The Initiative for CryptoCurrencies and Contracts

Frontrunning in Crypto and NFT Trading on DeFi Exchanges

(Can Academic Research Enhance Fair Treatment for DeFi Operators and Users?)

Flash Memory Summit 2022

August 3, 2022

Who is IC3? What Do we Pursue?

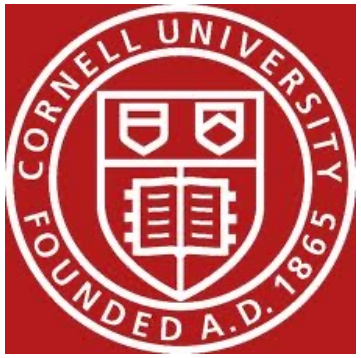
Faculty from 9 Universities + Industry & Foundation Stakeholders

1. World-class Research: Advancing the Science of Blockchains
2. Future-proofing Blockchains: Collaborating with IC3 Sponsors & the Community
3. Informing Public Policy Makers: Blockchain Limitations & Possibilities

The Initiative for CryptoCurrencies and Contracts

Andrew Miller

Eswar Prasad



Lorenzo Alvisi
Andrew Myers
Robbert Van Renesse

Sarah Meiklejohn

Srdjan Capkun

Christine Parlour

Dawn Song

Bryan Ford

Elaine Shi & Julia Fanti

Ari Juels, Rafael Pass
James Grimmelmann

Ittay Eyal

IC3 Partners and Donors

IC3 acknowledges and appreciates a generous gift from the VMware Foundation to advance the science and technology of blockchains.

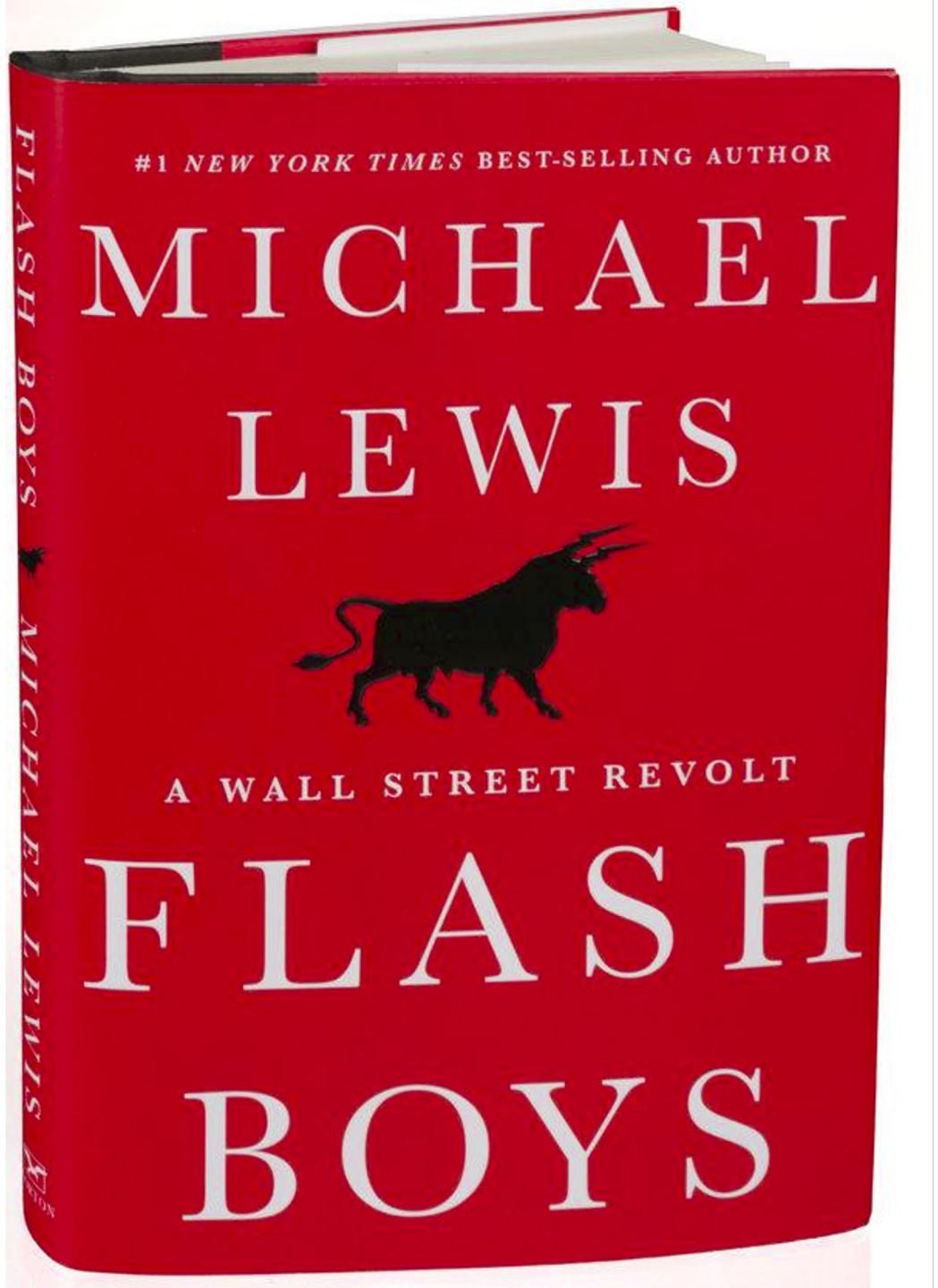
The Initiative for CryptoCurrencies and Contracts

IC3 Research: Driven by Grand Challenges

- **Secure Scaling and Performance**: Scaling up blockchains to handle intensive global workloads for both permissionless decentralized blockchains, and permissioned/consortium blockchains supporting >100,000 transactions/sec.
- **Correctness by Design and Construction**: Making it easy, and even automatic, for blockchain developers to produce secure protocols and code, by utilizing (1) programming language techniques to create correct code, and (2) cryptographic protocols with security proofs.
- **Confidentiality**: Combining transparency with confidentiality in blockchains, by utilizing (1) cryptographic techniques, as well as (2) trusted-hardware.
- **Authenticated Data Feeds**: Supporting a robust ecosystem of trustworthy data feeds for blockchains and contributing high-trust data feed solutions.
- **Safety and Compliance**: Enabling techniques and protocols for effective monitoring and targeted intervention in blockchains, informed by evaluations of traditional contract law and risks of crime in smart contracts.
- **Sound Migration**: Formulating practical migration paths to production blockchain deployments and enabling integration of new blockchain systems with legacy systems.
- **Social Good**: Applying cutting-edge blockchain technologies to pressing societal problems in order to illuminate overlooked technical needs and create impactful solutions.

IC3 DeFi Research Thrusts

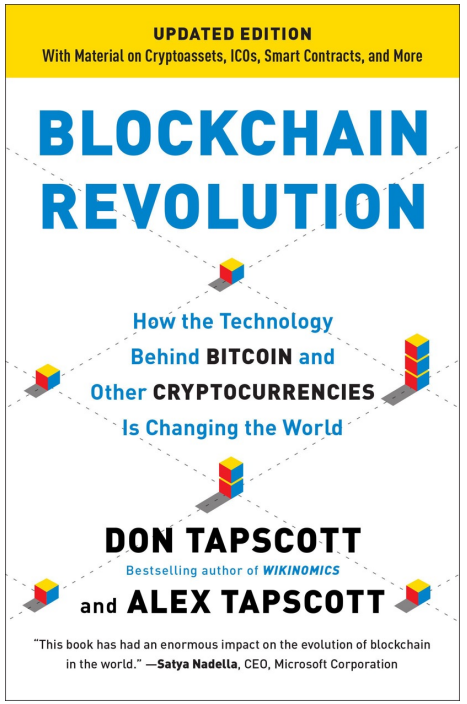
- Incentives (Dis-incentives), Cryptoeconomic Guarantees, Layer 1 and Layer 2 Solutions (e.g., Multi-party Computation 2.0)
- MEV Detection & Estimation & Mitigation/Prevention, Front/back-running, Transaction Editing/Censorship, etc. Is Fair Ordering Possible?
- Composing NEW & Reliable Financial Instruments: NFTs Drops, Fractionalizable NFT's, Multi-Party Flash Loans…
- Security and Decentralized Identity Solutions



