Foundations of Blockchain Systems

Course: EE 595, Autumn 2020.

Instructor: Sreeram Kannan

University of Washington Seattle

Bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System

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

BITCOIN IS A CRYPTOCURRENCY

LAUNCHED IN JANUARY 2009

VERY SECURE: SAFETY AND LIVENESS

Why Blockchain – 1: The Evolutionary Argument

"Humans cooperate flexibly in large numbers" – Harari in Sapiens

Why Blockchain -2: The Economic Argument

Digital Commons = controlled by a few digital platforms (intermediaries)

2018

RANK	COMPANY		FOUNDED	USBn
1.		*	1976	890
2.	Google	*	1998	768
3.	Microsoft	*	1975	680
4.	amazon	*	1994	592
5.		*	2004	545
6.	Tencent 腾讯	*	1998	526
7.	BERKSHIRE HATHAWAY		1955	496
8.	Alibaba.com	*	1999	488
9.	Johnson & Johnson		1886	380
10.	J.P.Morgan		1871	375

2008

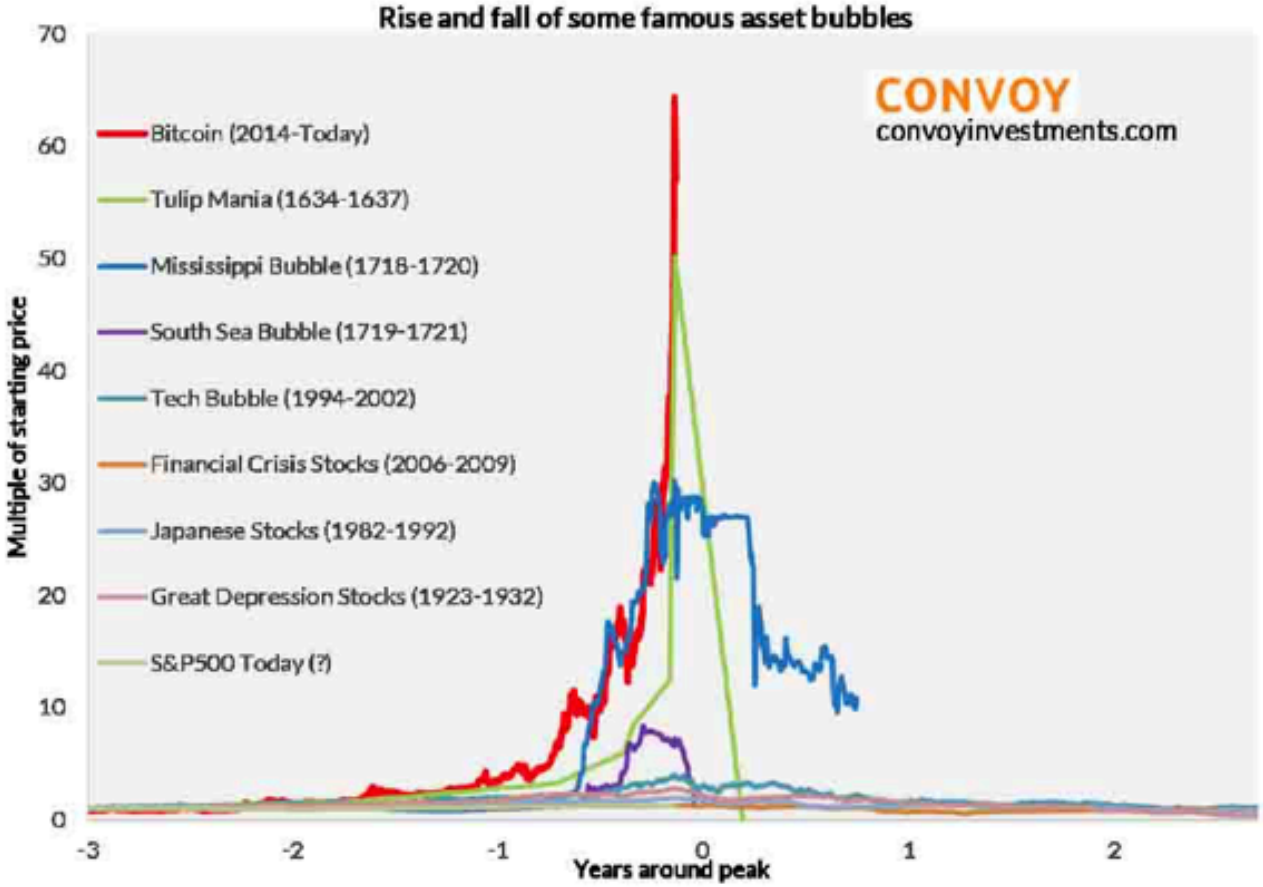
RANK	COMPANY	FOUNDED	USBn
1.	PetroChina	1999	728
2.	EXXON	1870	492
3.		1892	358
4.	中国移动 China Mobile	1997	344
5.	ICBC	1984	336
6.	GAZPROM	1989	332
7.	Microsoft	1975	313
8.		1907	266
9.	SINOPEC	2000	257
10.	AT&T	1885	238

