KU LEUVEN

DistriNet

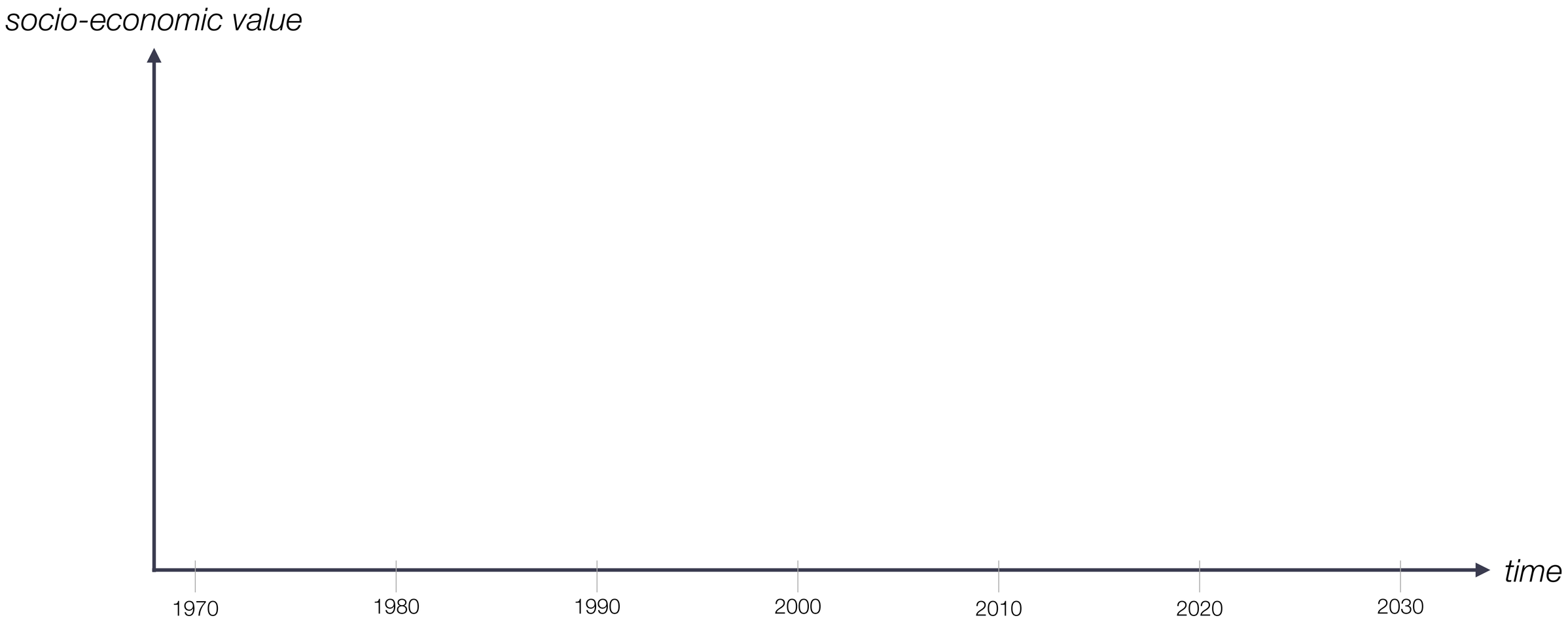
Inaugural Lecture

Secure and dependable software services for the Internet of Value

Tom Van Cutsem
November 2022

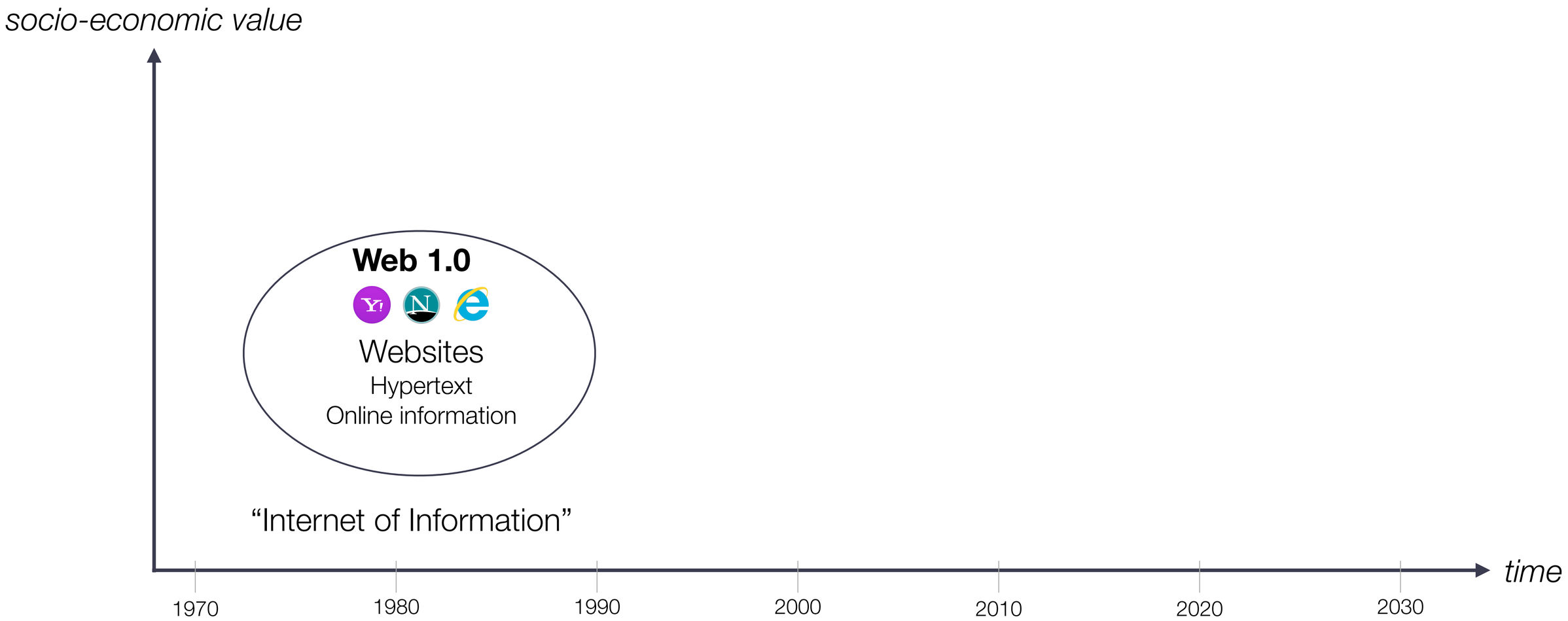
tvcutsem.github.io be.linkedin.com/in/tomvc github.com/tvcutsem twitter.com/tvcutsem

From the “Internet of Information” to the “Internet of Value”



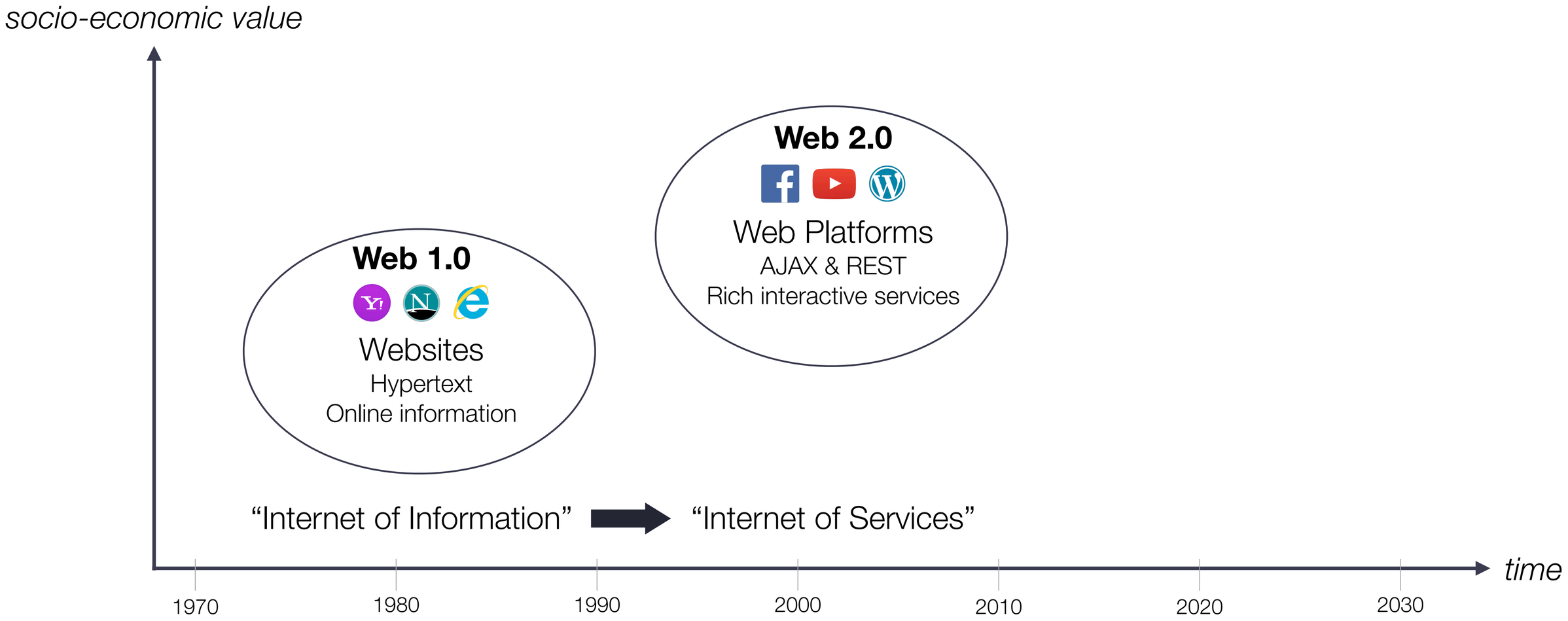
(source: “Token Economy”, Shermin Voshmgir, 2019 and “What exactly is Web3?”, Juan Benet, Web3 summit 2018)

