On Bitcoin and Red Balloons

MOSHE BABAIOFF
Microsoft Research, Silicon Valley
and
SHAHAR DOBZINSKI
Department of Computer Science, Cornell University
and
SIGAL OREN
Department of Computer Science, Cornell University
and
AVIV ZOHAR
Microsoft Research, Silicon Valley

In this letter we present a brief report of our recent research on information distribution mechanisms in networks [Babaioff et al. 2011]. We study scenarios in which all nodes that become aware of the information compete for the same prize, and thus have an incentive *not* to propagate information.

Examples of such scenarios include the 2009 DARPA Network Challenge (finding red balloons), and raffles. We give special attention to one application domain, namely Bitcoin, a decentralized electronic currency system. We propose reward schemes that will remedy an incentives problem in Bitcoin in a Sybil-proof manner, with little payment overhead.

---

1. INTRODUCTION

In 2009, DARPA announced the DARPA Network Challenge, in which participants competed to find ten red weather balloons that were placed at various locations across the United States [DARPA 2009]. Faced with the daunting task of locating balloons spread across a wide geographical area, participating teams attempted to recruit individuals from across the country to help. The winning team from MIT, incentivized balloon hunters by offering them rewards of $2000 per balloon they locate [Pickard et al. 2011]. Recognizing that notifying individuals from all over the US about these rewards is itself a difficult undertaking, the MIT team cleverly offered additional rewards of $1000 to a person who directly recruits a balloon finder, a reward of $500 to his recruiter, and so on. These additional payments created the incentive for participants to spread the word about MIT's offer of rewards and were instrumental in the team's success. In fact, the additional rewards are necessary: each additional balloon hunter competes with the participants in his vicinity, and

---

reduces their chances of getting the reward for finding a balloon.

MIT's scheme still requires further improvement. As it is, a participant can create a fake identity, invite the fake identity to participate, and use that identity to recruit others. This Sybil attack increases the participant's reward by 50%.[1] Reward schemes should be resistant to such attacks.

A related setting is a raffle, in which people purchase numbered tickets in hopes of winning some luxurious prize. Each ticket has the same probability of winning, and the prize is always allocated. As more tickets are sold, the winning probability of a specific ticket decreases. In this case again, there is a clear tension between the organizer of the raffle, who wants as many people to find out about the raffle, and the participants who have already purchased tickets and want to increase their individual chances of winning. The lesson here is simple, to make raffles more successful participants should be incentivized to spread the word. One example of a raffle already implementing this is Expedia's "FriendTrips" in which the more friends you recruit the bigger your probability of winning.

Our goal is to design reward schemes that incentivize *information propagation* and counter the dis-incentive arising from the competition from other nodes, and are *Sybil proof* while having a *low overhead* (a total reward that is not too high). In particular, we identify the need for such incentives in the Bitcoin protocol, our main example for the rest of this letter. First, we introduce Bitcoin and explain where the incentive problem shows up.

Bitcoin

Bitcoin is a decentralized electronic currency system proposed by Satoshi Nakamoto[2] in 2008 as an alternative to current government-backed currencies [Nakamoto 2008]. Bitcoin has been actively running since 2009, and has been getting a large amount of public attention over the last year. It represents a radical new approach to monetary systems which has appeared in policy discussions and in the popular press. Its cryptographic fundamentals have largely held up even as its usage has become increasingly widespread.

Bitcoin's appeal lies mainly in the ability to quickly transfer money over the internet, and in its relatively low transaction fees.[3] As of November 2011, there are 7.5 million units of currency in circulation (called *Bitcoins*) which are traded at a value of approximately 3 USD per bitcoin.

Bitcoin relies on a peer-to-peer network to verify and authorize all transactions that are performed with the currency. Transactions are cryptographically signed by the owner of the bitcoins that wishes to transfer them, and are sent to nodes in the peer-to-peer network for authorization. Each node in the network is supposed

---

[1]Indeed, we have no evidence of such attacks in the DARPA challenge. If no such attacks were made, one possible explanation is the short time span of the challenge and its non-commercial, scientific essence. It seems quite plausible that if the challenge is repeated several times such attacks on the MIT reward scheme would become common.