Digital Intermediaries run the modern world

Digital intermediates *aggregate information* and do *market making*

Leading to *high centralization of power* in the AI era

Bitcoin is THE bubble of all time



Source: Elliot Wave International, Yale SOM, St. Louis FRED, GlobalFin, and Convoy analysis

Why Blockchain -3: The Technical Argument

Central role for theoretical design

Adversarial behavior requires security proofs

Central role for theoretical analysis

Randomness for symmetry breaking & unpredictability

Resource-dependent randomness – Proof-of-work, proof-of-space, proof-of-stake

Many ideas required

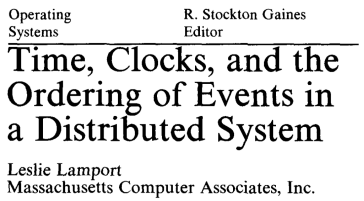
Information theory
Sharp threshold analysis
Typicality

Coding theory
Network coding
Distributed storage

Networking
P2P design

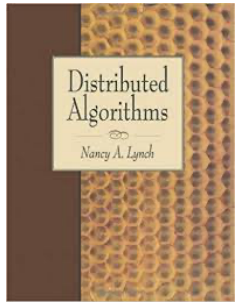
Game theory
Incentives

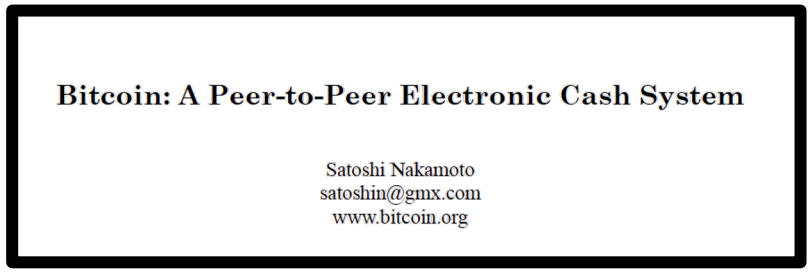
Distributed Computing -> Blockchain


Operating Systems
R. Stockton Gaines
Editor

Time, Clocks, and the Ordering of Events in a Distributed System

Leslie Lamport
Massachusetts Computer Associates, Inc.




Bitcoin: A Peer-to-Peer Electronic Cash System

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

Permissioned network
(*authorized* nodes)

Permissionless network
(*any* node)