From the “Internet of Information” to the “Internet of Value”



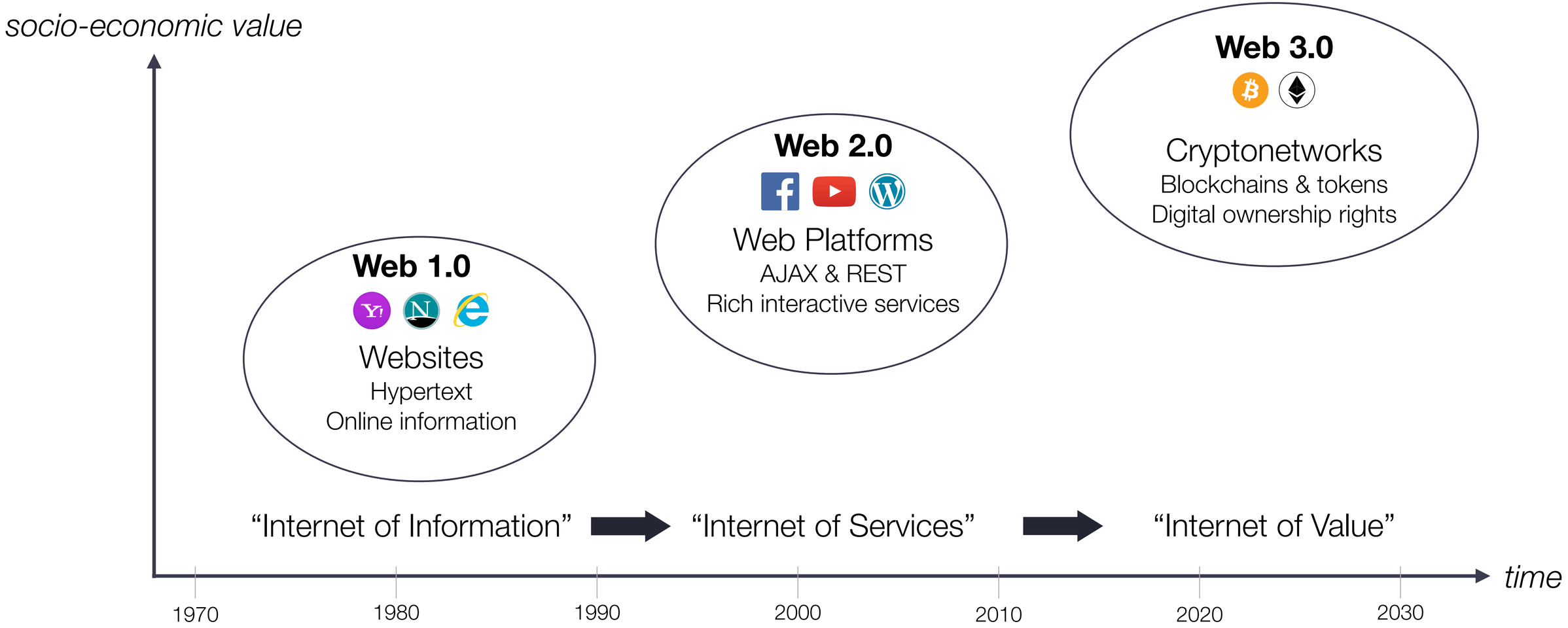
(source: “Token Economy”, Shermin Voshmgir, 2019 and “What exactly is Web3?”, Juan Benet, Web3 summit 2018)

From the “Internet of Information” to the “Internet of Value”



(source: “Token Economy”, Shermin Voshmgir, 2019 and “What exactly is Web3?”, Juan Benet, Web3 summit 2018)

From the “Internet of Information” to the “Internet of Value”

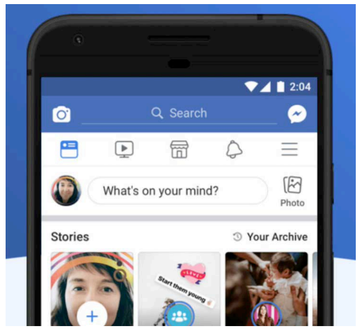


(source: “Token Economy”, Shermin Voshmgir, 2019 and “What exactly is Web3?”, Juan Benet, Web3 summit 2018)

How Web 2.0 internet services are typically architected

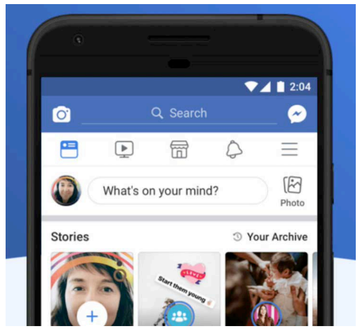
Based on an example taken from Ali *et al*, “Blockstack: A Global Naming and Storage System Secured by Blockchains”, USENIX ATC 2016

How Web 2.0 internet services are typically architected



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

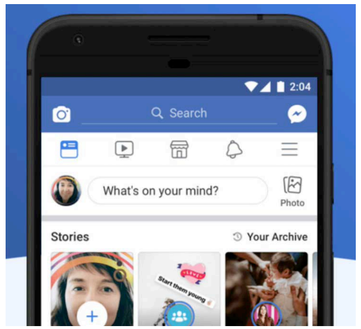
How Web 2.0 internet services are typically architected

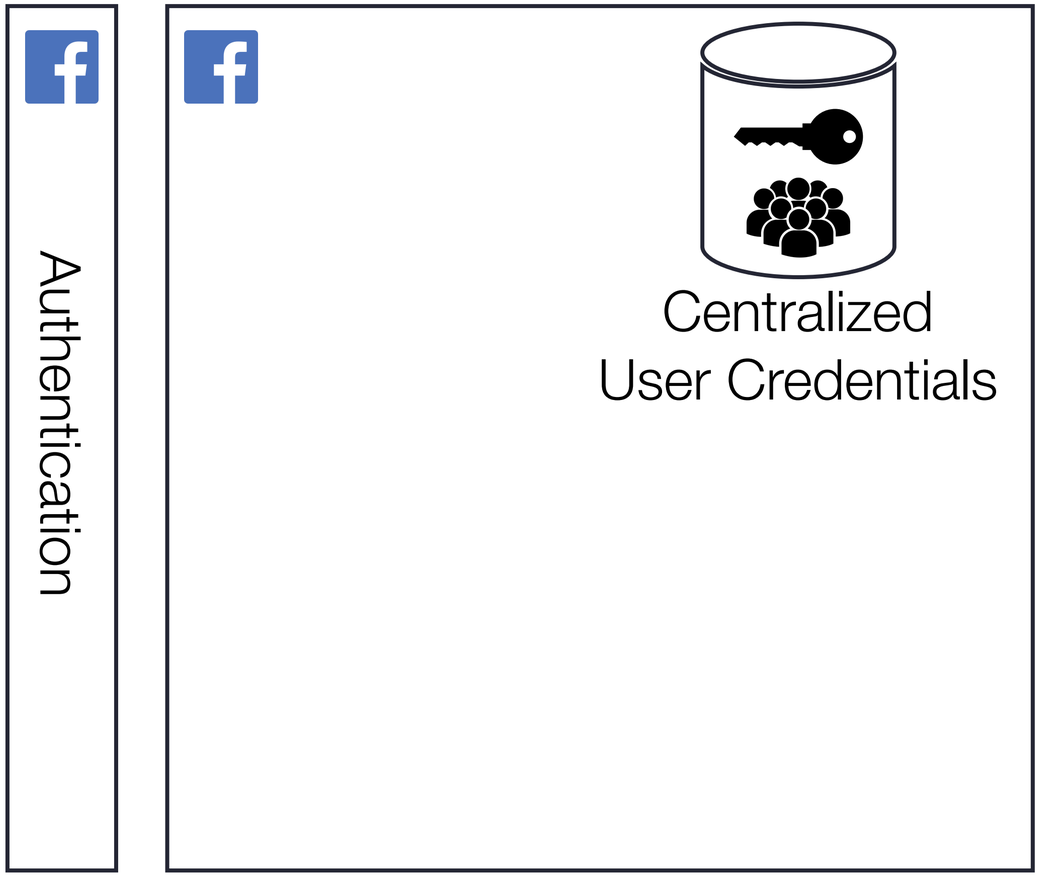


Authentication

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

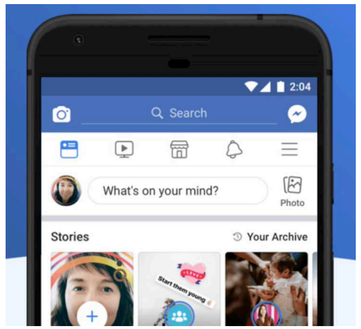
How Web 2.0 internet services are typically architected

