Decentralised Finance (DeFi)

5 key questions

What is DeFi?

```
In [ ]:
```

Why Would We Need DeFi?

```
In [ ]:
```

What are the New Actors in DeFi?

```
In [ ]:
```

What are the Main Risks in DeFi?

```
In [ ]:
```

Should DeFi be Regulated Differently?

```
In [ ]:
```

Map

1. `what`
2. `how`
3. `why`
4. DeFi world
5. Future of DeFi
6. Policy discussions

1. `What` is DeFi?

Computer in the `financial` sky

- **Blockchain** as the **computer in the sky**.
- **DeFi** commonly refers to the set of **financial applications** running on the blockchain machine.

Definition

Decentralized Finance (DeFi) is an **open digital** ecosystem where financial services are produced through **automated protocols** in order to eliminate **financial intermediation**.

DeFi inherits the blockchain properties:

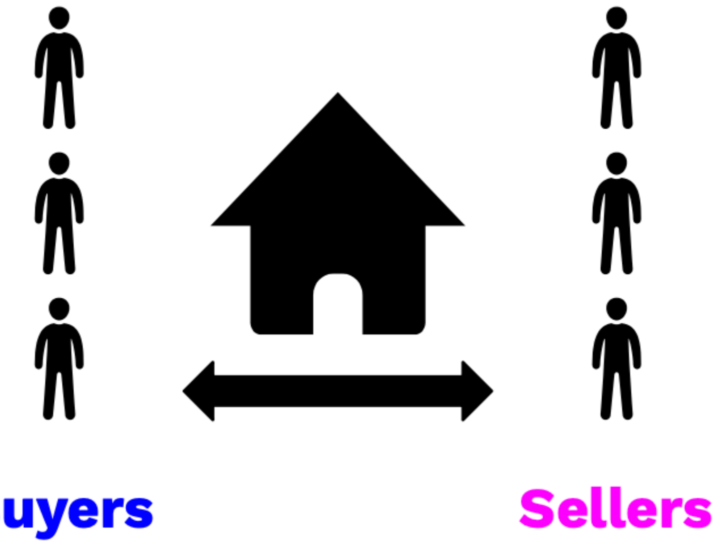
- A set of **public, interoperable and autonomous protocols** which are **universally accessible**
- Developed, maintained and used by an **open pool of pseudonymous agents** rather than a set of unique legal entities.

Example: how DeFi handles exchanges

Swap of securities (tokens): Ether x USDC

Traditional model of centralized exchanges (CEX)

Customers	Exchange
Sign in	Matches orders
Deposit	Settles
Submit orders `buy` / `sell`	Clears

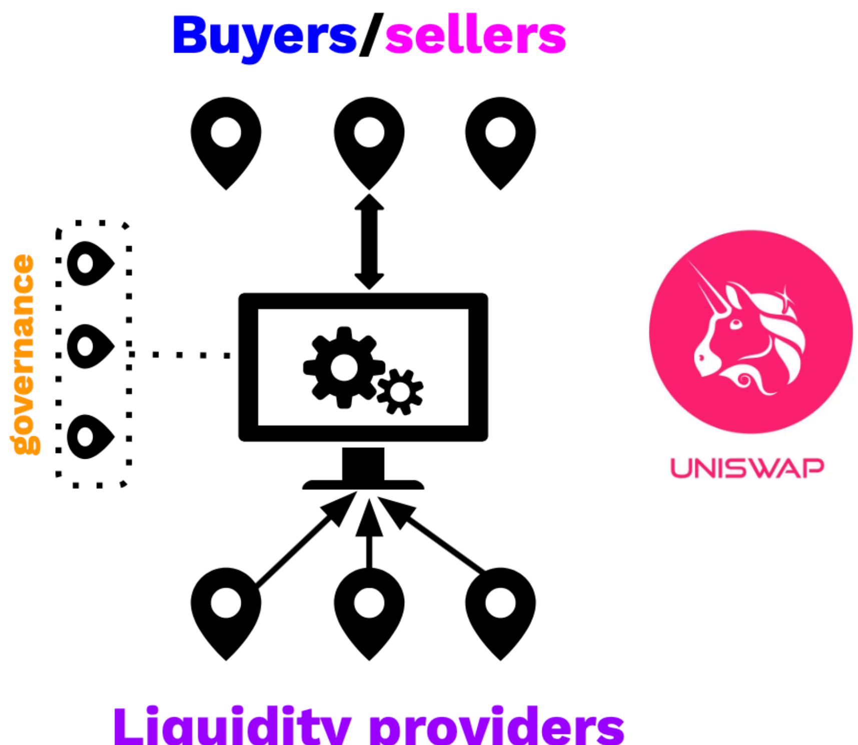


FTX BINANCE

coinbase

Decentralized exchanges (DEX) operate with Automated Market Makers (AMM)

Buyers/Sellers	AMM protocol	Liquidity providers	Governance protocol
Swap tokens	Set prices	Deposit tokens	
	Execute exchanges	Fee revenue	
	Manage liquidity balances `liquidity pool`		



Key parts:

- An **automated market maker** (`smart contract`) handles exchanges directly with buyers and sellers
  → No matching or asset custody by a central authority
- **Liquidity pool** hosts reserves of tokens

→ Provisioned by **liquidity providers** for profit (fee)

- **Anyone** can push a request to the protocol

→ AMM accesses the pool of tokens to meet the request and updates the reserve balances
→ Each transaction comes with a fee that is then redistributed to the liquidity providers.

