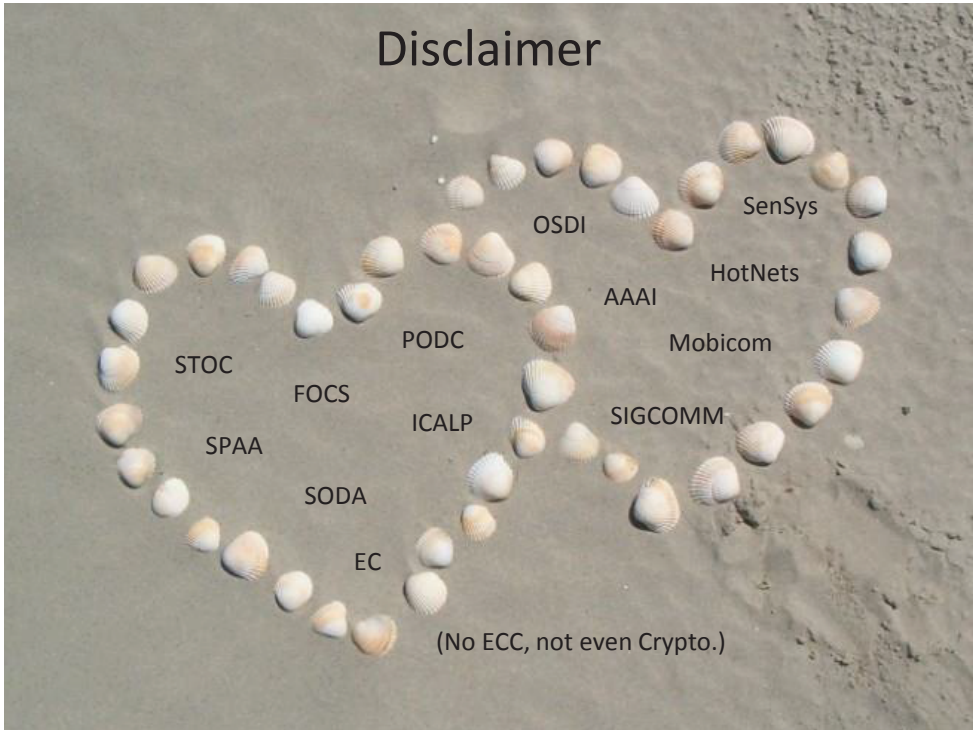
The Role of Cryptography in Distributed Systems

Roger Wattenhofer

ETH Zurich – Distributed Computing Group

Disclaimer



2008

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

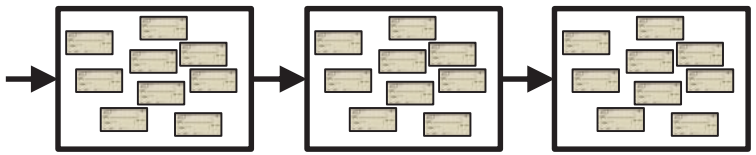
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort

