The Future of Trust: Research and Community Challenges -- A viewpoint

Jiangshan Yu
Monash University

The 84th IFIP WG10.4 Meeting
June-2023

MONASH University

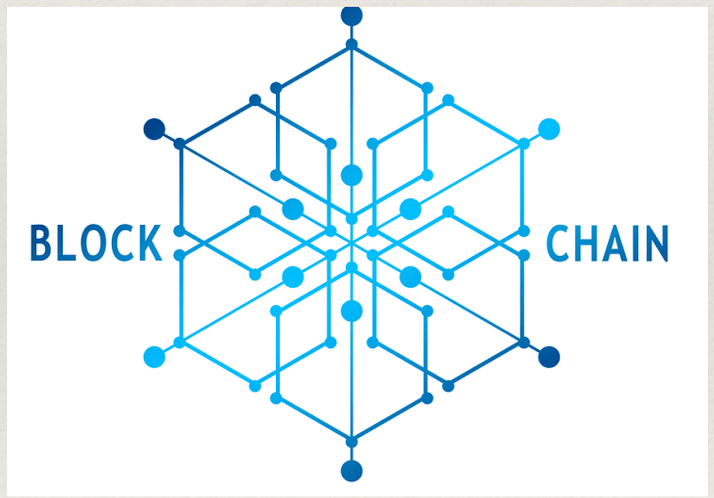
The Evolution of Trust

Uncertainty

Local

Institution

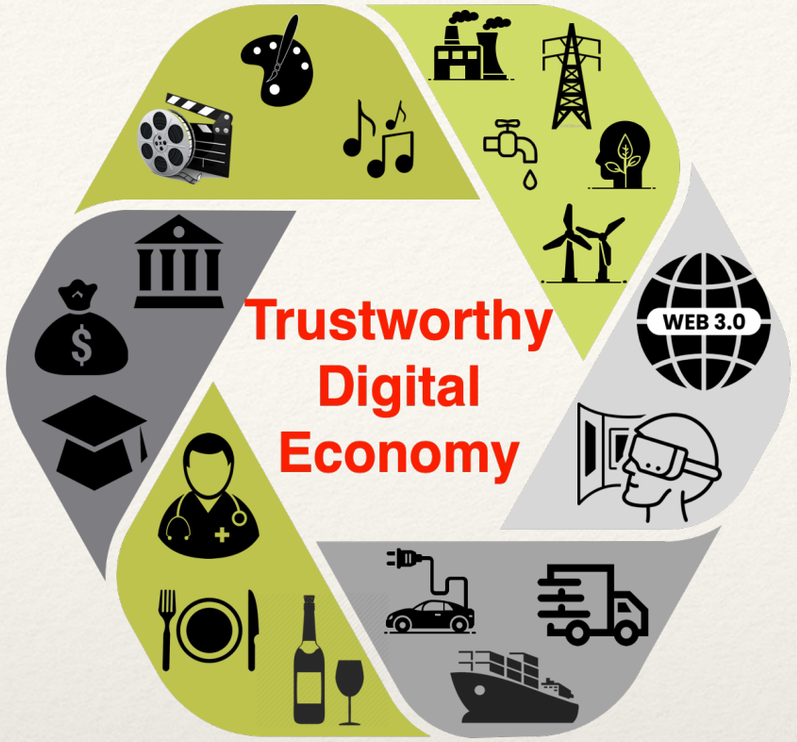
Technology



Scalability and Efficiency

MONASH University

Trustworthy Digital Economy



Web 1.0

read-only
static

Web 2.0

read-write
interactive

Web 3.0

read-write-trust
verifiable

MONASH University

My research vision/mission

Establish trust by using technology alone,
for a trustworthy digital economy!

Foundations → Systems → Digital Economy

- Consensus
- Fault tolerance
- Privacy-enhancing technologies
- Formal verification
- Trusted hardware

- Trustworthy Identify Management
- Trustworthy source of big data
- Trustworthy AI
  - LLM (e.g. ChatGPT)

- Web 3
- E-gov and public services
- Digital health
- Critical infrastructure
- Supply chain

The 83rd meeting: Future of blockchains

Some socio-technical dependability challenges

1. Performance at the scale of Internet (e.g. web 3.0)
2. Smart contract security
3. Diversity of devices in permissionless networks
4. Authenticated data feed
5. Finance ecosystem and application systems (NFT, DeFi, DAO, DApp, GameFi, Metaverse, etc.)
6. Many more challenges:
   - wallet security and key management
   - Responsible and dependable law and regulation
   - usability
   - privacy
   - deployment challenges
   - post-quantum security
   - human factor and culture impact
   - …