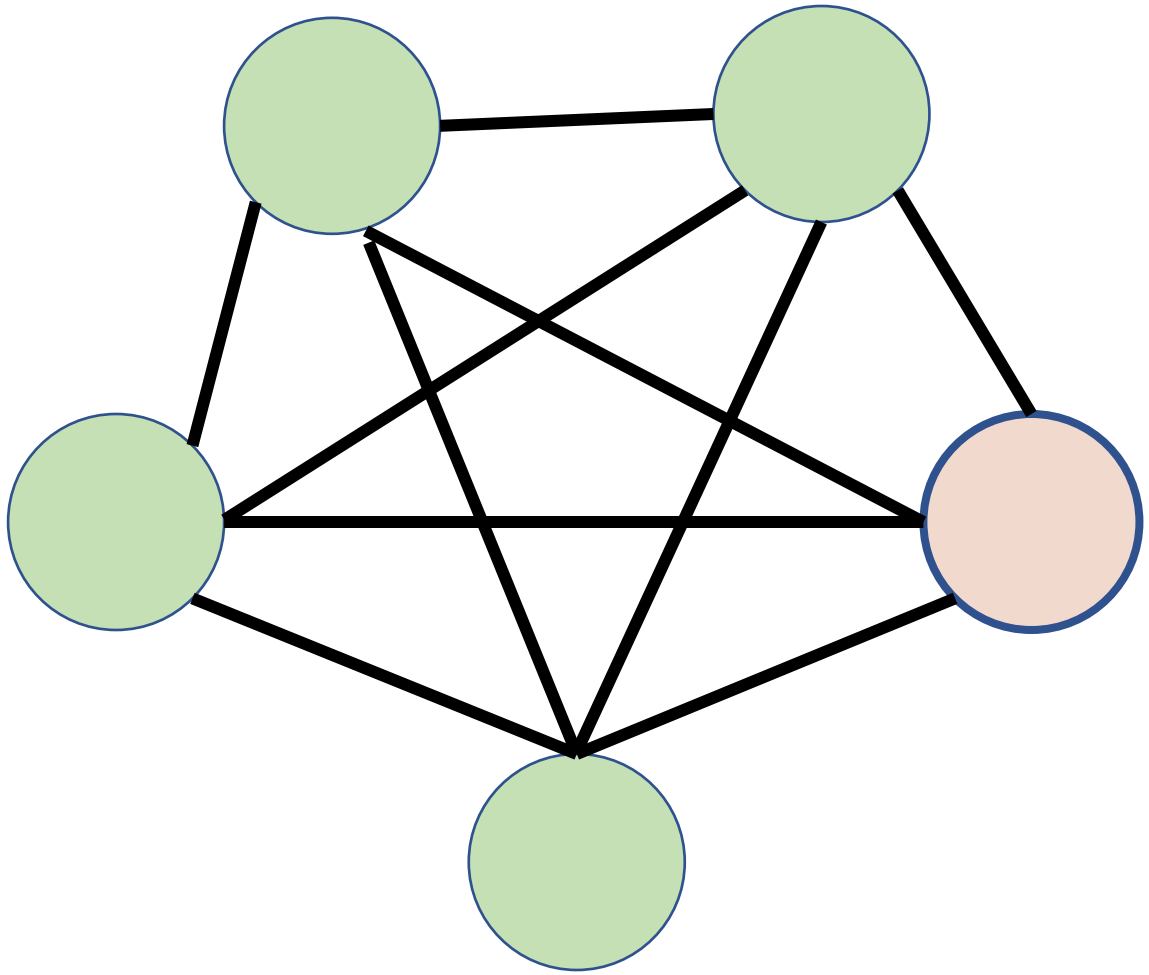
- 2014 exposé on *high-frequency trading*
- HFT characteristics:
  - Arbitrage bots / algorithms
  - Front-running
  - Big investment in low latency, i.e., *speed*
- Flurry of investigation and fines after Lewis book (FBI, SEC, etc.)
- Pros / cons of HFT heavily debated
- Strong case HFT is bad for consumers

Blockchains: This time it's different…

- Bitcoin born amid 2008 financial meltdown
- "A purely peer-to-peer version of electronic cash"
- *Blockchain Revolution*, 2017: "[Blockchains] can help build integrity into all our institutions and create a more secure and trustworthy world."

