Algorand BA

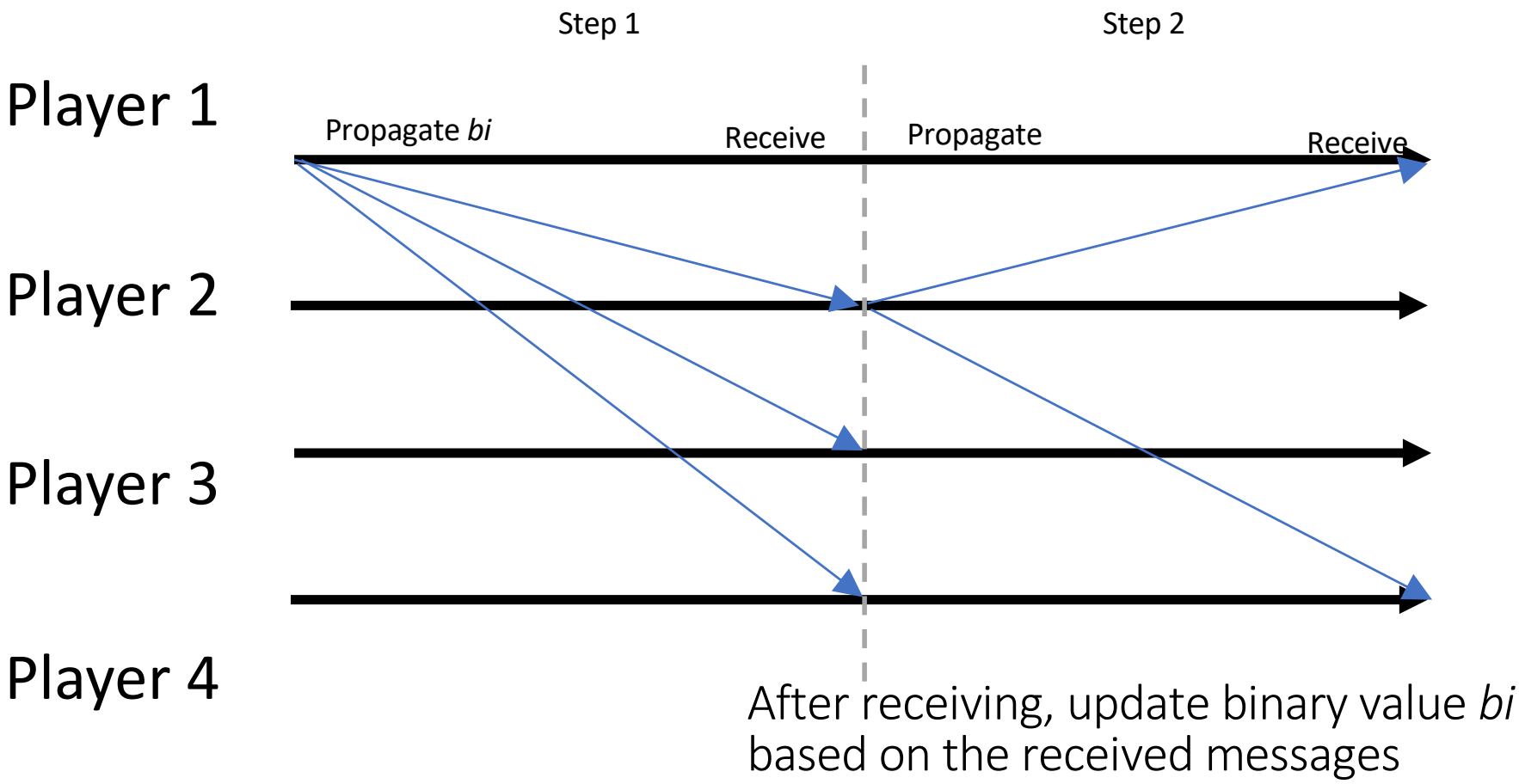
Principles of Blockchains, University of Illinois,
Professor: Pramod Viswanath

Gerui Wang

March 18, 2021

Warmup: The Binary BA Protocol BBA^*

- Although player-replaceability is a desired feature, let's start with a BA without player-replaceability.
- BBA^*: a probabilistic binary Byzantine agreement that targets $n = 3t + 1$ players and t-Byzantine fault tolerance.
- Each player i holds a binary value b_i on which they want to reach agreement.
- The protocol proceeds in synchronous steps, where messages are guaranteed to be delivered within a step.
- (Next slide shows an example of 2 steps)


Step 1
Step 2
Player 1
Player 2
Player 3
Player 4
Propagate *bi*
Receive
Propagate
Receive
After receiving, update binary value *bi* based on the received messages

A Straw-man Step

Intuition about *how player i updates b_i*.