OODA LOOP

HOME OODA ANALYSIS NEWS BRIEFS JOIN OODA LOOP ABOUT OODA LOOP MEMBER ME

TECHNOLOGY

DeFi security losses rose 47.4% in 2022 to hit $3.64B: Report

06 Jan 2023 | OODA Analyst

Share Tweet Post Reddit

According to a Jan. 5 report published by Chinese blockchain security firm LianAn Technology, decentralized finance (DeFi) exploits across blockchains worldwide totaled $3.64 billion in 2022. This represented a rise of 47.4% compared with the loss of $2.44 billion in 2021. The incidents increased in quantity despite a steep 80% loss in the total value locked in DeFi during the year. Out of the 2022 amount, funds lost during cross-chain bridge hacks amounted to $1.89 billion across 12 incidents — the highest in the category. Overall, attacks on Ethereum, BNB Chain and Solana accounted for the majority of exploits. Out of the 167 notable incidents in 2022, 51.5% of breaches occurred in audited projects, while 48.5% of breaches occurred in non-audited projects. In total, LianAn said 38.7%, or $1.40 billion, of stolen funds were laundered via cryptocurrency mixer Tornado Cash. Only $289 million worth of funds were recovered throughout the year. However, the number is likely higher, as several recoveries have yet to be publicly disclosed per law enforcement requests. Total global blockchain-related crimes (financial crimes excluded) amounted to $13.7 billion in 2022. Incidents of money laundering topped the list with $7.33 billion, followed by DeFi exploits ($3.6 billion), multilevel marketing scams ($1.0 billion) and fraud ($830 million). Aside from the collapse of cryptocurrency exchange FTX, there were 243 incidents of fraud and rug pulls during the period, with $425 million involved in total.

MONASH University

In this talk - our observation and lessons

Social-Technical Challenges:

1. **Meaningful guarantees of large scale systems**
    a. Diversity
    b. Trust
2. **Adapting blockchains**
3. **Communities**

Meaningful guarantees of large scale systems

Impasse Situation

Very-large scale BFT protocols

Great progresses:

- Hotstuff (PODC'19)
- Damysus (EuroSys'22)
- Narwhal and Tusk (EuroSys'22)
- Bullshark (CCS'22)
- Dumbo family (CCS'20, PODC'20, …)
- Mir-BFT (JSys'22)
- …

Diversity does not scale

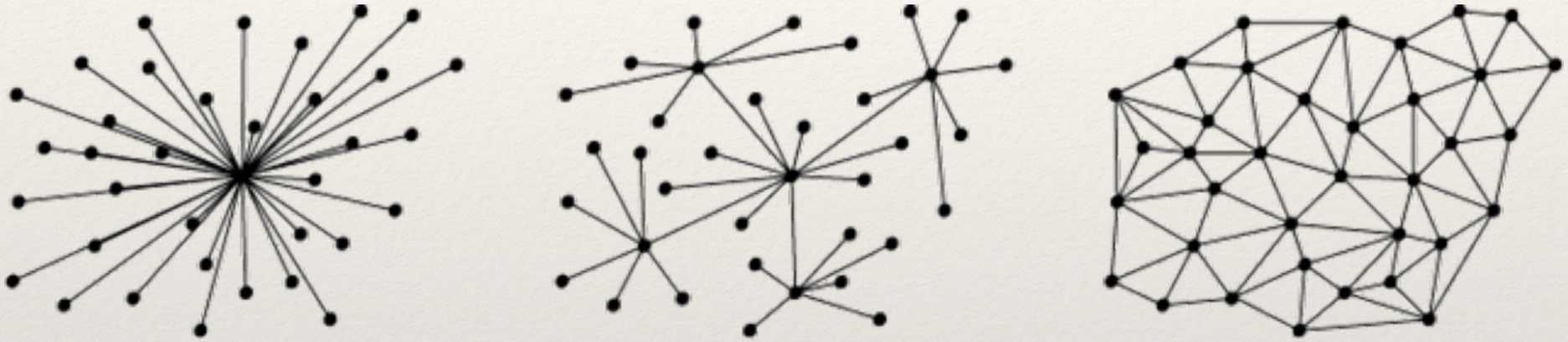
- All inevitably **assuming replica diversity** for fault independence
- Limiting practical and meaningful resilience

Meaningful guarantees of large scale systems

- How to improve diversity?
- Given an erratic permissionless system, what is is the optimal guarantee/bound?
- How to achieve it?

