

# *The Role of Cryptography in Distributed Systems*



*Roger Wattenhofer*

# 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

JOHN DOE OR JANE DOE 123 MAIN STREET ANYTOWN, TN 01234 PHONE 555-1212	2670 87-823/641
Pay to the Order of _____	19 _____ \$ _____
<i>Bank of Yourtown</i> YOURTOWN, TN	Dollars  Security Details 6-73 on back
For _____	MP _____
⑆0 12345678⑆	⑆98765432⑆

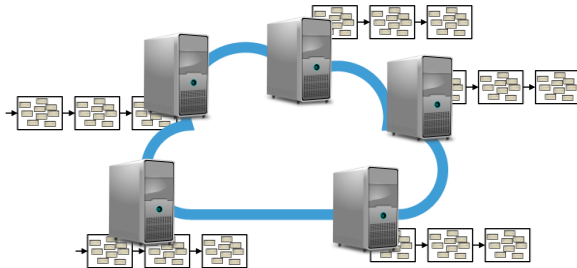
# Block



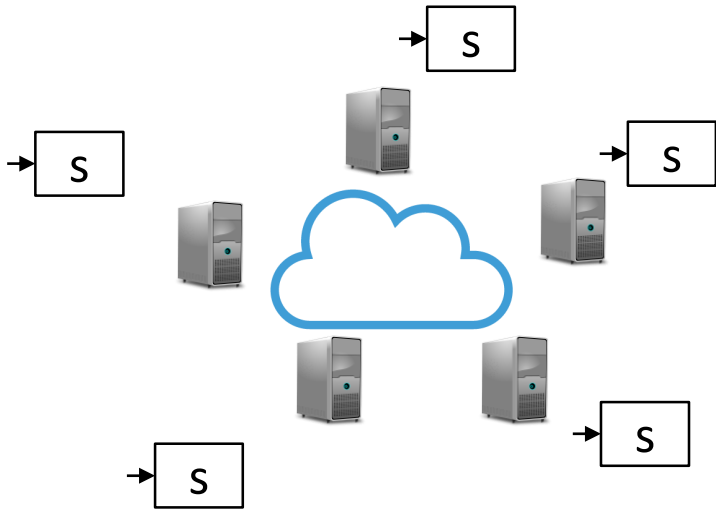
# Blockchain

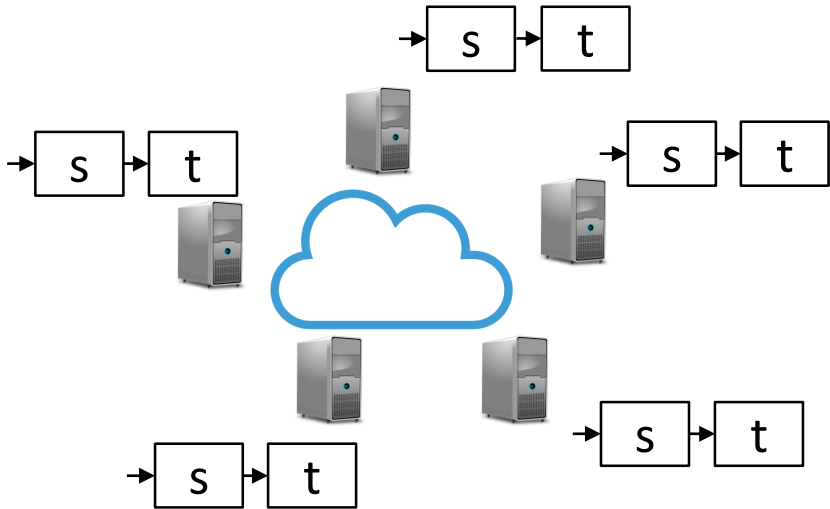


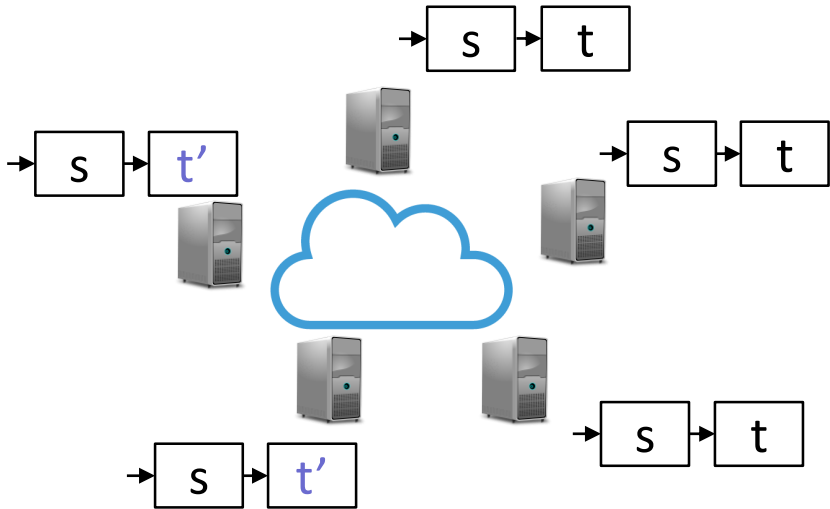
# Blockchain is Replicated

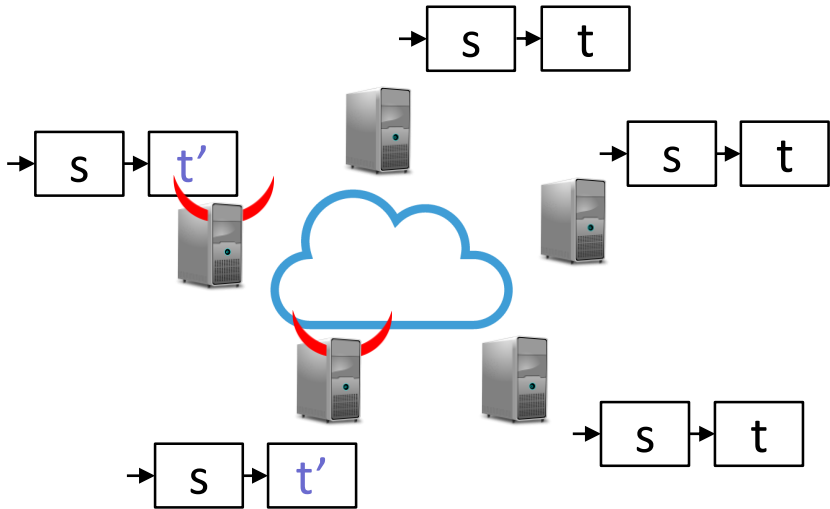


