BACK TO NEWS

June 25, 2019 . 5 min read

Storecoin compares practical security implications of Algorand's BFT consensus algorithm with ckfinBFT's.

StorecoinDev
@StorecoinDev

lgorand was in the news blockcrypto.com/tiny/algorand-…) recently. They ed over $60M in token sales at an implied ation of $24B.

About Storecoin

Storecoin is a zero-fee payment and p2p cloud computing platform that

will transform data into money (into datacoins).

The Block

Algorand, the proof-of-stake based blockchain protocol, has raised over $60 million in a token sale conducted on CoinList, according to the Algorand Foundation. This raise was on top of the $66...
theblockcrypto.com

31 7:02 PM - Jun 20, 2019

21 people are talking about this

StorecoinDev
@StorecoinDev

lying to @StorecoinDev
They implemented the Algorand consensus orithm (dl.acm.org/citation.cfm?i…) to evaluate its formance on 1,000 Amazon EC2 virtual chines, simulating up to 500,000 users.

7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev @StorecoinDev · Jun 20, 2019
Replying to @StorecoinDev
2/ They implemented the Algorand consensus algorithm (dl.acm.org/citation.cfm?i…) to evaluate its performance on 1,000 Amazon EC2 virtual machines, simulating up to 500,000 users.

StorecoinDev
@StorecoinDev

3/ Experimental results show that Algorand confirms transactions in under a minute and achieves 125 × Bitcoin's throughput.

7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

4/ In this thread we share practical security implications of Algorand's consensus algorithm based on our analysis.

7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

5/ The core of Algorand uses a Byzantine eement protocol called BA that scales to many rs and is fork-free.

7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

lying to @StorecoinDev

hese properties are similar to Storecoin's own ckFin consensus algorithm search.storecoin.com/blockfin), so it is interesting ompare the security properties of the two.

7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

7/ A key technique in BA is the use of verifiable random functions (VRFs) to randomly select users in a private and non-interactive way. The randomly chosen user proposes the new block.

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

8/ Then a small set of representatives are chosen randomly from the total set of users to form a committee. The proposed block is approved if the committee votes with > 2/3 majority. This threshold itself is a protocol defined parameter and their experiment uses a value of 80%.

7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

lying to @StorecoinDev

'his means, the proposed block is approved by a ımittee with a constant membership size, spective of the total number of users. In other 'ds, network size doesn't matter.

7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

10/ A large number of nodes sounds impressive, but doesn't affect the block approval speed because of the fixed size committee.

7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

11/ This also means, Byzantine tolerance is scoped to the committee. If the committee size is 1,000 and the threshold is 80%, the block is approved as long than > 800 users vote for it.

7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

lying to @StorecoinDev

The BA protocol is designed to scale to millions
isers, as per Algorand's white paper. The
bability of finding 200+ Byzantine actors in a
dom of sample of 1,000 increases as the total
nber of users increases.

Algorand faces three challenges. First, Algorand must
oid Sybil attacks, where an adversary creates many
udonyms to influence the Byzantine agreement protocol.
cond, *BA★* must scale to millions of users, which is far
her than the scale at which state-of-the-art Byzantine
eement protocols operate. Finally, Algorand must be re-

7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

13/ While their Sybil protection with assigning weights to users based on the balance in their accounts serves that purpose, it doesn't address collusion among malicious actors.

2 7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

14/ If sufficient number of users with more than 1/3 of the total money collude, they can approve chain forks or double spending.

1 7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

lying to @StorecoinDev

The probability of the above happening eases as more number of users exist in the work or a population of users controls large centage of the total money.

7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

16/ The committee selection process is based on the users' weights, which may result in users with large account balances getting selected more often. This in turn incentivizes them to act maliciously, especially if they control more than 2/3 of the total money.

sages, which allows them to learn the agreed-upon block. *BA*★ chooses committee members randomly among all users based on the users' weights. This allows Algorand to ensure that a sufficient fraction of committee members are honest. However, relying on a committee creates the possibility of

2 7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

Of course, malicious behaviors result in slashing, the point is that the protocol, by itself, doesn't courage or prevent such behaviors. External sequences like slashing must be used for ierence to protocol rules.

7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

lying to @StorecoinDev

"Strong synchrony" is challenging to achieve in real world environments where nodes (users) are distributed geographically across the globe. A committee of 1,000 users need 950 or more them to be reachable within a known timeout, which is a tall order in real world scenarios.

