Introduction to Blockchain Development for Software Engineer

<DEV> MOUNTAIN
TECH FESTIVAL

This is Subjective Session !!

NOT TECHNICAL ONE

Let start by knowing my Context first:

Rati Montreewat

SMART CONTRACT DEVELOPER & WEB3 ARCHITECT@ TOKENINE

MSC IN ACTUARIAL MANAGEMENT @ CASS BUSINESS SCHOOL

BSC IN ACTUARIAL SCIENCE @ CURTIN UNIVERSITY

Introduction to Blockchain Development for Software Engineer

It is fast-changing Industry

Why?

The killing feature of Blockchain is …

Composable without Permission

THE COMPONENTS ARE INTEROPERABLE.

PERMISSIONED CLOSED BEFORE ARE BECOMING OPEN

SUB-ECOSYSTEM ARE ENCOURAGED

Introduction to Blockchain Development for Software Engineer

Blockchain

EVERYONE KEEP THE SAME COPY OF DOCUMENT. THEY ARE UPDATED TOGETHER SO THEY TRUST THAT THEIR DOCUMENTS ARE IMMUTABLE

What is DeFi?

ON APPLICATION LAYER

TRADITIONAL BANK AS MIDDLEMAN

Composable without Permission

THE COMPONENTS ARE INTEROPERABLE.

PERMISSIONED CLOSED BEFORE ARE BECOMING OPEN

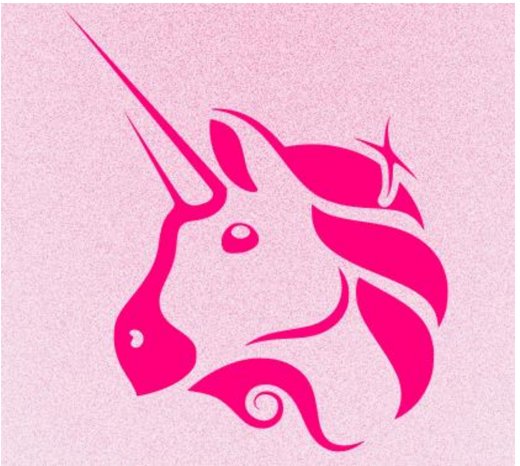
SUB-ECOSYSTEM ARE ENCOURAGED

Think as Fiat

ANYONE CAN ISSUE AND OWN STABLE COIN **WITHOUT ASKING REGULATOR**

Think as Fiat

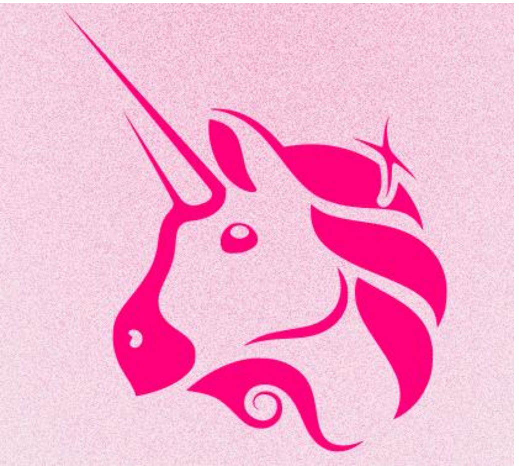
Think as Stock Exchange (IPO)



ANYONE CAN BECOME MARKET MAKER OR LIQUIDITY PROVIDER WITHOUT ASKING REGULATOR BY ADDING THEIR OWN TOKEN AND DAI AS LIQUIDITY TO UNISWAP

Think as Fiat

Think as Stock Exchange (IPO)