A Straw-man Step

Intuition about *how player i updates b_i*. Since the assumption of Byzantine players is $n/3$, honest $2n/3$, ($n = 3t + 1$):

If $\#_i(0) \geq 2t + 1$, then i sets $b_i = 0$.

Symmetrically, if $\#_i(1) \geq 2t + 1$, then i sets $b_i = 1$.

$\#_i(v)$ denotes the number of players from which i has received the value v.

A Straw-man Step: Analysis

If $\#_i(0) \geq 2t + 1$, *then* i *sets* $b_i = 0$.
Symmetrically, if $\#_i(1) \geq 2t + 1$, *then* i *sets* $b_i = 1$.

If there is a $2/3$ majority: reach agreement.

A Straw-man Step: Analysis

If $\#_i(0) \geq 2t + 1$, *then* i *sets* $b_i = 0$.
Symmetrically, if $\#_i(1) \geq 2t + 1$, *then* i *sets* $b_i = 1$.

If there is a $2/3$ majority: reach agreement.
An obvious question with the above step is what if $\#_i(0) < 2t + 1$ and $\#_i(1) < 2t + 1$?

A Straw-man Step: Analysis

If $\#_i(0) \geq 2t + 1$, *then* i *sets* $b_i = 0$.
Symmetrically, if $\#_i(1) \geq 2t + 1$, *then* i *sets* $b_i = 1$.

If there is a $2/3$ majority: reach agreement.
An obvious question with the above step is what if $\#_i(0) < 2t + 1$ and $\#_i(1) < 2t + 1$?
We need a cryptographic primitive called *common coin*: a new randomly and independently selected bit c for each step. (We will show how to implement it later.) Just let players set $b_i = c$.

A Straw-man Step: Analysis

A Step: Player i propagates b_i.

1. If $\#_i(0) \geq 2t + 1$, then i sets $b_i = 0$.
2. Else, if $\#_i(1) \geq 2t + 1$, then i sets $b_i = 1$.
3. Else, i sets $b_i = c$.

A Straw-man Step: Analysis

A Step: Player i propagates b_i.

1. If $\#_i(0) \geq 2t + 1$, then i sets $b_i = 0$.
2. Else, if $\#_i(1) \geq 2t + 1$, then i sets $b_i = 1$.
3. Else, i sets $b_i = c$.

Easy to see the following properties,

A Straw-man Step: Analysis

A Step: Player i propagates b_i.

1. If $\#_i(0) \geq 2t+1$, then i sets $b_i = 0$.
2. Else, if $\#_i(1) \geq 2t+1$, then i sets $b_i = 1$.
3. Else, i sets $b_i = c$.

Easy to see the following properties,

(A) If, at the start of a step, the honest players (at least $2t+1$) are in agreement on a bit b, (i.e., if $b_i = b$ for all honest player i), then they remain in agreement on b by its end.

A Straw-man Step: Analysis

A Step: Player i propagates b_i.

1. If $\#_i(0) \geq 2t+1$, then i sets $b_i = 0$.
2. Else, if $\#_i(1) \geq 2t+1$, then i sets $b_i = 1$.
3. Else, i sets $b_i = c$.

Easy to see the following properties,

(A) If, at the start of a step, the honest players (at least $2t+1$) are in agreement on a bit b, (i.e., if $b_i = b$ for all honest player i), then they remain in agreement on b by its end.

(B) If the honest players are not in agreement (on any bit) at the start of a step, then with probability $1/2$, they will be in agreement (on some bit) by its end.

(B) If the honest players are not in agreement (on any bit) at the start of a step, then with probability $1/2$, they will be in agreement (on some bit) by its end.

A brief explanation for property (B) is that when honest players are not in agreement, they can be in either condition 1 and 3 (sets $b_i = 0$ and $b_i = c$) or condition 2 and 3 (sets $b_i = 1$ and $b_i = c$). In either case, coin c is equal to the bit with probability $1/2$.

A Straw-man Step: Analysis

A Step: Player i propagates b_i.

