KU LEUVEN

DistriNet

Blockchains as Trusted Computers: Unraveling the tech behind Web 3

Tom Van Cutsem
May 2024

tvcutsem.github.io
be.linkedin.com/in/tomvc
github.com/tvcutsem
x.com/tvcutsem
@tvcutsem@techhub.social

The bottom line

1. Blockchains are computers. Software platforms, like the Cloud.

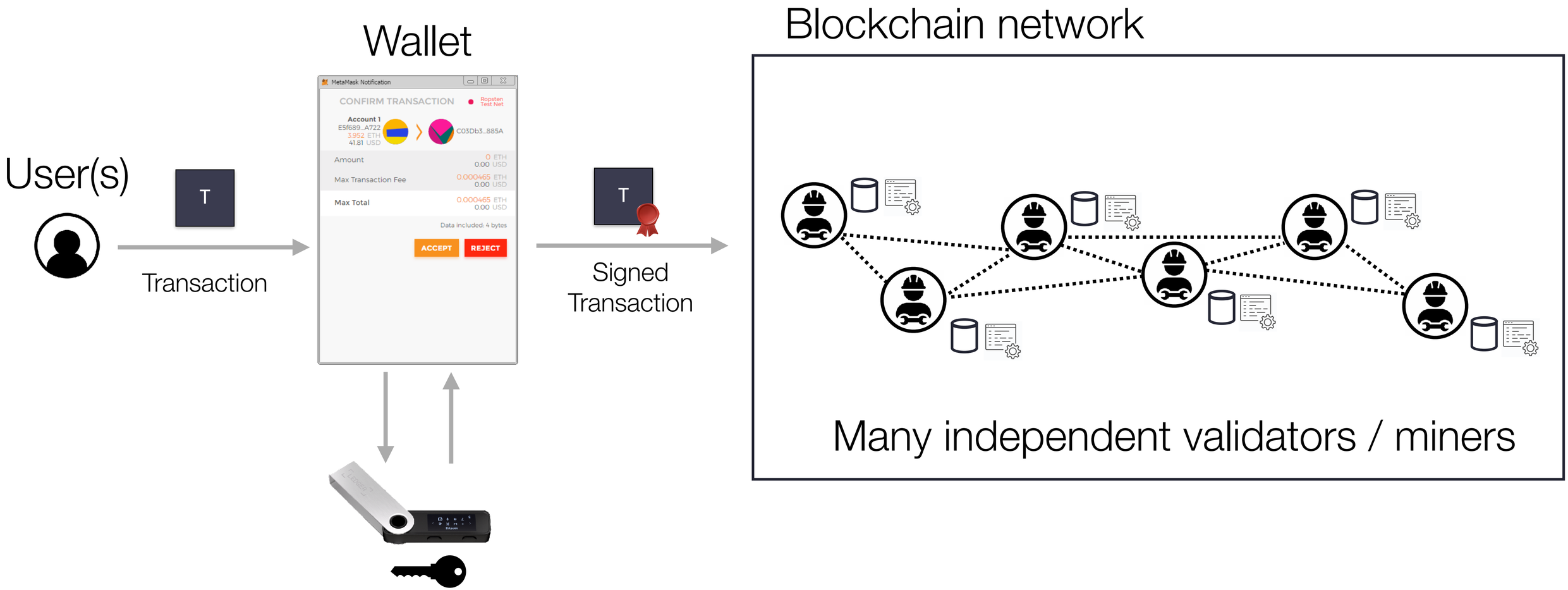
2. They are rapidly becoming faster, cheaper, more connected & programmable.

3. Why is this a Big Deal? The foundation for a new online era - “Web3”.

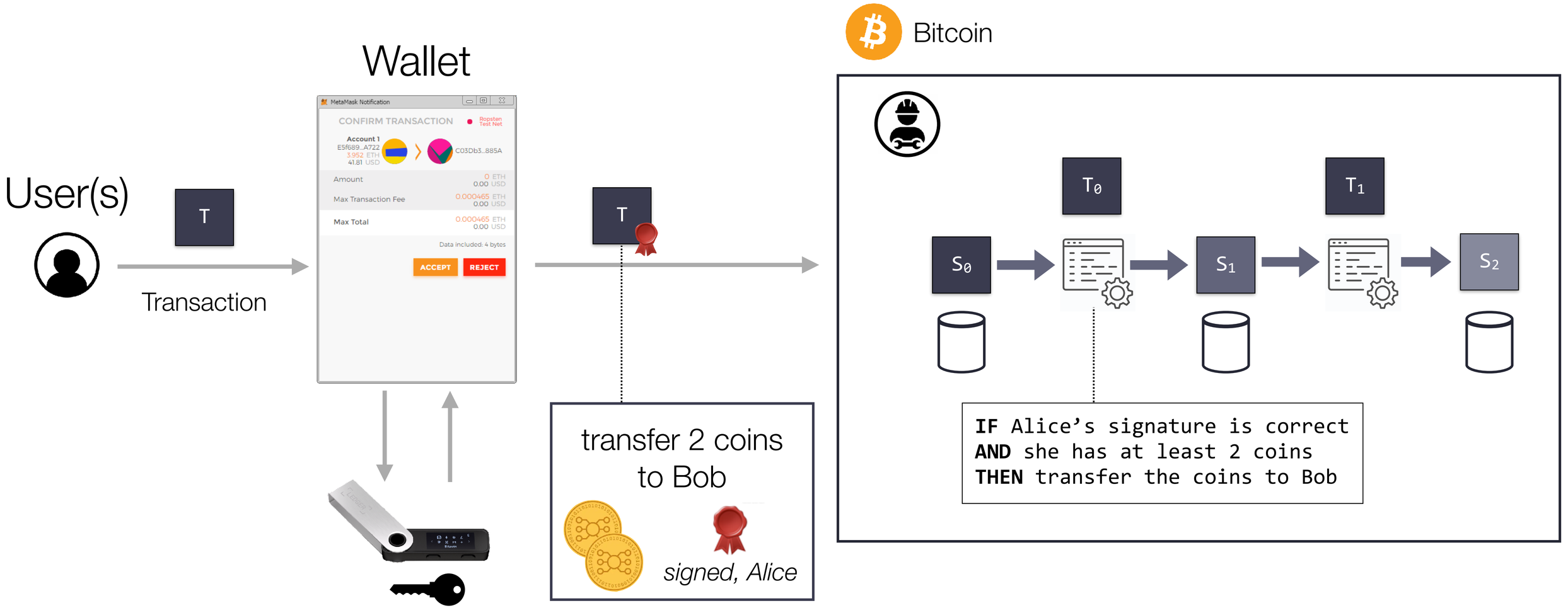
4. Long-term progress is driven by strategic academic research