Blockchain Basics

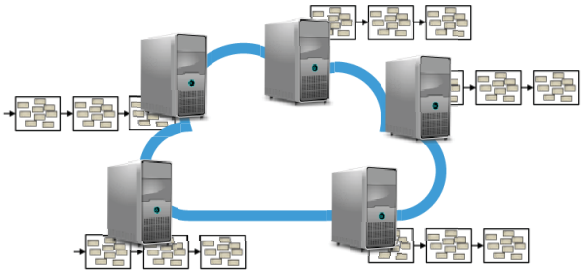
Transaction

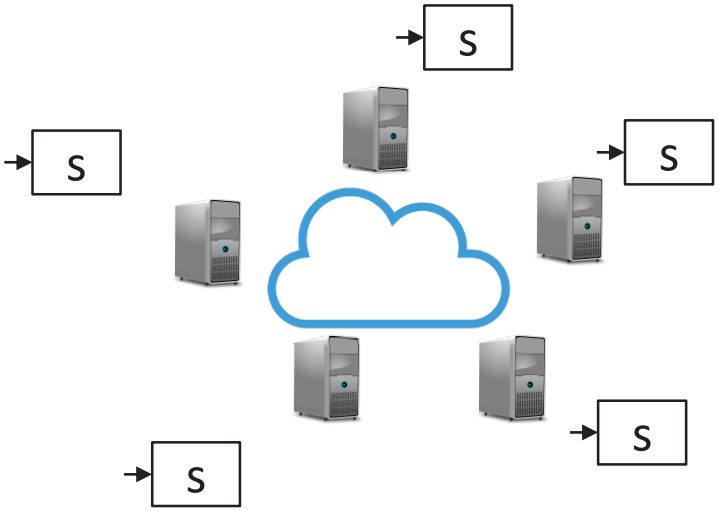
Block

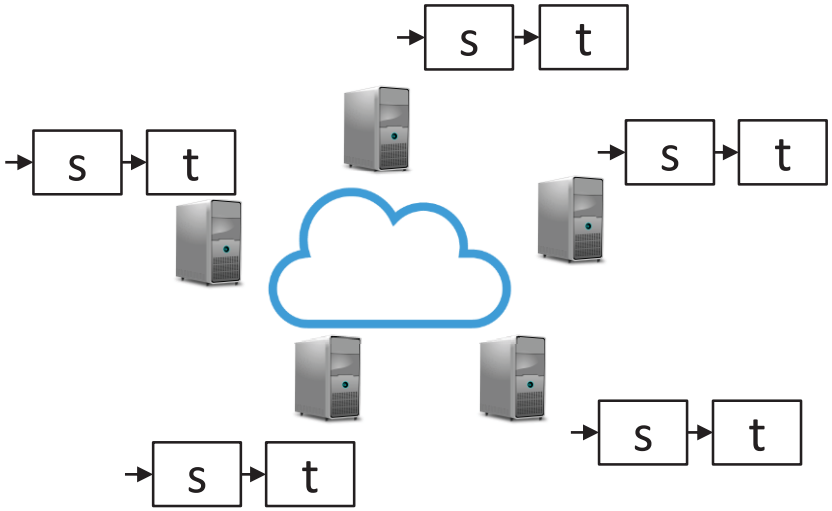
Blockchain

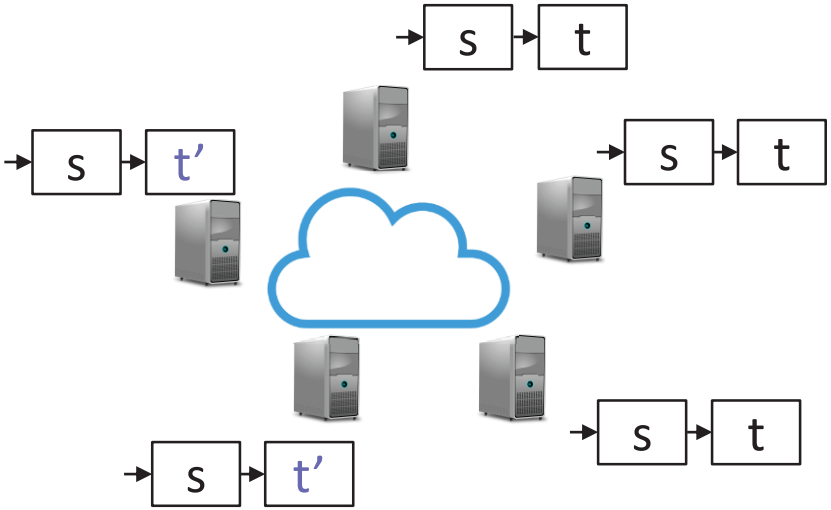


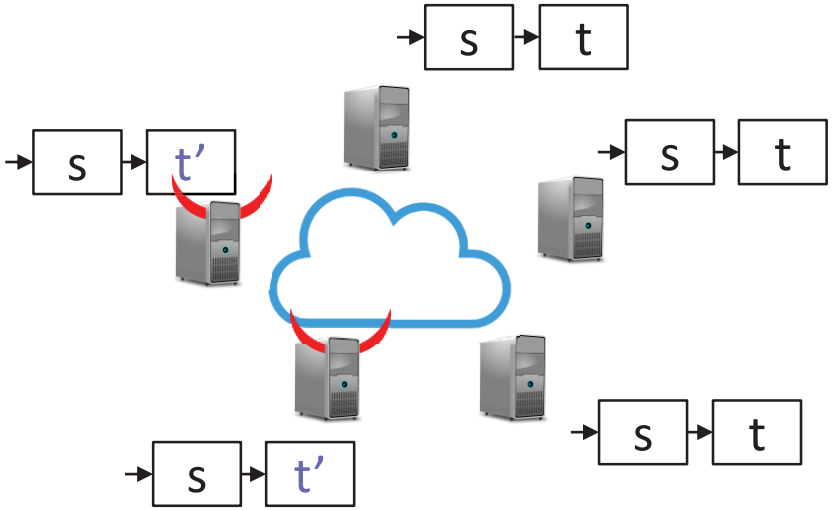
Blockchain is Replicated