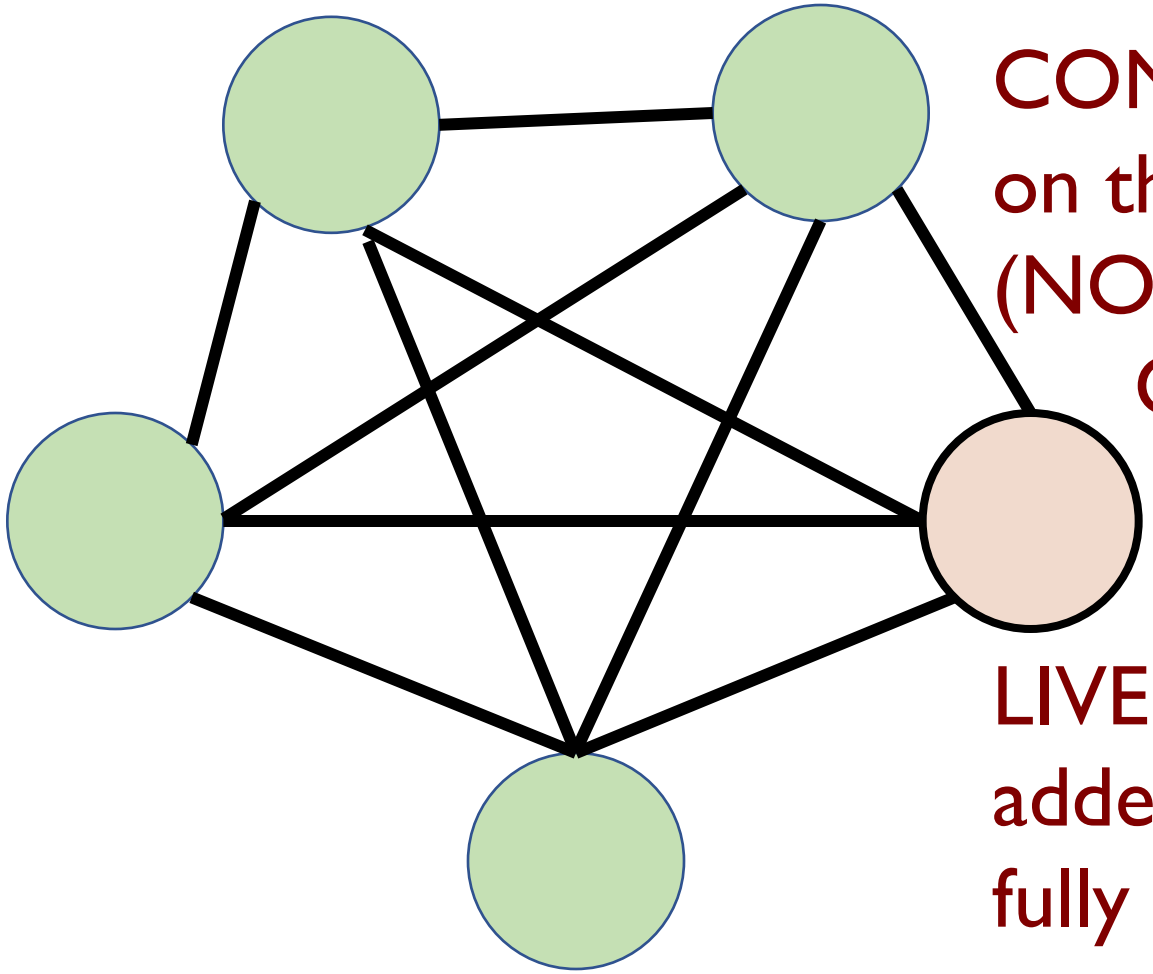


Byzantine Agreement



Goal: Set of nodes agree on a single message

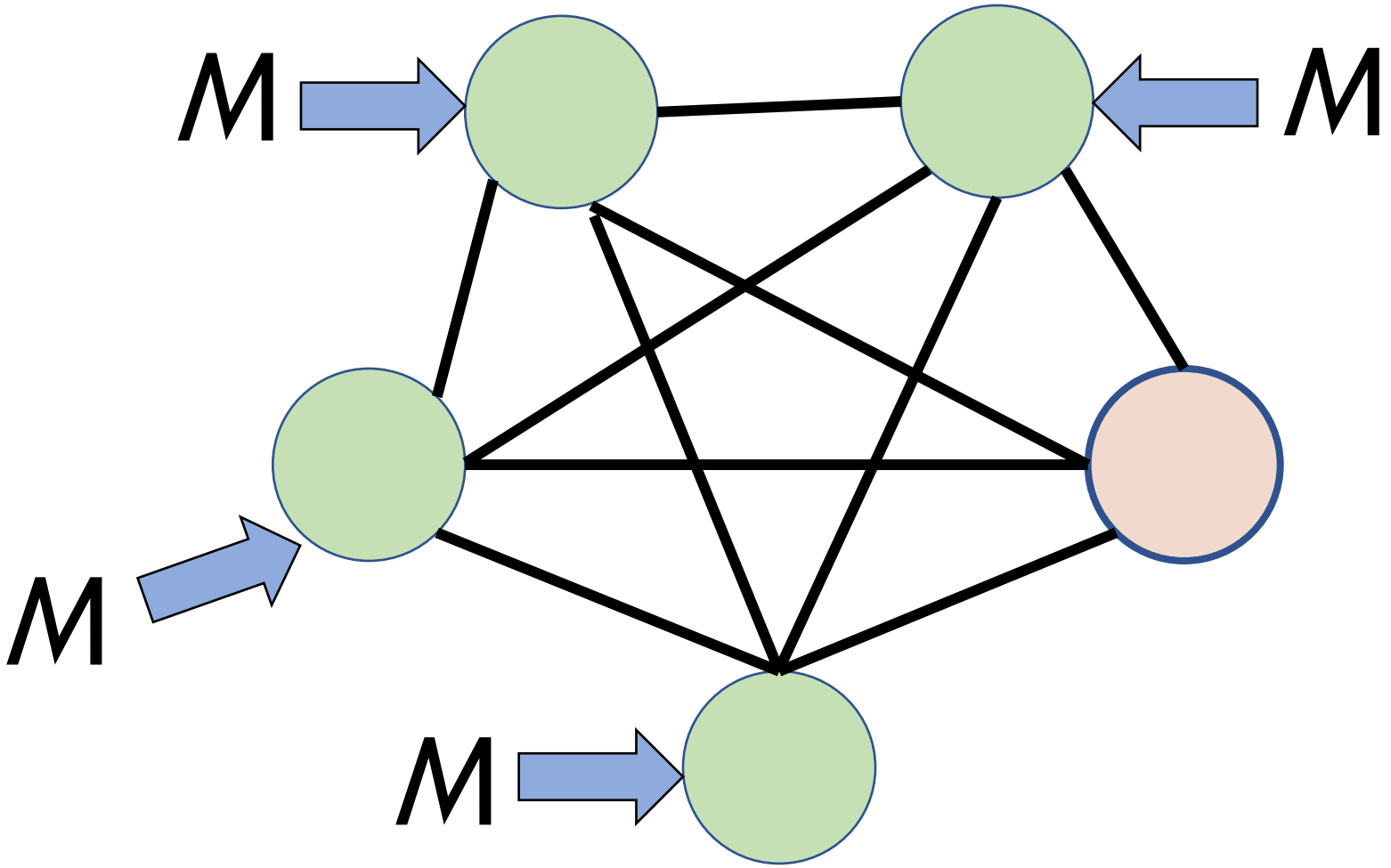
Validity (Byzantine Agreement)



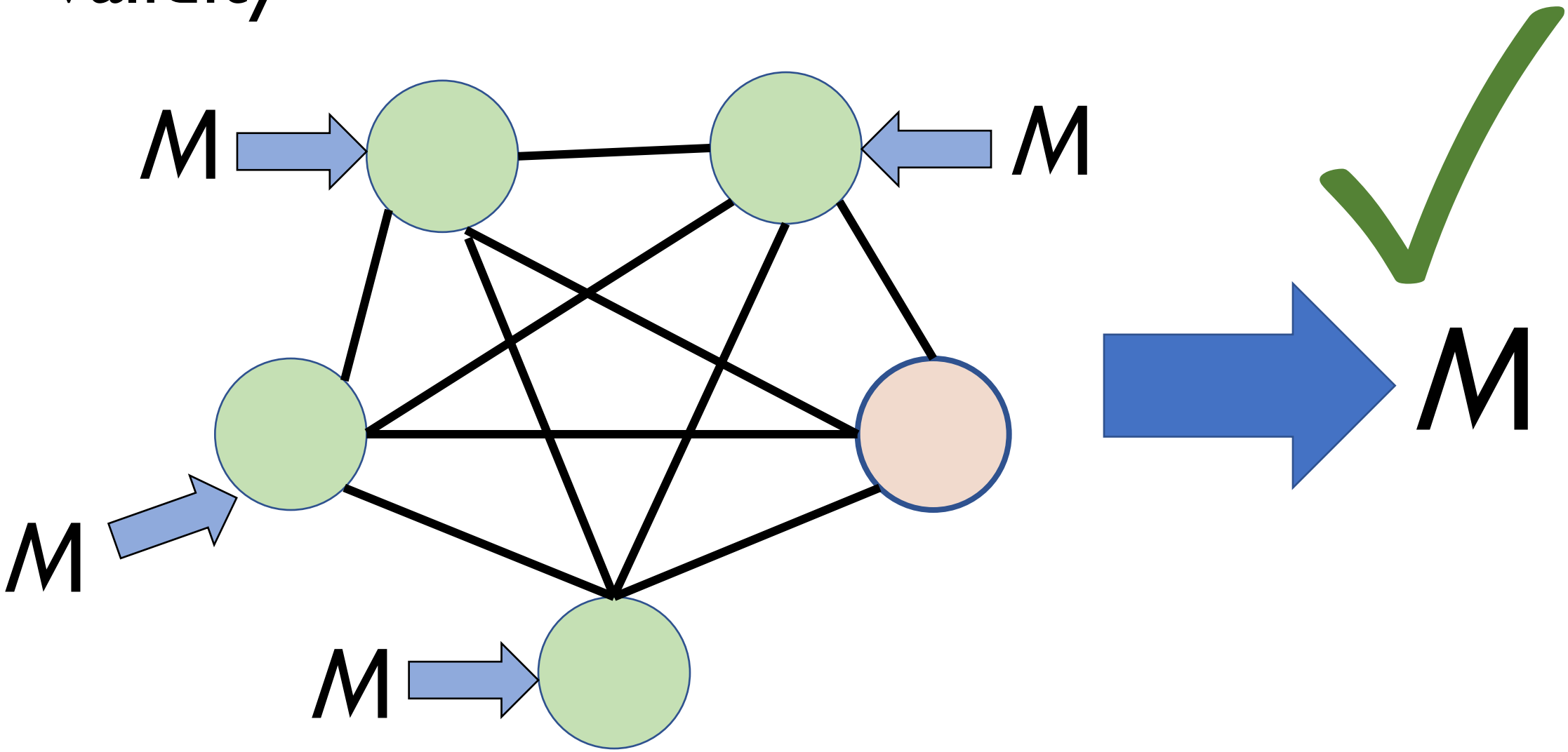
CONSISTENCY: Nodes agree on the transaction order (NO guarantee the order is fair. Order can be altered.)

LIVENESS: Transactions are added promptly, and hope-fully in order of their arrival.