1. Blockchains are computers

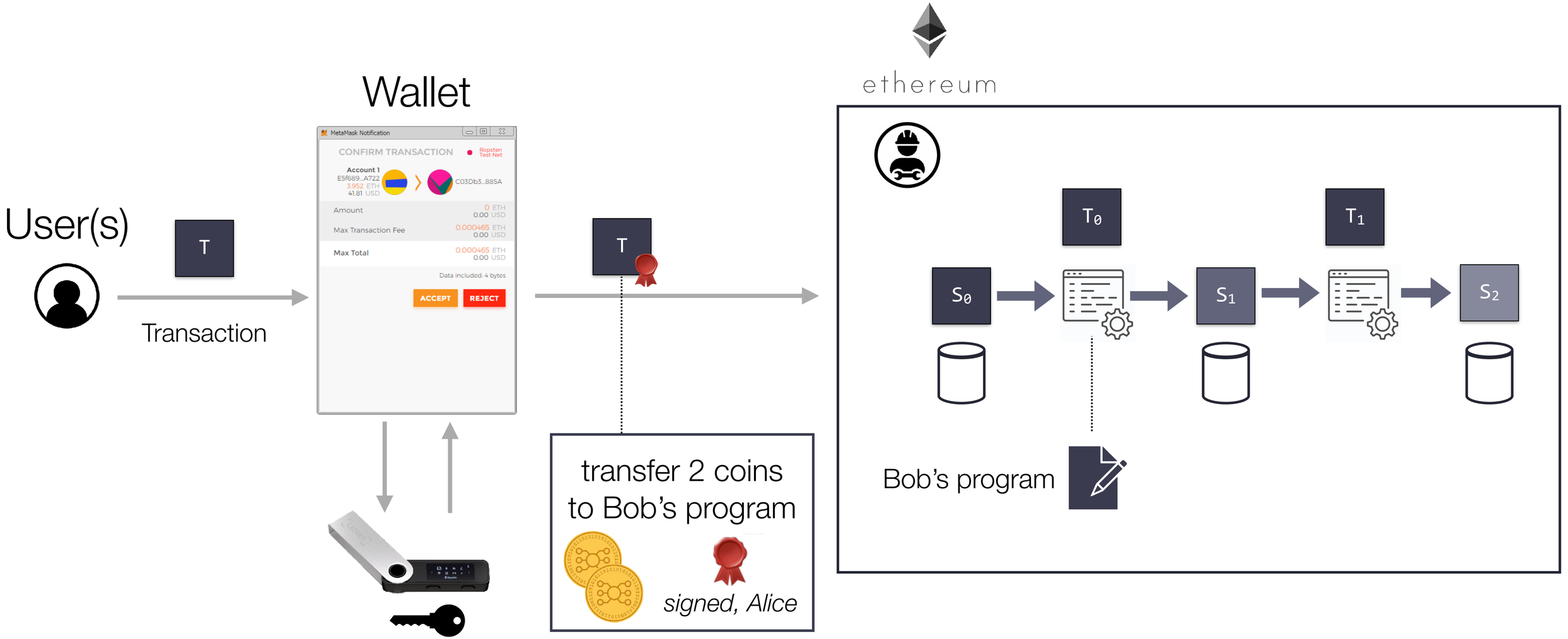
A blockchain as a physical network of many computers



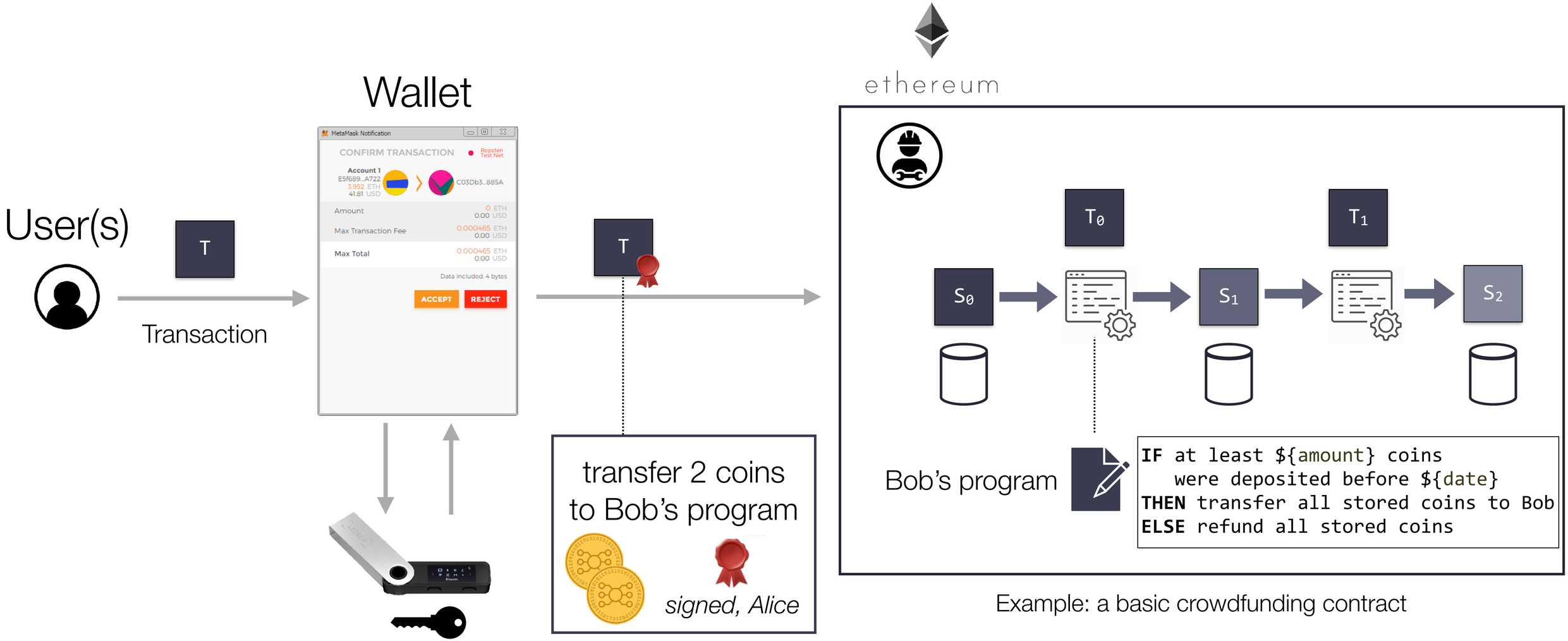
A blockchain as a single logical transaction processing machine



Ethereum’s innovation: make the transactions programmable!

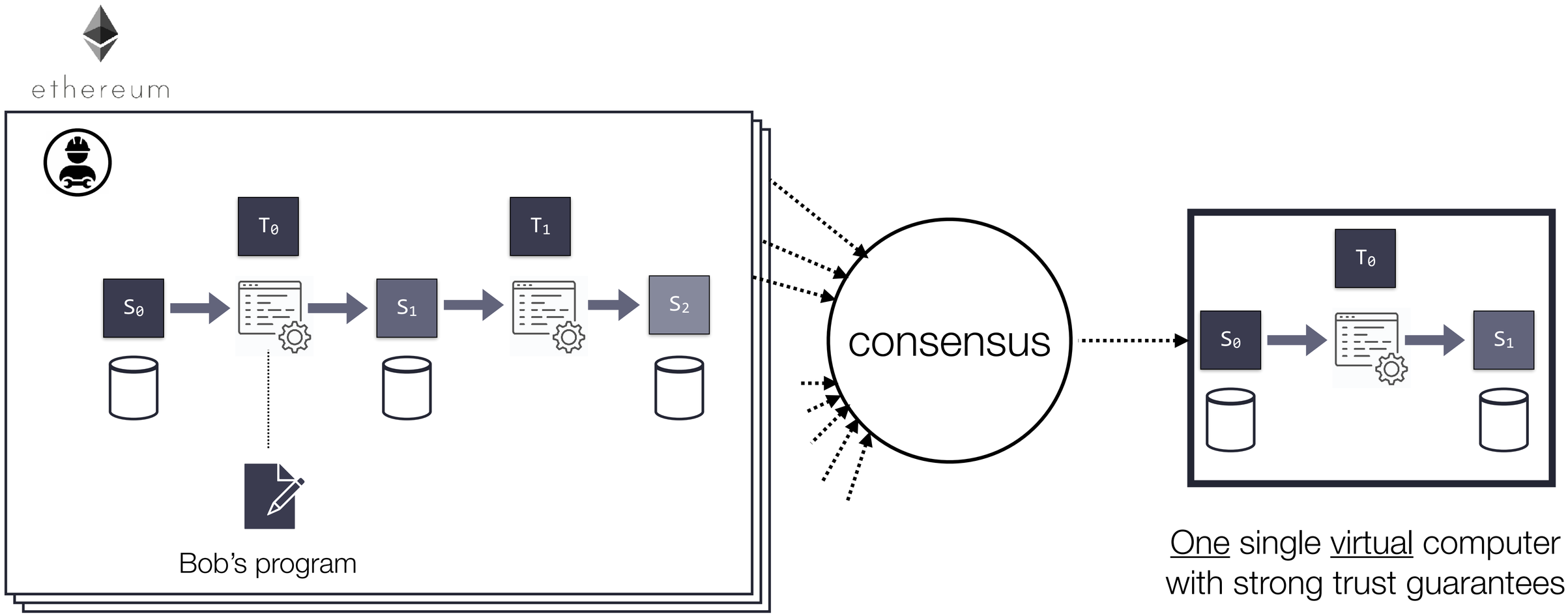


Ethereum's innovation: make the transactions programmable!