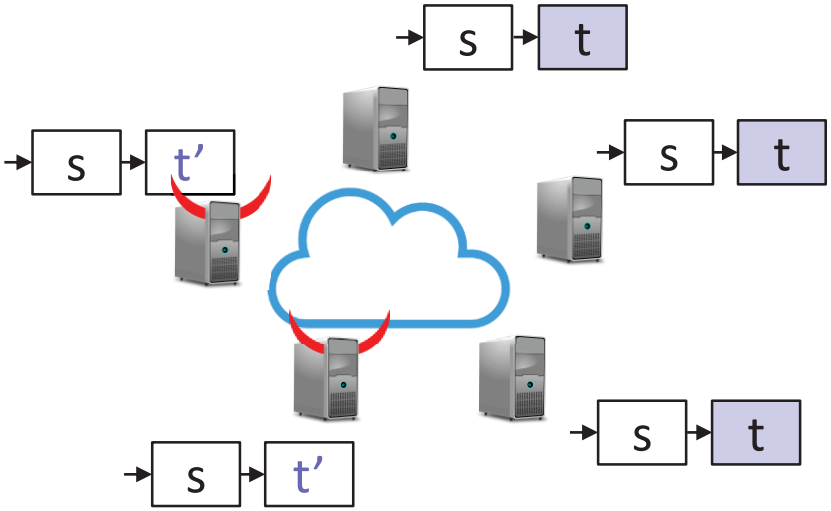



s
s
s
s
s


s
t
s
t
s
t
s
t
s
t

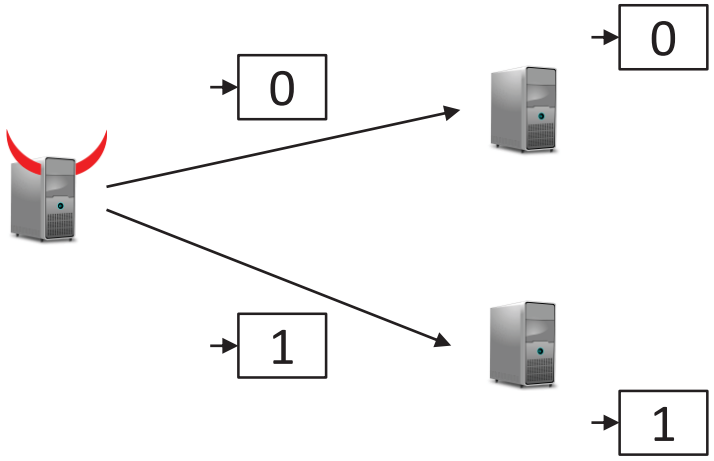

s
t
s
t'
s
t
s
t
s
t'


s
t
s
t'
s
t
s
t
s
t'

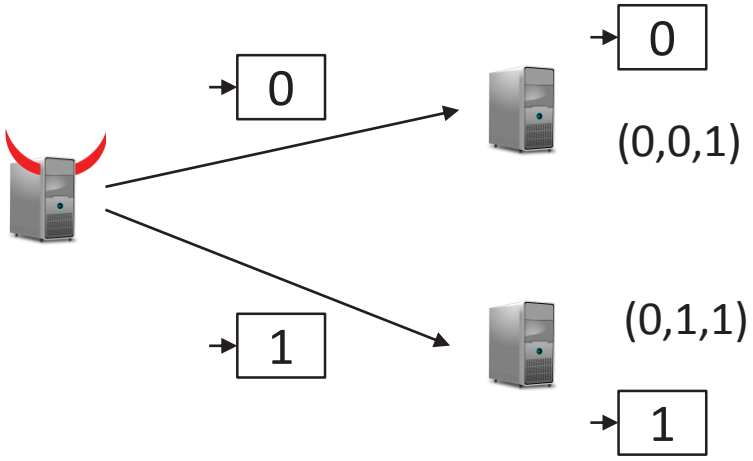


Fundamental Problem: Byzantine Agreement (Consensus)