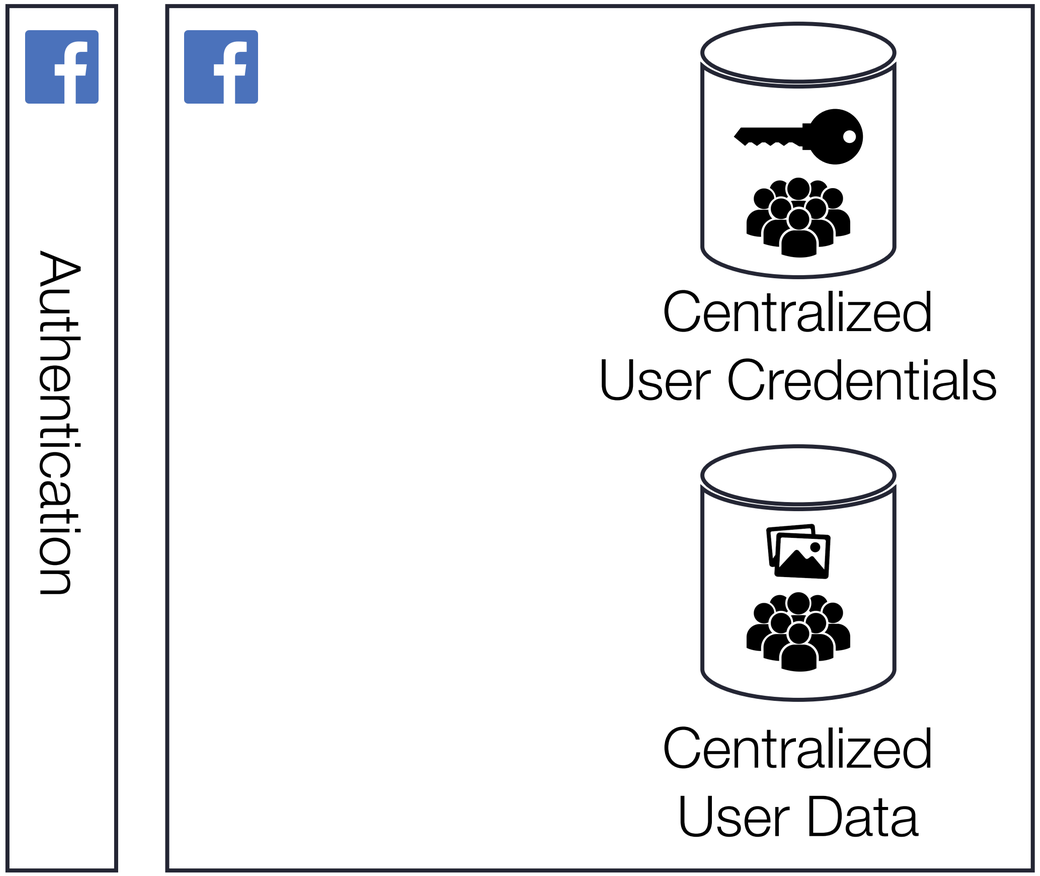




Based on an example taken from Ali *et al*, “Blockstack: A Global Naming and Storage System Secured by Blockchains”, USENIX ATC 2016

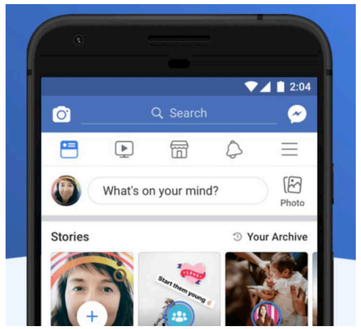
How Web 2.0 internet services are typically architected

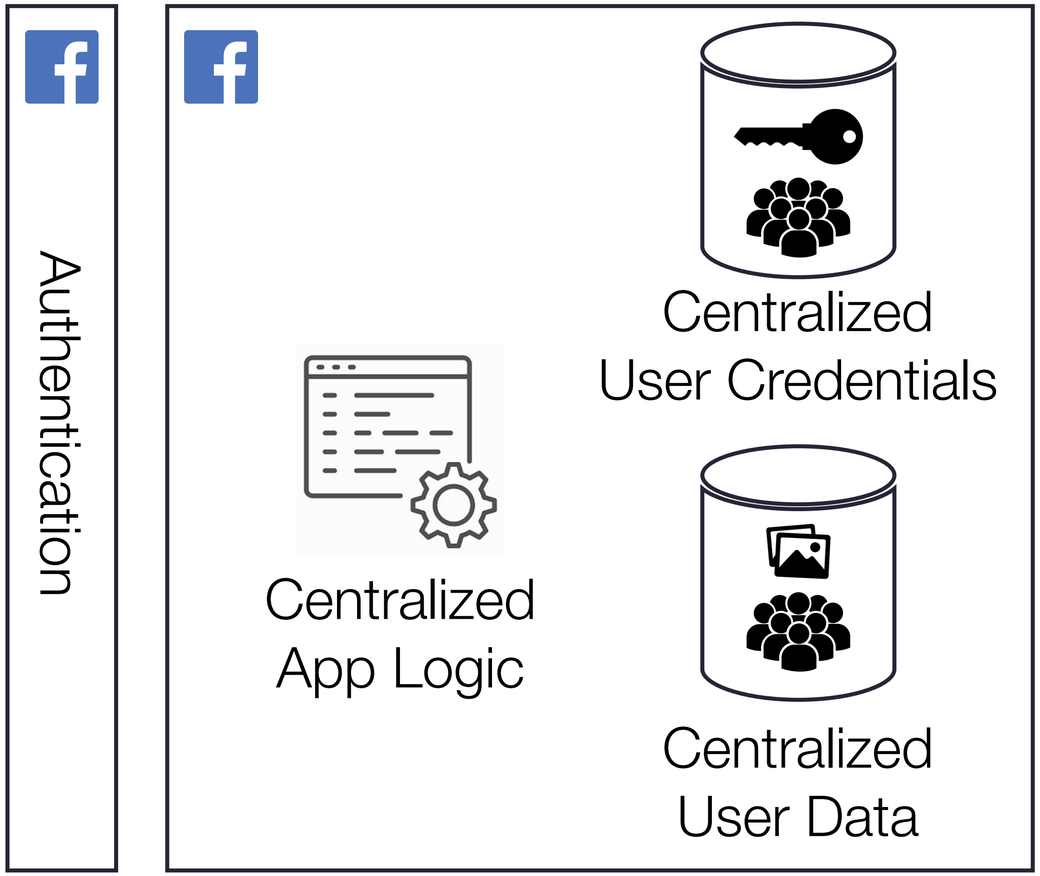




Based on an example taken from Ali *et al*, “Blockstack: A Global Naming and Storage System Secured by Blockchains”, USENIX ATC 2016

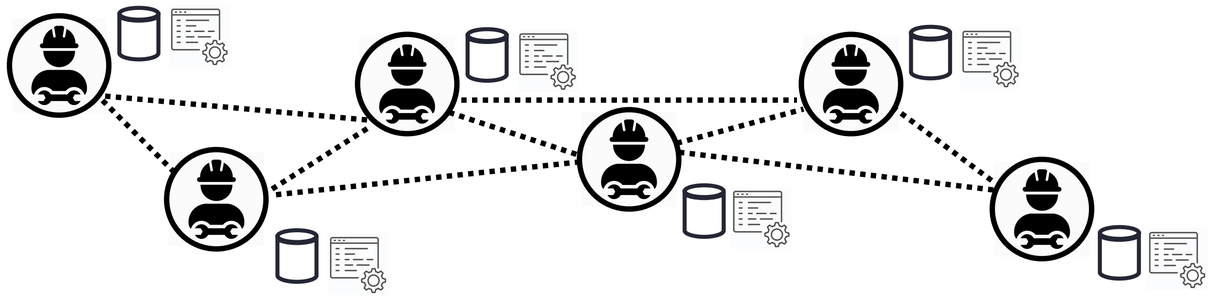
How Web 2.0 internet services are typically architected





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

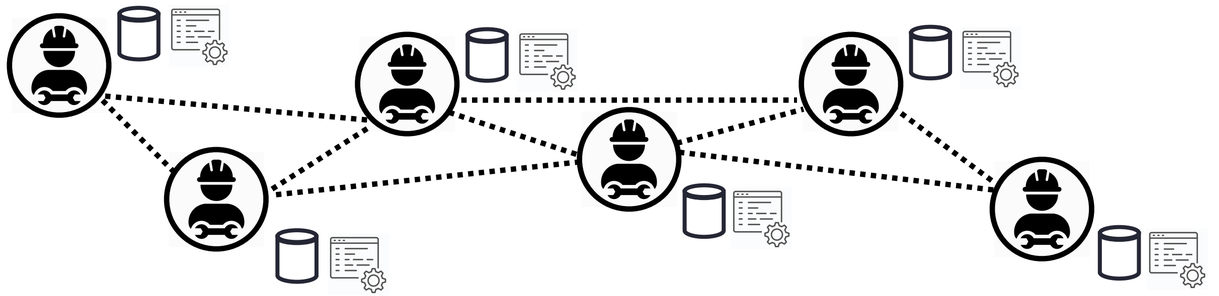
How Web 3.0 internet services are typically architected