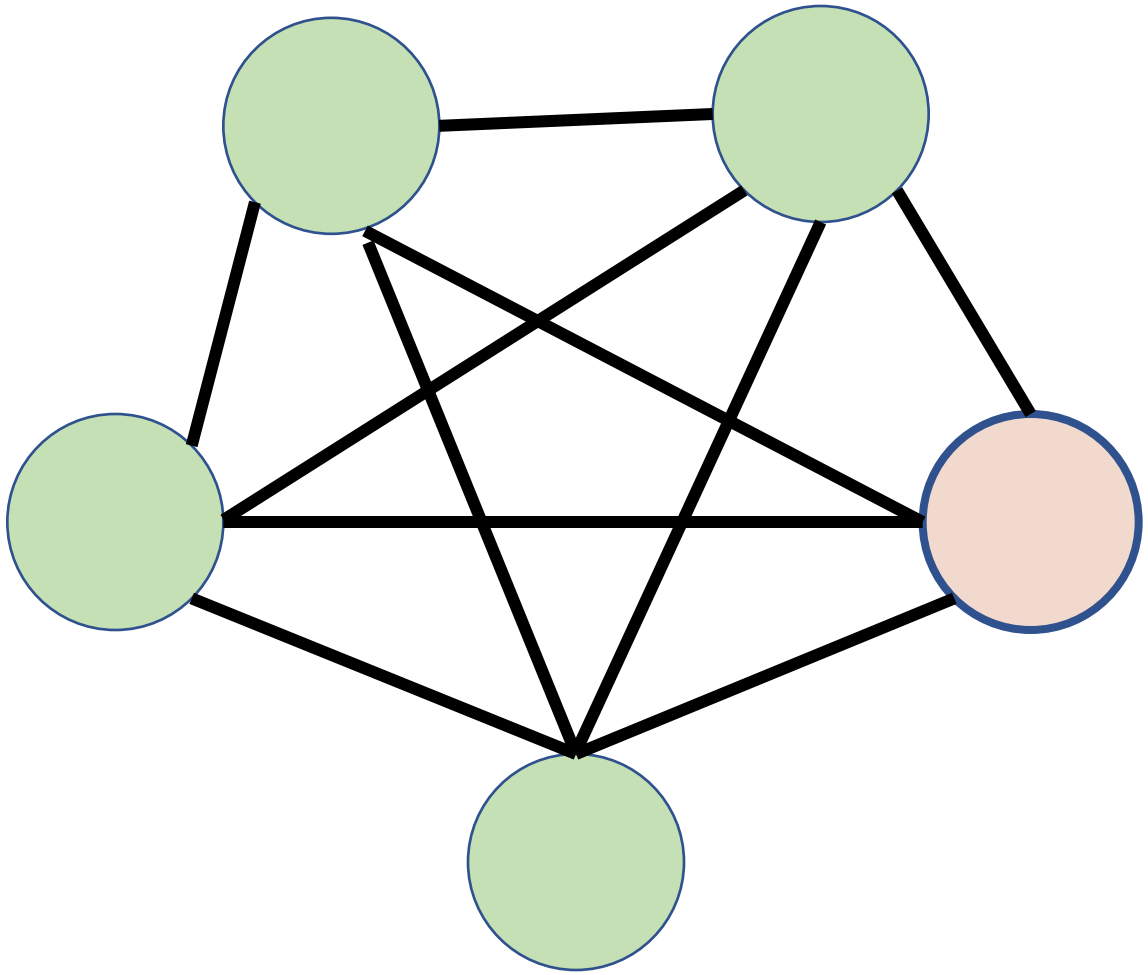
Validity



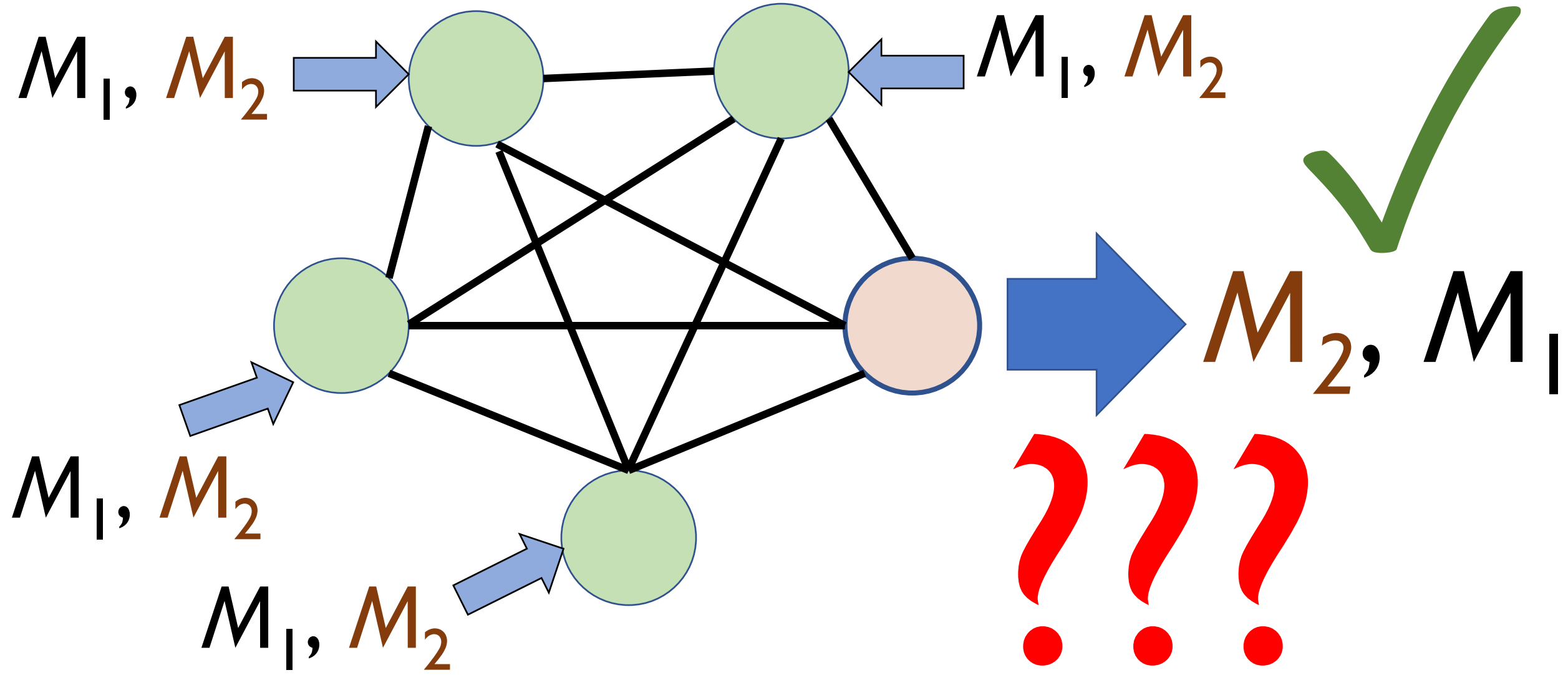
Validity



Multi-Round Byzantine Agreement (Consensus)