1. If $\#_i(0) \geq 2t + 1$, then i sets $b_i = 0$.
2. Else, if $\#_i(1) \geq 2t + 1$, then i sets $b_i = 1$.
3. Else, i sets $b_i = c$.

by running this straw-man step sufficiently many times, honest players will reach an agreement with overwhelming probability.

3 Steps of *BBA**

For the straw-man step, honest players are not aware when they are in agreement and can terminate early.

3 Steps of *BBA**

For the straw-man step, honest players are not aware when they are in agreement and can terminate early. To solve this problem, *BBA** uses 3 different types of steps, modified from the straw-man step.

- Coin-Fixed-To-0 Step. The common coin is replaced by a fixed bit 0.

3 Steps of BBA^*

For the straw-man step, honest players are not aware when they are in agreement and can terminate early. To solve this problem, BBA^* uses 3 different types of steps, modified from the straw-man step.

- Coin-Fixed-To-0 Step. The common coin is replaced by a fixed bit 0.
- Coin-Fixed-To-1 Step. The common coin is replaced by a fixed bit 1.

3 Steps of BBA^*

For the straw-man step, honest players are not aware when they are in agreement and can terminate early. To solve this problem, BBA^* uses 3 different types of steps, modified from the straw-man step.

- Coin-Fixed-To-0 Step. The common coin is replaced by a fixed bit 0.
- Coin-Fixed-To-1 Step. The common coin is replaced by a fixed bit 1.
- Coin-Genuinely-Flipped Step. The common coin is the genuinely random coin.

3 Steps of BBA^*: Analysis

- Coin-Fixed-To-0 Step and Coin-Fixed-To-1 Step: once the agreement has already been reached on some bit, an honest player can learn this is the case, and terminate with the bit.

3 Steps of BBA^*: Analysis

- Coin-Fixed-To-0 Step and Coin-Fixed-To-1 Step: once the agreement has already been reached on some bit, an honest player can learn this is the case, and terminate with the bit.

They have this property:

(C) If, at Coin-Fixed-To-0 or Coin-Fixed-To-1 step, an honest player i outputs, then agreement will hold at the end of the step.

3 Steps of BBA^*: Analysis

- Coin-Fixed-To-0 Step and Coin-Fixed-To-1 Step: once the agreement has already been reached on some bit, an honest player can learn this is the case, and terminate with the bit.

They have this property:

(C) If, at Coin-Fixed-To-0 or Coin-Fixed-To-1 step, an honest player i outputs, then agreement will hold at the end of the step.

A brief explanation is, taking Coin-Fixed-To-0 as an example, if an honest player i outputs, players can be in either condition 1 or 3, since there are at most t Byzantine players who vote twice so condition 2 is unreachable.

3 Steps of BBA^*: Analysis

These 3 properties make BBA^* a correct BA.

(A) If, at the start of a step, the honest players (at least $2t+1$) are in agreement on a bit b, (i.e., if $b_i = b$ for all honest player i), then they remain in agreement on b by its end.

(B) If the honest players are not in agreement (on any bit) at the start of Coin-Genuinely-Flipped step, then with probability $1/2$, they will be in agreement (on some bit) by its end.

(C) If, at Coin-Fixed-To-0 or Coin-Fixed-To-1 step, an honest player i outputs, then agreement will hold at the end of the step.

BBA^*: wrap up. Next: player-replaceability.

[Coin-Fixed-To-0 Step] Each player i propagates b_i.

1.1 If $\#_i(0) \geq 2t+1$, then i sets $b_i = 0$. Outputs 0 and do not change b_i. That is, for future steps, propagates 0.

1.2 If $\#_i(1) \geq 2t+1$, then i sets $b_i = 1$.

1.3 Else, i sets $b_i = 0$.

[Coin-Fixed-To-1 Step] Each player i propagates b_i.

2.1 If $\#_i(1) \geq 2t+1$, then i sets $b_i = 1$. Outputs 1 and do not change b_i. That is, for future steps, propagates 1.

2.2 If $\#_i(0) \geq 2t+1$, then i sets $b_i = 0$.

2.3 Else, i sets $b_i = 1$.

[Coin-Genuinely-Flipped Step] Each player i propagates b_i.