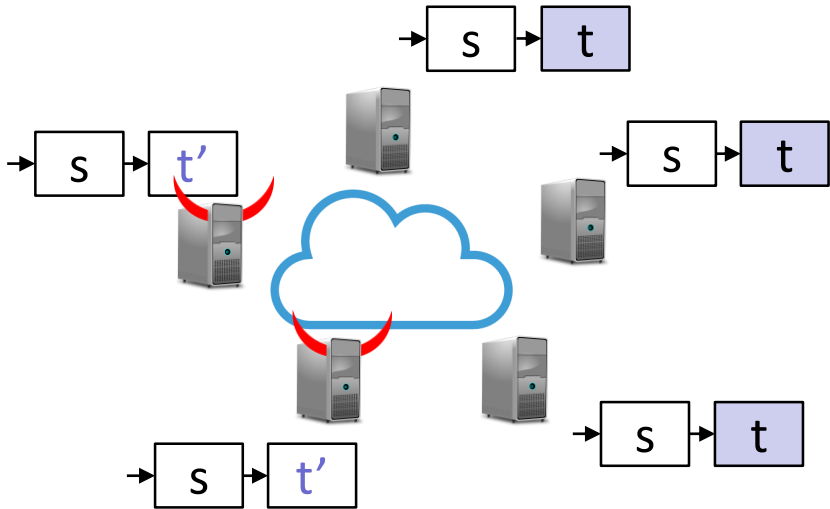






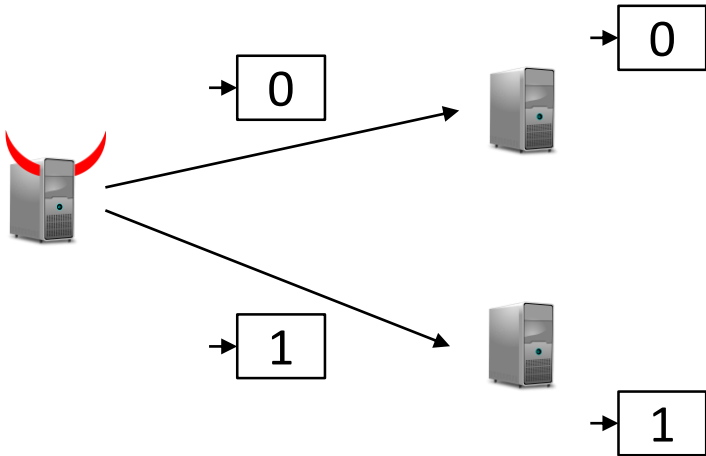




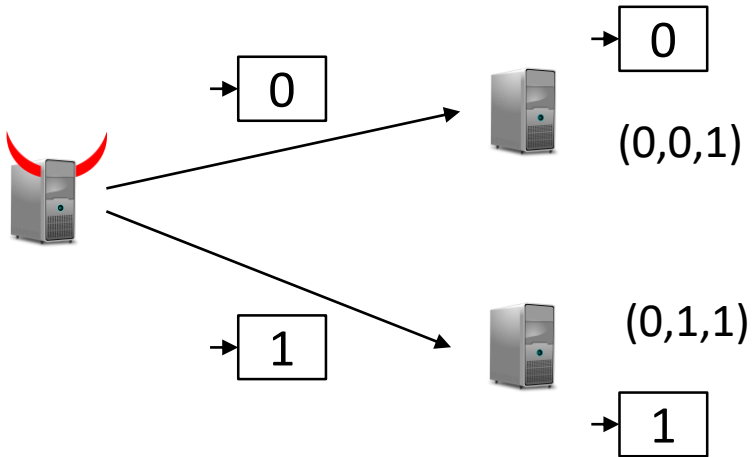


Fundamental Problem:  
Byzantine Agreement  
(Consensus)

# 3 nodes



# 3 nodes

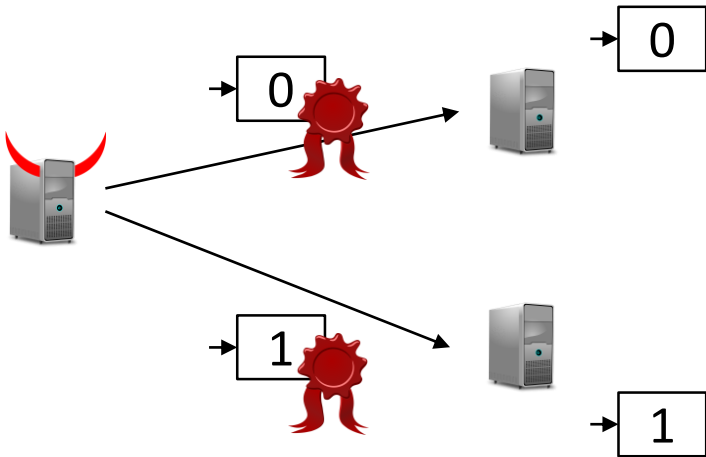




Byzantine Agreement  
Impossible with  $1/3$  Baddies...

... unless we use Crypto!

