Blockchain programmation

ESILV 2019/2020

What is Defi

What is Defi

- DEFI stands for Decentralized Finance
- Open financial system living on public blockchains
- Various economic functions:
  - Exchanges
  - Lending
  - Borrowing
  - Derivatives
  - Options

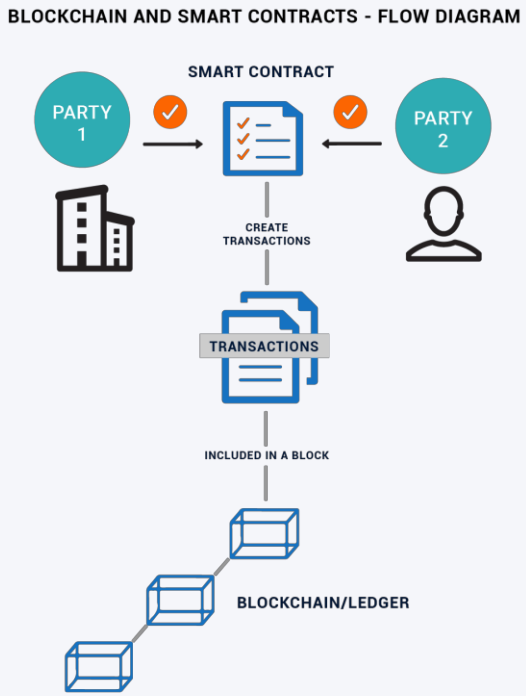
Is Bitcoin Defi?

- Bitcoin is a decentralised currency
- Currencies are the building blocks of a financial system
- So yes, probably

Trustless bitcoin apps

- However, if bitcoin as an asset class is probably Defi, the Bitcoin network is not great for DEFI apps
- The lack of expressivity of script language makes it hard to build complex logic on top of Bitcoin
- As a result, most Bitcoin financial apps are off chain trusted companies
  - Coinbase, Binance
  - Blockfi, Nexo
- Some decentralised alternatives are popping up, such as LN Markets

Smart contracts on Ethereum



- Ethereum on the other hand offers more expressivity in its programming language
- More complex use cases can be coded
- More financial primitives can be built
- EG Tokens
- These dapps have their backend fully operated on chain
- Decentralisation is a spectrum; not everything is 100% centralised/decentralised
- Other chains try to develop a DEFI ecosystem (Tezos, Solana, EOS)

Open access

- Having the backend on a public chain means anyone can access it
  - Use it, directly on chain
  - Integrate in another system
  - Build an alternative frontend for it
- KYC is not techically required
  - No need to access legacy banking system
- KYC can be implemented
  - At the UX level
  - At the contract level
- DEFI defaults to open vs legacy defaults to close

Worldwide market

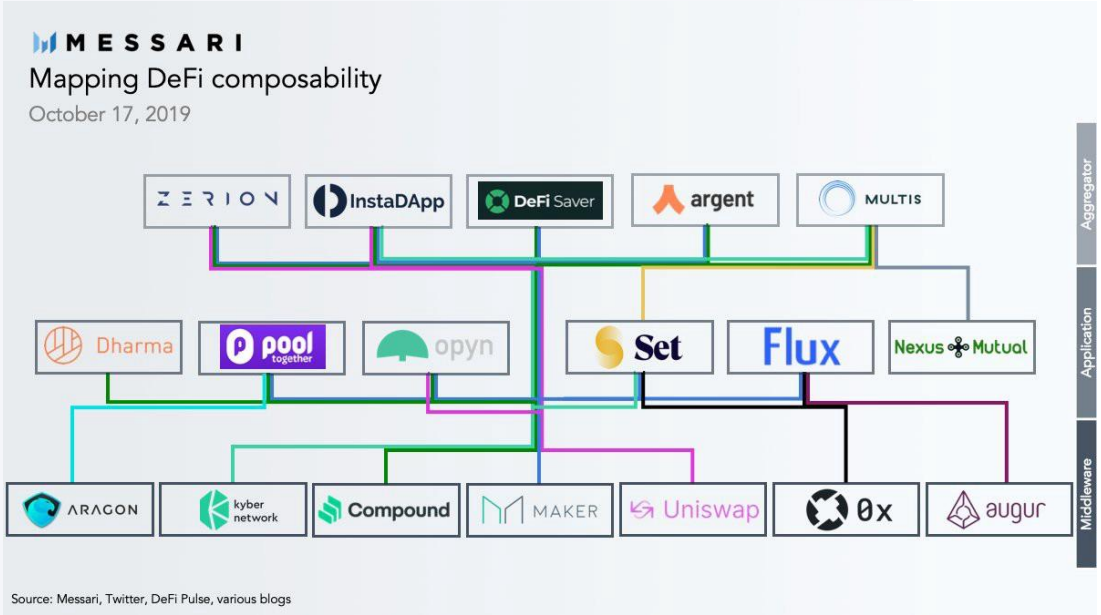
- Public chains are accessible to anyone with an internet connection
- No concept of geographical borders on the internet
- Permissionless global network anyone can join, vs regional banking networks (SEPA in Europe, Fedwire in the US...)
- Addressable market of Defi Dapps is global by default

Transparency

- DEFI Dapps backend are by default transparent
  - Real time Proof of reserve
  - Reduced risk of Ponzi
  - Reduced risk of fractional operations
- Usage metrics are fully accessible
  - # of users
  - Frequency of usage
  - Volume involved
- Auditing is still complex; because it is transparent does not mean it is safe

Composability

- Composability is the ability to reuse financial byproducts in other apps
- EG
  - Depositing ERC20 in App A
  - Receiving tokens B to represent Deposit in A
  - A can be easily redemeed for B
  - So B can be used as deposit in another Dapp C
  - And again...
- Composability applies both to financial value as well as to usage
  - Anyone can integrate a Dapp in its own Dapp



No safety belt

- Defi comes with no guarantee whatsoever
  - No insurance
  - No regulation
  - No funds recovery
  - No reversing theft
- It's a financial wild west: High risk, high rewards
- It will settle down over time
  - Regulation WILL catch up
  - Insurance products are being built
  - Protocol governance are organizing to offer funds recovery/guarantees
- We're witnessing the creation of a new, global financial system defaulting to open
  - Open source
  - Open access
  - Open auditability

Thank you

For your attention ！