- **Governance**: the protocol is updated through voting by holders of governance tokens

2. `Why` DeFi?

The crypto value proposition

DeFi value proposition is a new **information governance** model

> *Technology that **shifts in the information structure** upon which financial services can be deployed.*

Goal of Cryptography and DLT:

- Offer a **guarantee** of information **publicly** in **absence of a central authority**
  - Technological solution to an information problem
- <u>Claim</u>: for contracts strictly relying on such information: **no need for intermediation**

Example: digital payments

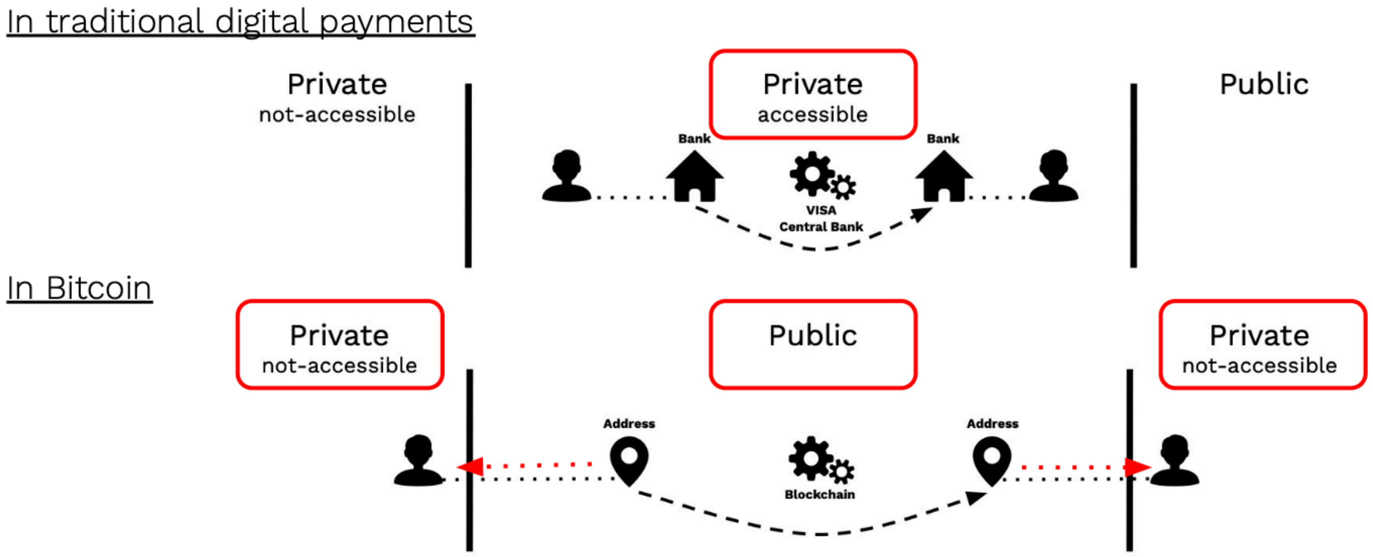
Key friction in payments: the privacy value (**confidentiality**) of transaction information

Traditional payment systems and the Bitcoin model offer two **different solutions to this problem**.

Example: digital payments

Key friction in payments: the privacy value (**confidentiality**) of transaction information

Traditional payment systems and the Bitcoin model offer two **different solutions to this problem**.


In traditional digital payments

In Bitcoin

Under the crypto information structure

- NO **confidential** information
    - Source of power in intermediated markets
- ❗ Misleading claims
    - **Transparency**
        - From confidentiality to **pseudonymity**
    - **Replicability** of standard financial instruments
        - Absence of confidentiality **restricts** contracting space

Information and economics

Different information structures

↓

Different market dynamics

↓

Different policy treatments

Different information structures / different economic forces / different policy treatments

	Friction Fix	Welfare Gains	Welfare Losses
Traditional Payments	Confidentiality	Liability of parties Dispute resolution Screening (AML/KYC)	Centralized control Market power Lack of innovation Single point failure
Bitcoin, Ethereum	Pseudonymity	No rent No arbitrary control Innovation Resilient	No dispute resolution No Screening (AML/KYC) Limited contracting space

3. DeFi world

3.1 The DeFi stack

Layer	Description	Examples
Settlement Layer	Processes and records all transactions securely and transparently.	Ethereum, Binance Smart Chain, Solana
Asset Layer	Tokens or digital assets that represent value on the blockchain and can be traded or used in DeFi protocols.	ETH, BTC, Stablecoins (USDC, DAI), Wrapped Assets
Protocol Layer	Smart contracts defining financial logic for decentralized services.	Uniswap, Aave, Compound, MakerDAO
Application Layer	User-facing interfaces and dApps (decentralized applications) that interact with protocols.	MetaMask, Argent, Zerion, Yearn Finance
Aggregation Layer	Platforms that combine multiple DeFi services.	1inch, Zapper, DeFi Saver, Yearn