Example: a basic crowdfunding contract

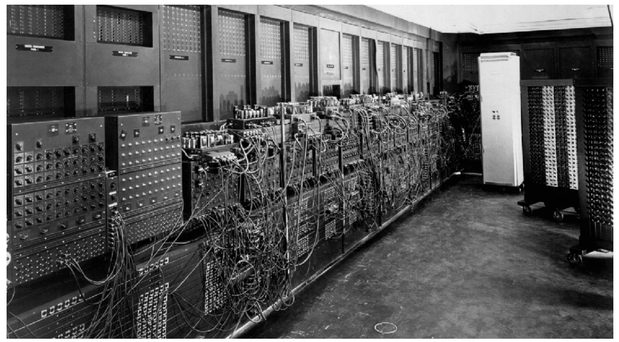
Blockchains as *trusted* virtual computers



Many (1000s) untrustworthy physical computers

Computers are defined by what they do, not by what they are made of

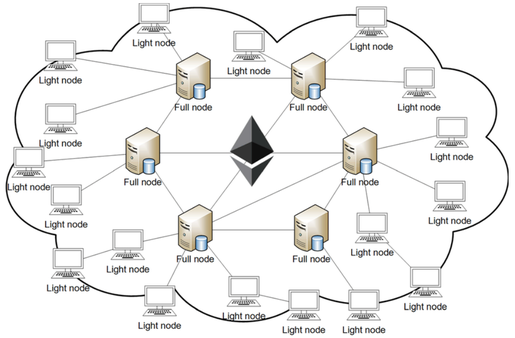
(Credit: Chris Dixon, Read Write Own)



ENIAC
Computers are *rooms*

Personal Computers
Computers are *desktops*

Datacenters (“The Cloud”)
Computers are *warehouses*



Blockchains
Computers are *networks*

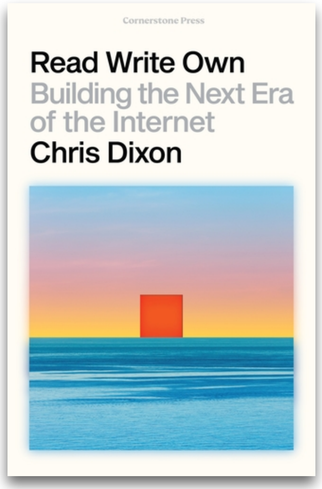
Electric

Interactive

Utility

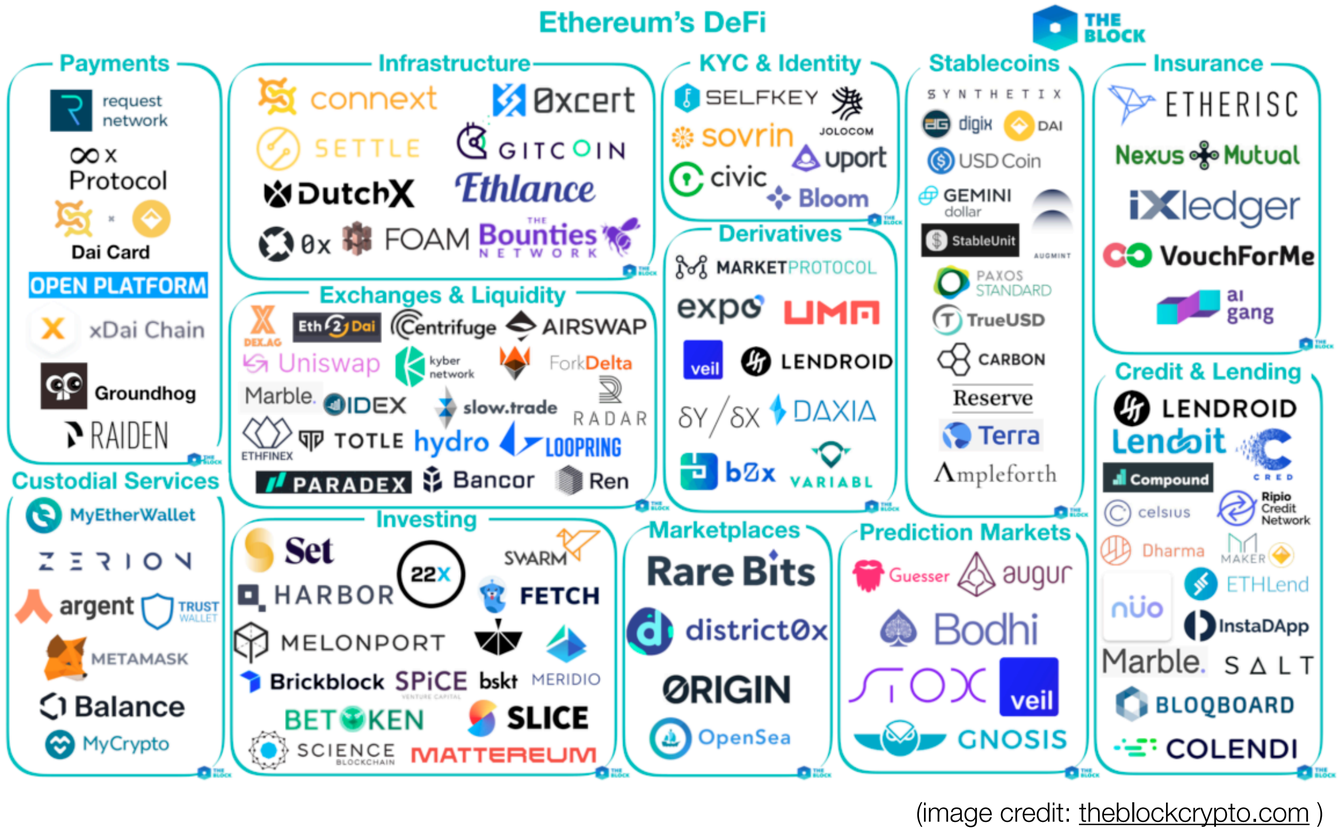
Trusted

“Blockchains are computers that can make *credible commitments*”

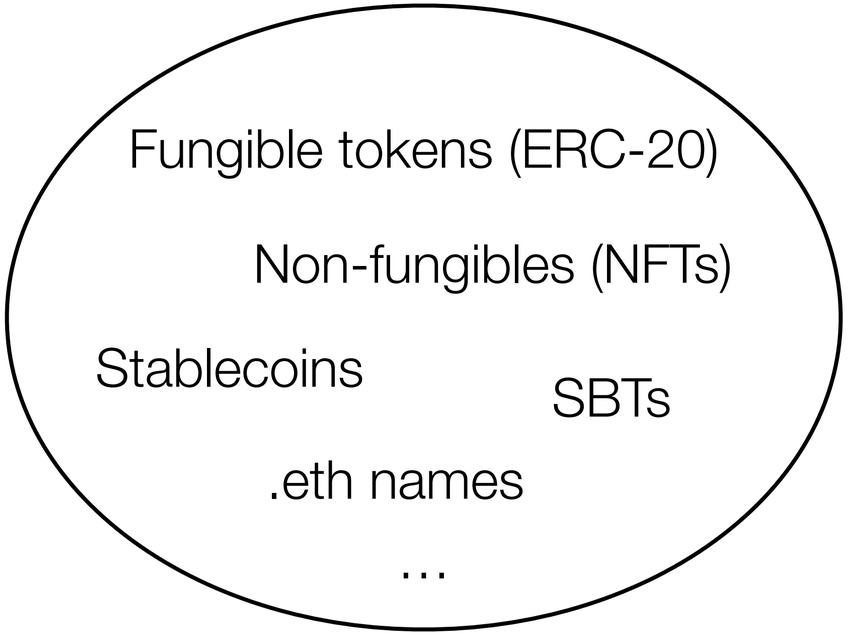


(Source: Chris Dixon, Crypto Networks and Why They Matter, 2020)

Applications? Ethereum's "Decentralized Finance"