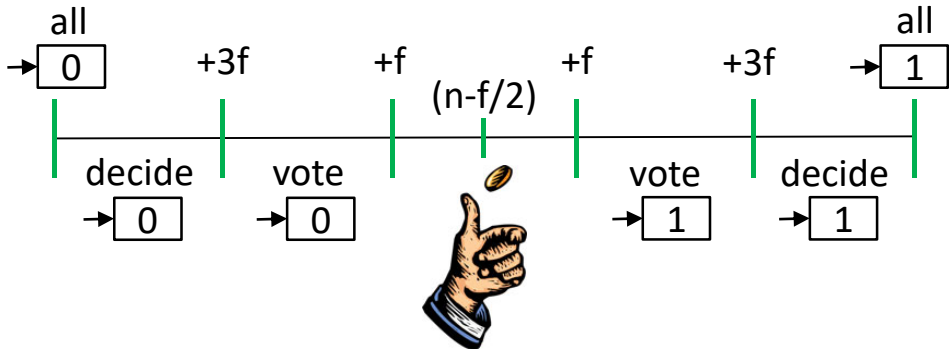
# 3 nodes, signatures



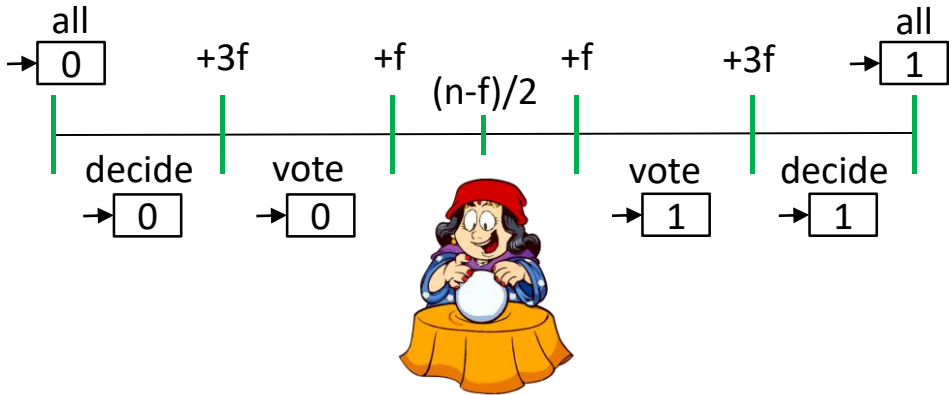
But Without Crypto?!

# Voting Framework

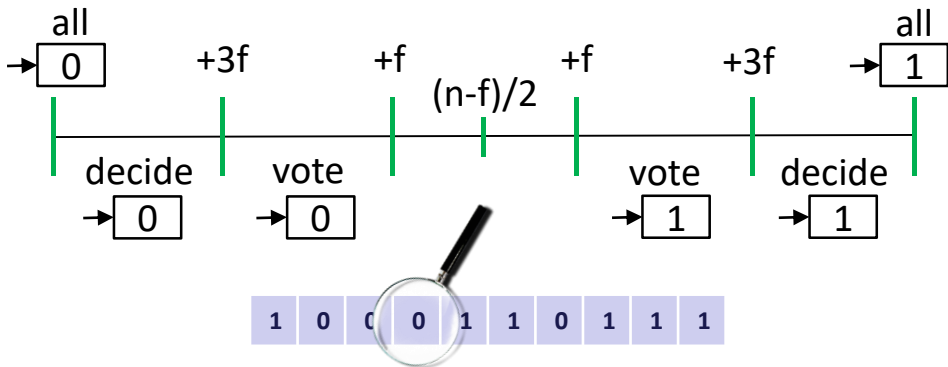
vote = input  
send vote to all  
wait for  $n-f$  votes