3.2 Protocols

Category	Description	Examples
Stablecoins	Crypto assets w/ value pegged to a given asset (e.g., US dollar).	`USDT` (Tether) `USDC` (Circle) `Dai` (MakerDAO)

Exchanges (DEX)	Exchange of tokens via liquidity	`Uniswap`
		`Sushiswap`
		`Curve`

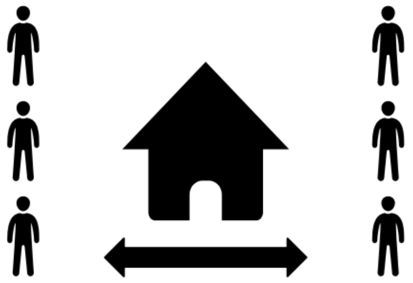
Credit	Credit services via liquidity pools (collateralized or flash loans).	`Compound` `Aave`
Derivatives/Insurance	Futures and synthetic exposures provided by liquidity pools with collateralized positions.	`dYdX` `Synthetix`

Portfolio Management	Vaults of assets governed and managed by smart contracts.	`Set Protocol`
		`PieDAO`

Exchange in traditional setting and in DeFi

Centralized exchange

Limit order book



Buyers

Sellers

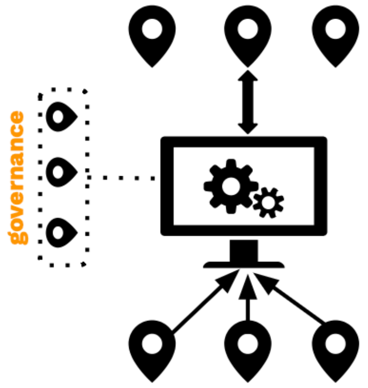
FTX BINANCE

coinbase

Decentralised exchange

Automated Market Maker

Buyers/sellers



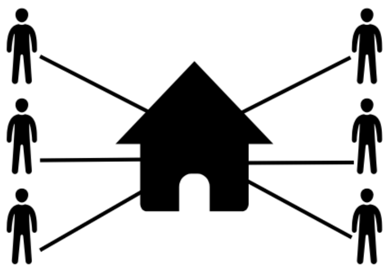
Liquidity providers

UNISWAP

Lending in traditional setting and in DeFi

- ! Large **collateral** requirements to compensate **limited information**

Centralized credit



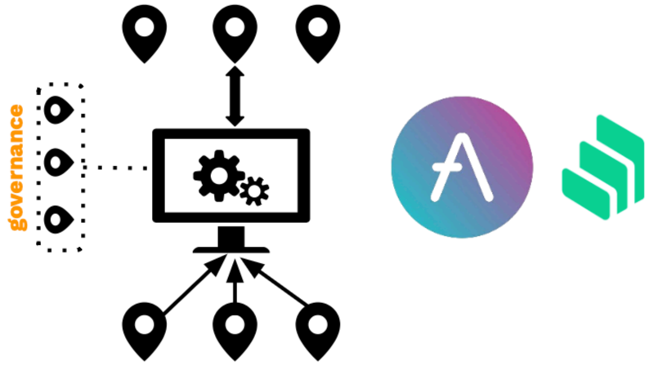
Depositors

Borrowers

Decentralised credit

Collateralised positions

Borrowers

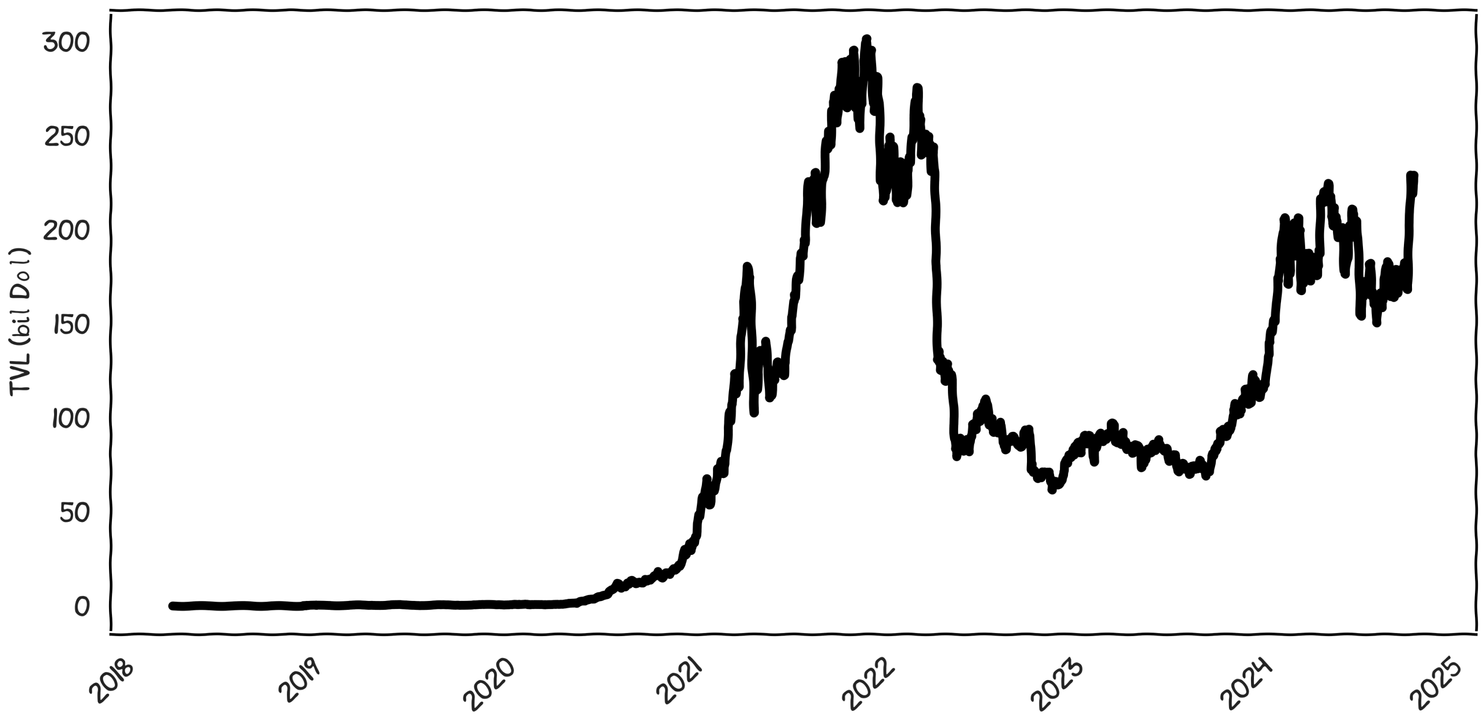


Liquidity providers

3.3 Some statistics

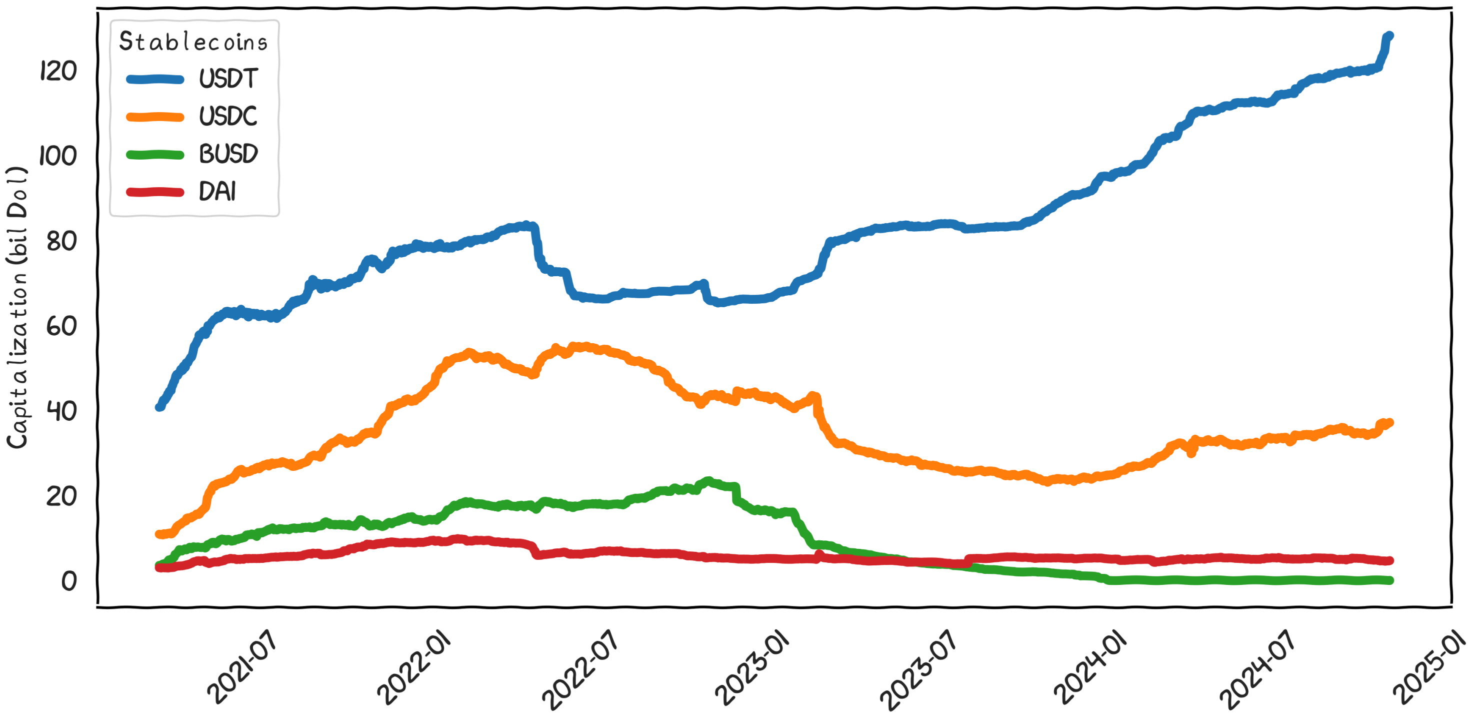
- Multiple **seasons**
- Significant **growth** and uptake at times
- Still **limited** compared to the rest of the financial world