Think as Broker

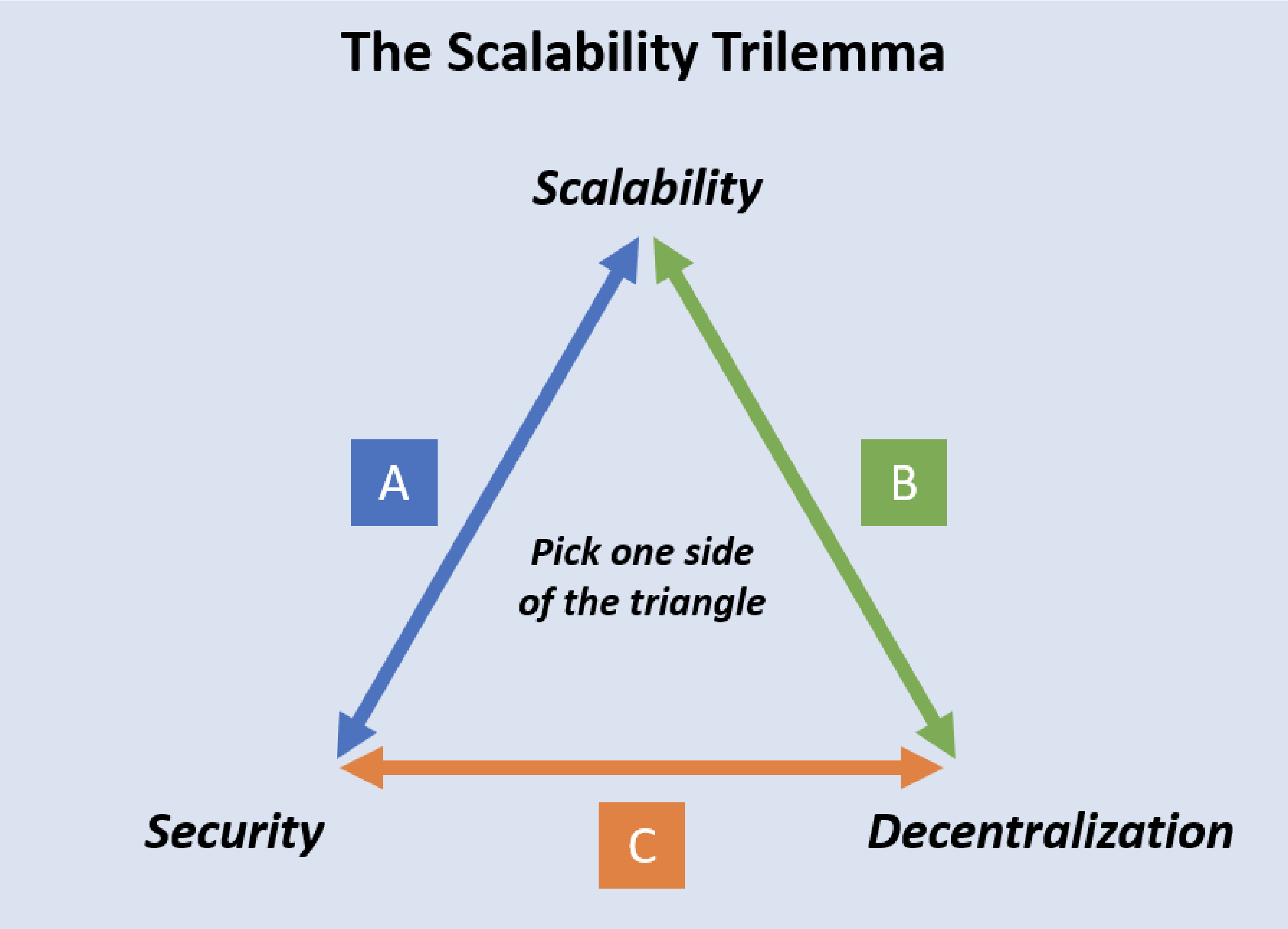
ANYONE CAN BECOME BUILT PROTOCOL ON TOP OF UNISWAP WITHOUT ASKING MARKET MAKER

Introduction to Blockchain Development for Software Engineer

Before you develop blockchain, do you understand what do you want to solve?