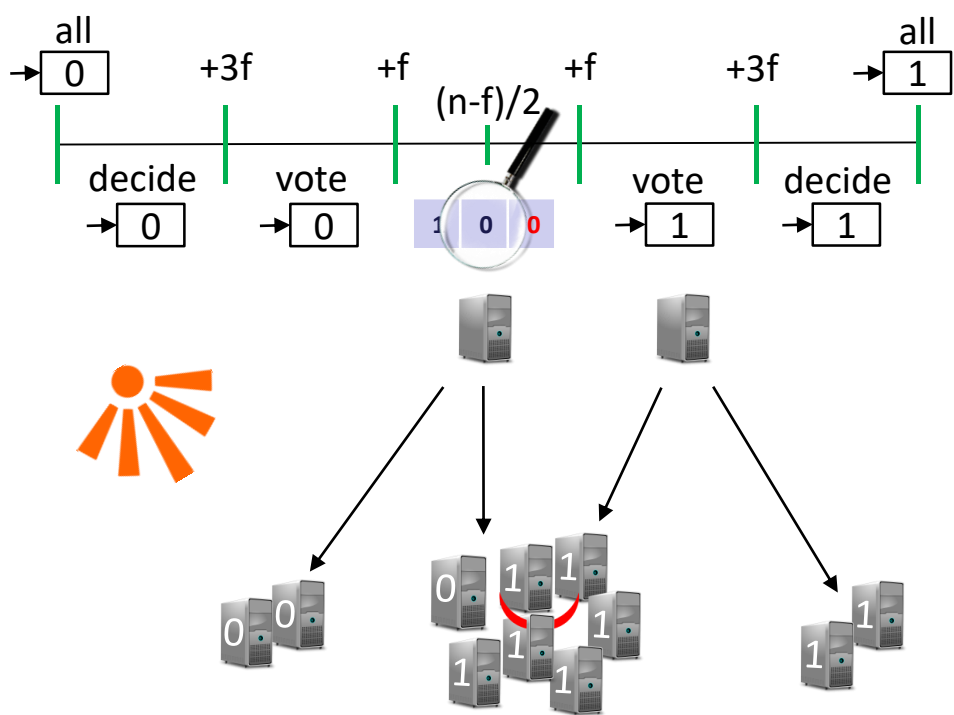


# Voting Framework

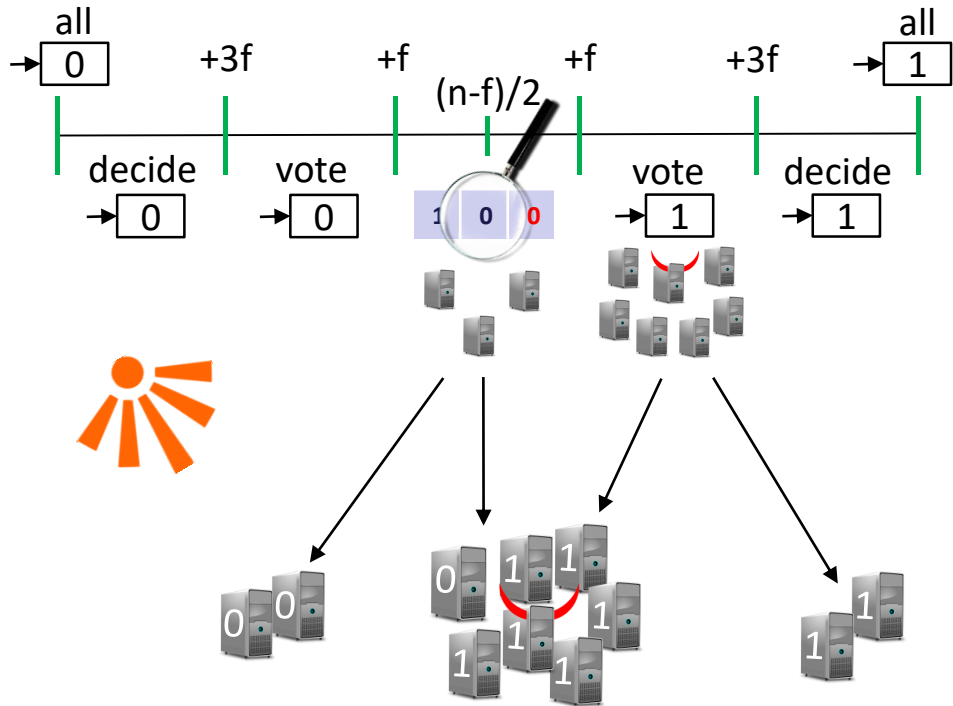


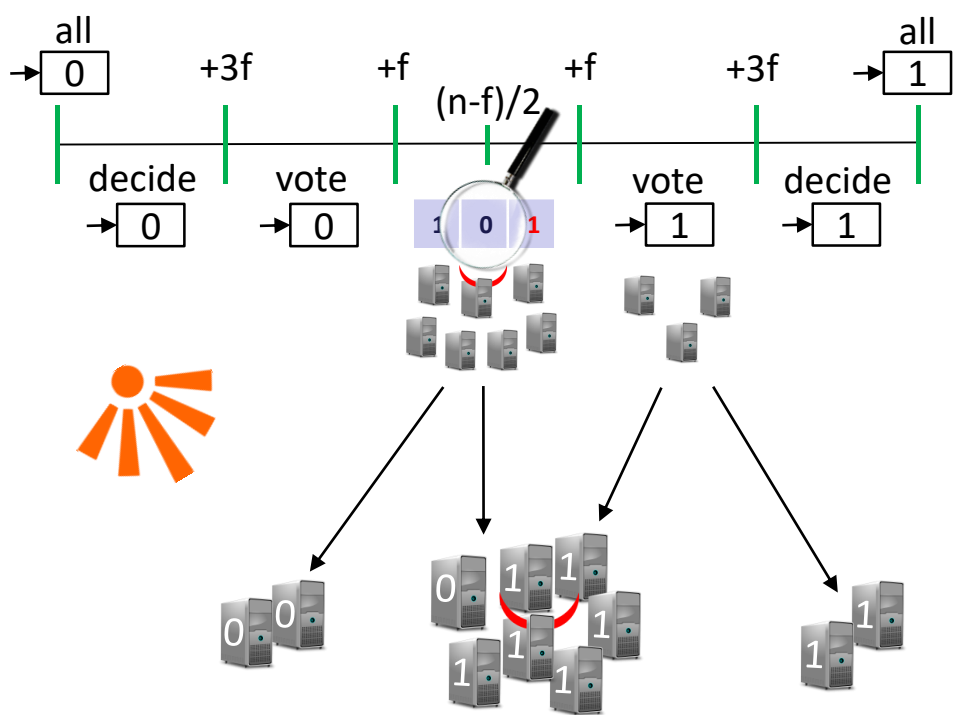
# Voting Framework





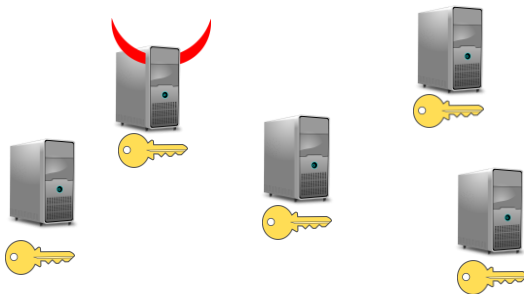
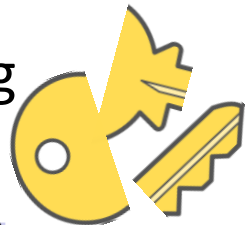
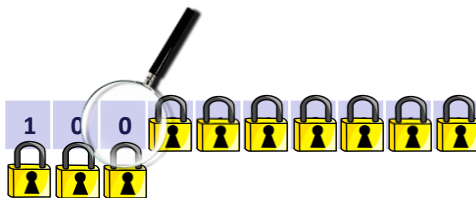




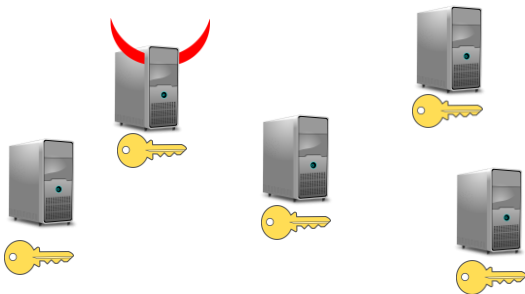


Boundary between  
Crypto and No Crypto?