(image credit: theblockcrypto.com)



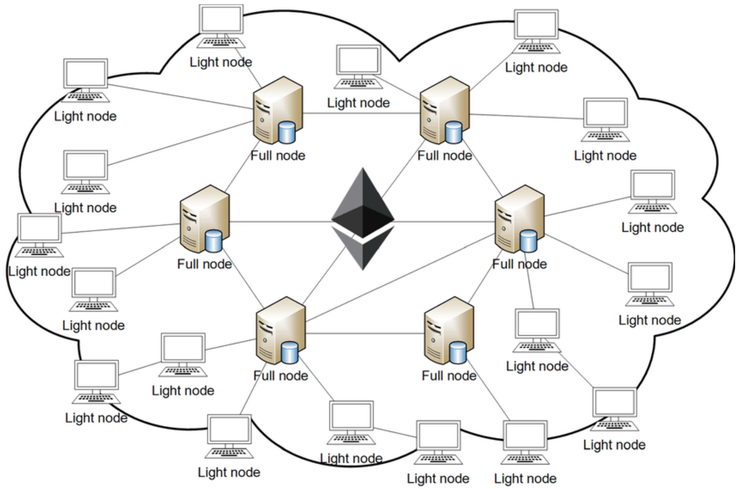
New kinds of **electronic rights** collectively worth over **$100 Billion**

(source: coingecko.com, retrieved May 2024)

2. Blockchains are evolving

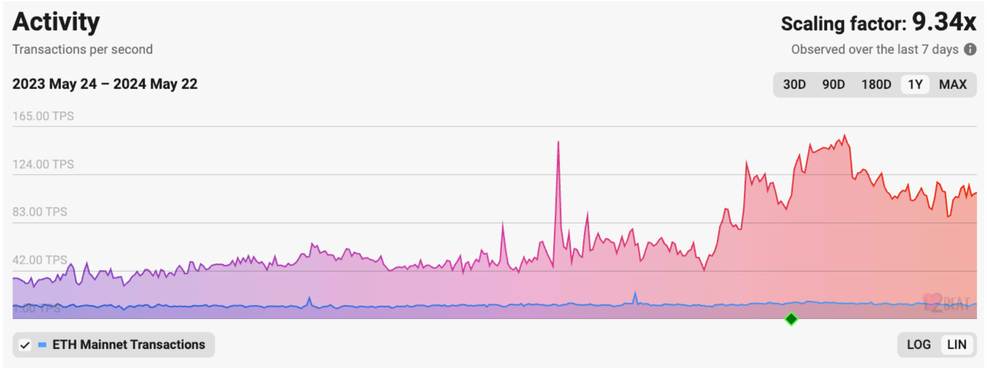
First-generation programmable blockchains (like Ethereum)

- Expensive
- Slow
- Poor I/O with external world
- Hard to program



Next-generation blockchains: cheaper and faster

- Thanks to “Layer 2” roll-up architectures
  - Lower transaction fees (< $0.01 / tx)
  - Higher transaction throughput (100-1000 tps at ~13min finality)



(Source: L2Beat)

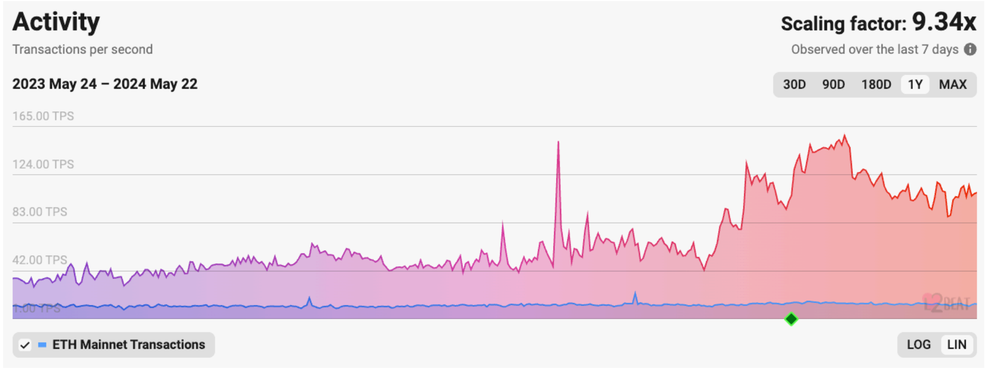
All L2s | Full Rollups

Name	Send ETH	Swap tokens
StarkNet	< $0.01	< $0.01
Arbitrum One	< $0.01	$0.01
Optimism	< $0.01	$0.02
Polygon zkEVM	$0.02	$0.32
Metis Network	$0.03	$0.14
Loopring	$0.05	-
zkSync Lite	$0.06	$0.14
DeGate	$0.17	-

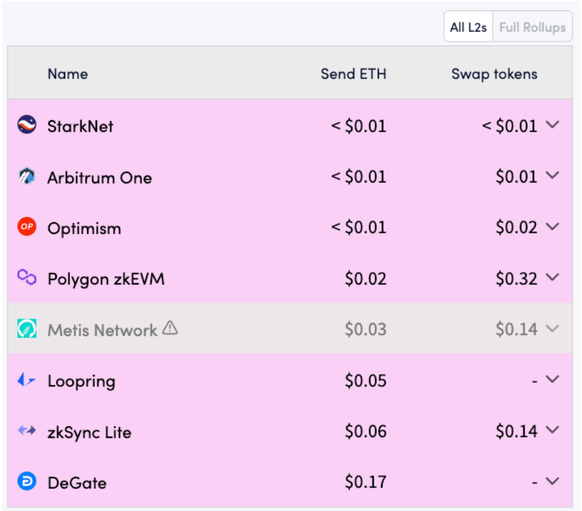
(Source: l2fees.info)

Next-generation blockchains: cheaper and faster

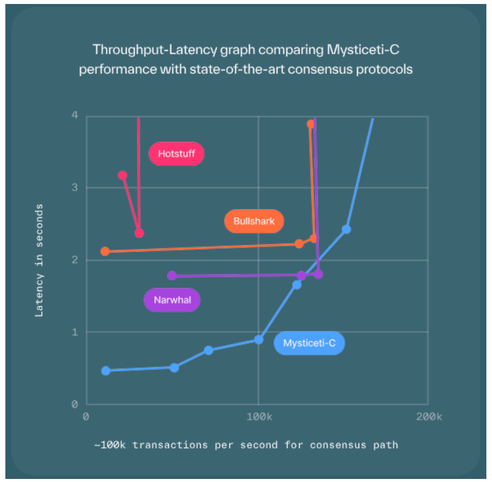
- Thanks to “Layer 2” roll-up architectures
  - Lower transaction fees (< $0.01 / tx)
  - Higher transaction throughput (100-1000 tps at ~13min finality)
- Bleeding-edge “Layer 1” blockchains achieve even better scaling
  - Sui Mysticeti: 100.000 tps at <1sec finality



(Source: L2Beat)