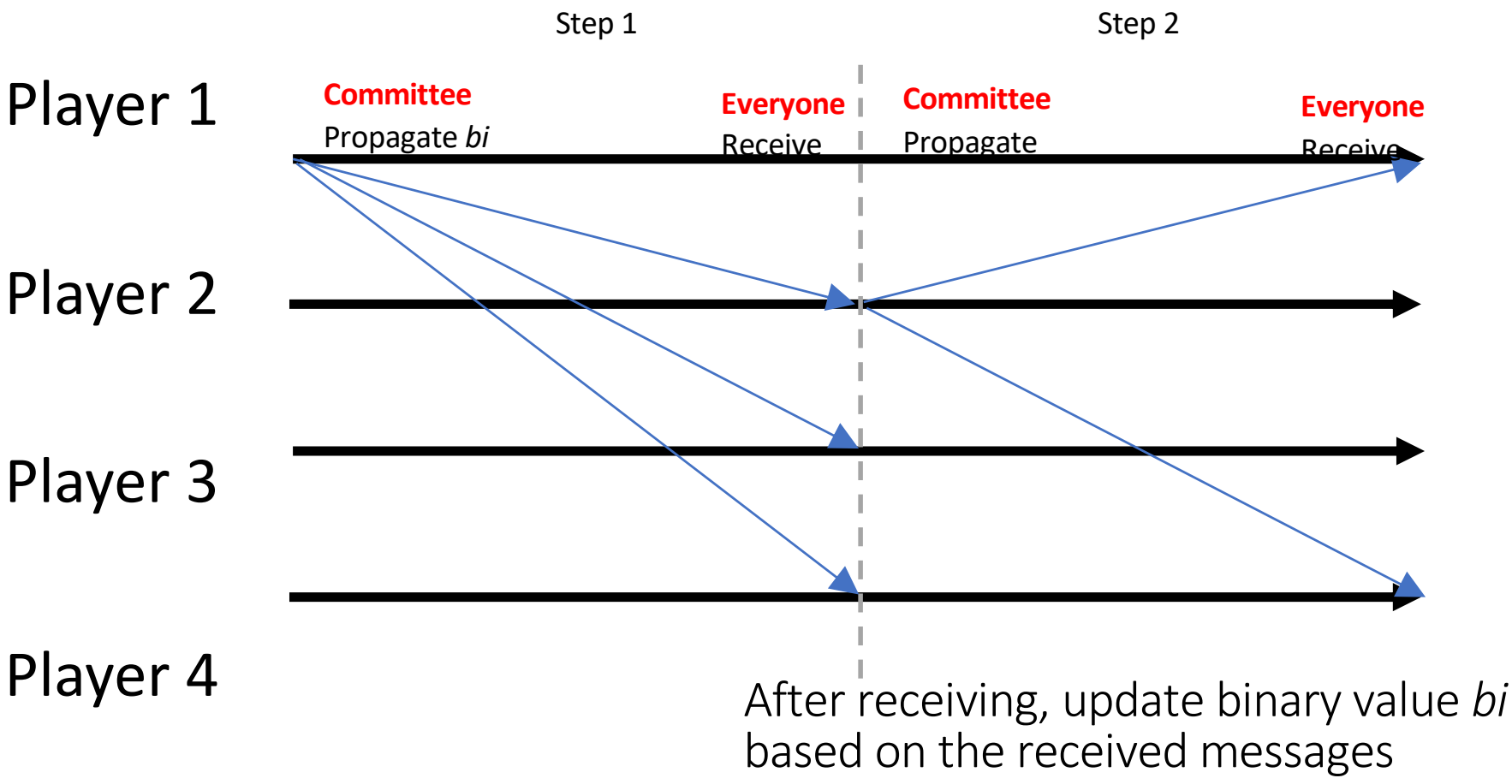
3.1 If $\#_i(0) \geq 2t+1$, then i sets $b_i = 0$.

3.2 If $\#_i(1) \geq 2t+1$, then i sets $b_i = 1$.

3.3 Else, i sets b_i to the common coin c.

Player-replaceability: selecting committees

Each step is assigned to a totally new committee, which is independently and randomly selected among all players by *sortition*.


Step 1
Step 2
Player 1
Player 2
Player 3
Player 4
Committee
Propagate bi
Everyone
Receive
Committee
Propagate
Everyone
Receive
After receiving, update binary value bi
based on the received messages

Player-replaceability: selecting committees

- Player i uses a quantity *credential* σ to secretly determines whether it is selected.