Total Value Locked in DeFi protocols



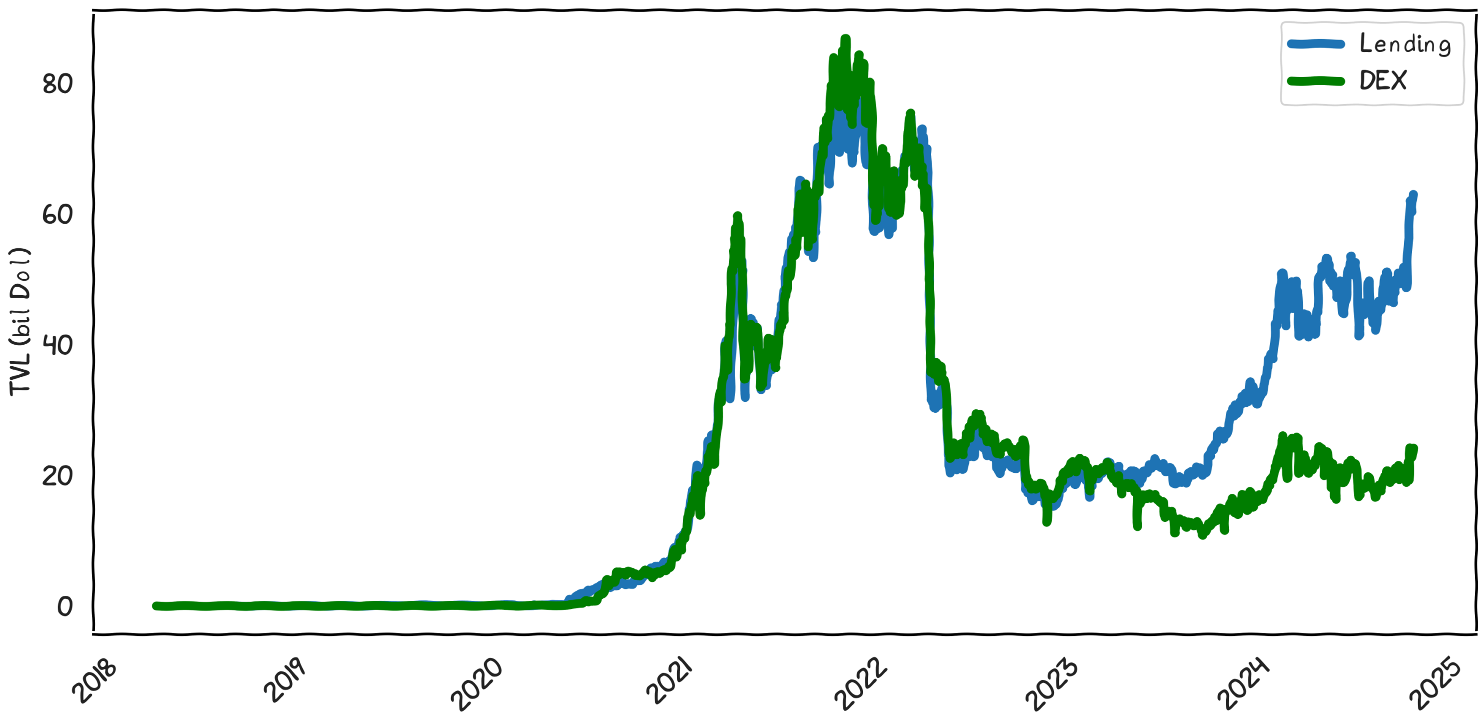
source: DeFi LLama

Funds Locked in Stablecoins



source: DeFi LLama

Total Value Locked in DEX and lending



source: DeFi LLama

4. The future of DeFi

The fundamental challenge

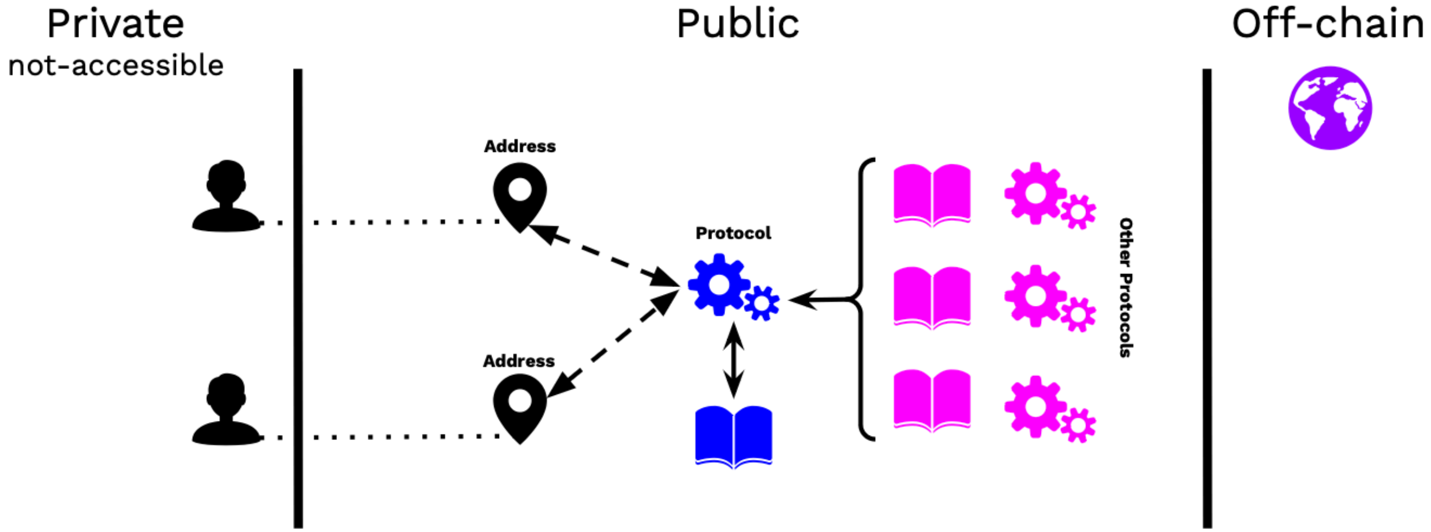
Recall the binary information structure

- **Public (`on-chain`)**
  - Verification at (almost) zero cost
  - Transaction transparency: any activity on DeFi is public and can be contracted upon.
- **Private (`off-chain`)**
  - Infinitely costly to verify