3 nodes



3 nodes

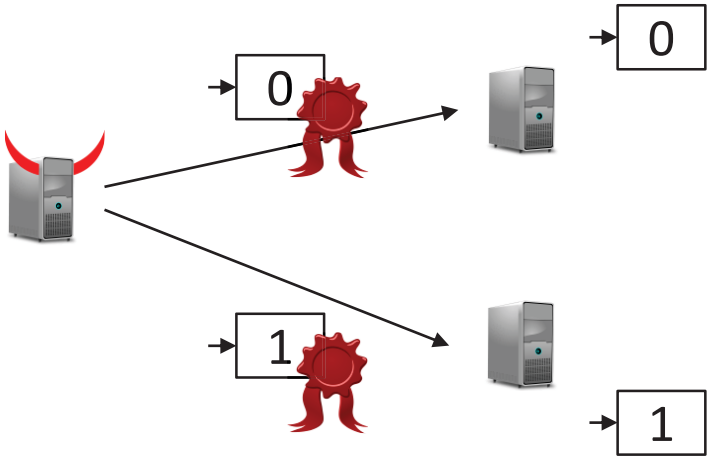


[Lamport, Shostak, Pease, 1982]

Byzantine Agreement
Impossible with 1/3 Baddies…

… unless we use Crypto!

3 nodes, signatures



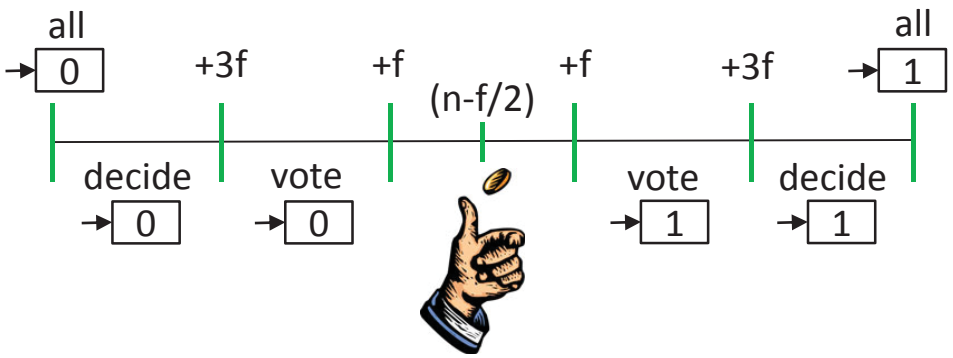
But Without Crypto?!