Player-replaceability: selecting committees

- Player i uses a quantity *credential* σ to secretly determines whether it is selected.
- σ is derived by VRF from a random quantity Q^r that is deduced from block B^{r-1} (assuming block available on the blockchain).

Player-replaceability: selecting committees

- Player i uses a quantity *credential* σ to secretly determines whether it is selected.
- σ is derived by VRF from a random quantity Q^r that is deduced from block B^{r-1} (assuming block available on the blockchain).
- i is committee in round r and step s if $H(\sigma_i^{r,s}) < p$ (H is a hash function, p is a threshold)

Player-replaceability: selecting committees

- Player i uses a quantity *credential* σ to secretly determines whether it is selected.
- σ is derived by VRF from a random quantity Q^r that is deduced from block B^{r-1} (assuming block available on the blockchain).
- i is committee in round r and step s if $H(\sigma_i^{r,s}) < p$ (H is a hash function, p is a threshold)
- i propagates $\sigma_i^{r,s}$ with its message so that other players can verify it.

BBA^* player-replaceability. Just change $2t+1$ to $t_H \approx 2/3|\text{committee}|$

[Coin-Fixed-To-0 Step] Each player i propagates b_i.

1.1 If $\#_i(0) \geq 2t+1$, then i sets $b_i = 0$. Outputs 0 and do not change b_i. That is, for future steps, propagates 0.

1.2 If $\#_i(1) \geq 2t+1$, then i sets $b_i = 1$.

1.3 Else, i sets $b_i = 0$.

[Coin-Fixed-To-1 Step] Each player i propagates b_i.

2.1 If $\#_i(1) \geq 2t+1$, then i sets $b_i = 1$. Outputs 1 and do not change b_i. That is, for future steps, propagates 1.

2.2 If $\#_i(0) \geq 2t+1$, then i sets $b_i = 0$.

2.3 Else, i sets $b_i = 1$.

[Coin-Genuinely-Flipped Step] Each player i propagates b_i.

3.1 If $\#_i(0) \geq 2t+1$, then i sets $b_i = 0$.

3.2 If $\#_i(1) \geq 2t+1$, then i sets $b_i = 1$.

3.3 Else, i sets b_i to the common coin c.

Ephemeral keys

Although the adversary cannot predict beforehand which users will be the committee, it would know their identities after seeing their messages, and could then corrupt all of them.

Ephemeral keys

Although the adversary cannot predict beforehand which users will be the committee, it would know their identities after seeing their messages, and could then corrupt all of them.
To deal with this, players use ephemeral keys: public/secret key pairs that are single-use-only, and once used, are *destroyed*.

Implement the common coin

- In Coin-Genuinely-Flipped step, a player should receives messages from many players, denoted by SV. It picks the smallest credential hash from SV, hash the credential with the step counter s, and use the least significant bit as the coin c.
- Since the least significant bit of a hash is random, this coin implementation is almost a random common coin.

Extending BBA^* to multi-valued (block) Byzantine agreement

- Elect a leader (just like electing a committee), let the leader propagate a valid block for round r, B^r.

Extending BBA^* to multi-valued (block) Byzantine agreement

- Elect a leader (just like electing a committee), let the leader propagate a valid block for round r, B^r.
- two-round voting to ensure that if two honest players receive a block and enough votes, they have the same block B^r.

Extending BBA^* to multi-valued (block) Byzantine agreement

- Elect a leader (just like electing a committee), let the leader propagate a valid block for round r, B^r.
- two-round voting to ensure that if two honest players receive a block and enough votes, they have the same block B^r.
- Decide the input b_i to BBA^*:
  - if receive a valid block B^r from the leader and enough votes, $b_i = 0$.
  - otherwise, $b_i = 1$.

Extending BBA^* to multi-valued (block) Byzantine agreement

- Elect a leader (just like electing a committee), let the leader propagate a valid block for round r, B^r.
- two-round voting to ensure that if two honest players receive a block and enough votes, they have the same block B^r.
- Decide the input b_i to BBA^*:
  - if receive a valid block B^r from the leader and enough votes, $b_i = 0$.
  - otherwise, $b_i = 1$.
- Just run BBA^*!
- Players will agree on either $b_i = 0$ and a valid block, or $b_i = 1$ (in this case they use a default empty block).

Proof-of-Stake (PoS) Algorand

If we involve the stake held by a public key into the committee/leader selection, then we end up with a PoS blockchain.

Q and A