I believe some of you saw this

Blockchain Trilemma



The Scalability Trilemma

Scalability

A

B

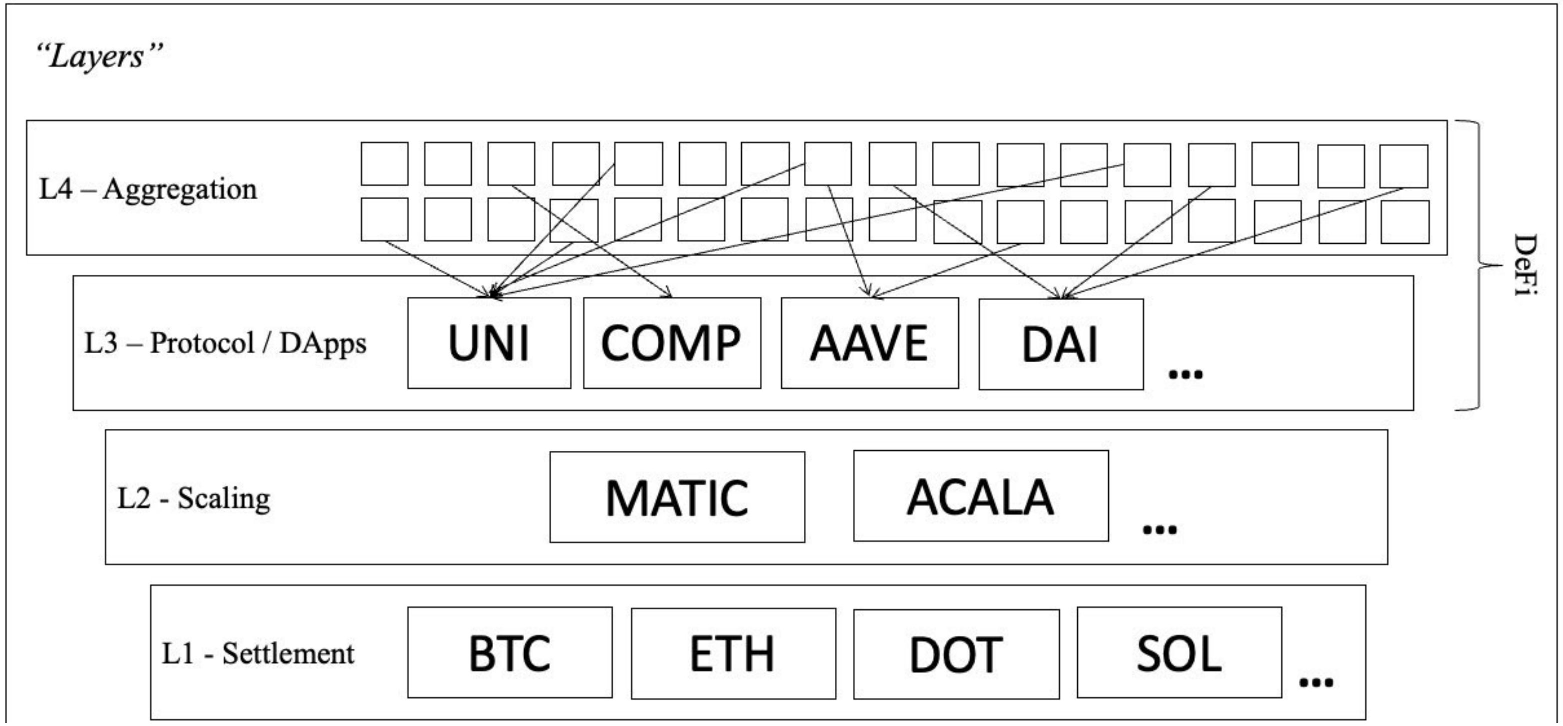
Pick one side of the triangle

Security

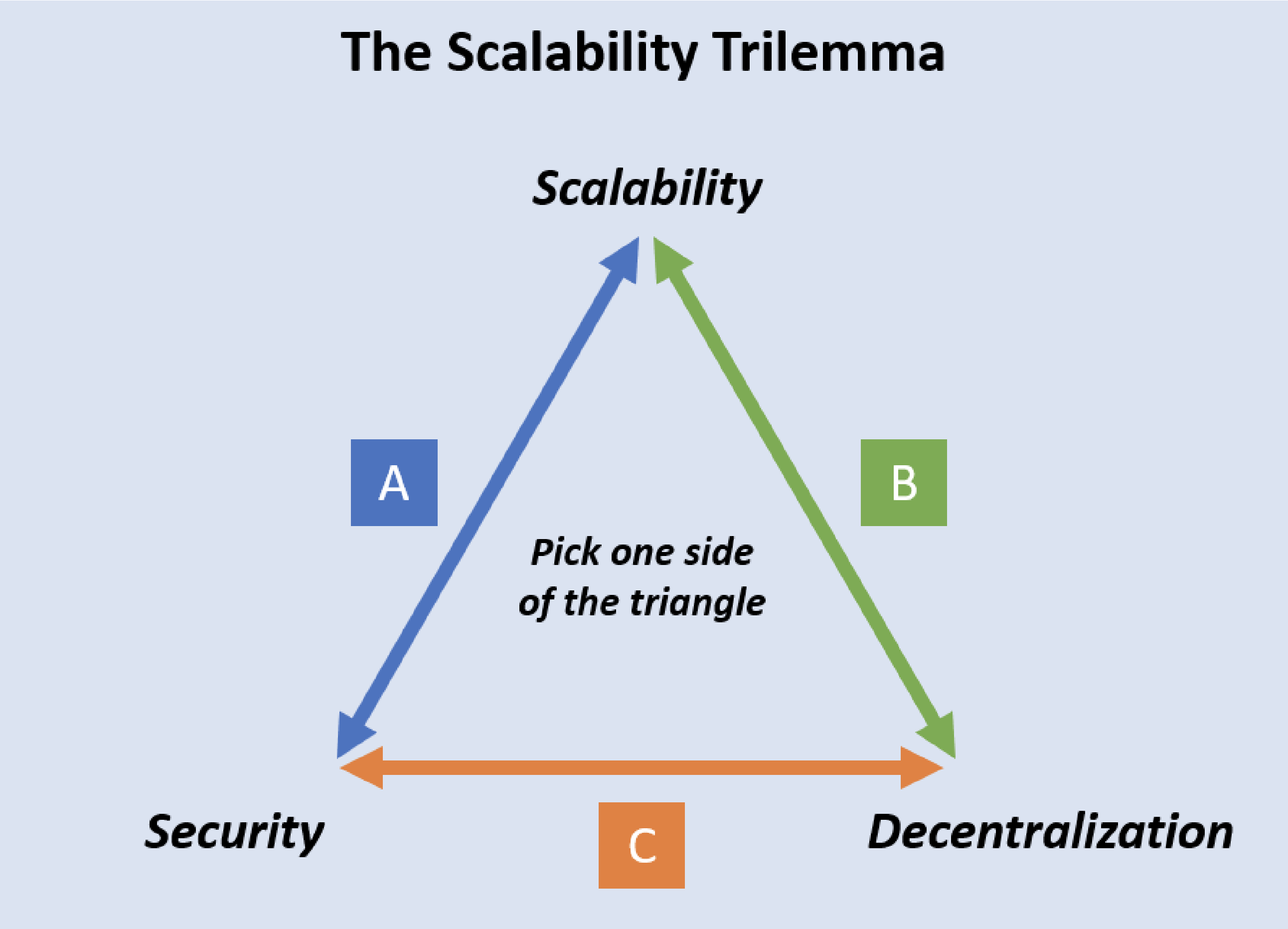
C