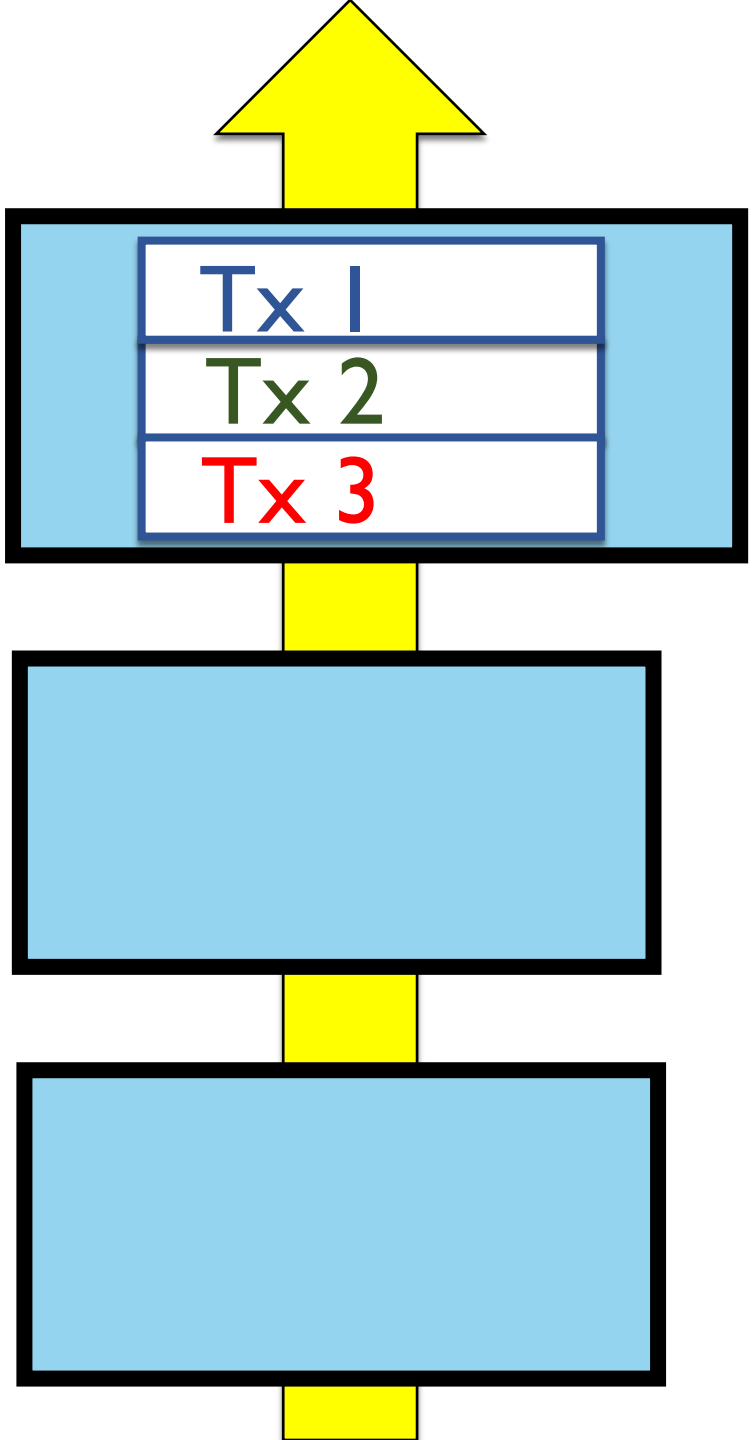


Multi-Round Byzantine Agreement (Consensus)



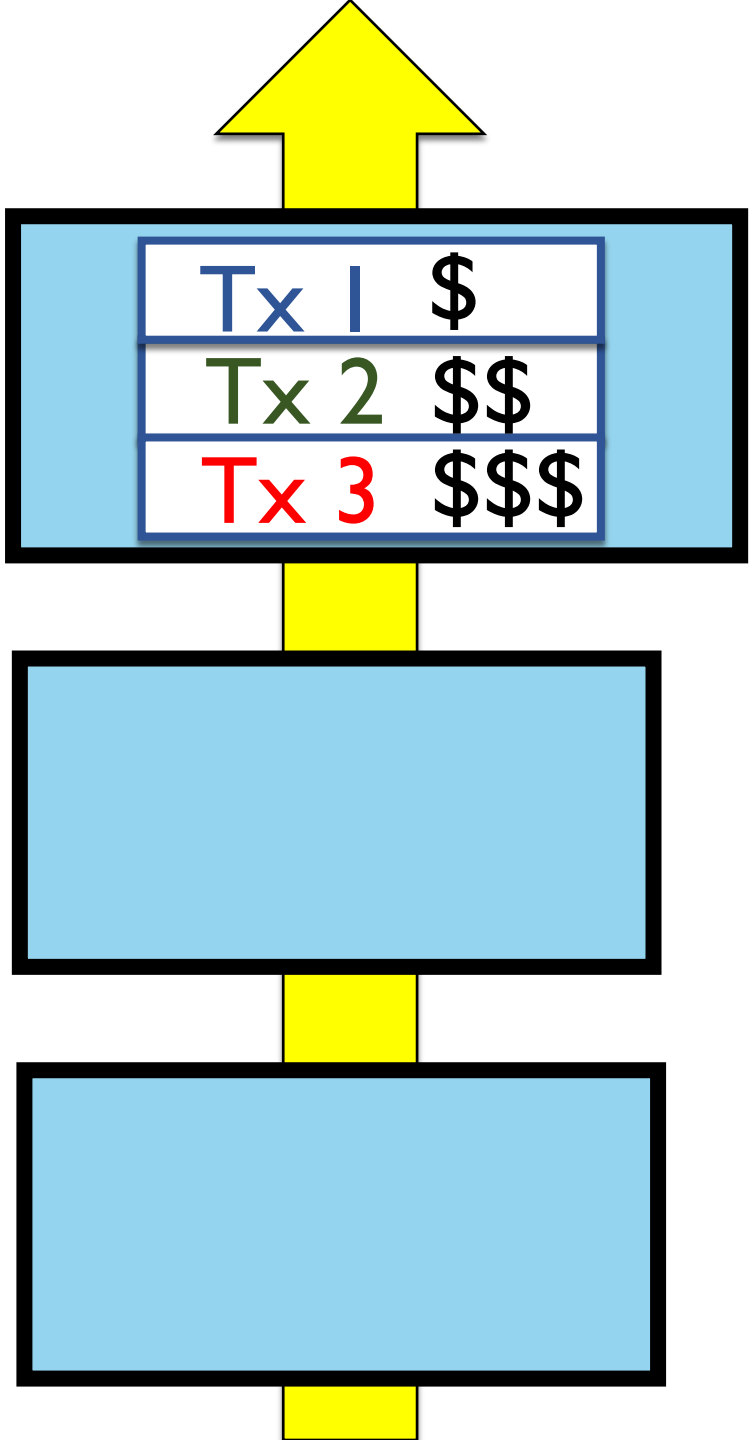
Blockchains

- Validator (e.g., Miner/Staker) can choose transaction order!!