Many service operators

How Web 3.0 internet services are typically architected

Decentralized service

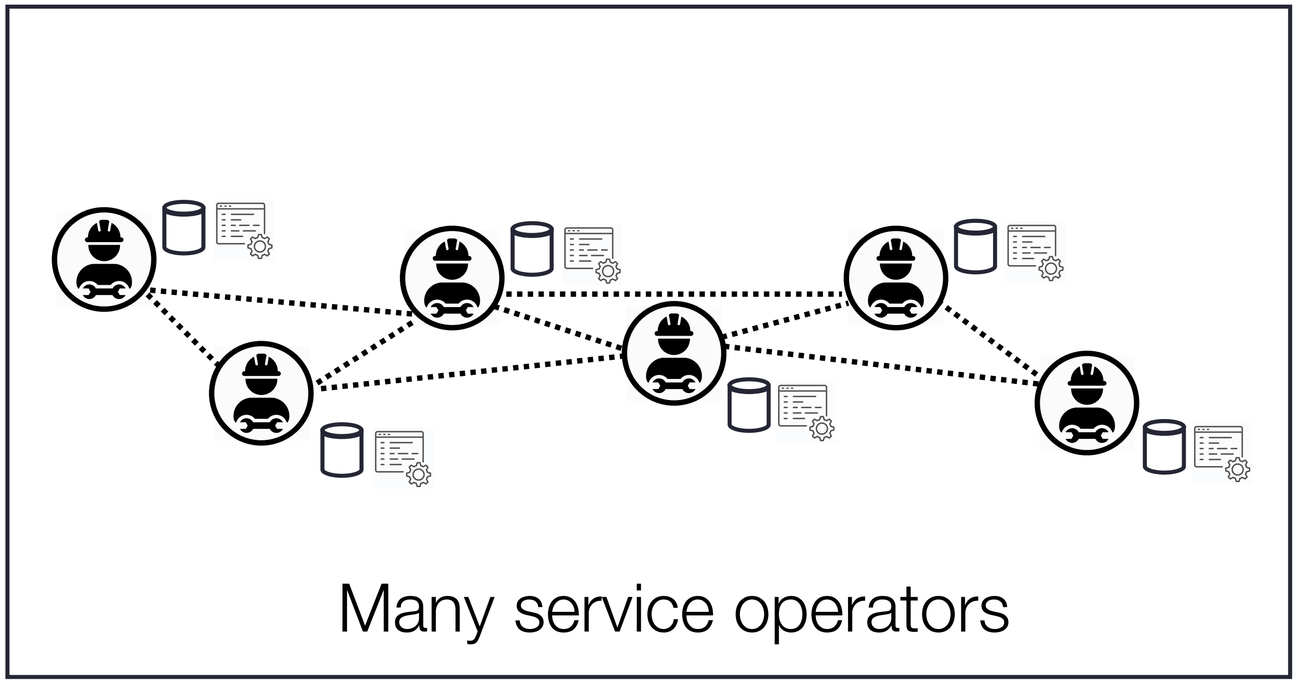


Many service operators

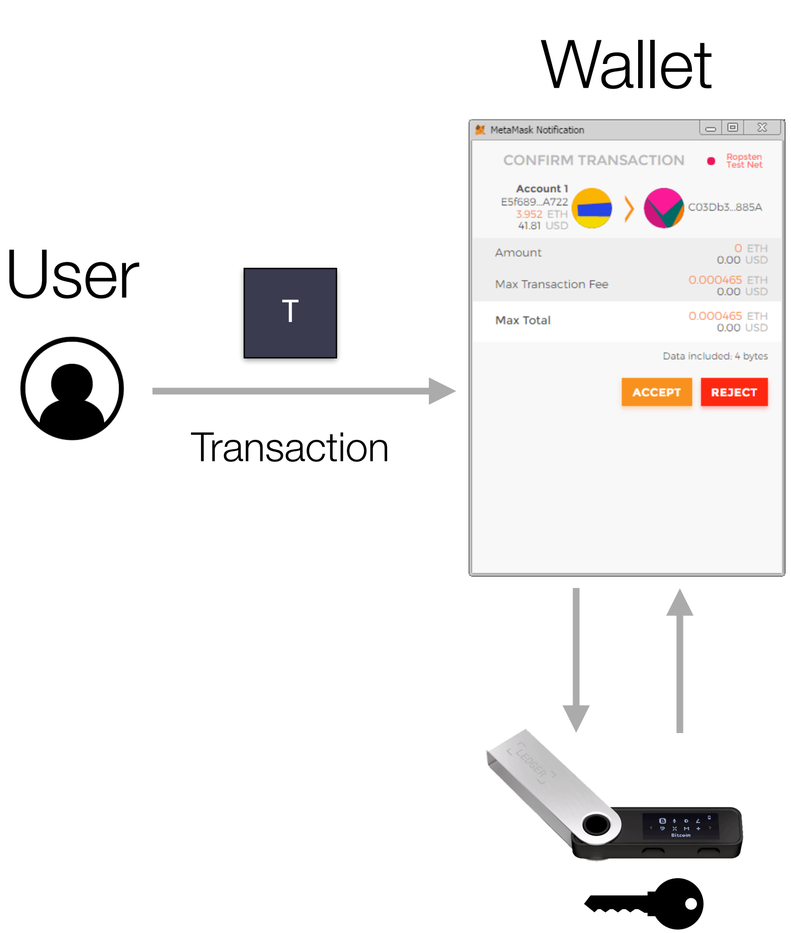
How Web 3.0 internet services are typically architected

