The Notion of Byzantine Agreement

April 9, 2017

Byzantine agreement is a key ingredient of Algorand. Indeed, it is through the use of such a BA protocol that Algorand is unaffected by forks. However, to be secure against our powerful Adversary, Algorand must rely on a BA protocol that satisfies the new player-replaceability constraint. In addition, for Algorand to be efficient, such a BA protocol must be very efficient.

BA protocols were first defined for an idealized communication model, *synchronous complete networks* (SC networks). Such a model allows for a simpler design and analysis of BA protocols.

We start by recalling the traditional SC networks and their corresponding adversarial model.

1 Synchronous Complete Networks and Adversaries

In a SC network, there is a common clock, ticking at each integral times $r = 1, 2, \ldots$

At each even time click r, each player i instantaneously and simultaneously sends a single message $m_{i,j}^r$ (possibly the empty message) to each player j, including himself. Each $m_{i,j}^r$ is received at time click $r + 1$ by player j, together with the identity of the sender i.

Again, in a communication protocol, a player is *honest* if he follows all his prescribed instructions, and *malicious* otherwise. All malicious players are totally controlled and perfectly coordinated by the *adversary*.[1]

The Adversary also has the ability to instantaneously see, at each even round, the messages that the currently honest players send, and instantaneously use this information to choose the messages the malicious players send at the same time tick.

The adversary can immediately make malicious any honest user he wants at any odd time click he wants. A *t-adversary* is an adversary who is capable of corrupting at most t players.

kThe adversary, (1) cannot monitor the information of honest players, (2) has no information about the messages exchanged by any two (currently) honest players, and (3) "cannot interfere with the messages already sent by an honest user i", which will reach, unaltered, their respective recipients.

Remarks

- *Adversary Power.* The above setting is very adversarial. Indeed, in the Byzantine agreement literature, many settings are less adversarial. However, some more adversarial settings have also been considered, where the Adversary, after seeing the messages sent by an honest player i

[1] In particular, the adversary knows all information known to malicious players, receives all messages addressed to them, and chooses all actions, and thus all messages, on their behalf.

at a given time click r, has the ability to erase all these messages from the network, immediately corrupt i, choose the message that the now malicious i sends at time click r, and have them delivered as usual. The envisaged power of the Adversary matches that he has in our setting.

- *Physical Abstraction.* The envisaged communication model abstracts a more physical model, in which each pair of players (i, j) is linked by a separate and private communication line $l_{i,j}$. That is, no one else can inject, interfere with, or gain information about the messages sent over $l_{i,j}$. The only way for the Adversary to have access to $l_{i,j}$ is to corrupt either i or j.

- *Privacy and Authentication.* In SC networks message privacy and authentication are guaranteed by assumption. By contrast, in our communication network, where messages are propagated from peer to peer, authentication is guaranteed by digital signatures, and privacy is non-existent. Thus, to adopt protocol $BA^\star$ to our setting, each message exchanged should be digitally signed (further identifying the state at which it was sent). Fortunately, the BA protocols that we consider using in Algorand do not require message privacy.

- *Historical Note.* The notion of Byzantine agreement was introduced by Pease Shostak and Lamport [1] for the *binary* case, that is, when every initial value consists of a bit. However, it was quickly extended to arbitrary initial values. By a BA protocol, we mean an arbitrary-value one.

1.1 Two Notions of Byzantine Agreement

Definition 1 *In a SC network, let $\mathcal{P}$ be a n-player protocol, t a positive integer such that $n \geq 2t + 1$. We say that $\mathcal{P}$ is an* arbitrary-value *(respectively,* binary*)* (n, t)-Byzantine agreement protocol *with* soundness $\sigma \in (0, 1)$ *if, for all sets of values V not containing the special symbol $\perp$ (respectively, for $V = \{0, 1\}$), all t-adversaries A, and all executions of P with A, in which i starts with an* initial value $v_i \in V$*, every honest player j halts with probability 1, outputting a value $out_i \in V \cup \{\perp\}$ so as to satisfy, with probability at least σ, the following two conditions:*

1. Agreement: *There exists $out \in V \cup \{\perp\}$ such that $out_i = out$ for all honest players i.*

2. Consistency: *if, for some value $v \in V$, $v_i = v$ for all players i, then $out = v$.*

We refer to out as $\mathcal{P}$'s output*, and to each out_i as* player i's output*.*

Definition 1′ *As in Definition 1, except for the following change:*

2′. Consistency: *if, for some value $v \in V$, $v_i = v$ for all honest players i, then $out = v$.*

Homework *You will be asked to compare the two notions.*

References

[1] *M. Pease, R. Shostak, and L. Lamport.* Reaching agreement in the presence of faults. *J. Assoc. Comput. Mach., 27 (1980), pp. 228-234.*