  - Pseudonymity: identity-related information cannot be contracted upon in DeFi

$\exists$ **bound on the contracting space** and the **scope of applications** for DeFi protocols.

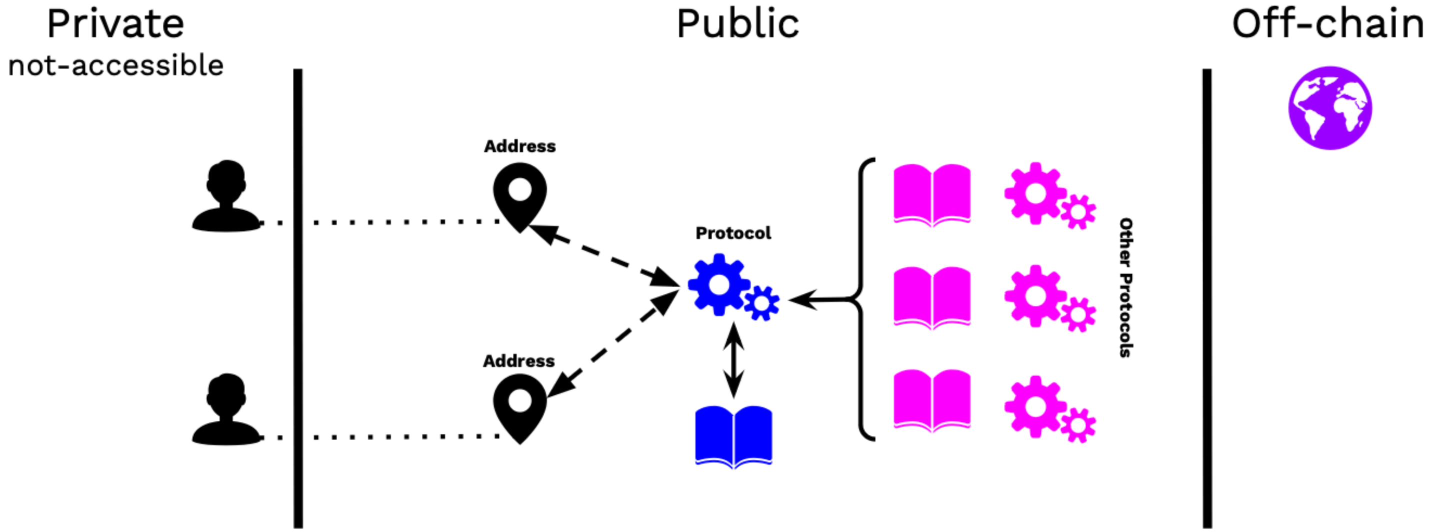
→ The smart contract challenge

Verification vs Contracting power



→ The smart contract challenge

Verification vs Contracting power



→ Growth perspective for DeFi?

→ Value of DeFi for the real economy?

The new intermediaries

The solution to expanding contracting power is to introduce **new forms of intermediation**: **information bridges**