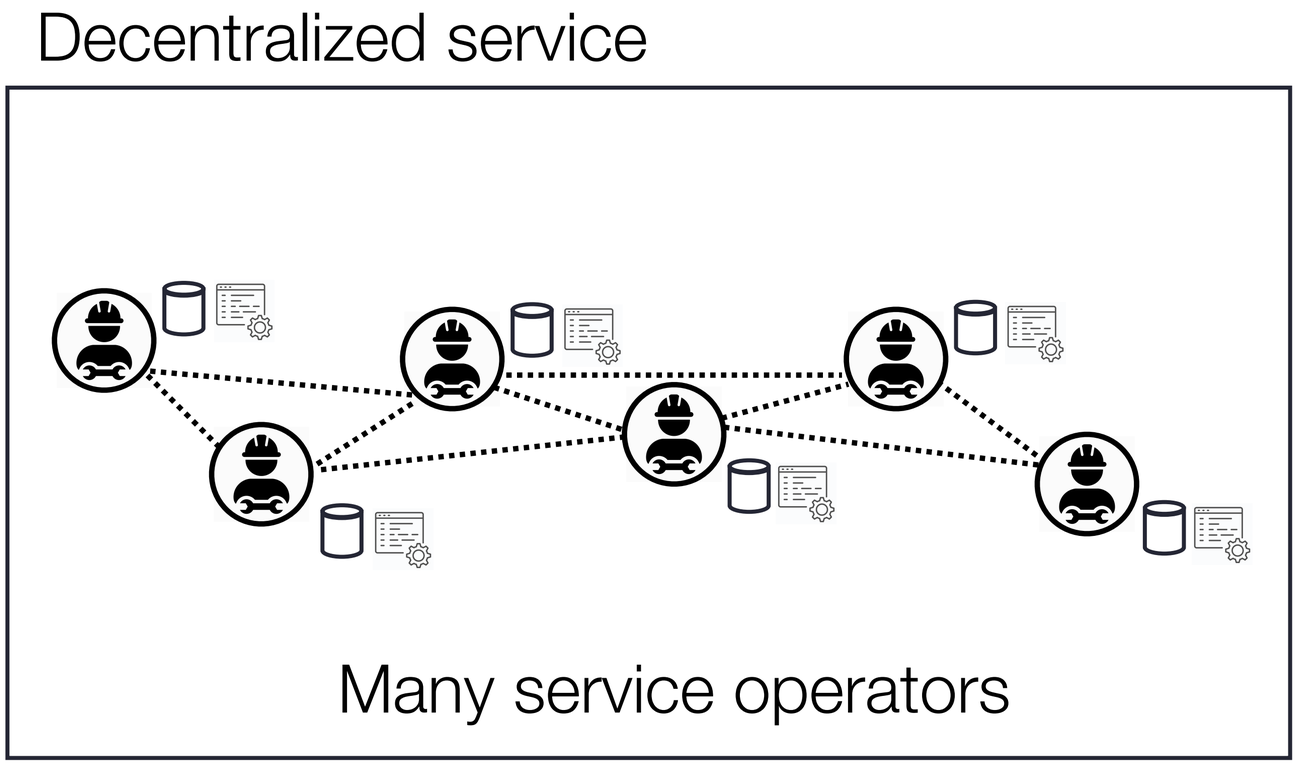
User

Decentralized service

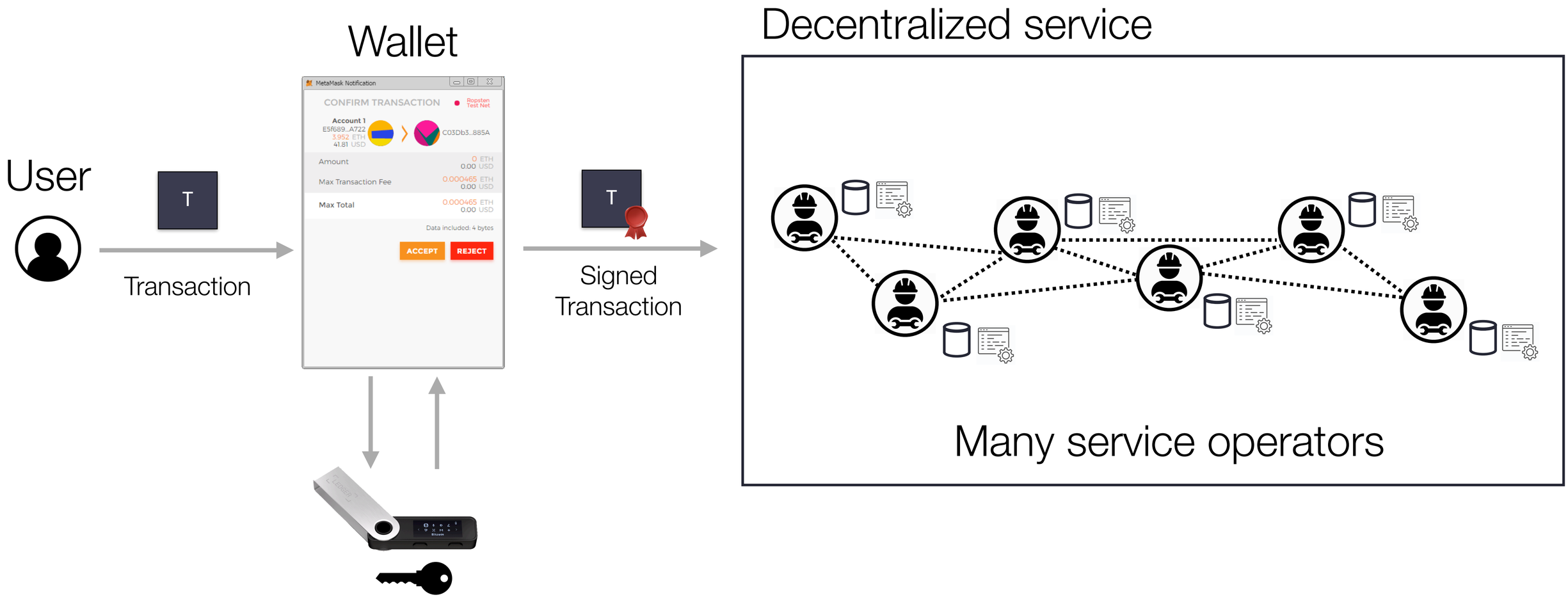


How Web 3.0 internet services are typically architected

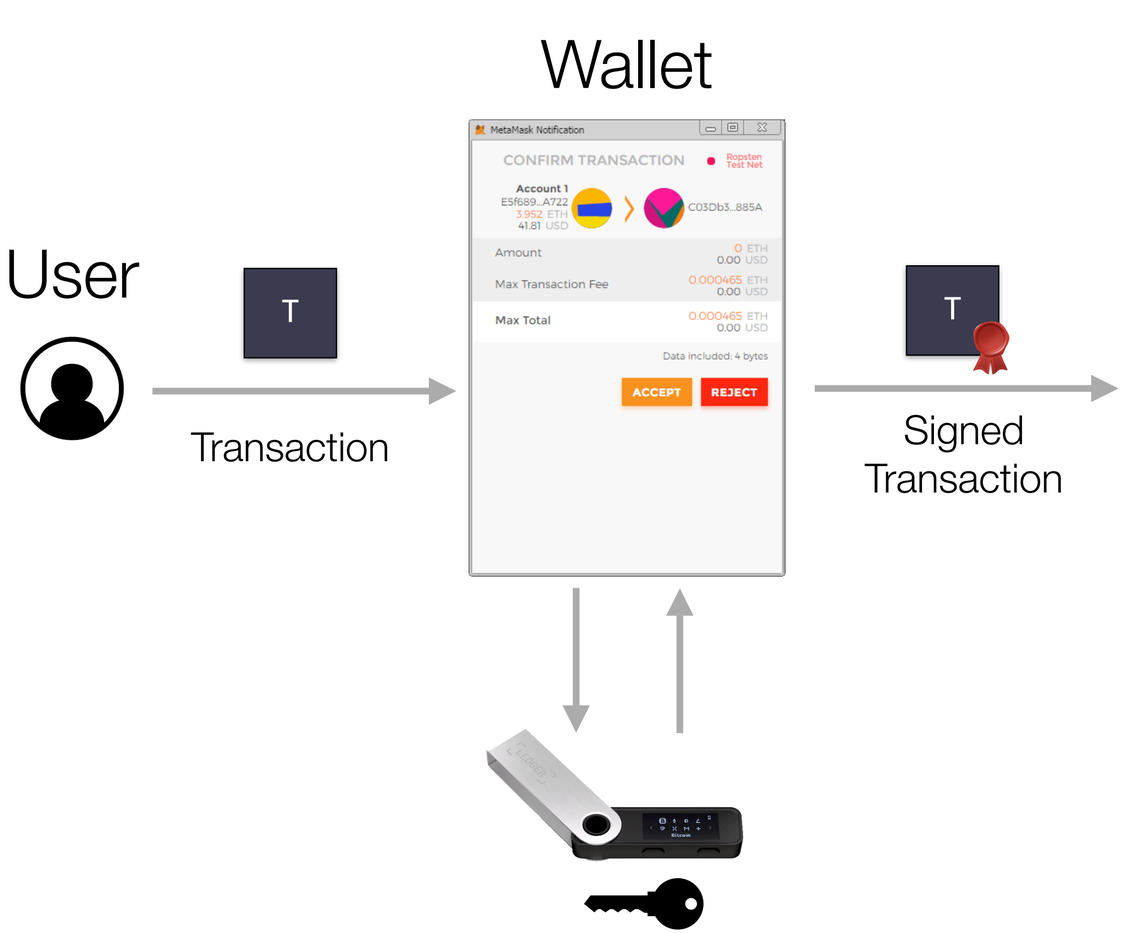




How Web 3.0 internet services are typically architected



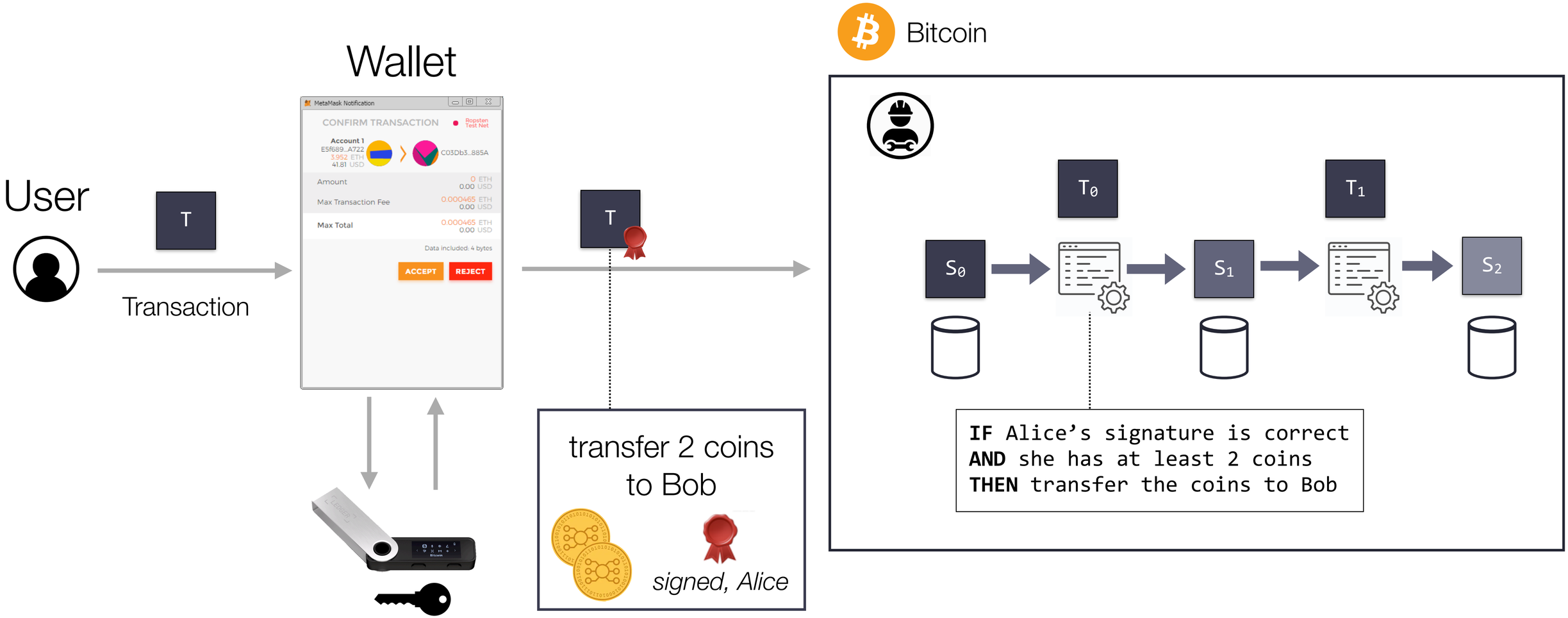
How Web 3.0 internet services are typically architected