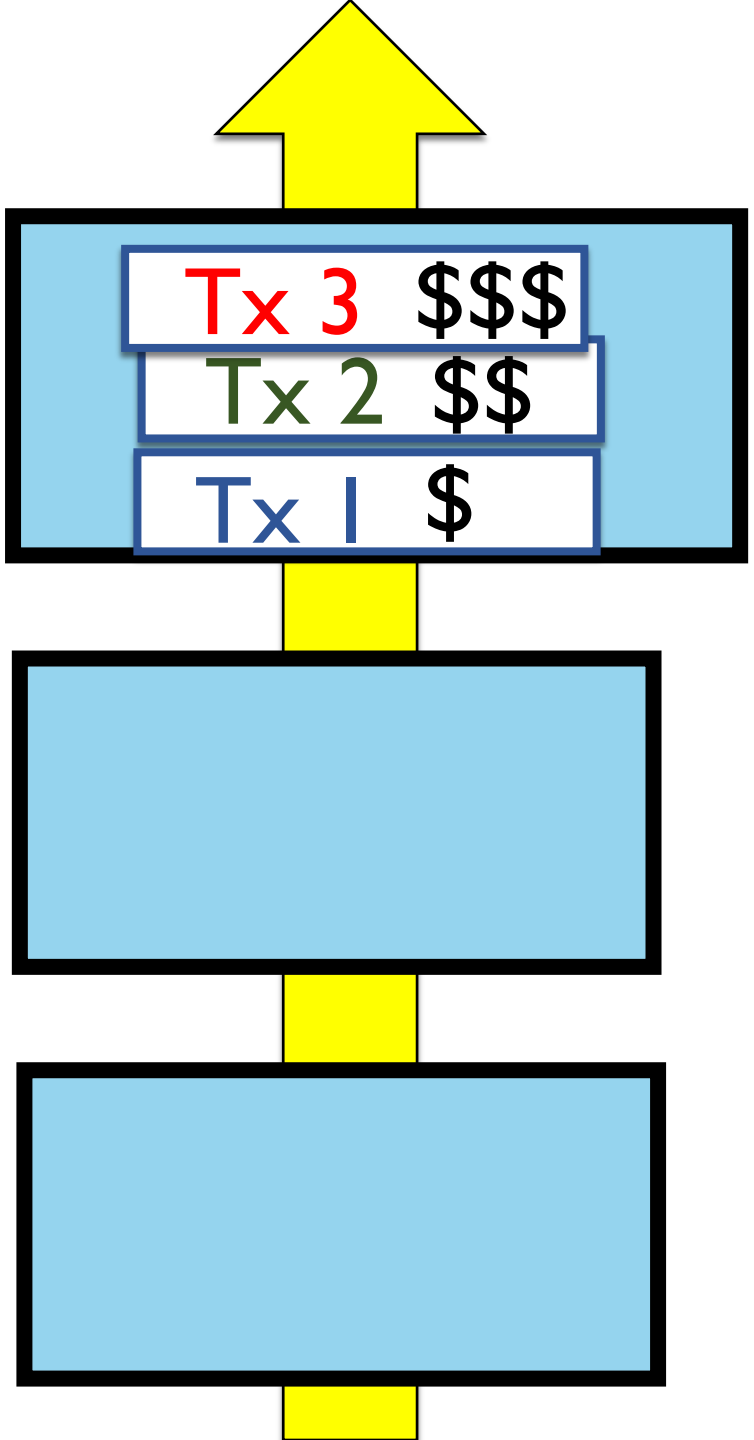
Blockchains

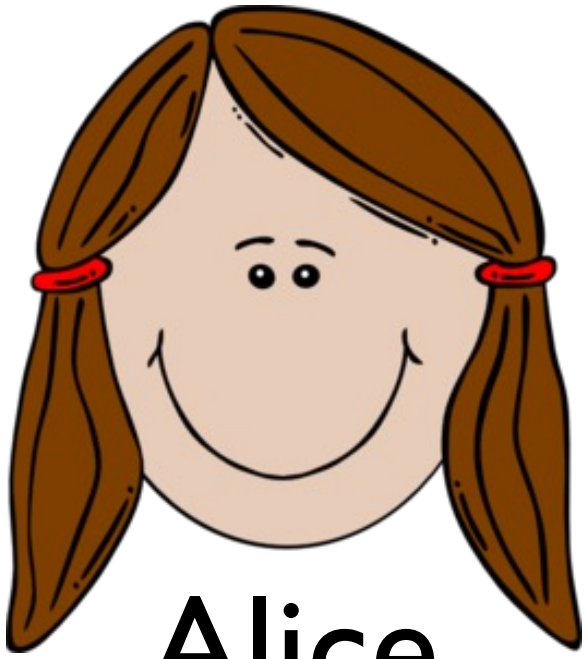
- Validator (e.g., Miner/Staker) can choose transaction order!
- Often based on fee amount ($ for miner/staker)



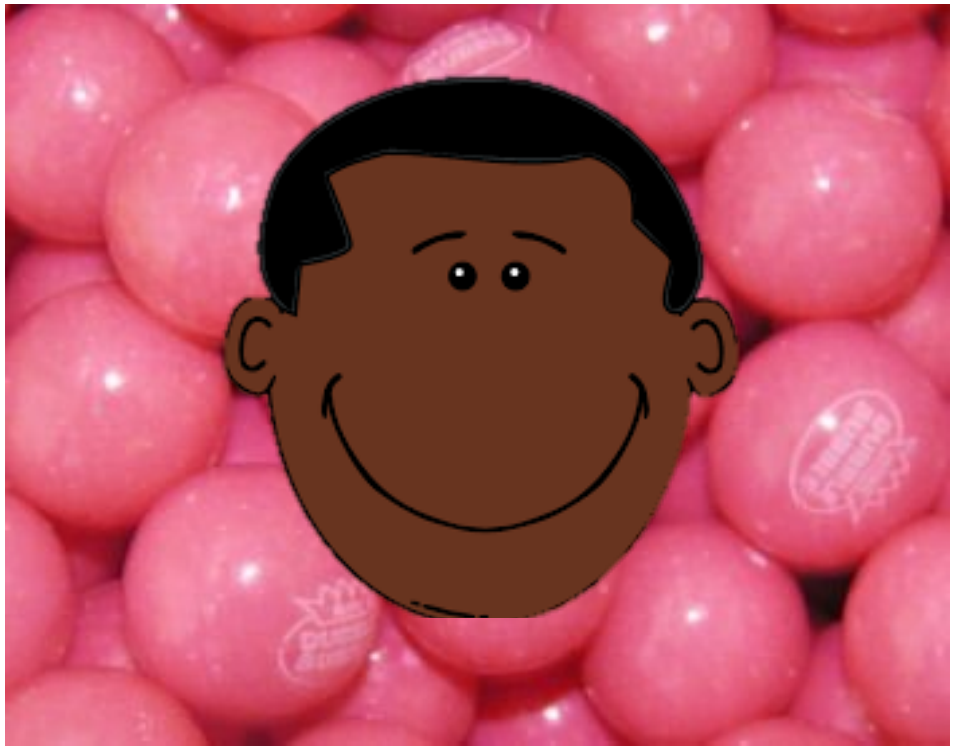
Blockchains

- Validator (e.g., Miner or Staker) can choose transaction order!
- Often based on fee amount ($ for miner/staker)
- Dirty little secret: ephemeral *centralization*
- So what?





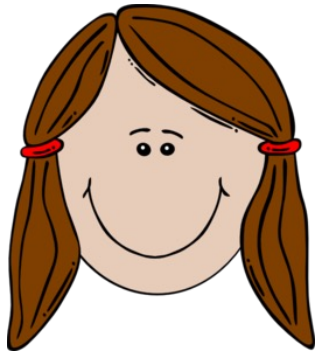
Alice



Bob's Bubble Tokens (BBT)

Alice wants to buy a Bubble Token (BBT)

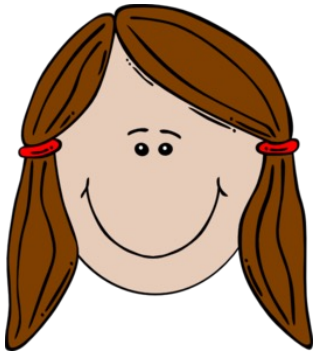
She submits a buy order to blockchain (exchange)



Buy 1 BBT for $1

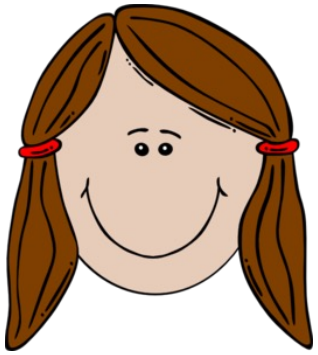
Blockchain System

But suppose Alice makes a typo…



Buy 1 BBT for $10

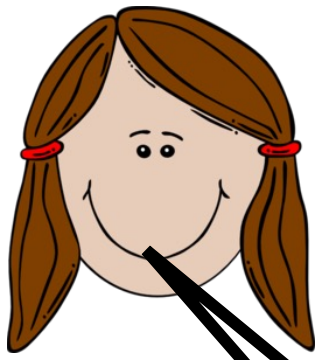
Blockchain System



Buy 1 BBT for $10

Buy 1 BBT for $10

Blockchain System



Buy 1 BBT for 10 ETH

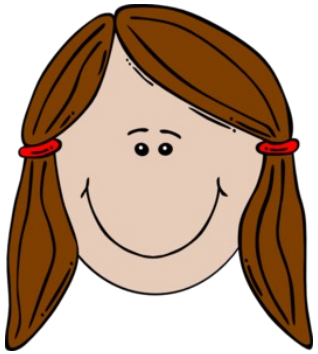
Oops!

Buy 1 BBT for $10

Blockchain System

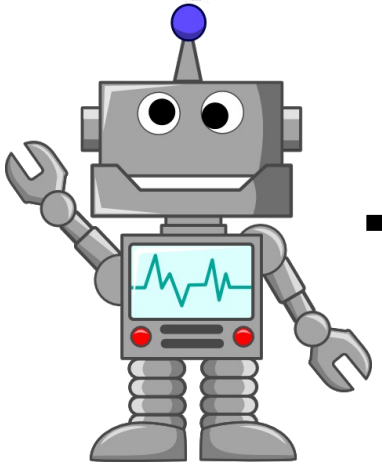
Front-running in action

Buy 1 BBT for $10



Cancel!