- Oracles
- Ramps

Trade-off: **verification vs contracting power**

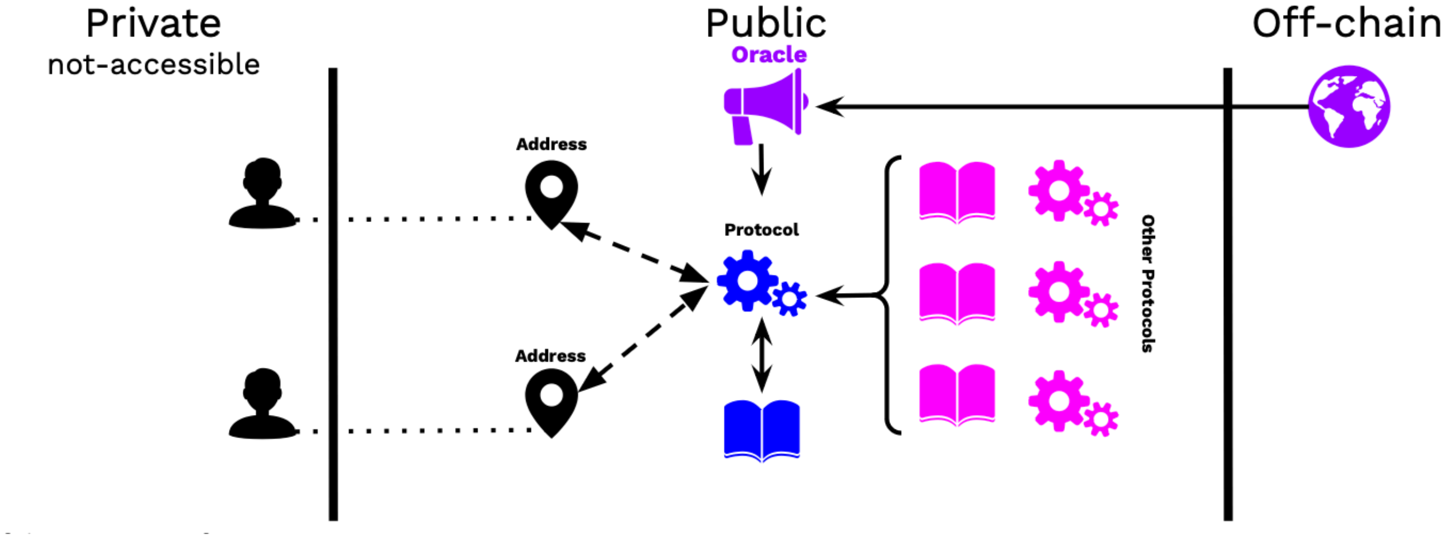
Oracles

Definition

Oracles provide the necessary **bridge to unify `off-chain` and `on-chain` worlds**

- Service that **connects smart contracts** with **external data sources**.

Oracles **expand the contracting space** of DeFi applications at the cost of **on-chain (public) verification**.



Private

not-accessible

Public

Oracle

Off-chain

Address

Protocol

Address

Other Protocols

Applications

1. **Price Feeds**
    - Oracles fetch and deliver real-time price data for assets (e.g., cryptocurrencies, commodities) to DeFi platforms.
        - Example: collateral and liquidation thresholds.
2. **External Event Verification**
    - Oracles confirm external events, such as sports results or weather conditions, enabling platforms like prediction markets or insurance dApps.
3. **Cross-Chain Communication**
    - Some oracles facilitate interactions between different blockchains, making cross-chain DeFi products possible.

The private and social costs of unverifiable information

- Centralization
- Inefficiency
- Vulnerabilities

Opportunities for public interventions: traditional market failures in information markets

- Public oracle
- Licensed oracles
- Regulated oracle markets

Ramps & Tokenisation

Definition

> *Tokenization refers to the process of generating a **digital represantion of traditional assets** on a blockchain by **on and off ramps**.*

FSB(2023)

Benefits

- Automation and trade speed & efficiency
- New contracting opportunities: information space and composability

Applications

- Cross-border payments currently relying on banks (correspondent) and message platforms (swift)
- Foreign exchanges (payment vs payment)
- Mortgage-backed-securities (dozen intermediaries in the process)

Challenges

- Some economic frictions not resolved (moral hazard and adverse selection)
- Legal challenges: who has what **right**?
- Technical challenges: **design of ramps** (cf. Oracles)

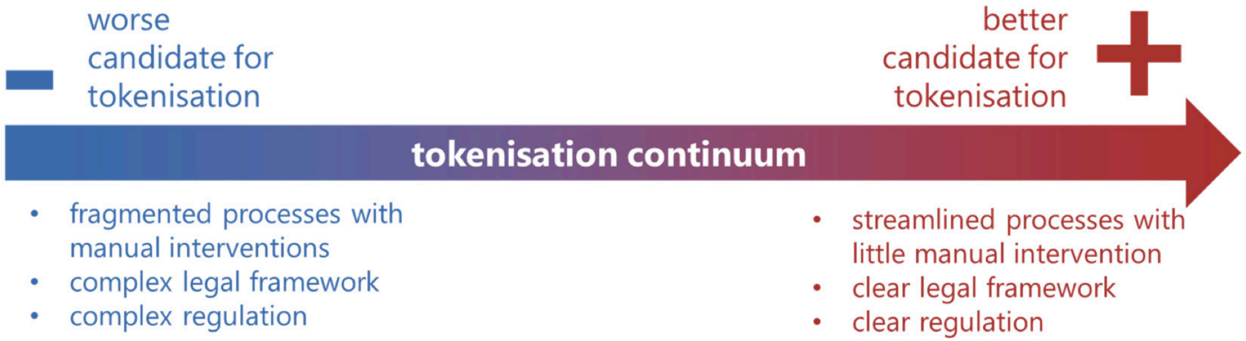
Tokenization continuum

Not all digital assets offer the same tokenization value:

- Worse candidates: syndicated loans or commercial real estate.
- Better candidates: FX or MBS

The tokenisation continuum

Graph 4



worse candidate for tokenisation

better candidate for tokenisation

tokenisation continuum

- fragmented processes with manual interventions
- complex legal framework
- complex regulation

- streamlined processes with little manual intervention
- clear legal framework
- clear regulation

Source: Authors' elaboration.