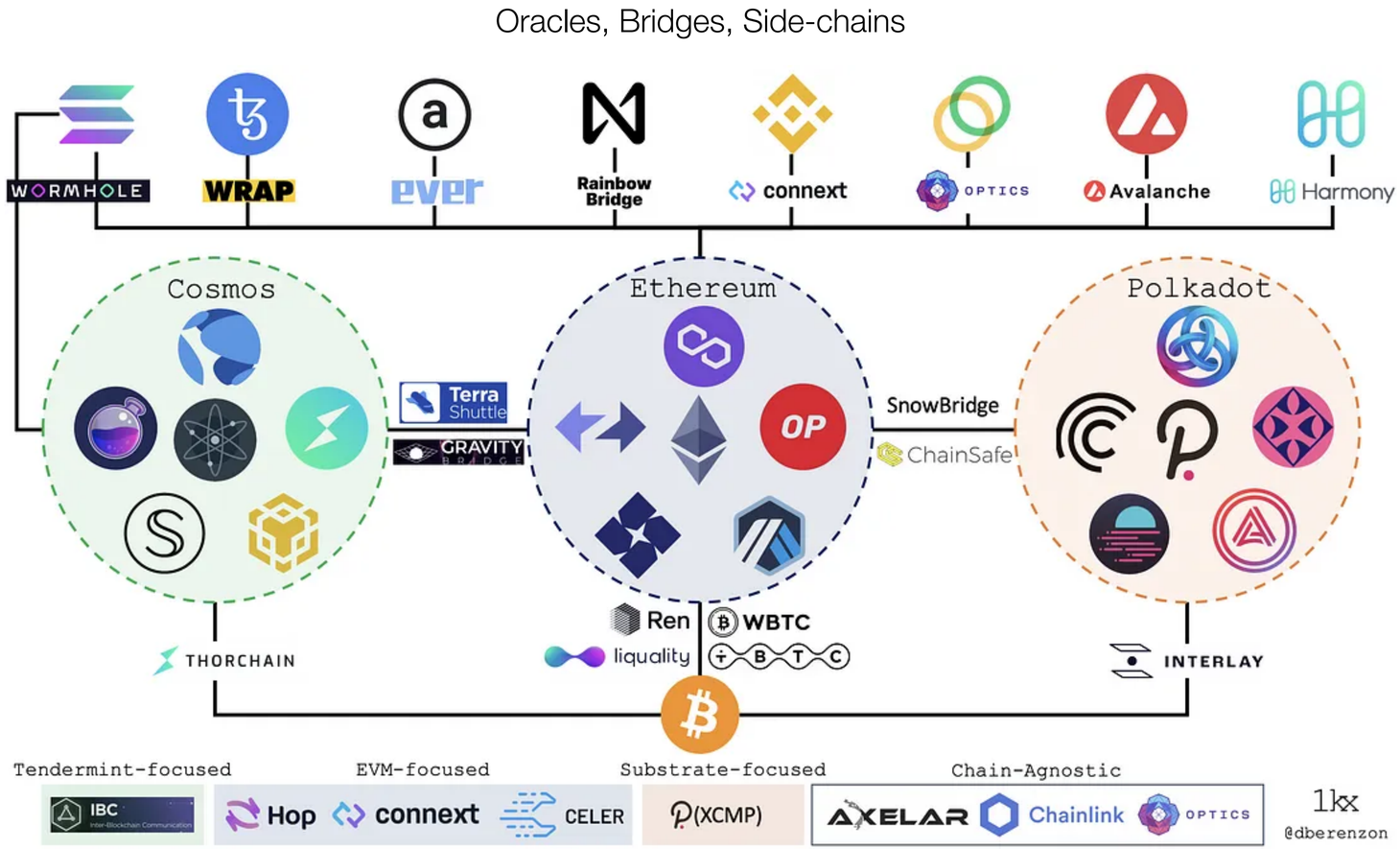
(Source: l2fees.info)



(Source: Sui / Mysten Labs, 2024)

KU LEUVEN DistriNet

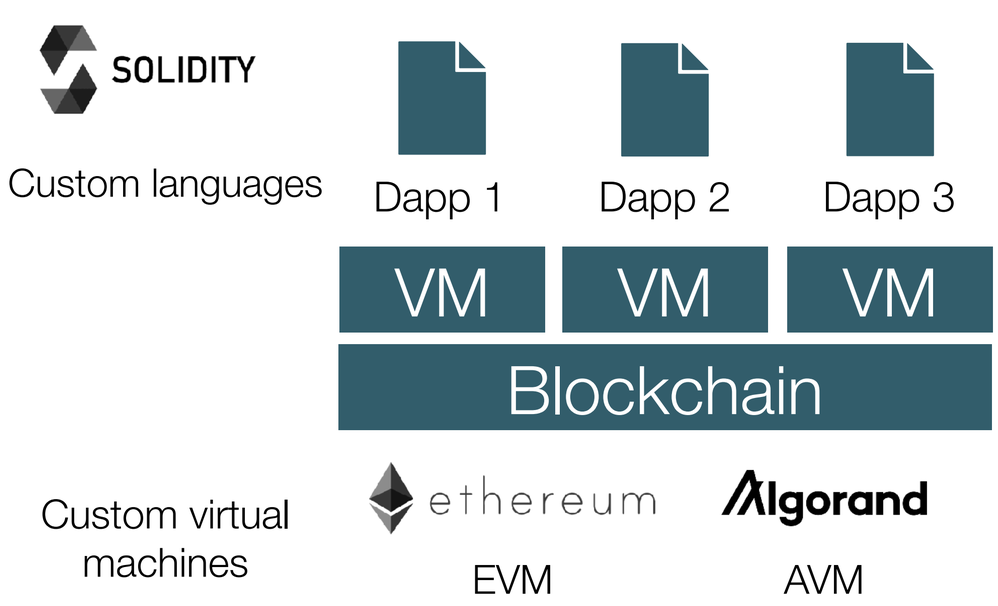
Next-generation blockchains: better I/O



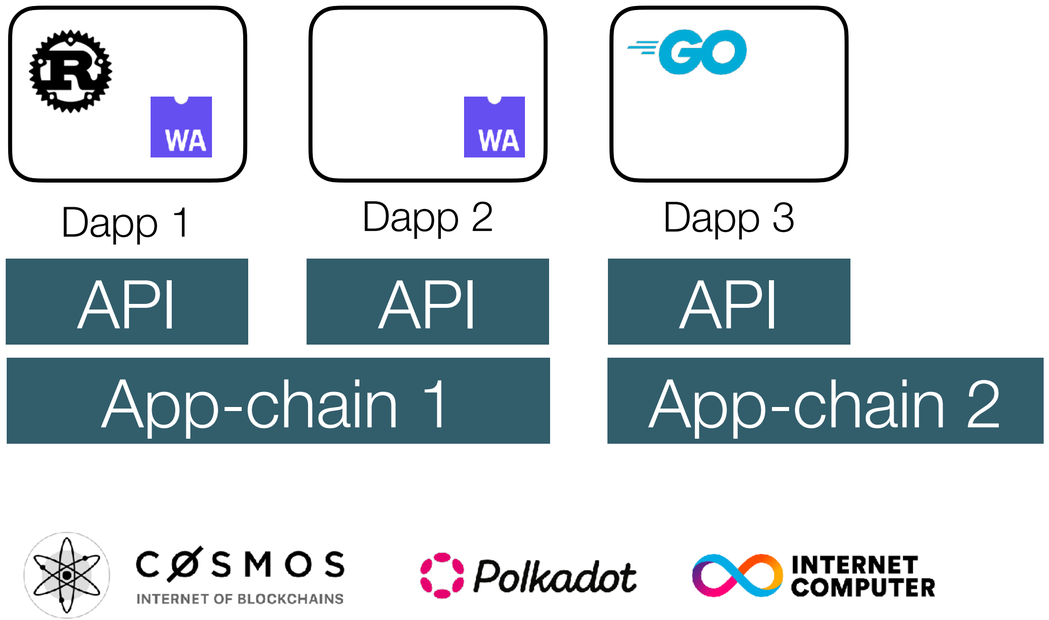
(Source: Dmitriy Berenzon, medium.com)