Fee: $



Sell 1 BBT!

Fee: $$$

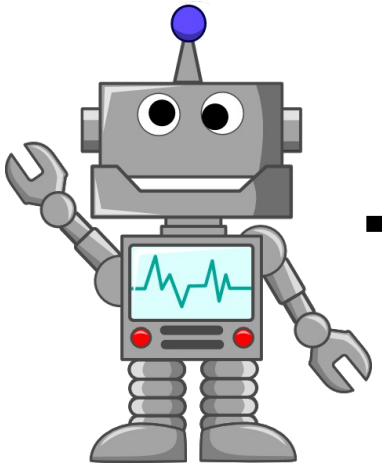
Blockchain System

Front-running in action

Buy 1 BBT for $10

Cancel!

Fee: $



Sell 1 BBT!

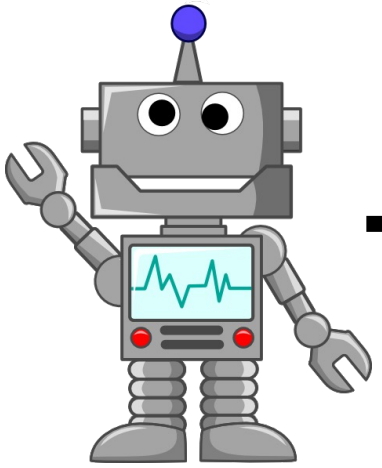
Fee: $$$

tx_1

tx_2

Blockchain System

Front-running in action



Intuition: Bot pays high fee to miner to front-run Alice!

Alice isn't alone!

Julien Feyen • a month ago

Hello, It appears that your contract took advantage of a mistaken order that was placed for a couple seconds today. The price any quantity where inverted which resulted in a HUGE loss on my end. We both know 1.4 ETH is worth far less then 28 ETH. Would you have the heart to return 24 ETH to my address. I am a stay at home parent and day trade to keep my family above water. I've helped others in similar situations. In your heart you know this isn't right.

Transaction: 0x846b1ba4976b793386c94589ea1edaef33a69018f0f3d41782ac46fdd2390fc8
My Address: 0xfc15c3468d5eb384eac73528a4c53c9545a39ab4

Thank you for your understanding.

Reply • Share ›

Source: etherscan.io comments, 0x67d1f31eeEF182cFB40c0719A8c0000fA7DDCAA9

Alice isn't alone!

Georgiy • 10 months ago

Hey - I bought 0.000078 LEND for 3200 ETH each, 0.25 ETH in total
my address is 0x386E6881E67E0C1eF032A6DB500Ca807257B0cD3

4 ^ | v • Reply • Share ›

This comment was deleted.

Mary ➦ Guest • 9 months ago

Hello, i made a mistake on a fortuna trade. Lost like 5.00ETH. pleassee dear send it back. I really need it.
0x2e3128F2e13F417B8F2fa3D8622FA6EC97998ce3

^ | v • Reply • Share ›

Edem ➦ Guest • 9 months ago

I have fate in you man... Pleassseee.... 0xa4691b7c799f4fefc10988f92c7e1ab01e8b68fb

^ | v • Reply • Share ›

Alice isn't alone!

Benjamin • 9 months ago

Please Please Please. This was an accident. I did not mean to make this transaction. Please can we reverse this. Please! I was trying to buy PPT. Please help me with this. This was an accident. Please, I did not mean this. This is very terrible for me. Please be kind and karma will be kind to you too. Please help me out. I spent 6.2 ETH on 110 PLR At least send me back 5 ETH you can have the rest. Please send back to address 0xDB50DFd230dB0f7a2Deb95A14DdA7a65334e59bE

I am a single parent trying to make ends meet at a job I hate. Please have some mercy

3 ^ | v • Reply • Share ›

Alice isn't alone!

Alfie • 9 months ago

Hello, I bought 0.00144 COV by mistake for 1.921 Eth. Please I ask you to send me the ETH back as I really need it to continue my education. I might need to sell my car to pay what is already due for this semester. Please Please Please return AT LEAST 1 ETH and I give you willingly the rest if GOD ever asked you about it. This is my ETH address:
0x5e51F64ac374340bdE87535eac3243b6C4578597
Thank you so much

2 ^ | v • Reply • Share ›

There are many, many more of these…we found thousands of instances.

NEWS DEX

DEX protocol Bancor suffered security vulnerability, migrated $455K worth of user funds

by Yogita Khatri

Download PDF / Print

June 18, 2020, 8:10AM EDT · 2 min read

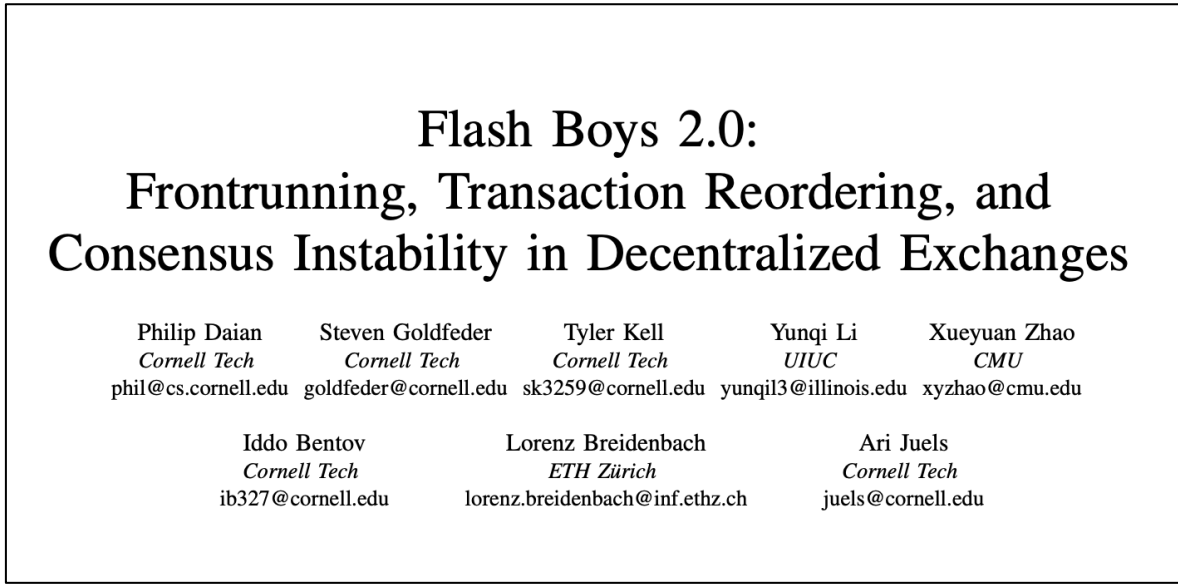
THE BLOCK

While Bancor initiated the white-hat activity, two arbitrage bots detected the incoming transactions and front-run Bancor with profits of $135,229.

"Our team [Bancor] initiated a white-hat attack using that same vulnerability in order to migrate $455,349 of funds at risk to a safe wallet. Alongside our white-hat activity, two more arbitrage bots detected the incoming transactions, leading to the transactions being front-run by these bots with profits of $135,229. We have since been in contact with the owners of these bots and are working with them to return the amounts to the rightful owners in exchange for a bug bounty."