Meaningful guarantees of large scale systems

Uncertainty: Who are we trusting?



centralised decentralised distributed

REACHABLE BITCOIN NODES

Updated: Sat Jun 24 00:28:05 2023 WEST

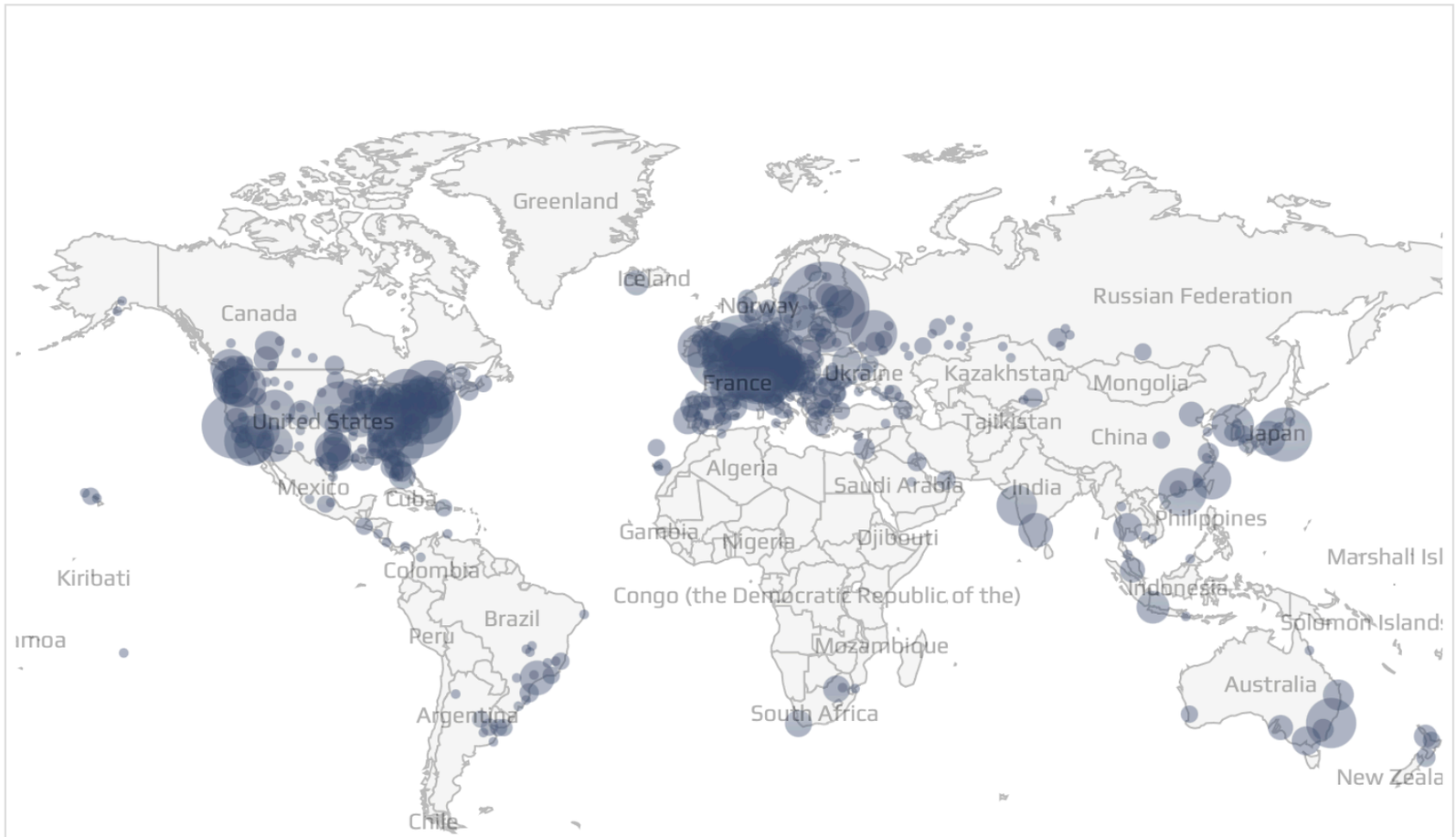
17052 NODES

CHARTS

IPv4: -2.1% / IPv6: -1.3% / .onion: -0.1%

Top 10 countries with their respective number of reachable nodes are as follows.