Voting Framework

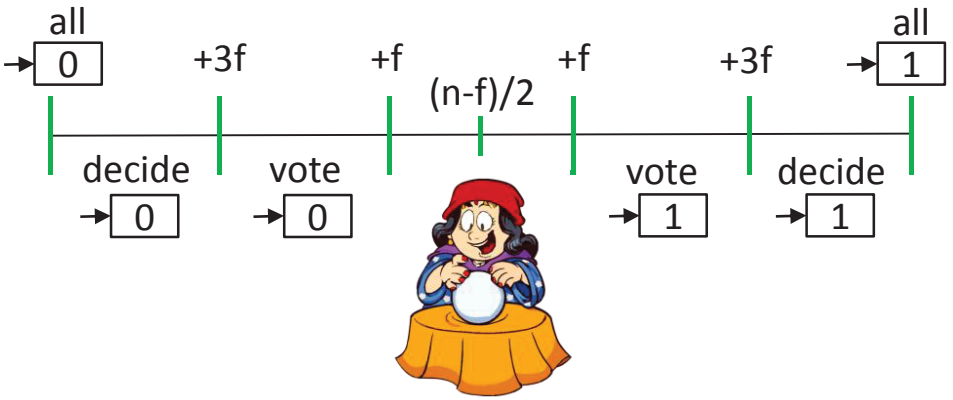
vote = input

send vote to all

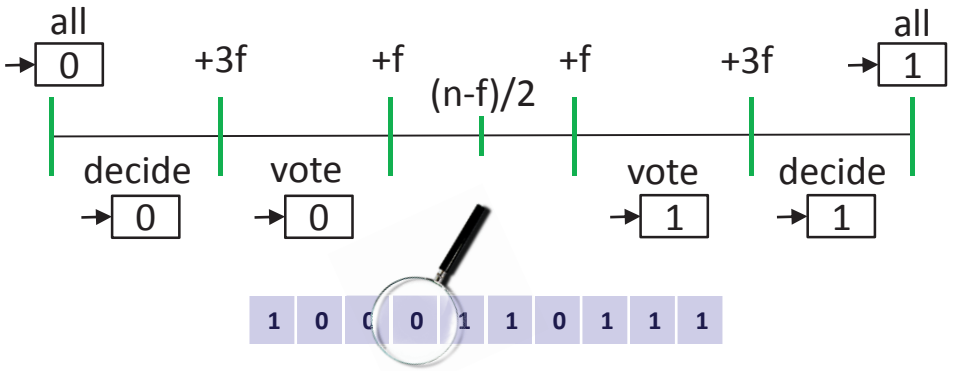
wait for n-f votes

