On Offline Payments with Bitcoin (Poster Abstract)

Alexandra Dmitrienko[1(✉)], David Noack[2], Ahmad-Reza Sadeghi[2], and Moti Yung[3]

[1] Fraunhofer SIT/CASED, Darmstadt, Germany
alexandra.dmitrienko@sit.fraunhofer.de
[2] TU Darmstadt/CASED, Darmstadt, Germany
{ahmad.sadeghi,david.noack}@trust.cased.de
[3] Google, New York, USA
moti@cs.columbia.edu

Bitcoin [2] is a decentralized digital currency which relies neither on banks nor on any other central authority for issuing of coins or transaction verification. Currently, Bitcoin experiences enormous success driven by large interest from users, politics, but also by speculation. Particularly, despite being conjured to be a giant bubble, the value of a bitcoin[1] increased from USD $5 in May 2012 to temporarily over USD $1,200 in December, and fluctuating between USD 500$ and USD 800$ since then. According to coinmap.org, as of February 2014 there are at least over 3000 shops, hotels, bars or even medical practices worldwide that accept local Bitcoin payments. This is an increase of 2000 locations over the last 3 month and not including online-shops or online-services[2].

The two most important challenges of digital cash, explicit and undeniable ownership of coins and double-spending prevention, are addressed in Bitcoin by means of asymmetric cryptography and a distributed time-stamping service based on proof-of-work (PoW). Users of the Bitcoin network own addresses in form of asymmetric key pairs. To spend bitcoins, a user issues a transaction that, amongst others, includes a signature of the sender, the amount and the address (public key) of the receiver. All transactions are committed to the Bitcoin network and recorded in a public transaction history known as the blockchain. Building the blockchain requires solving cryptographic puzzles which is computationally hard to perform, but easy to verify. Special Bitcoin clients, called miners, are working on integration of new transactions into the blockchain, and get awarded with bitcoins as soon as they discover a new valid block. Regular Bitcoin clients can track the transaction history to ensure that the bitcoin they are going to receive has never been spent before.

An important characteristic of the Bitcoin system is that clients require *online access* to the blockchain for a certain amount of *time* to be able to verify any transaction. However, these requirements render Bitcoin *not* suitable for offline payment scenarios, where neither the sender nor the receiver have

[1] As usual we use capitalized Bitcoin to denote the system and lowercase bitcoin to refer to monetary currency.
[2] https://en.bitcoin.it/wiki/Trade

R. Böhme et al. (Eds.): FC 2014 Workshops, LNCS 8438, pp. 159–160, 2014.
DOI: 10.1007/978-3-662-44774-1_11

connection to the Bitcoin network. Furthermore, immediate payments with Bitcoin, where transactions have to be accepted or rejected immediately, are insecure [1] even in online settings.

In this work we aim to overcome these shortcomings and extend the existing Bitcoin system. Particularly, we propose a solution which allows for *offline* and *immediate* secure payments with Bitcoin. We rely on a trusted wallet, a trusted resource-constrained platform component which cannot be tampered with and controls usage of private keys of corresponding Bitcoin addresses. It prevents the user from spending a single coin twice, rendering double-spending attacks impossible by design. However, using trusted wallet is not sufficient to enable secure offline payments. This is because any input to the trusted wallet can be manipulated and due to resource constrains of typical wallet environments, which makes transaction verification challenging. For instance, these constraints render full blockchain validation within the wallet environment infeasible, as downloading and verification the whole blockchain takes days even on resource-rich platforms such as PCs[3].

To address these challenges, we design a lightweight transaction verification mechanism. Our solution exploits the fact that valid transactions and their confirmations expose a unique signature consisting of the computational effort and time required to generate them that only the Bitcoin network can achieve, but unlikely the adversary. We provide a thorough security and risk analysis of our solution and suggest concrete security parameters for a reasonable trade-off between adversary model and efficiency. Moreover, we eliminate small remaining risks of attacks by introducing an additional security parameter which limits transaction amounts to keep them smaller than costs of potential attacks. We then perform rigorous analysis of associated attack costs and show that a reasonable transaction limit lies in a range of thousands of dollars (per transaction), which is sufficient to satisfy most payment scenarios. Further, if larger transactions are required, they can be split into several smaller transactions, transparently to the user.

We prototyped our solution for mobile Android clients and utilized a microSD security card as a wallet environment. Our performance analysis demonstrates the feasibility of our approach in practice. Furthermore, our extension is compatible to the original Bitcoin system which makes our solution suitable for immediate deployment.

References

1. Karame, G.O. Androulaki, E., Capkun, S.: Double-spending fast payments in bitcoin. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security (2012)
2. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Technical report (2008). www.bitcoin.org/bitcoin.pdf

[3] http://bitcoin.stackexchange.com/questions/9816/how-long-does-it-take-to-download-the-blockchain-its-been-over-a-day-and-still