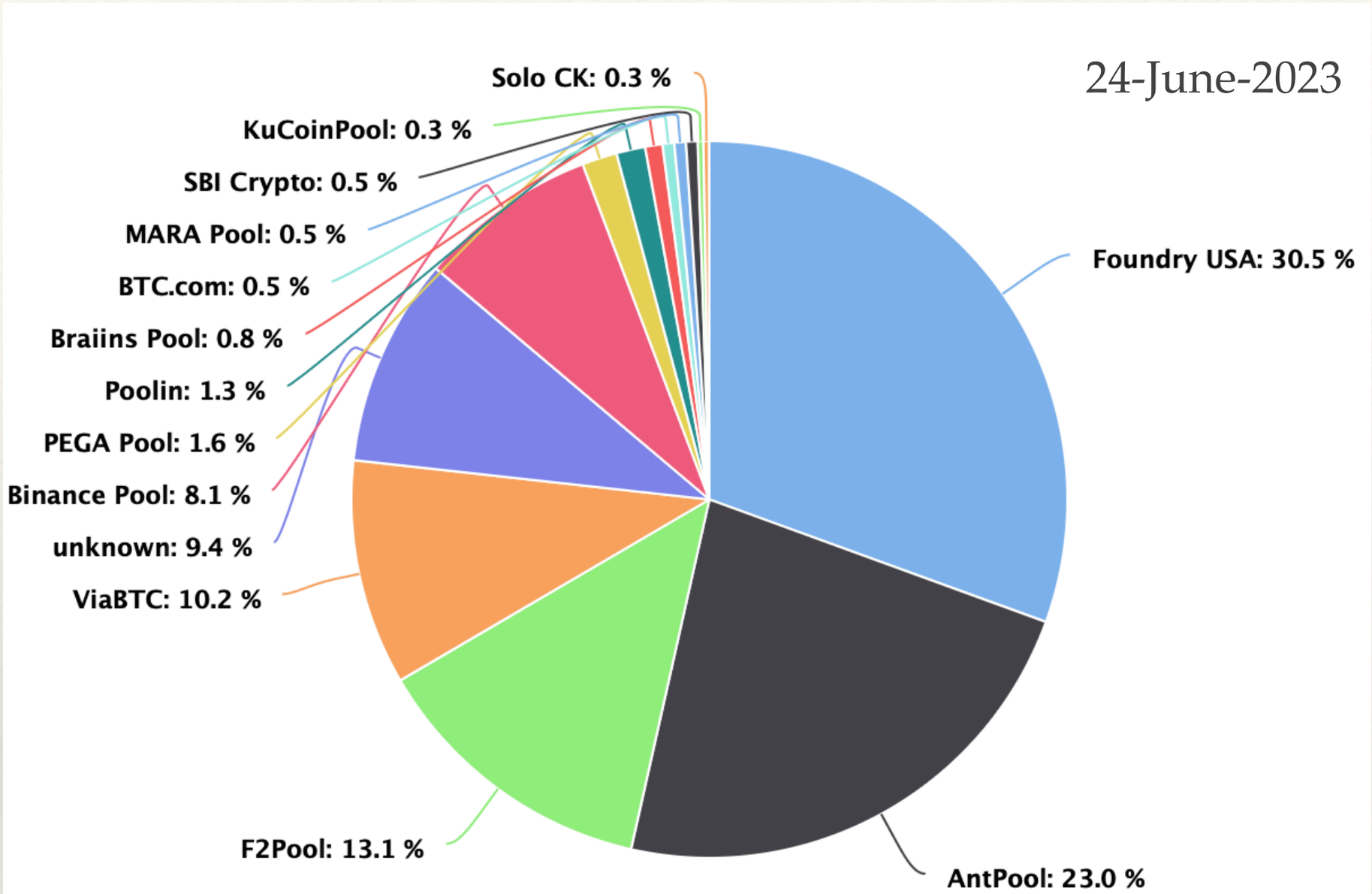
RANK	COUNTRY	NODES
1	n/a	10435 (61.20%)
2	United States	1628 (9.55%)
3	Germany	1397 (8.19%)
4	France	461 (2.70%)
5	Netherlands	347 (2.03%)
6	Canada	283 (1.66%)
7	Finland	272 (1.60%)
8	United Kingdom	207 (1.21%)
9	Russian Federation	182 (1.07%)
10	Switzerland	162 (0.95%)



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

MONASH University



2 mining pools control >50%;
14 mining pools control 99.5% mining power

MONASH University

How to measure uncertainty?

Adapting blockchains

Replacing/advancing existing (critical) infrastructure is very challenging

Example: Digital health

- A great diversity of medical machines
  (manufactured by different companies, in different generations);
- Many don't have open APIs, cannot export data easily

Community

Dependability and fault tolerance have made huge progress,
we are everywhere!