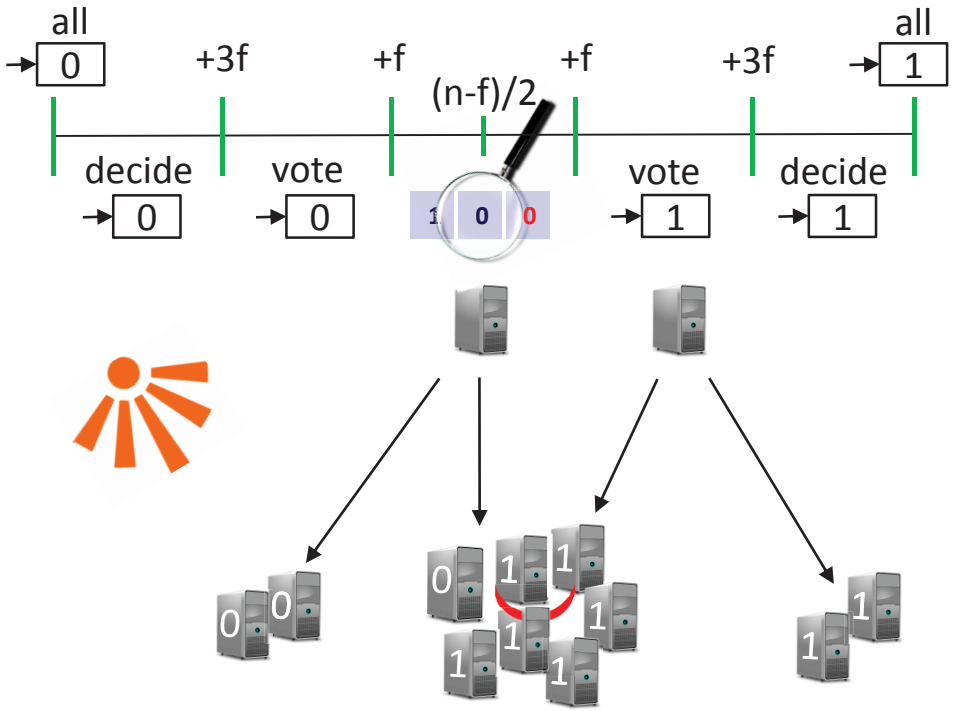


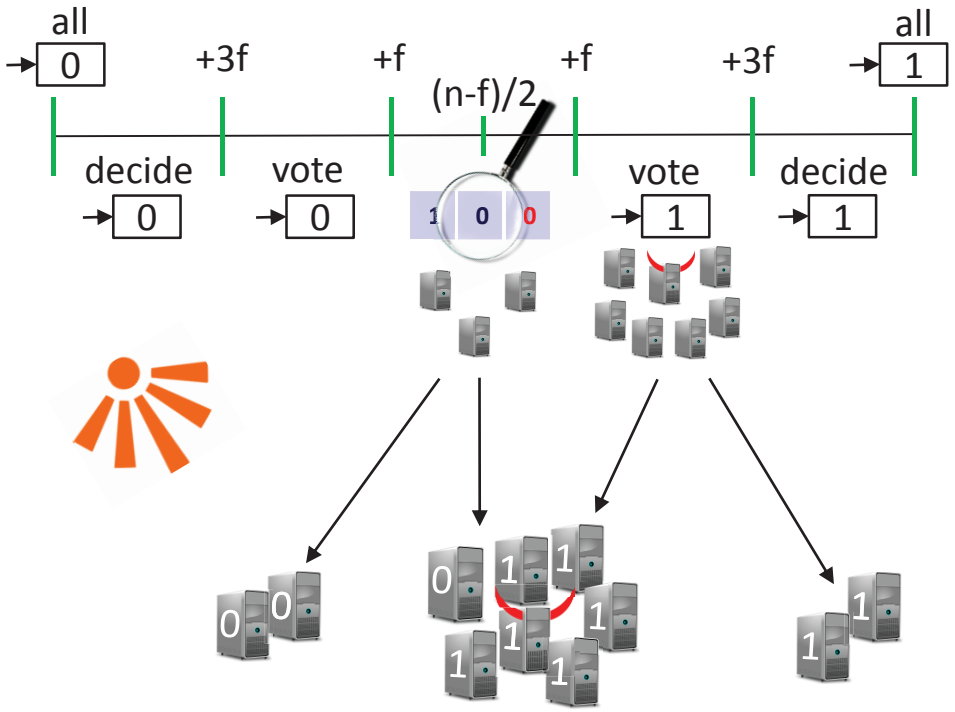
Voting Framework

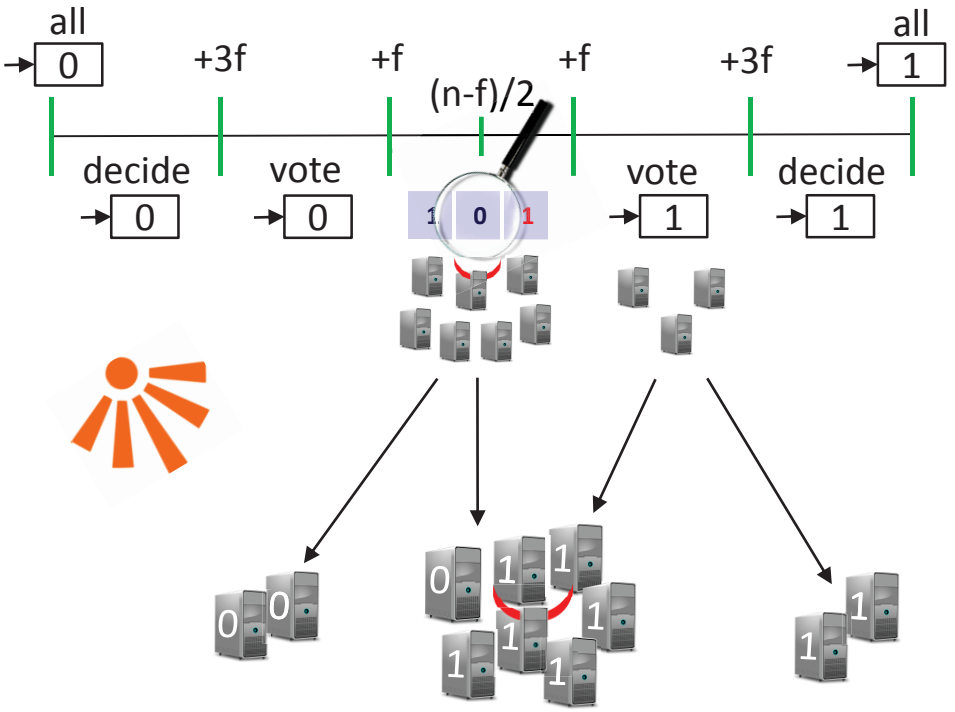