Next-generation blockchains: simpler to program

Single shared chain with
special-purpose language & runtime

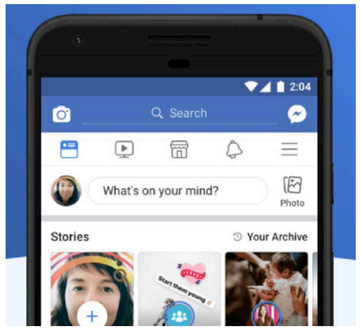


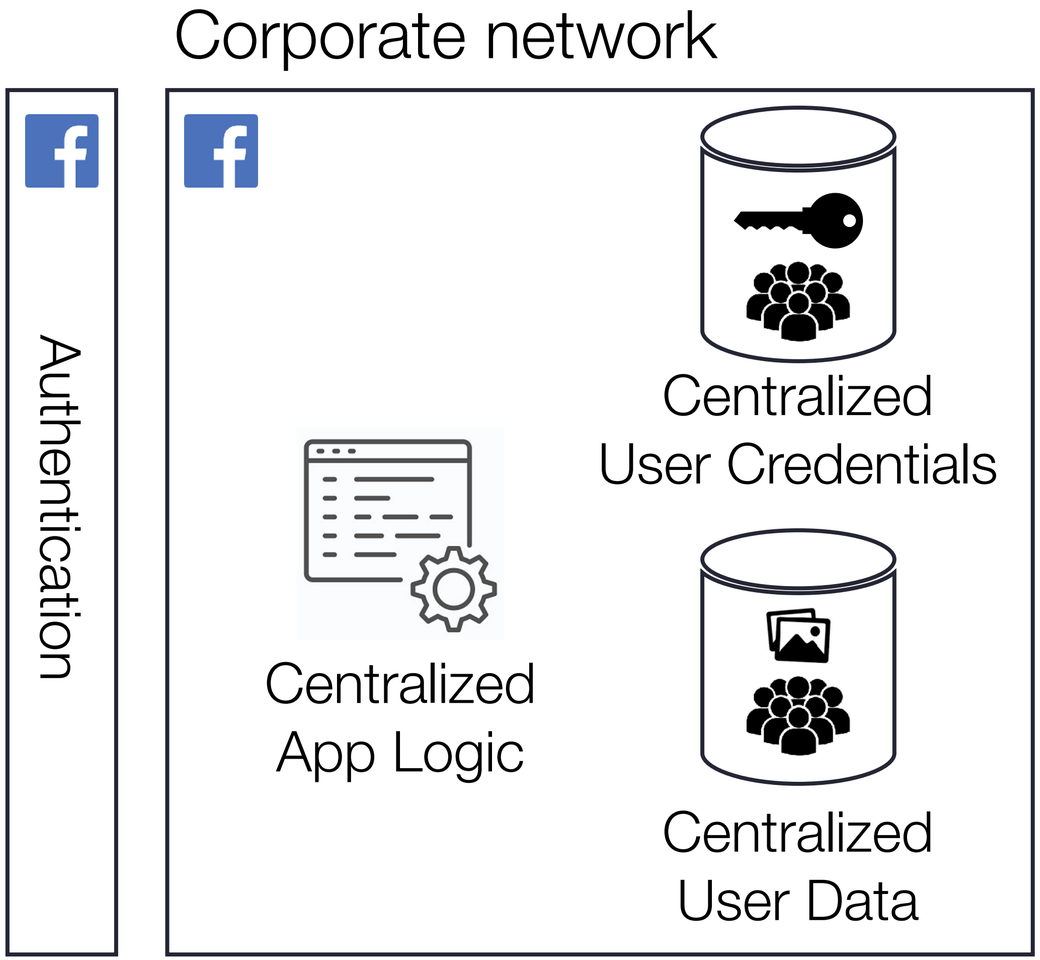
Many “application-specific” but interoperable chains
with **general-purpose** languages & runtimes



3. Blockchains enable a new way of building internet applications

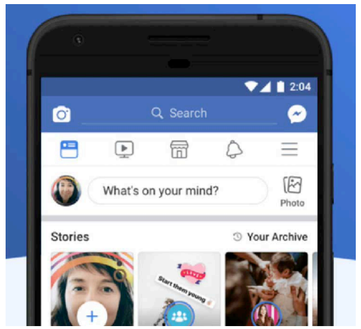
Today’s internet applications: corporate networks





Based on an example taken from Ali *et al*, “Blockstack: A Global Naming and Storage System Secured by Blockchains”, USENIX ATC 2016