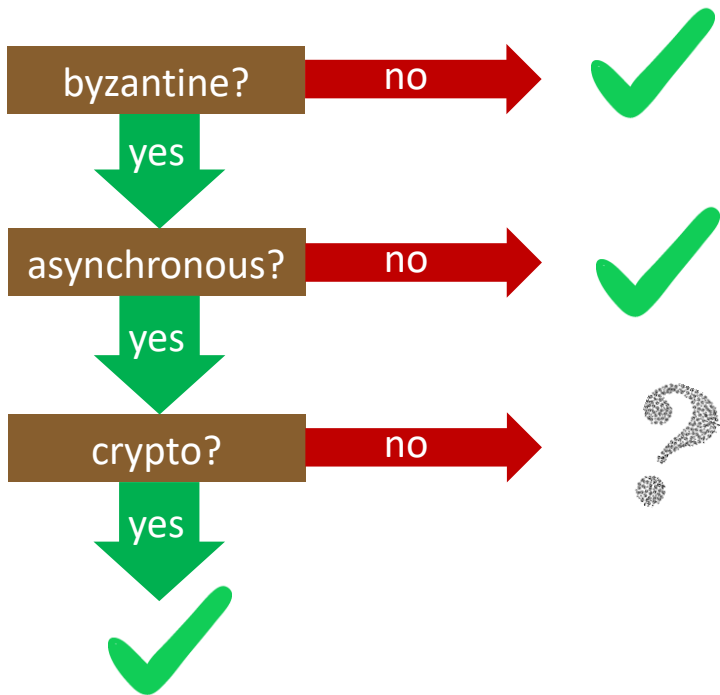
# Encrypted Bitstring



# Encrypted Bitstring



# Overview



# Challenge: Fast Byzantine Agreement Without Crypto

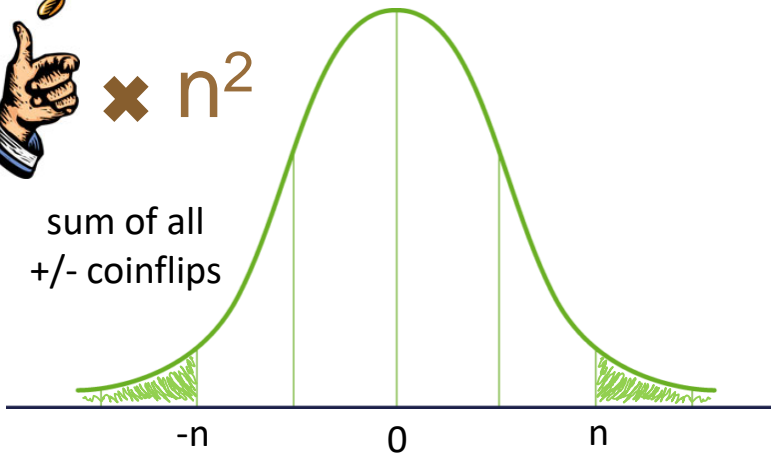


# Detecting Byzantine nodes



$$\times n^2$$

sum of all  
+/- coinflips

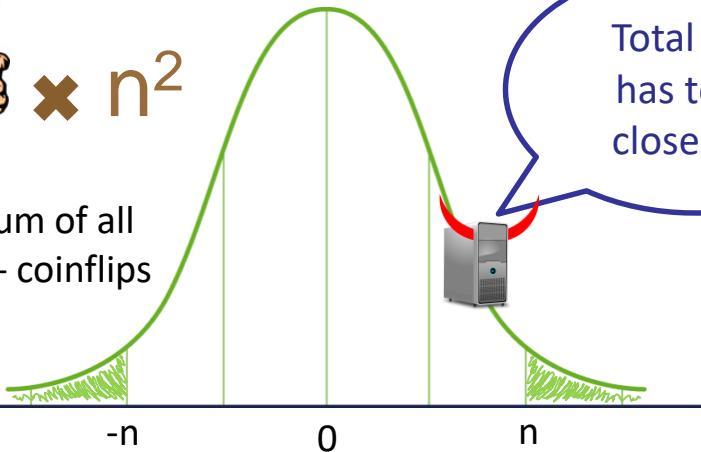


# Detecting Byzantine nodes









$\times n^2$

sum of all  
+/- coinflips



Total sum  
has to be  
close to 0







# Detecting Byzantine nodes

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

# Detecting Byzantine nodes



# Detecting Byzantine nodes

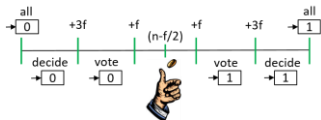
					
+	+	-	-	+	+
+	+	-	+	+	-
-	-	-	+	+	-
+	+		-	-	+
+	+		-	-	+
-	-			-	-

# Or Rather...?



crypto?

no



[King & Saia, 2016]



[Ben-Or, 1983]

[Melnyk, Wang, W,  
Draft only]

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

# Fast Byzantine Agreement Without Crypto Still Open!



What is the Power of Crypto?

What is Crypto?

# Thank You!

Questions & Comments?



Thanks to my co-authors  
Darya Melnyk, Yuyi Wang

[www.disco.ethz.ch](http://www.disco.ethz.ch)