Decentralization

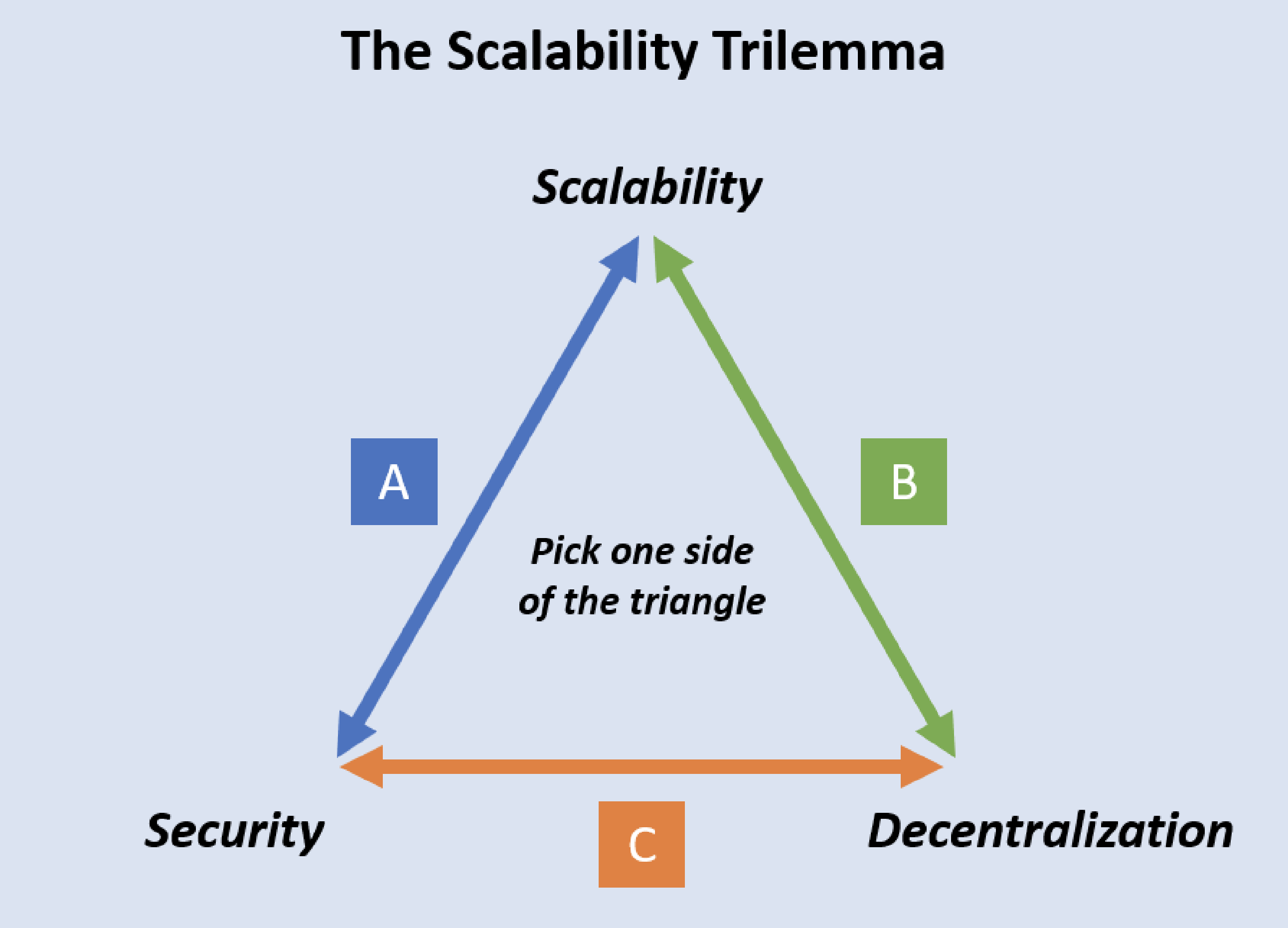
(Building on top of) Different Blockchain Layers