The dark side of corporate networks



Kill third-party integrations
Walled Garden

Authentication

Corporate network

Massive
Data leaks

Deplatforming

Centralized
User Credentials

Centralized
App Logic

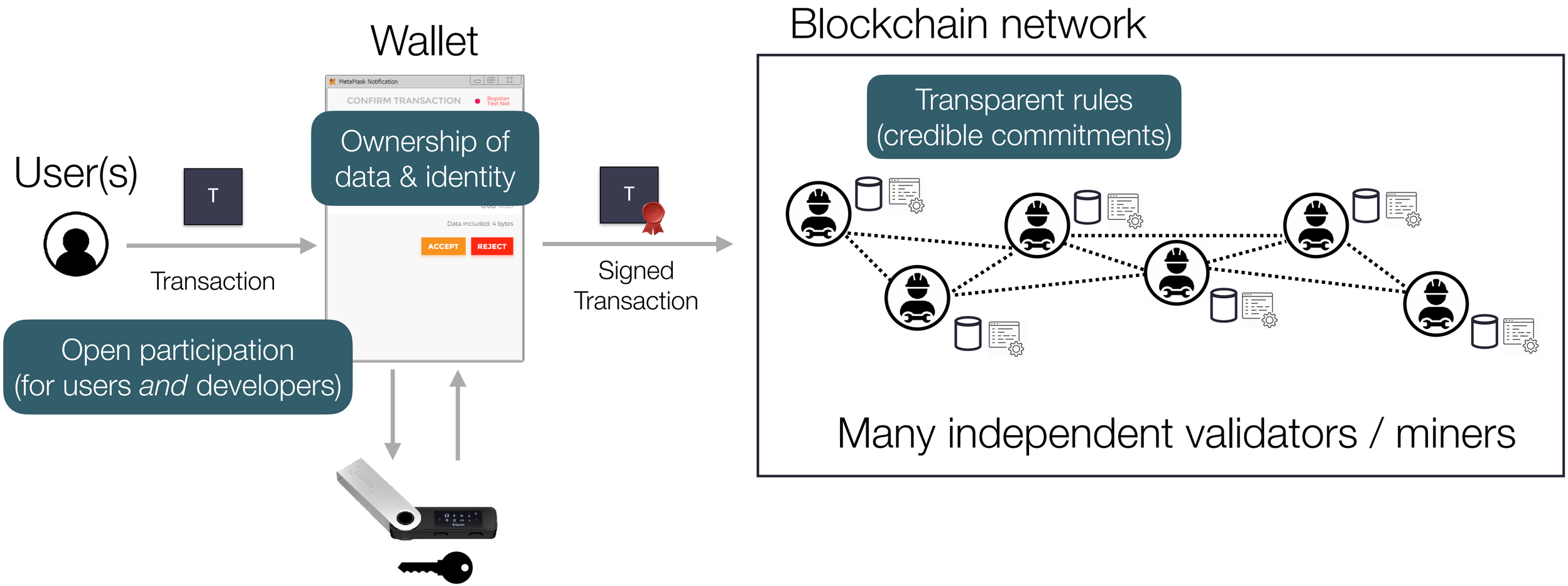
Corporate
interests

Centralized
User Data

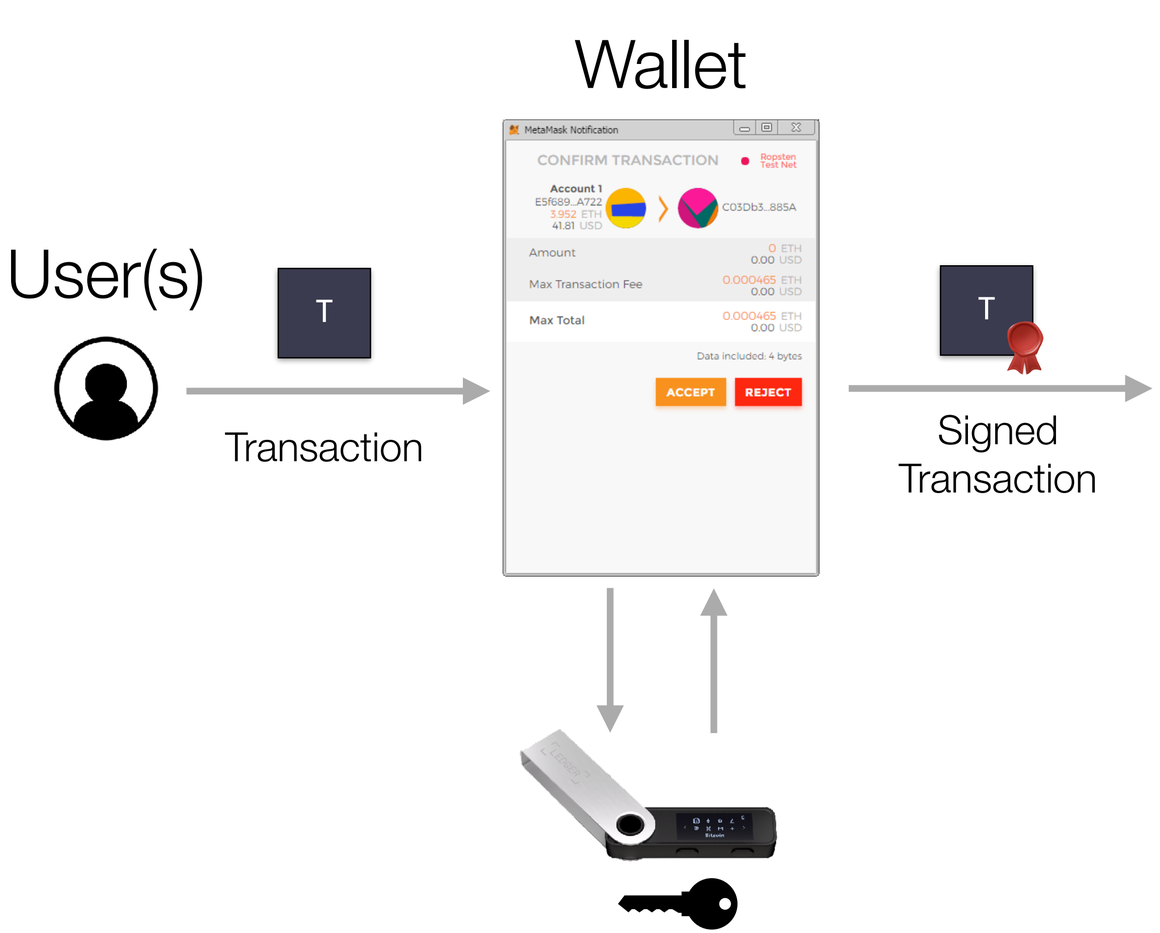
Surveillance
capitalism

Based on an example taken from Ali *et al*, “Blockstack: A Global Naming and Storage System Secured by Blockchains”, USENIX ATC 2016

A new way to build internet applications



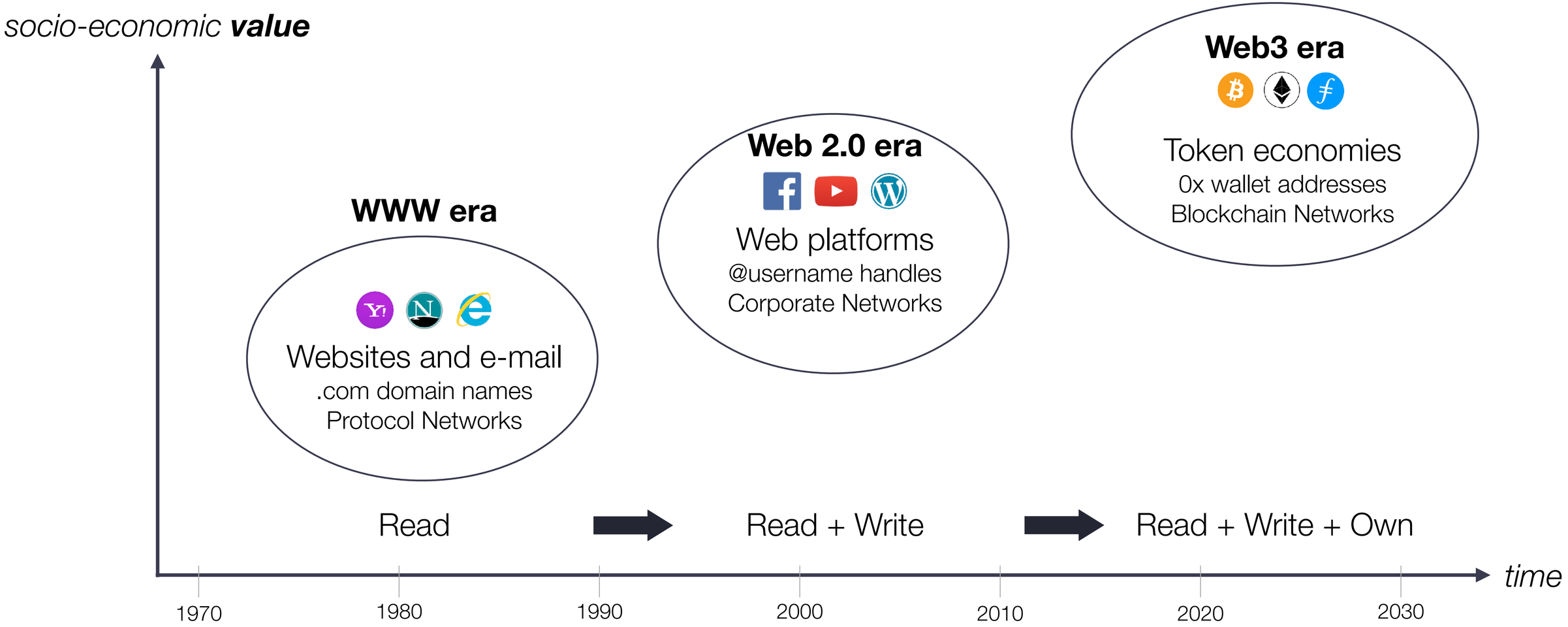
A new way to build internet applications



Decentralized services

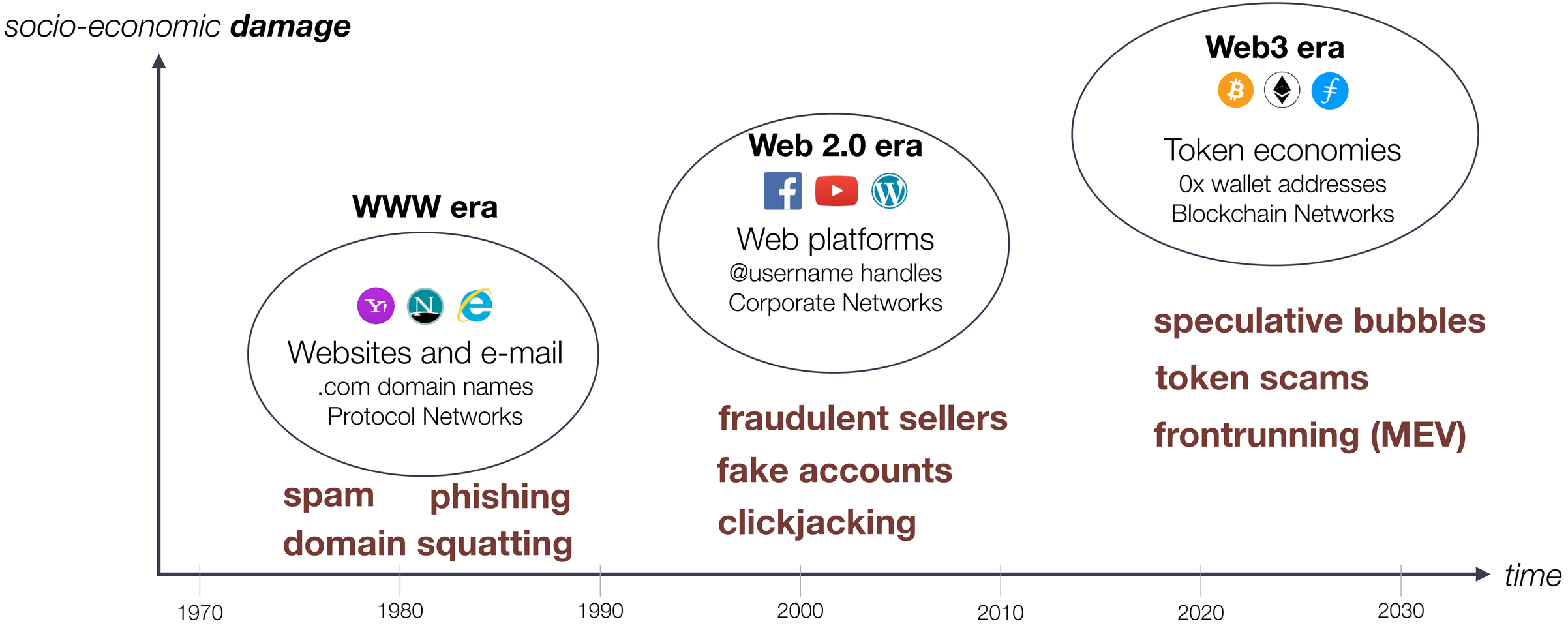
Payments	Bitcoin
Storage	Filecoin
Connectivity	Helium
Social media	Farcaster
Maps	Hivemapper
…	…