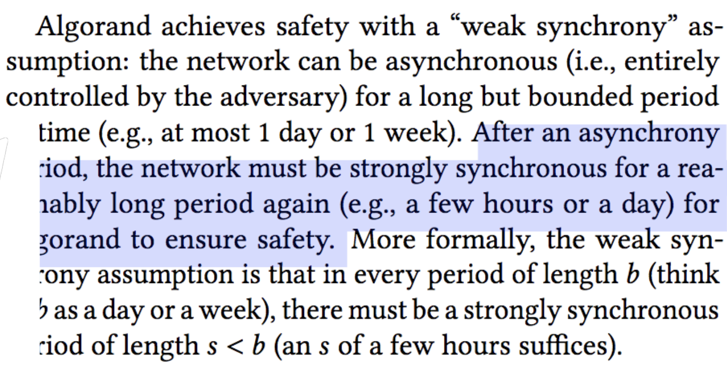
To achieve liveness, Algorand makes a "strong synchrony" assumption that most honest users (e.g., 95%) can send messages that will be received by most other honest users (e.g., 95%) within a known time bound. This assumption allows the adversary to control the network of a few honest users, but does not allow the adversary to manipulate the network at a large scale, and does not allow network partitions.

1 7:02 PM - Jun 20, 2019

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

19/ If the committee cannot agree on the block, the process is repeated with no guarantees of success the next time. The safety is guaranteed only if there is a period of "strong synchrony" of sufficient length, which again, it hard to guarantee in real world scenarios.


Algorand achieves safety with a "weak synchrony" assumption: the network can be asynchronous (i.e., entirely controlled by the adversary) for a long but bounded period time (e.g., at most 1 day or 1 week). After an asynchrony riod, the network must be strongly synchronous for a reanably long period again (e.g., a few hours or a day) for gorand to ensure safety. More formally, the weak synrony assumption is that in every period of length b (think b as a day or a week), there must be a strongly synchronous riod of length $s < b$ (an s of a few hours suffices).

7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

lying to @StorecoinDev

When a committee is elected their network characteristics are unknown. The necessary quorum may not be reached if the required number of users are not online or have poor connectivity.

2 7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

surface sooner or later.

3 7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

22/ If there is an economic incentive to cheat, people do cheat as long as the reward eclipses the penalty. The problem with distributed computing problems or icious behaviors due to economic incentives is : it is hard to model them and they show up in xpected places.

2 7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

lying to @StorecoinDev

BlockFin attempts to avoid some of these pitfalls s design. It doesn't assume strong synchrony. consensus rounds make progress without repeating the work at the speed of respective nodes.

1 7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

24/ There is no "waste" arising from new committees being formed, who repeatedly try to validate a

See StorecoinDev's other Tweets

StorecoinDev @StorecoinDev · Jun 20, 2019
Replying to @StorecoinDev
24/ There is no "waste" arising from new committees being formed, who repeatedly try to validate a proposed block, but couldn't do so because of poor synchrony.

StorecoinDev
@StorecoinDev

BlockFin extends Storecoin's "one entity, one
e" governance model to "one entity, one
nature" during consensus. The votes are not
ghed based on the users' account balance or
ke, but purely by their count.

2 7:02 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

So, one entity cannot accumulate
proportionately large sum of balance to own
disproportionately large percentage of votes or malicious entities pool their balances together to breach the BFT threshold.

7:05 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

nodes, but millions of nodes don't need to repeatedly do the same work to achieve decentralization.

7:05 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

28/ Equitable block reward incentive model -- all nodes share the block reward for all blocks they validated -- ensures there is no advantage in cheating the protocol rules.

7:05 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

29/ A node earns its share of the block reward only if it's up and running and performs its duties. It doesn't have to compete with other nodes in the consensus race.

7:05 PM - Jun 20, 2019

See StorecoinDev's other Tweets

StorecoinDev
@StorecoinDev

Replying to @StorecoinDev

30/ We want to highlight these protocol design decisions that don't typically get discussed, but they are as important in converging a large number of

See StorecoinDev's other Tweets

Share:

BACK TO NEWS

Get invited to our next Milestone Token Offering (MTO)

er your email

GET STARTED

KYC/AML checks are required for securities law compliance. This will be a Reg D and Reg S global offering.

DISCLAIMER

Nothing herein is intended to be an offer to sell or solicitation of offer to buy, Storecoin tokens or rights to receive Storecoin tokens in the future. In the event that Storecoin conducts an offering of Storecoin tokens (or rights to receive Storecoin tokens in the future), Storecoin will do so in compliance with all applicable laws which may include the Securities Act of 1933 and the rules and regulations promulgated thereunder, as well as applicable state and foreign law. Any offering for sale to US Persons