IBM HYPERLEDGER

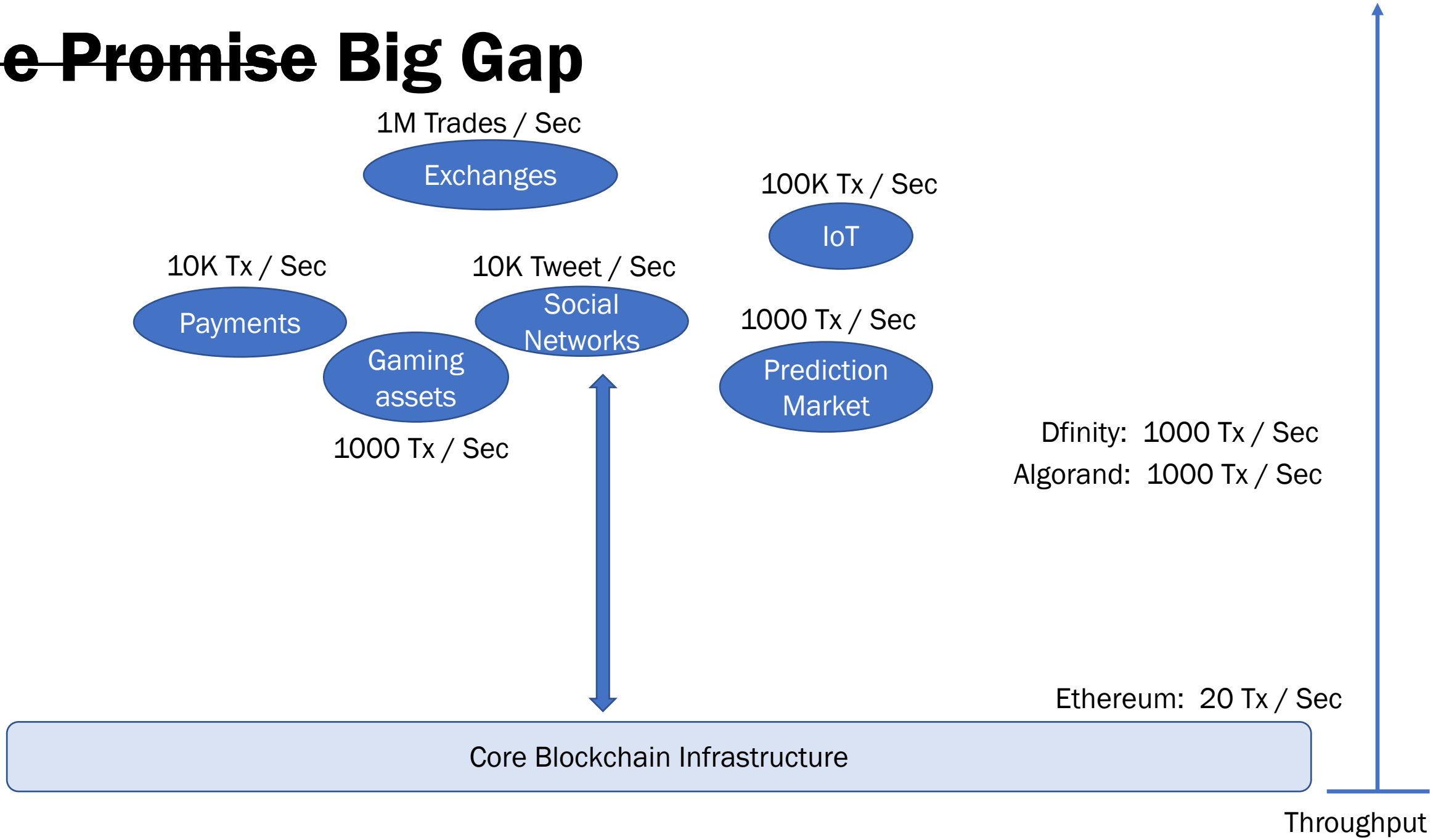
libra

ethereum

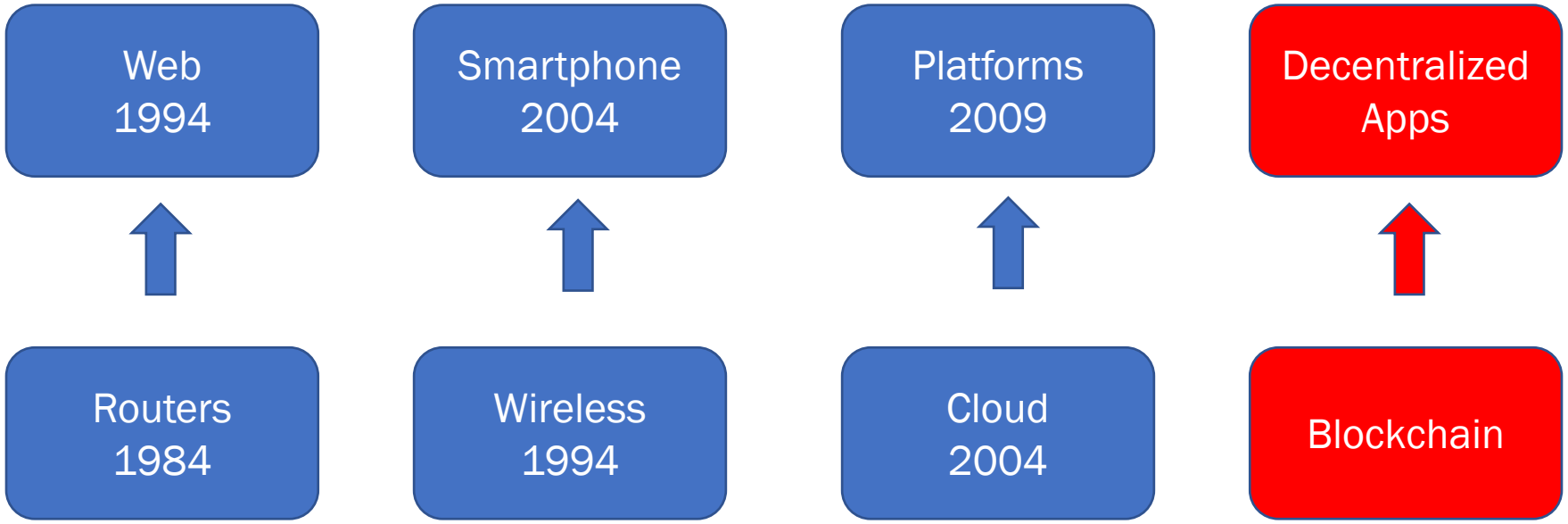
chia

Applications far beyond currencies
=> *Cooperate without digital intermediary*

~~The Promise~~ Big Gap



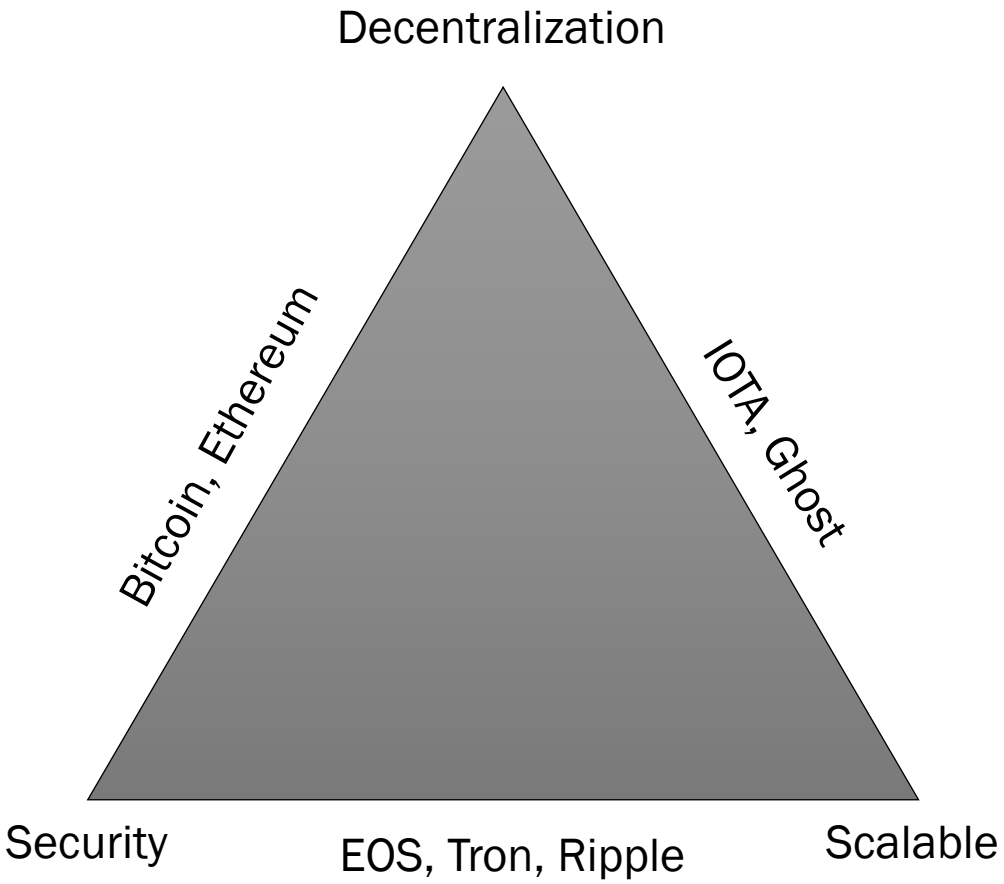
Infrastructure to applications



Blockchain Today

	Security	Latency	Energy Efficiency	Throughput
Bitcoin	✓ 50% adversary	✗ 3 hours	✗ ~Sweden	✗ 10 Tx/Sec
Desired	50% adversary	200 ms	No wastage	1 Million Tx/Sec

The blockchain trilemma



Principal challenge: Scalability

Solving Blockchain's Biggest Problem: 5 Projects Working On Scalability

August 23, 2018 By Jorn van Zwanenburg 1

Blockchain's Scaling Problem, Explained

Connor Blenkinsop AUG 22, 2018

7 Challenges That Need to be Addressed Before Blockchain Mass Adoption is Possible

Blockchain Scalability: The Issues, and Proposed Solutions

BitRewards Follow

Apr 25, 2018 · 4 min read

Consensus protocol mania

- Different security guarantees and decentralization
- How far can we go?

Layers of Blockchain

	Metrics	Ideas
Application	Decentralized finance	Game theory and Mechanism design
Sharding	Scale storage and compute	Codes for blockchain Resource allocation
Consensus	Security, throughput, latency, fairness	Protocol design Stochastic analysis
Peer2Peer	Optimize Latency and bandwidth	Network design for broadcast / multicast

Two distinct Lens: Adversarial & Rational

Two models

Adversarial

<50% of nodes are adversarial

Remaining honest nodes follow protocol

Rational

Each node acts on self-interest

Is the protocol a Nash-equilibrium?
Dominant strategy?
- Do we need to assume that the node colludes in only small coalition?