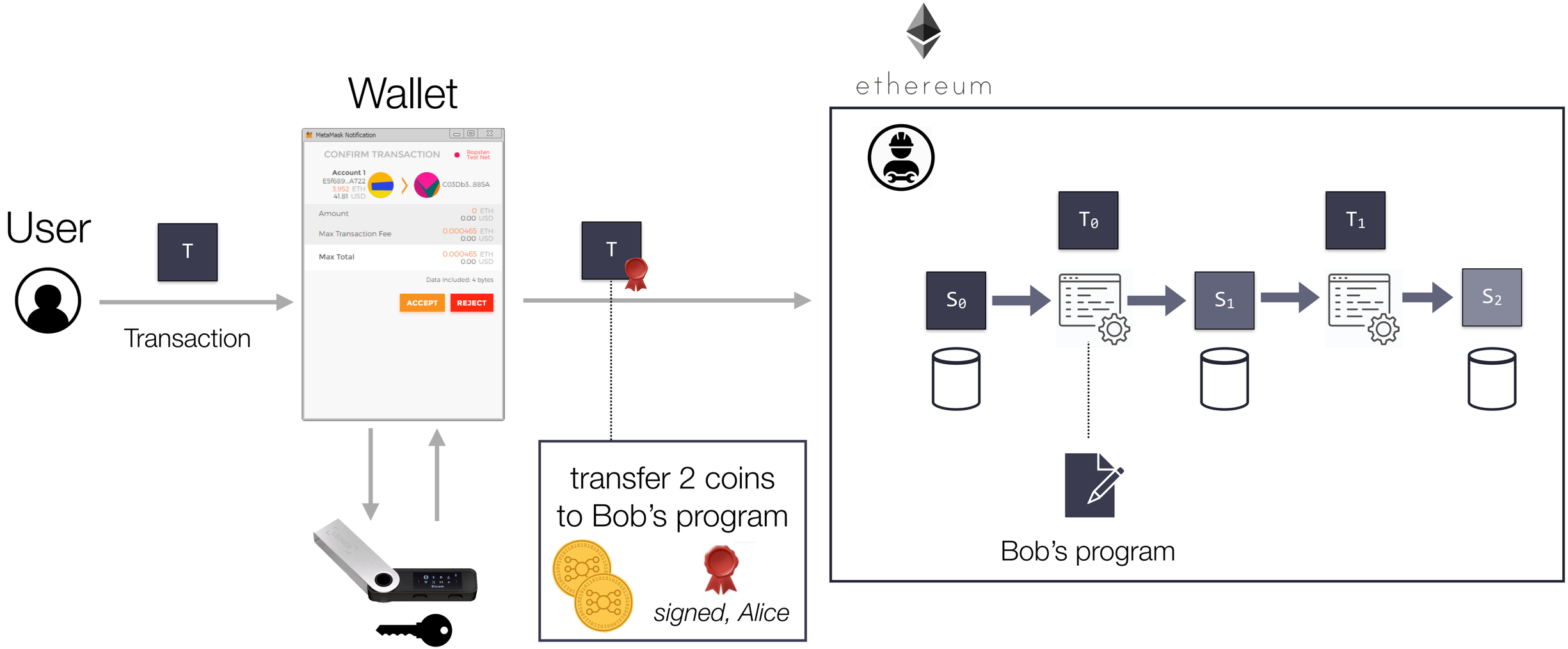
Decentralized service

Payments	Bitcoin
Storage	Filecoin
Naming	ENS
Identity	Civic
Wireless	Helium

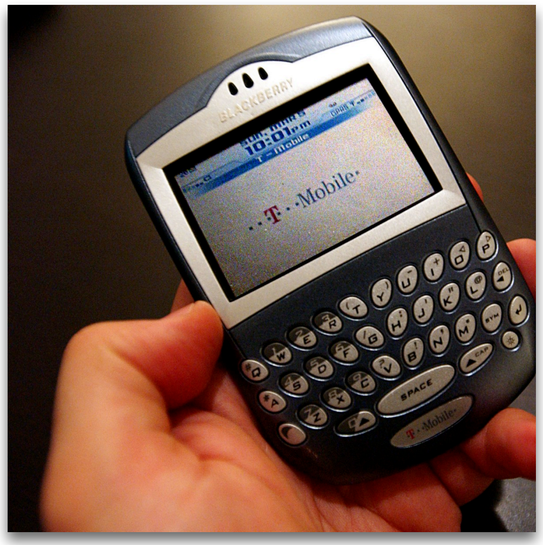
Web 3.0 services as highly reliable transaction processing machines



Ethereum: general-purpose Web 3.0 service infrastructure



Application-specific

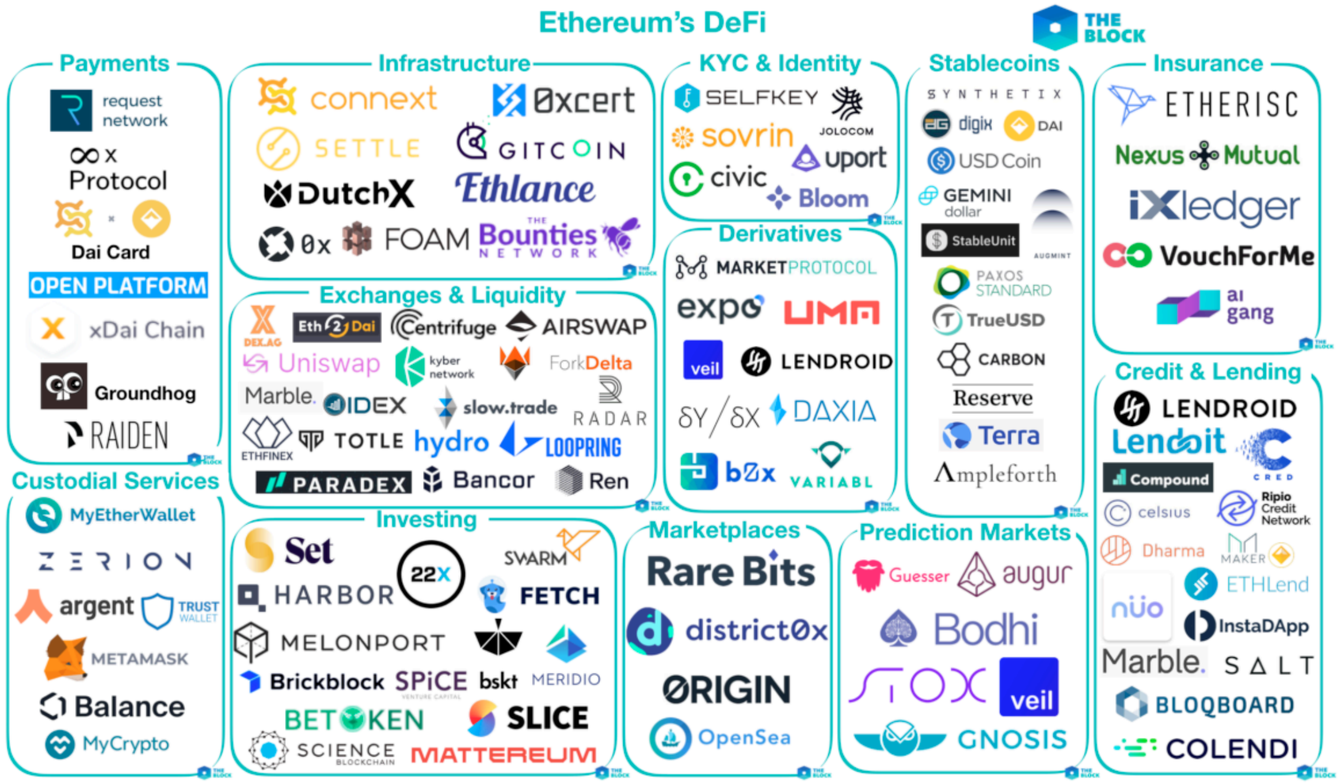


VS

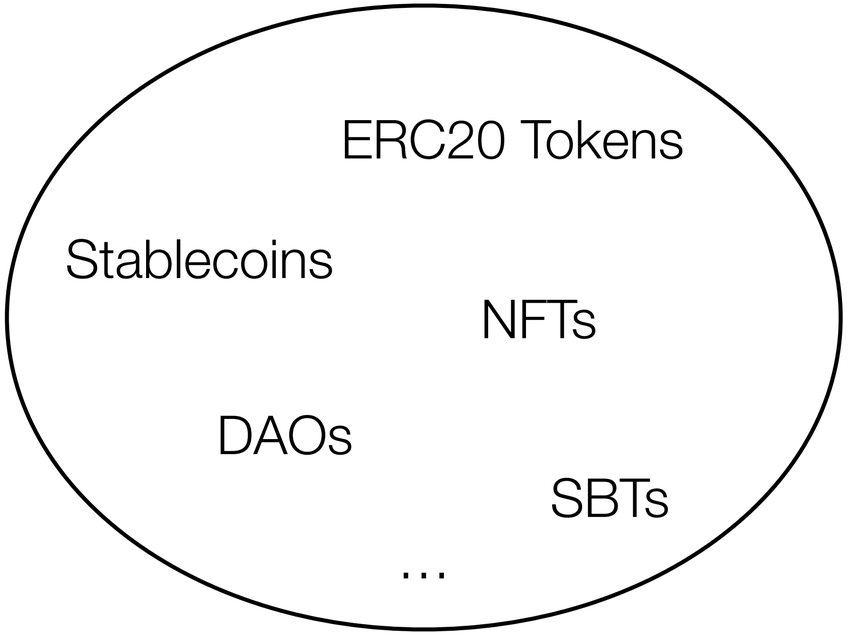
General-purpose

ethereum

Ethereum's "decentralized applications" ecosystem



(image credit: theblockcrypto.com)

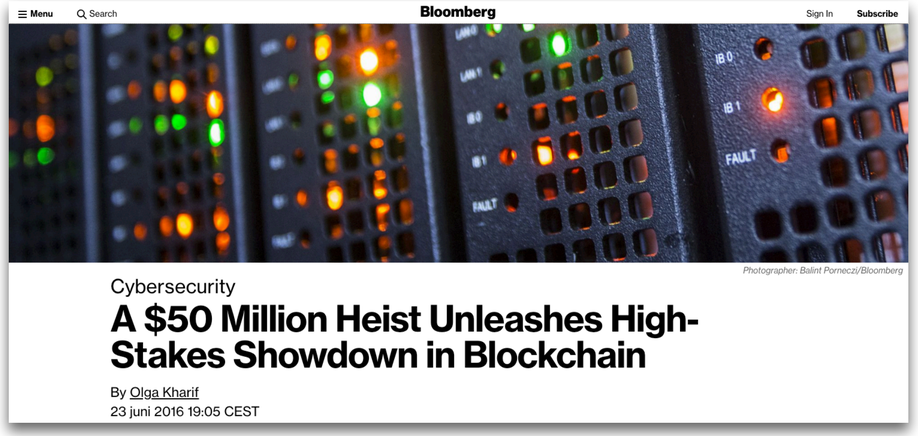


New kinds of **electronic rights** collectively worth over **$80 billion**

(source: coincodex.com, retrieved November 2022)

Substantial Application Security Risks

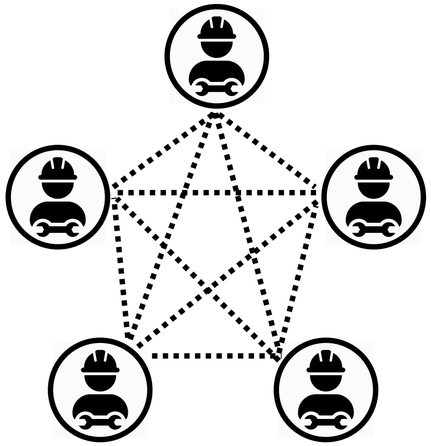
```
contract TomCoin {

    address public minter;
    mapping (address => uint) public balances;

    constructor() public {
        minter = msg.sender;
    }

    function mint(address receiver, uint amount) public {
        require(msg.sender == minter);
        balances[receiver] += amount;
    }

    function transfer(address receiver, uint amount) public {
        require(balances[msg.sender] >= amount);
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
    }
}
```