[2]The name Satoshi Nakamoto appears to be an alias. The real identity of Bitcoin's creator remains a mystery.

[3]There are additional properties that some consider as benefits: Bitcoins are not controlled by any government, and its supply will eventually be fixed. Additionally, it offers some degree of anonymity.

to propagate the transaction to its neighbors. Upon receiving a transaction, each node verifies that it is properly signed by the bitcoins' owner, and then tries to "authorize" the transaction by attempting to solve a computationally hard problem (basically inverting a hash function). This authorization process is a key ingredient in maintaining Bitcoin's security (refer to [Nakamoto 2008] for details). Once a node successfully authorizes a transaction, it sends the "proof" (the inverted hash) to all of its neighbors. They in turn, send the "proof" to all of their neighbors and so on. Finally, all nodes in the network "agree" that the transaction has taken place and was authorized.

In compensation for their efforts, nodes are offered a payment in bitcoins for successful authorizations. The system is currently in its initial stages, in which nodes are paid a predetermined amount of bitcoins that are created "out of thin air". This also slowly builds up the bitcoins supply. But Bitcoin's protocol specifies an exponentially decreasing rate of money creation that effectively sets a cap on the total number of bitcoins that will be in circulation. As this payment to nodes is slowly phased out, bitcoin owners that want their transactions approved are supposed to pay fees to the authorizing nodes.

This is where the incentive problem manifests itself. A node in the network has an incentive to keep the knowledge of any transaction that offers a fee for itself, as any other node that becomes aware of the transaction will compete to authorize the transaction first and claim the associated fee. The consequences of such behavior may be devastating: as only a single node in the network works to authorize each transaction, authorization is expected to take a very long time.

We stress that false identities are a prominent concern in Bitcoin. In fact, the Bitcoin protocol is built around the assumption that nodes can create false identities, thus, for a transaction to be approved, nodes that control a majority of the CPU power in the network should accept it, rather than just a majority of the nodes. The latter is vulnerable to Sybil attacks. Therefore any reward scheme for transaction distribution must discourage such attacks.

2. THE MODEL

We present our model for information propagation in Bitcoin's authorization protocol. For a more detailed presentation, refer to [Babaioff et al. 2011].

We assume for simplicity that the network consists of a forest of complete d-ary directed trees, each of them of height H.[4] We model the authorization process of a single transaction in two phases: a distribution phase and a computation phase.

In the beginning of the *distribution phase* the buyer sends the details of the transaction to the t roots of the trees (which we term *seeds*). Each node v that is aware of the transaction can send the information to any of its children. Before sending to any child it can add any number of fake identities. All of v's fake identities are connected to the same set of children. A node can condition its

---

[4]The intuition for this simplification is that the number of nodes that are aware of the transaction multiplies by some constant for every additional layer that the transaction travels to. A more exact model would be that of a random graph, but this is harder to solve for. In some sense, building the right incentives in the case of trees is harder, as each node monopolizes the flow of information to its descendants.

behavior only on the *length* of the referral chain above it, which can possibly include false identities that were produced by its ancestors.

In the *computation phase* each node that is aware of the transaction tries to authorize it. If there are k such nodes, each of them has the same probability of $\frac{1}{k}$ to authorize it first. We assume that there is a minimal payment for authorization, normalized to 1, which is necessary to motivate the nodes to work on authorizing the transaction.

When a node succeeds in authorizing a transaction we can reward nodes on the chain (starting at some seed) to that node. This chain may contain false identities as well, but cryptographic tools ensure that no node can remove its ancestors from the chain.

3. REWARD SCHEMES

We suggest a rewarding scheme family called the $(\beta, \mathcal{H})$-almost-uniform family. We then combine schemes from this family to create a hybrid scheme that possesses better qualities.

