ABSTRACT

CFEM & CTIC workshop:
Theory and Practice of Secure Multiparty Computation
May 30 to June 3, 2016
Aarhus University, Denmark

Title: Analysis and Design of Blockchains

Author: Rafael Pass, Cornell University, USA

Nakamoto's famous blockchain protocol enables achieving consensus in a so-called *permissionless* setting---anyone can join (or leave) the protocol execution, and the protocol instructions do not depend on the identities of the players. His ingenious protocol prevents "sybil attacks" (where an adversary spawns any number of new players) by relying on computational puzzles (a.k.a. "moderately hard functions") introduced by Dwork and Naor (Crypto'92).

Prior works that analyze the blockchain protocol either make the simplifying assumption that network channels are fully synchronous (i.e. messages are instantly delivered without delays) (Garay et al, Eurocrypt'15) or only consider specific attacks (Nakamoto'08; Sampolinsky and Zohar, FinancialCrypt'15); additionally, as far as we know, none of them deal with players joining or leaving the protocol.

We prove that the blockchain consensus mechanism satisfies a strong forms of consistency and liveness in an asynchronous network with adversarial delays that are a-priori bounded, within a formal model allowing for adaptive corruption and spawning of new players, assuming that the computational puzzle is modeled as a random oracle. (We complement this result by showing a simple attack against the blockchain protocol in a fully asynchronous setting, showing that the "puzzle-hardness" needs to be appropriately set as a function of the maximum network delay.)

As an independent contribution, we define an abstract notion of a blockchain protocol and identify appropriate security properties of such protocols; we prove that Nakamoto's blockchain protocol satisfies them and that these properties are sufficient for typical applications. We finally show how to use our analysis to build *new* blockchain protocols that overcome some of the bottlenecks in Nakamoto's original protocol.

The analysis of Nakamoto's blockchain is based on joint work with Lior Seeman and abhi shelat, and the new blockchain protocols are based on joint work with Elaine Shi.
No prior knowledge of Bitcoin or the blockchain will be assumed.