Voting Framework

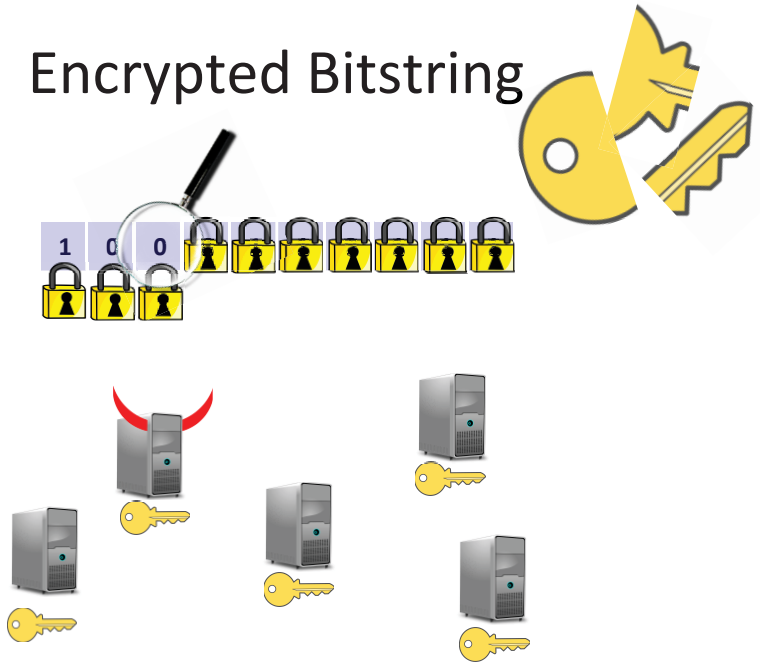


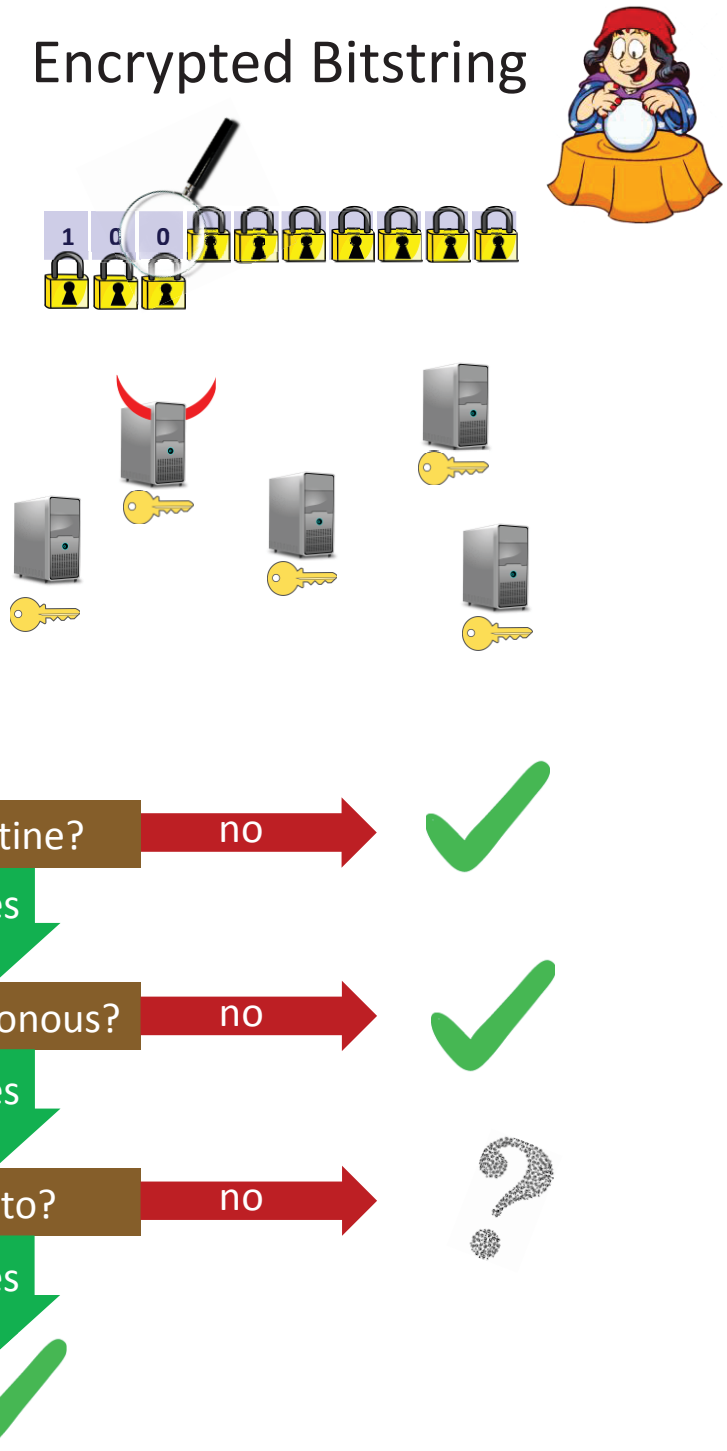






Boundary between
Crypto and No Crypto?