The evolution of the Web's application network architectures



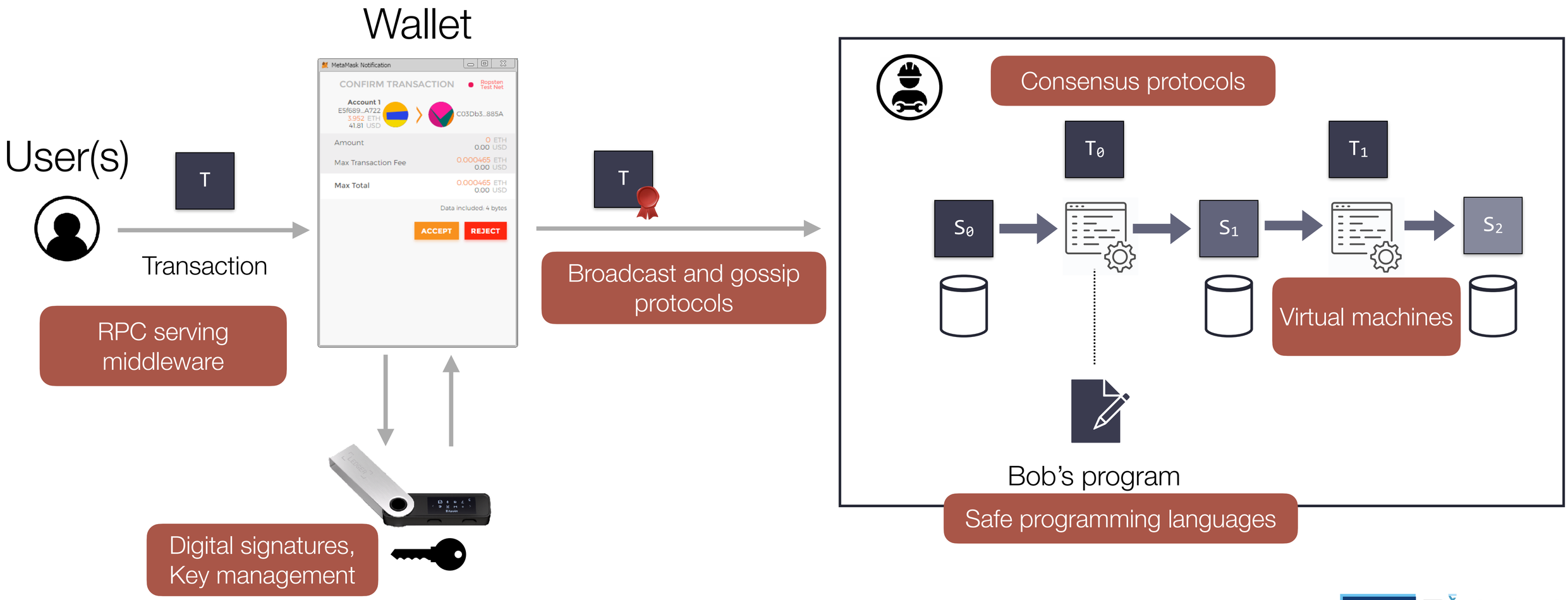
(sources: "Read Write Own", Chris Dixon, 2024 ; "Token Economy", Shermin Voshmgir, 2019 ; "What exactly is Web3?", Juan Benet, Web3 summit 2018)

The Web's dark side

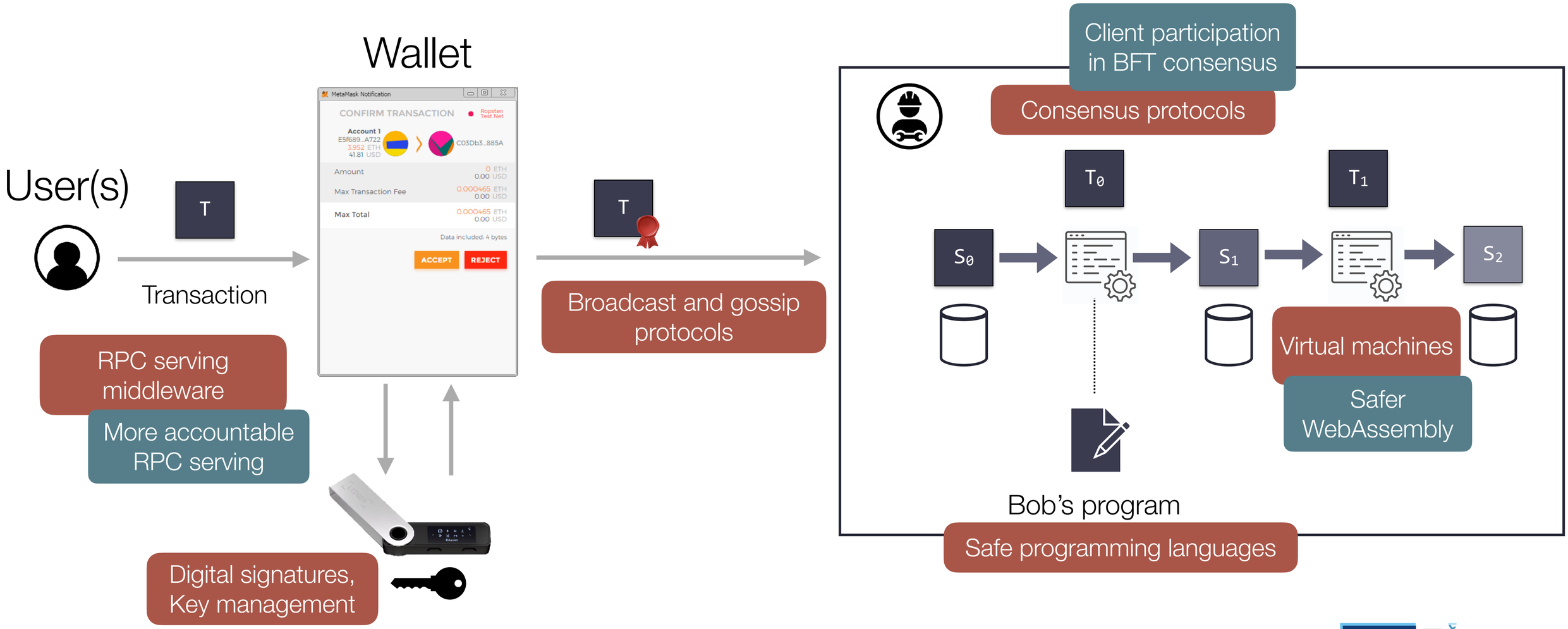


4. The role of academic research in Blockchain

Blockchain technology is deeply rooted in academic research



Strategic Research @ DistriNet: middleware, languages, protocols



KU LEUVEN DistriNet

Take-home messages

- 1. Blockchains are computers. Software platforms, like the Cloud.
- 2. They are rapidly becoming faster, cheaper, more connected & easier to program.
- 3. Why is this a Big Deal? The foundation for a new online era - “Web3”.
- 4. Strategic academic research is the foundation for future progress.
- Get ready for the next shift in computing.

KU LEUVEN

DistriNet

Blockchains as Trusted Computers: Unraveling the tech behind Web 3

Tom Van Cutsem
May 2024

Thank you for listening

tvcutsem.github.io be.linkedin.com/in/tomvc github.com/tvcutsem x.com/tvcutsem @tvcutsem@techhub.social