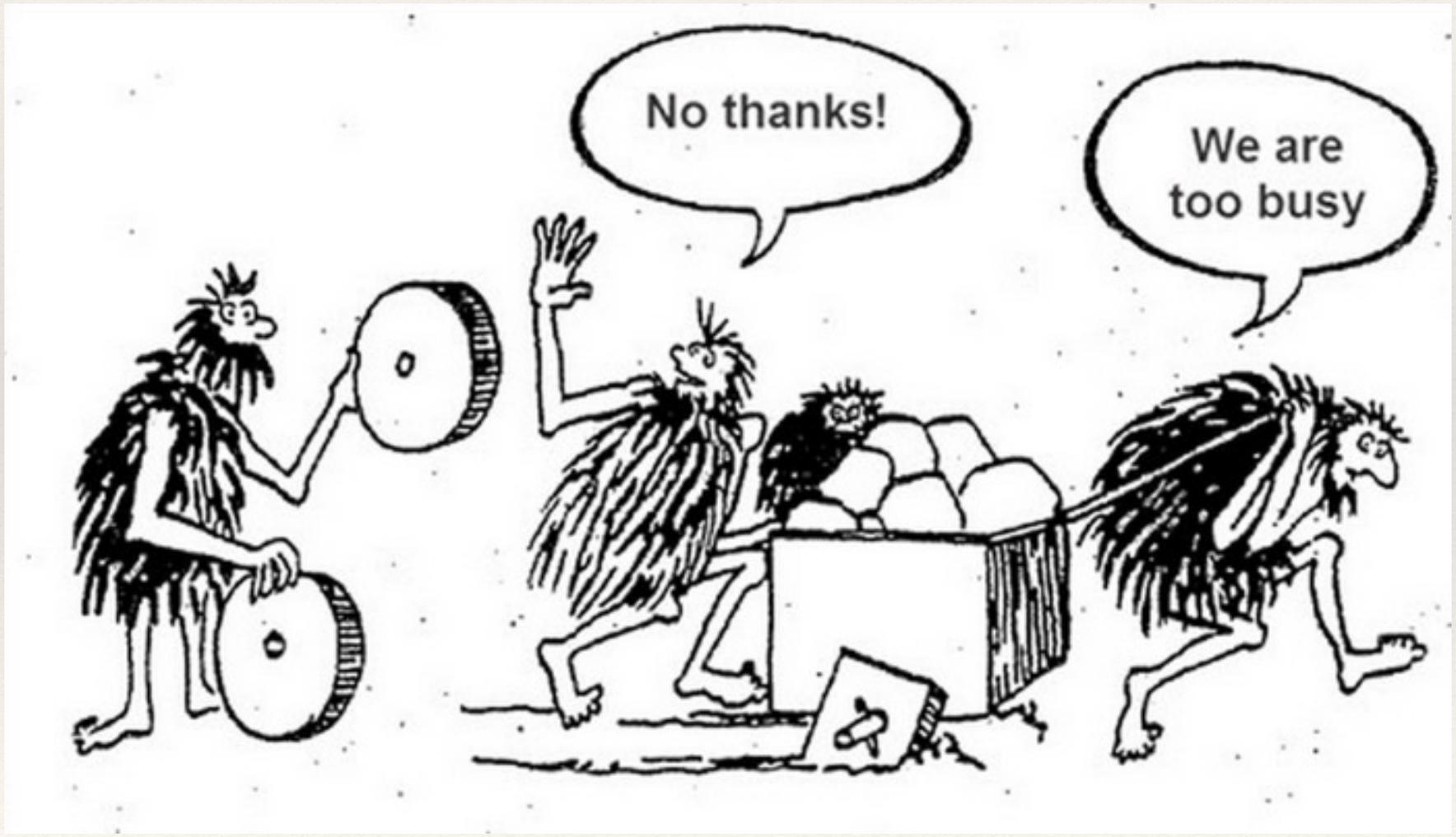
(e.g. awareness of dependability and fault tolerance in blockchain, AI, autonomous driving, smart city, etc.)

Community

Gap between communities

(Dependability, Systems, Database, Security, …)

Seeing papers at **Top** security/database/system/AI/etc conferences, such as CCS, VLDB, SIGMOD, EuroSys, SOSP, NuroIPS, ICDE, etc.



MONASH University

Community

Do we need a go-to community for dependability?

Are we (or why aren't we) the go-to community for dependability issues?

What's our (IFIP WG 10.4) mission and value?

- What have we done?
- What should / will we do?

Discussions

Social-Technical Challenges:

1. **Meaningful guarantees of large scale systems**
   a. Diversity (Disrupt@DSN'23)
   b. Trust
2. **Adapting blockchains**
3. **Communities**

1. Do we need a go-to community for dependability?
2. Are we (or why aren't we) the go-to community for dependability issues?
3. What's our (IFIP WG 10.4) mission and value?
   1. What have we done?
   2. What should/will we do?