BIS (2024)

5. Policy discussion

> *Regulatory regimes built around intermediaries as regulated processors of transaction information may* ***fit poorly with a disintermediated market structure****.*

WEF (2021)

5.1 A New Policy Framework?

Should DeFi receive a different policy treatment?

↳ How do DeFi services differ in their treatment of information frictions?

Claim: Understanding the shift in information structure sheds light on

- the scope of DeFi applications
- risks and inefficiencies (new and old)
- appropriate policy approaches (warranted and feasible actions)

Elements of reflection

- **Limits on policy enforcement power and information acquisition**
    - Computer in the sky: no shutting down, no liability, etc.
- **New targets**: validators, protocols and oracles.
- **Eligible proposals:** warranted & feasible
    - **Warranted**
        - Several frictions can be best addressed by the private sector
        - Find cases with limits to the production of private solutions
            - ↳ likely benefits from public support.
    - **Feasible**
        - Subset of warranted actions satisfying the technological constraints of DeFi

5.2 Major Risks Associated With DeFi

DeFi recreates core financial functions—trading, lending, liquidity provision — but **without traditional intermediaries or enforcement mechanisms**.

This produces a distinctive risk landscape:

Risk Category	Description
Smart Contract & Protocol Risk	Bugs, exploits, flash-loan attacks. Code replaces institutions → vulnerabilities are immediate and global.
Governance & Centralisation Risk	Concentrated voting power (whales, VCs). Hidden centralisation in admin keys, upgradeability, sequencers.
Oracle & Data Integrity Risk	Off-chain data cannot be perfectly verified. Oracle manipulation → mispriced collateral, forced liquidations.
Liquidity & Market Structure Risk	AMMs can break under stress (impermanent loss, liquidity dry-ups). Fragmented liquidity across chains → unstable price discovery.
Interconnectedness & Contagion	Protocols heavily interlinked (collateral loops, rehypothecation). Failure of one stablecoin or protocol → instant systemic spillovers.
Regulatory & Compliance Risk	Pseudonymous participation → AML/KYC gaps. Liability unclear across validators, developers, and front-end operators.

5.3 Why Stablecoins Create Structural Risks in DeFi

Stablecoins are both the **weakest link** and the **most feasible regulatory touchpoint** → hence the focus of MiCAR and the Genius Act.

Stablecoins are the **monetary foundation** of DeFi. They act as unit of account, settlement asset, and core collateral across protocols.

Because they mimic money **without public guarantees**, they introduce *systemic vulnerabilities*:

Stablecoin Risk	Description
Run Risk & Redemption Externalities	Fragile confidence in reserves → **sudden redemptions**. Forced liquidation of assets → **fire sales** affecting broader markets.
Opacity & Information Asymmetry	Users cannot fully verify reserve quality or composition. Solvency uncertainty increases → **panic amplifies**.
Peg Instability & Propagation	Depeggings spill into AMMs, lending markets, and cross-chain bridges. Triggers liquidation cascades and liquidity spirals.
Collateral Channel Risk	Stablecoins widely used as collateral. Value drops → reduced collateralization → mass liquidations.
Centralisation & Operational Risk	Issuers concentrate key operational and governance functions. Sanctions, banking outages, or governance failures can freeze DeFi activity.

5.4 Recent Regulatory Developments: MiCAR & the U.S. "Genius Act"

Both initiatives show how policymakers test the limits of enforceability, accountability, and information acquisition in decentralized settings.

5.4.1 EU – Markets in Crypto-Assets Regulation (MiCAR, 2024–2025)

Focus: Stablecoins & centralized service providers

- EU-wide licensing for **CASPs** (exchanges, custodians, brokers).
- Strong **reserve, governance, and disclosure** rules for ARTs & EMTs.
- **Market abuse** and **consumer protection** frameworks imported from traditional finance.
- **DeFi carve-out:** MiCAR targets *intermediated* services only.
    - Mandates an EU **DeFi report & potential rulemaking** (2025–26).

Relevance: MiCAR regulates where **enforcement is technologically feasible**—centralized issuers, service providers, and verifiable reserves.

5.4.2 U.S. – The "Genius Act" (2024 Proposal)

Focus: Stablecoins + responsibilities in DeFi

- Federal or state licensing for stablecoin issuers.
- Mandatory **1:1 HQLA reserves** and redemption rights.
- Monthly attestations → reduces **information asymmetry**.
- Defines obligations for:
  - **Front-end operators**,
  - **Protocol controllers**,
  - **Large validators / governance actors**.
- Emphasis on **systemic risk**, **operational resilience**, **illicit finance**.

Relevance: Tackles the **liability-under-pseudonymity** problem and uses stablecoins as an anchor for broader DeFi oversight.

5.5 Open policy issues

- How much **decentralisation** is good for the economy?
  - Centralisation of DeFi
- How to enforce **liabilities** in a pseudonymous ecosystem? (public-private issue)
  - AML-KYC
- How to manage **unverifiable** information? (public-private issue)
  - Embedding off chain information introduces a new information friction
  - Policing **oracles** and **ramps** (new intermediaries)
    - Recovering the value of traditional frameworks
- How to think about **macro-prudential regimes** in absence of enforcement powers?
  - Interconnected protocols
  - Misaligned incentives to audit
  - Contagion to the real economy