Substantial Engineering Challenges

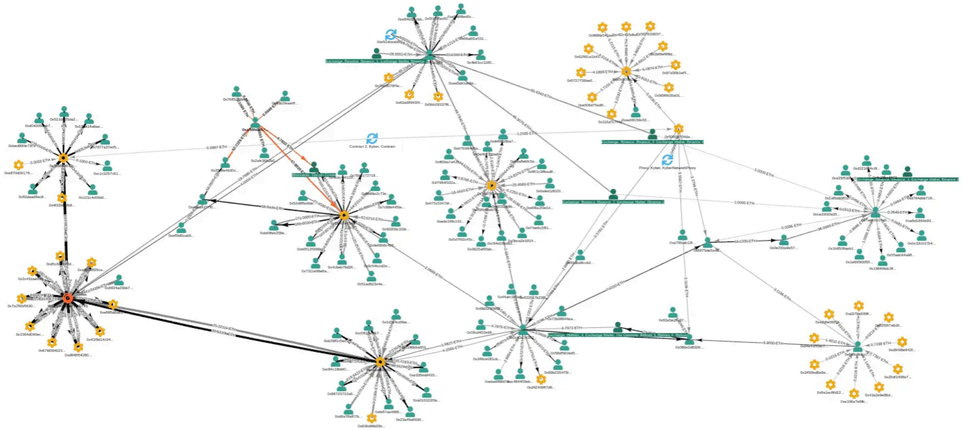
Transaction Scalability

Throughput    Decentralization

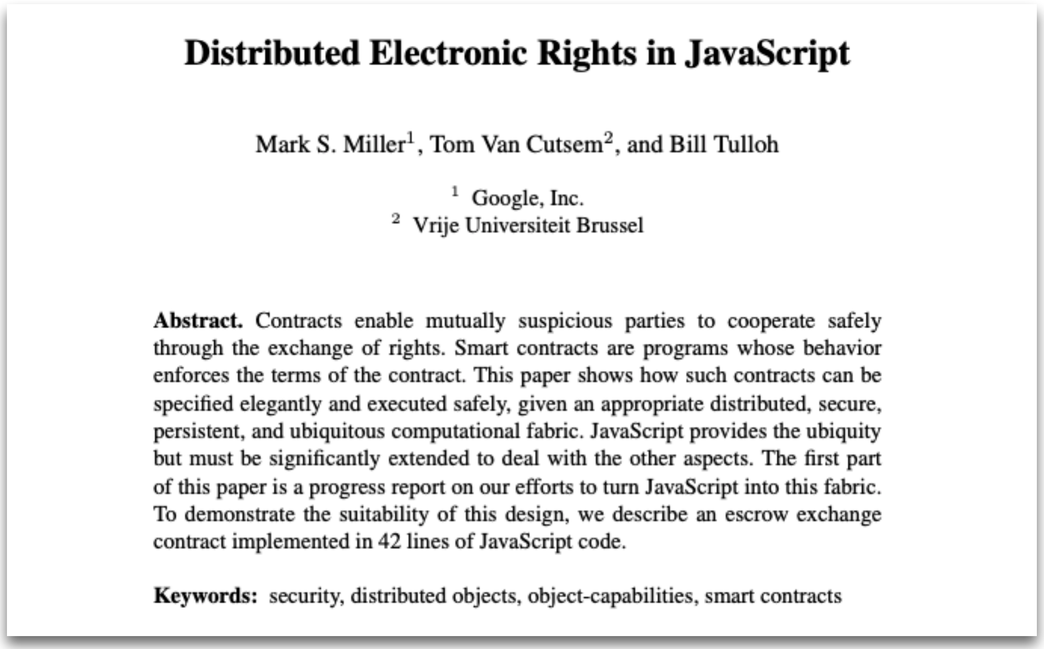


User Privacy

Privacy    Verifiability



Where do we start? Rethinking electronic rights as distributed objects



Distributed Electronic Rights in JavaScript

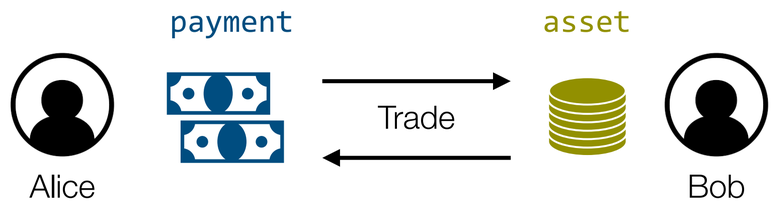
Mark S. Miller[1], Tom Van Cutsem[2], and Bill Tulloh

[1] Google, Inc.
[2] Vrije Universiteit Brussel

Abstract. Contracts enable mutually suspicious parties to cooperate safely through the exchange of rights. Smart contracts are programs whose behavior enforces the terms of the contract. This paper shows how such contracts can be specified elegantly and executed safely, given an appropriate distributed, secure, persistent, and ubiquitous computational fabric. JavaScript provides the ubiquity but must be significantly extended to deal with the other aspects. The first part of this paper is a progress report on our efforts to turn JavaScript into this fabric. To demonstrate the suitability of this design, we describe an escrow exchange contract implemented in 42 lines of JavaScript code.

Keywords: security, distributed objects, object-capabilities, smart contracts

(Miller, Van Cutsem and Tulloh, ESOP 2013)

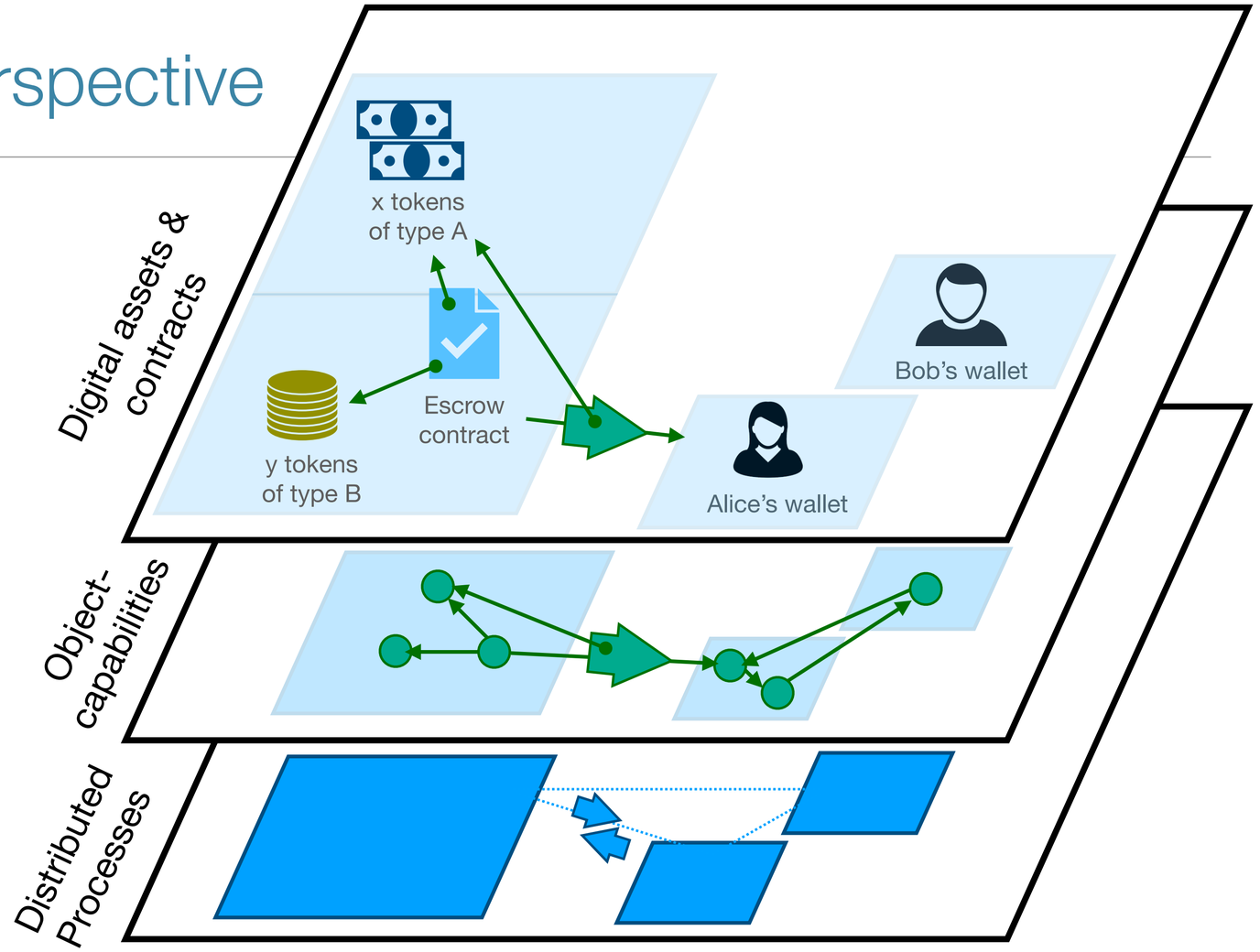



```
let payment = myPurse ! makePurse();
let ack = payment ! deposit(10, myPurse);
let asset = ack.then(_ => bob ! buy(desc, payment));
```