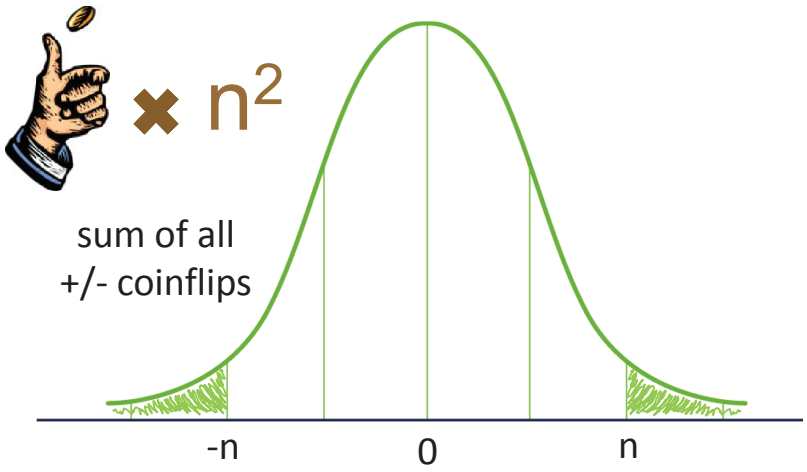




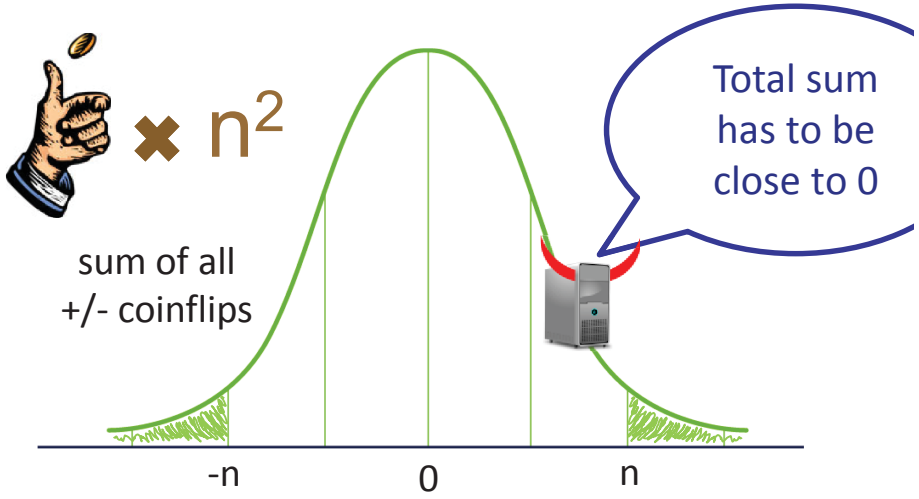
Overview

Challenge: Fast Byzantine Agreement Without Crypto

Detecting Byzantine nodes



Detecting Byzantine nodes



Detecting Byzantine nodes

+	+	-	-	-	+
+	+	-	+	-	-
-	-	-	+	+	+
+	+	+	-	-	-
+	+	+	-	-	-
-	-	+	+	+	-

[King & Saia, 2016]

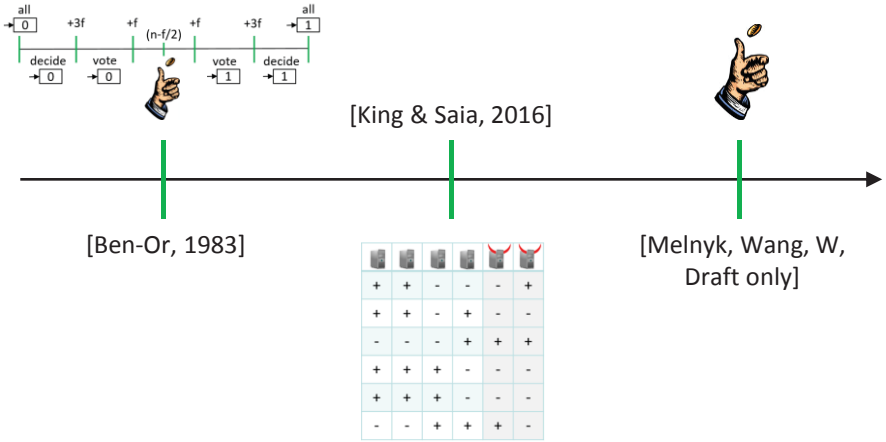
Detecting Byzantine nodes

Detecting Byzantine nodes

+	+	-	-	+	+
+	+	-	+	+	-
-	-	-	+	+	-
+	+		-	-	+
+	+		-	-	+
-	-			-	-

Or Rather...?

crypto? no



Fast Byzantine Agreement Without Crypto Still Open!

What is the Power of Crypto?

What is Crypto?