Algorand: BA*  
Neil Agarwal
In public ledger based cryptocurrencies, the question is:

WHICH BLOCK DO WE ADD NEXT???
The next block is decided through

Bitcoin

MINING
The next block is decided through Algorand VOTING
HOW?
BYZANTINE AGREEMENT
BYZANTINE AGREEMENT (BA*)

SCALABLE!

FAST!
Let’s break it down
Let’s start with the original Byzantine Agreement Protocol.
And repeat.
But what if you have 1 MILLION USERS??
But can’t the those committee members get targeted?
And again...
Cryptographic Sortition & Verifiable Random Function (VRF)
IN A SINGLE STEP...

1. Set up a COMMITTEE & VOTE
2. COUNT the VOTES
COUNTING THE VOTES

1. MESSAGE IS PROCESSED + VERIFIED
2. TALLIED UP

Otherwise, threshold
TIMEOUT
How does BA* work in ALGORAND?
What if we get stuck in binaryba?
The Common Coin
FINAL v. TENTATIVE

FINAL: BA*() will not reach consensus on any other block for that round

TENTATIVE: BA*() was unable to guarantee safety due to network asynchrony or malicious users
Committee Size

Tradeoff between bandwidth and protection against adversary
DISCUSSION
"In a **Sybil** attack, the attacker subverts the reputation system of a peer-to-peer network **by creating a large number of pseudonymous identities**, using them to gain a disproportionately large influence.” – Wikipedia

**HOW DOES ALGORAND PREVENT SYBIL ATTACKS?**
WHY IS BA* SCALABLE?
What can happen when a weighted fraction (greater than $\frac{1}{3}$) of users are malicious?
The end.