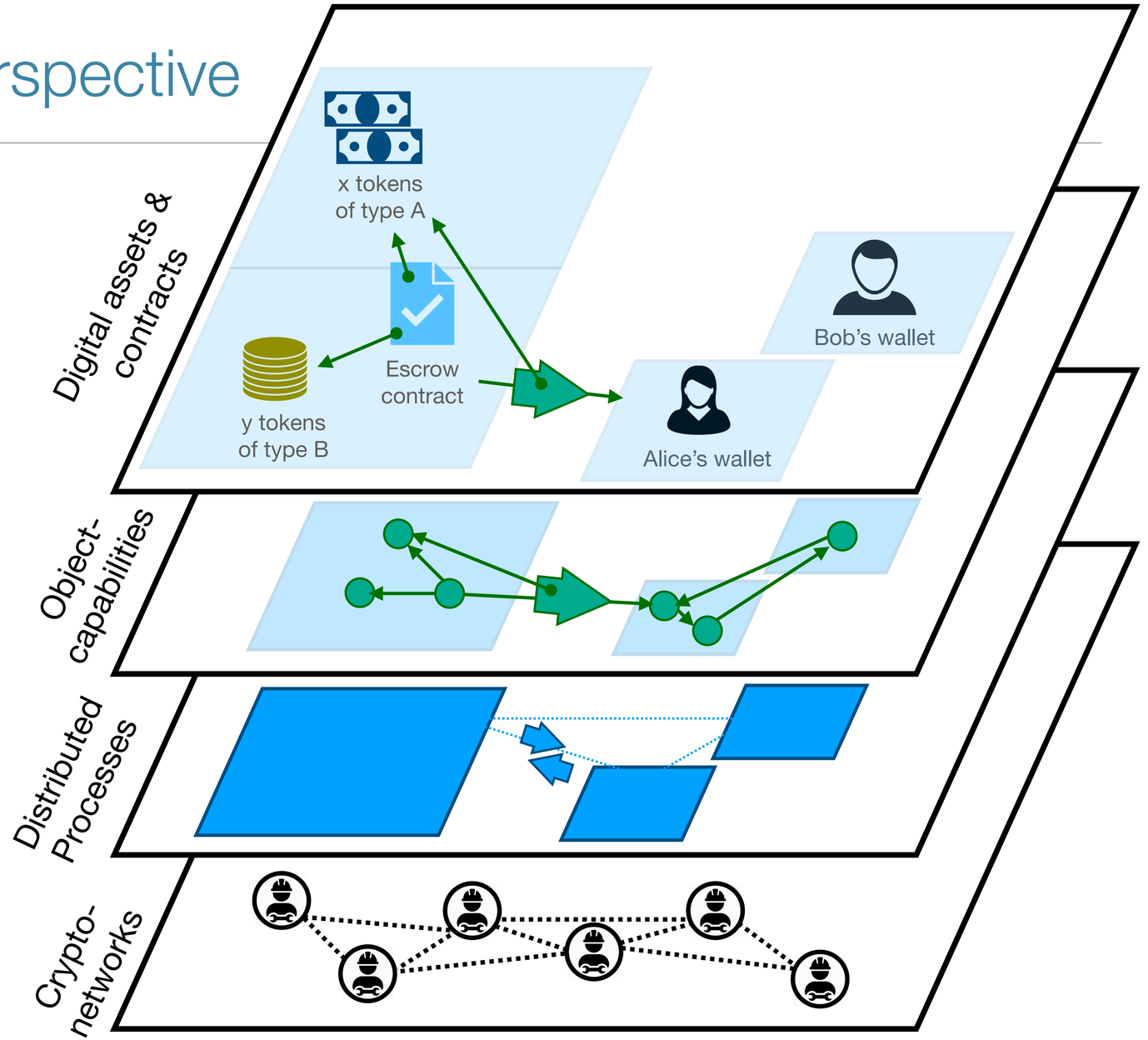

```
function buy(desc, payment) {
  return (myPurse ! deposit(10, payment)).then(_ => asset);
}
```

Secure Distributed JavaScript dialect ("hardened JS")

A holistic Web 3.0 systems perspective



A holistic Web 3.0 systems perspective



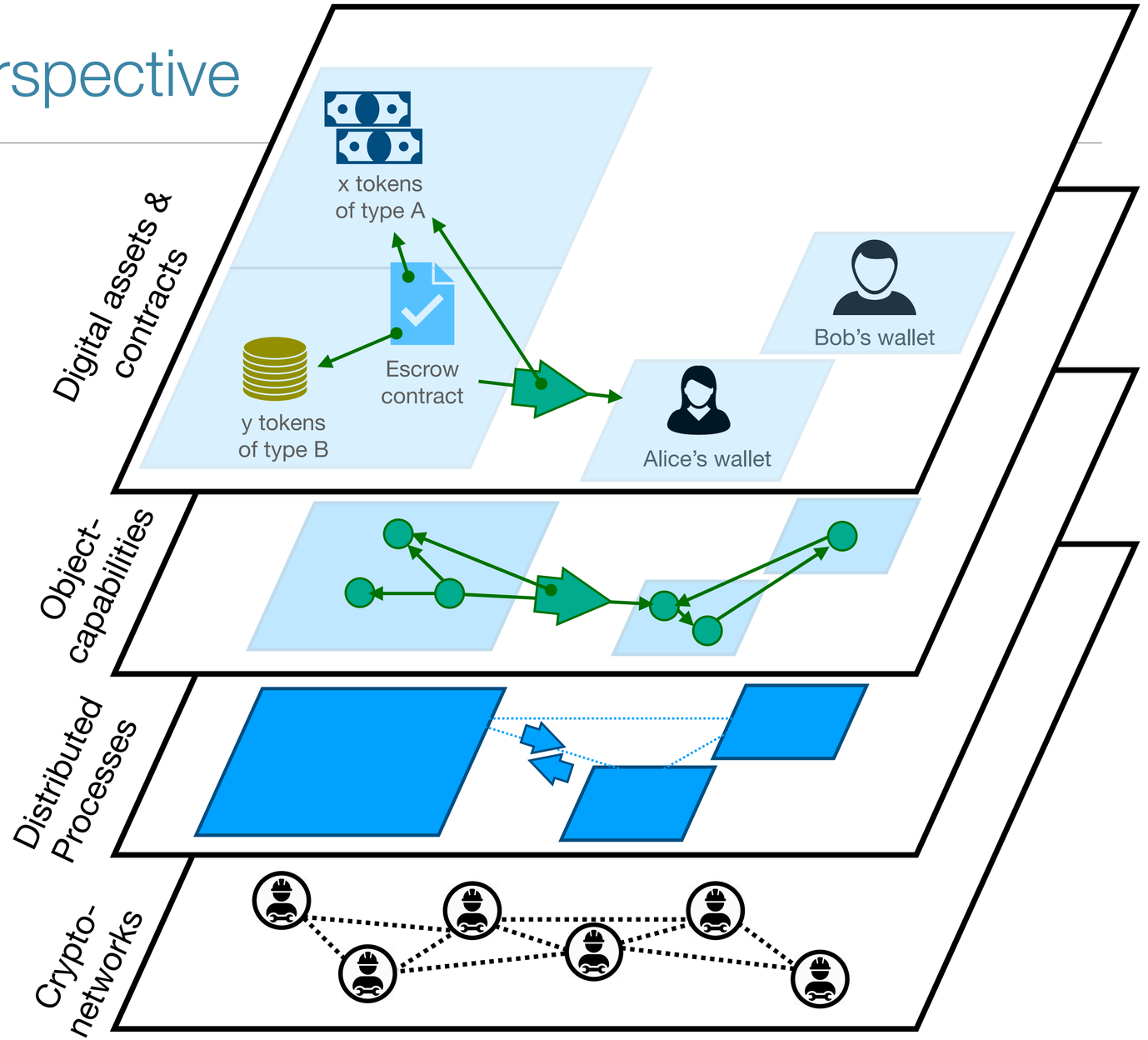
A holistic Web 3.0 systems perspective

Decentralized applications

Secure programming models

Distributed middleware

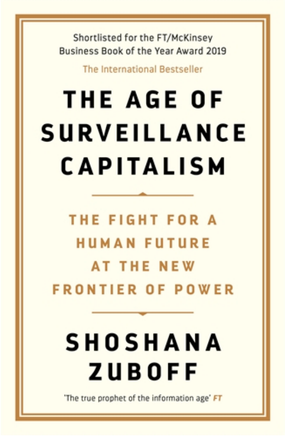
Scalable & private blockchains



Why decentralization matters: how technology affects society

Walled Gardens
No interoperability

Surveillance Capitalism



Pervasive
data leaks

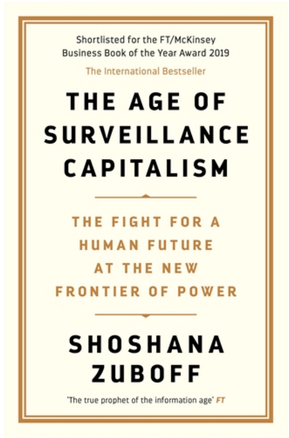
Censorship, deplatforming,
Opaque Terms of Service

Why decentralization matters: how technology affects society

Walled Gardens
No interoperability

Open & interoperable internet services

Surveillance Capitalism



Self-sovereign digital property rights

Pervasive **data leaks**

Secure **personal data** pods

Censorship, deplatforming, Opaque Terms of Service

Transparent rules & **governance**

KU LEUVEN

DistriNet

Inaugural Lecture

Secure and dependable software services for the Internet of Value

Tom Van Cutsem
November 2022

Thank you for listening

tvcutsem.github.io be.linkedin.com/in/tomvc github.com/tvcutsem twitter.com/tvcutsem