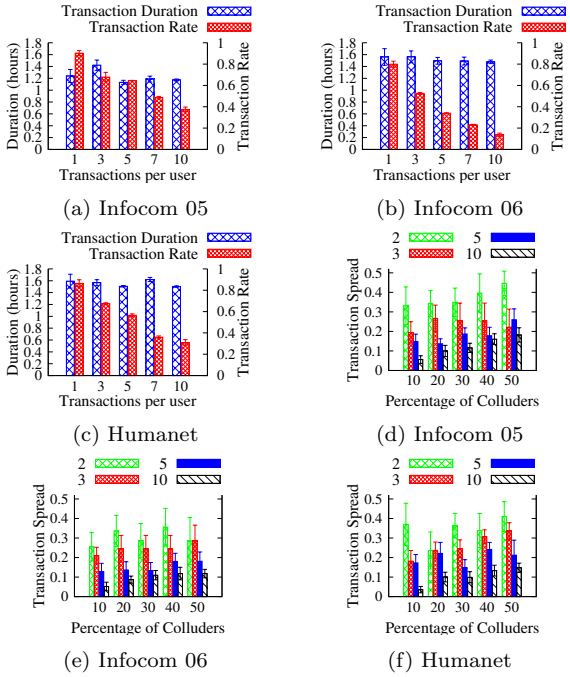
increases the probability of some trusted user to detect if the same input is used in another transaction. Any initiated transaction is signed by the sender and we assume that it is impossible for a malicious user to fake a transaction by pretending to be another user. **(ii)** During the block creation process, every participant checks for double spending attempts. To avoid fake block creation attempts by a set of collaborative malicious users, LocalCoin enforces that the *average distance between the users that will verify the creation of a new block* exceeds a certain threshold (aVd). This last constraints tends to scatter the block creation messages among a very diverse set of users.

(3) We propose an incentive scheme based on transaction and block fees that are adjusted to the ad-hoc networks.We extend the transaction fee schema in order to motivate mobile users to participate. We use *transaction fees* to motivate users to forward messages and *block fees* to motivate them to store as many blocks from the distributed block chain as possible. Transaction fees are important because mobile users are competing for them by broadcasting any received transaction. Block fees are important because users store the created blocks in order to be able to verify the creation of new ones. We envision LocalCoin as a location based cryptocurrency that enables small payments. Apart from conventional money transactions, LocalCoin can also be applied to mobile computing/networking applications such as computation offloading or downloading/streaming services.

2. EVALUATION

We implemented an event-driven simulator in Java in order to evaluate the performance of LocalCoin in practice. We used three datasets, Infocom'05 and Infocom'06 from the Haggle project [3] and Humanet [1], which contain user mobility traces in different environments. The duration of the simulation is one day. We select the first day of the first two datasets, while Humanet is one day long. We considered all the mobile users, which are 41, 78 and 56 respectively.

We introduce the datasets using the concepts of **Transaction Rate** and **Transaction Spread**. We define transaction rate as the fraction of the completed transactions and the transaction spread as the average fraction of the users that have stored the transaction. Figures 1a, 1b and 1c show the average time needed for one transaction to reach its destination and the transaction rate for different number of transactions per user. The receiver and the time of the transaction occurrence are generated uniformly between the users and the day. Note that all datasets are sparse with small number of users and hence, the transaction spread is slow resulting into the small values of transaction rate and transaction spread. Next, we examine the chances a malicious user (m) has to deliver multiple transactions with the same input (**fake transactions**) to more than one users. m tries to double spend by making at least two of the receivers of his fake transactions to accept them. However, double spending will not be successful before the creation of two blocks that contain these fake transactions, which is not possible if aVd is large enough. To simulate a double spending attack, m creates 2, 3, 5 or 10 fake transactions. Figures 1d, 1e and 1f show the average transaction spread of the fake transactions for variable number of colluders ($\mathcal{M}$). Multiple copies of the same transaction decrease the average spread of the fake transaction because the normal users ($\mathcal{U} \setminus \mathcal{M}$) receive at least two fake transactions with higher probability. Furthermore, most of these duplicates are stored by the colluders and not by the normal users.



(a) Infocom 05 (b) Infocom 06

(c) Humanet (d) Infocom 05

(e) Infocom 06 (f) Humanet

Figure 1: Analysis of LocalCoin using users' mobility traces.

3. DISCUSSION

Device to device architectures, with the main representative being 5G, are becoming more and more popular. The Wifi-direct technology is getting more mature and is adapted by many customer products, while, the design of LTE-direct is moving in this route. Motivated by advances in this direction and considering that any existing infrastructure, like an institutional network in a university campus, can only improve the coverage of LocalCoin, we argue that protocols like LocalCoin are applicable and implementable.

4. ACKNOWLEDGEMENTS

This research has been supported, in part, by General Research Fund 26211515 from the Research Grants Council of Hong Kong and the Innovation and Technology Fund ITS/369/14FP from the Hong Kong Innovation and Technology Commission.

5. REFERENCES

[1] J. M. Cabero, V. Molina, I. Urteaga, F. Liberal, and J. L. Martin. CRAWDAD data set tecnalia/humanet (v. 2012-06-12). http://crawdad.org/tecnalia/humanet/, June 2012.

[2] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009.

[3] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau. CRAWDAD data set cambridge/haggle (v. 2006-01-31). Downloaded from http://crawdad.org/cambridge/haggle/, Jan. 2006.

[4] E. Syta, I. Tamas, D. Visher, D. I. Wolinsky, and B. Ford. Decentralizing authorities into scalable strongest-link cothorities. *CoRR*, abs/1503.08768, 2015.