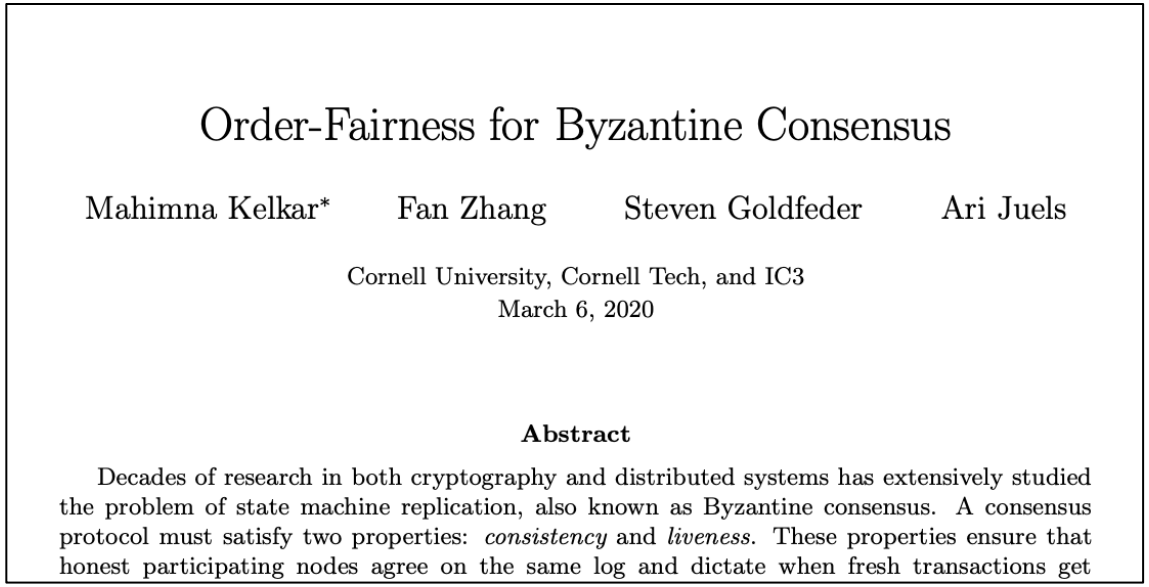
Take-aways

- Validity forgotten in consensus
- Blockchains' dirty little secret: Transaction ordering temporarily *centralized*
- Unfair transaction ordering hurts users and systems
- Key questions:
  - How bad is the problem?
  - What, formally, is fair transaction ordering?
  - How to achieve fair transaction ordering?



Flash Boys 2.0:
Frontrunning, Transaction Reordering, and
Consensus Instability in Decentralized Exchanges

Philip Daian, *Cornell Tech*, phil@cs.cornell.edu
Steven Goldfeder, *Cornell Tech*, goldfeder@cornell.edu
Tyler Kell, *Cornell Tech*, sk3259@cornell.edu
Yunqi Li, *UIUC*, yunqil3@illinois.edu
Xueyuan Zhao, *CMU*, xyzhao@cmu.edu
Iddo Bentov, *Cornell Tech*, ib327@cornell.edu
Lorenz Breidenbach, *ETH Zürich*, lorenz.breidenbach@inf.ethz.ch
Ari Juels, *Cornell Tech*, juels@cornell.edu



Order-Fairness for Byzantine Consensus

Mahimna Kelkar* Fan Zhang Steven Goldfeder Ari Juels

Cornell University, Cornell Tech, and IC3

March 6, 2020

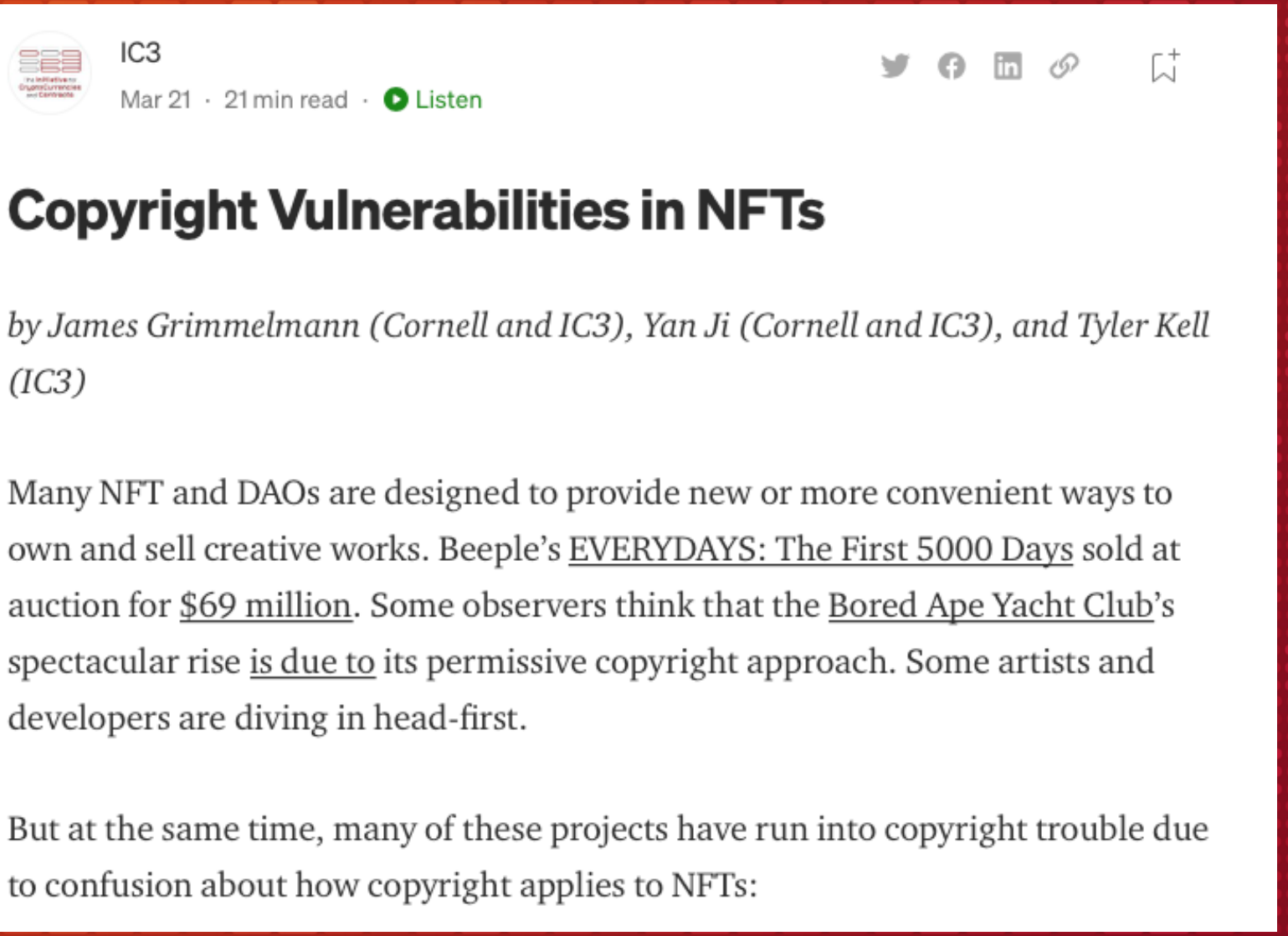
Abstract

Decades of research in both cryptography and distributed systems has extensively studied the problem of state machine replication, also known as Byzantine consensus. A consensus protocol must satisfy two properties: *consistency* and *liveness*. These properties ensure that honest participating nodes agree on the same log and dictate when fresh transactions get

IC3 DeFi Research Thrusts

- Incentives (Dis-incentives), Cryptoeconomic Guarantees, Layer 1 and Layer 2 Solutions (e.g., Multi-party Computation 2.0)
- MEV Detection & Estimation & Prevention, Front/back-running, Transaction Editing/Censorship, etc. Is Fair Ordering Possible?
- Composing NEW & Reliable Financial Instruments: NFTs Drops, Fractionalizable NFT's, Multi-Party Flash Loans…
- Security and Decentralized Identity Solutions

NFT Research – "Code is Law!" (really?)



IC3

Mar 21 · 21 min read · Listen

Copyright Vulnerabilities in NFTs

by James Grimmelmann (Cornell and IC3), Yan Ji (Cornell and IC3), and Tyler Kell (IC3)

Many NFT and DAOs are designed to provide new or more convenient ways to own and sell creative works. Beeple's EVERYDAYS: The First 5000 Days sold at auction for $69 million. Some observers think that the Bored Ape Yacht Club's spectacular rise is due to its permissive copyright approach. Some artists and developers are diving in head-first.

But at the same time, many of these projects have run into copyright trouble due to confusion about how copyright applies to NFTs:

The Initiative for CryptoCurrencies and Contracts

Join Us!

For more info, please www.initc3.org

For inquiries, please email the IC3 directors through ic3-directors@cornell.edu

The Initiative for CryptoCurrencies and Contracts