3.1 $(\beta, \mathcal{H})$-Almost-Uniform Schemes

The rewards of schemes in this family are defined as follows: Suppose that a node v has authorized the transaction, and has a chain of l nodes through which it has received the transaction. If $l > \mathcal{H}$ no node is rewarded (so nodes "far" from the seed do not attempt to authorize the transaction). Otherwise, each node in the chain except v gets a reward of β, and v gets a reward of $1 + (\mathcal{H} - l + 1)\beta$.

Given that there are $\Omega(\beta^{-1})$ seeds, the $(\beta, \mathcal{H})$-almost-uniform scheme creates the incentives for each node to propagate information to all its children without duplicating itself. Specifically, we show:

(INFORMAL) THEOREM 1. *If there are $\Omega(\beta^{-1})$ seeds, the $(\beta, \mathcal{H})$-almost-uniform scheme guarantees that only strategy profiles that exhibit information propagation and no duplication survive every order of iterated removal of dominated strategies. Furthermore, there exists an order in which no other strategy profiles survive.*

This gives us two interesting schemes, for two different values of β, that offer tradeoffs between the total payment and the number of seeds that need to be initially notified. The first scheme is the $(1, \mathcal{H})$-almost-uniform scheme which requires only a constant number of seeds and its total payment is always $O(\mathcal{H})$. The second scheme is the $(\frac{1}{\mathcal{H}}, \mathcal{H})$-almost-uniform scheme. This scheme works if the number of seeds is $\Omega(\mathcal{H})$. Its total payment is 2.

3.2 The Hybrid Scheme

We combine the $(\frac{1}{\mathcal{H}}, \mathcal{H})$- and $(1, 1 + \log_d \mathcal{H})$-almost-uniform schemes to create a hybrid scheme that requires only a constant number of seeds and pays only a constant amount in expectation. We obtain the following result:

(INFORMAL) THEOREM 2. *In the hybrid rewarding scheme, if the number of seeds is at least 14, the only strategies that always survive iterated elimination of dominated strategies exhibit information propagation and no duplication. In addition, there exists an elimination order in which the only strategies that survive*

exhibit information propagation and no duplication. Furthermore, the expected sum of payments is at most 3*.*

4. DOMINANT STRATEGY MECHANISMS

Iterated removal of dominated strategies is a strong solution concept, but ideally we would like our rewarding scheme to achieve all desired properties in the stronger notion of dominant strategies equilibrium. However, we show that in every dominant strategy scheme either the amount that the scheme must pay in equilibrium is huge, or the number of initial seeds t must be very large.

(INFORMAL) THEOREM 3. *Every individually rational reward scheme that propagates information to at least half of the network, and in which no-duplication and information-propagation is a dominant strategy for all nodes, has expected payment of at least* $\frac{1}{10}\left(\frac{2^{H-4}}{t^2} + \frac{1}{t} \cdot \left(\frac{H-3}{t \cdot e}\right)^{H-3}\right)$.

Notice that for the sum of rewards to be constant the number of seeds t has to be a significant part of the network. This implies that dominant strategy schemes are quite impractical.

5. CONCLUSION AND FUTURE RESEARCH

We propose a novel low cost reward scheme that incentivizes information propagation and is Sybil proof. Currently we model the network as a forest of t complete d-ary trees. A challenging open question is to consider the setting where the network is modeled as a random d-regular graph. Other interesting extensions to consider are models that account for the different computation power of nodes, costs of communication, and non-regular graphs (with varying degrees at each node).

REFERENCES

BABAIOFF, M., DOBZINSKI, S., OREN, S., AND ZOHAR, A. 2011. On bitcoin and red balloons (full version). Available online: http://research.microsoft.com/apps/pubs/?id=156072q.

DARPA. 2009. The DARPA network challenge. Available online at http://archive.darpa.mil/networkchallenge/.

NAKAMOTO, S. 2008. Bitcoin: A peer-to-peer electronic cash system. Available online at http://bitcoin.org/bitcoin.pdf.

PICKARD, G., PAN, W., RAHWAN, I., CEBRIÁN, M., CRANE, R., AND MADAN, A. 2011. Time critical social mobilization. *Science 334*, 509–512.