Before Going Any Further: Let me ask this



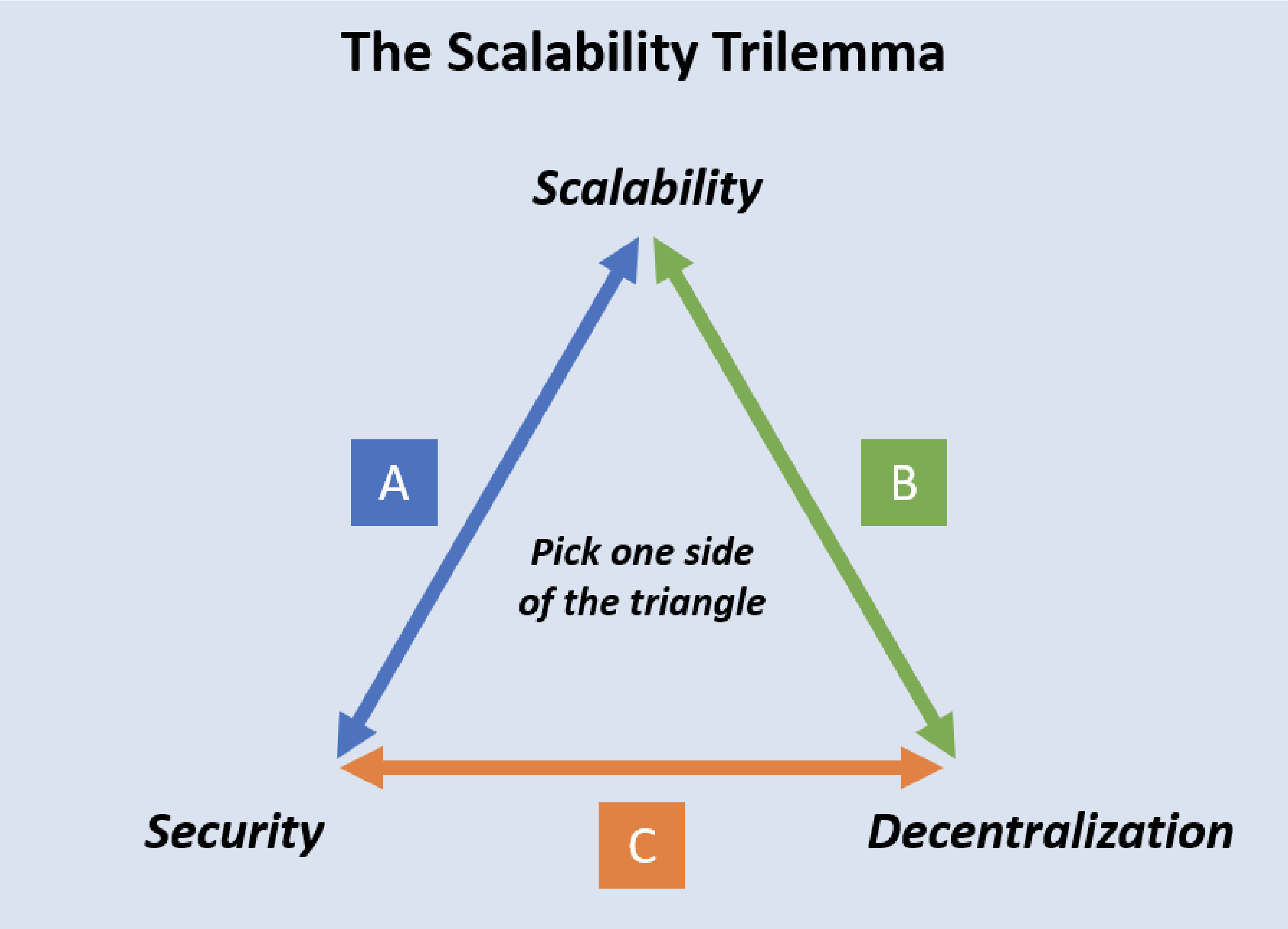
What is the hardest part of blockchain development?



The Scalability Trilemma

Again, this is subjective Session !!

let revisit the definition



The Scalability Trilemma

Pick one side of the triangle

Scalability

Again, this is subjective Session !!

Scalability in Blockchain ?

Transactions **speed** – average wait time

- **Bitcoin**: new block mined in ~ **9-10 minutes**
- **Ethereum**: new block mined in ~ **10-15 seconds**
- Business needs **real-time transactions** (milliseconds)

Transactions **throughput** – transactions per second (tps)

- **Bitcoin**: 2000-3000 / transactions per block → **3-5 tps**
- **Ethereum**: 200-300 / transactions per block → **10-15 tps**
- Business needs **thousands tps** (e.g. VISA performs 2000 tps)

Look at these two statements

1) Business needs **real-time transactions**

2) Business needs **thousands transaction per second**

Look at these two statements

1) Business needs **real-time transactions**

2) Business needs **thousands transaction per second**

But This MAY NOT always be true

Let revisit the definition

SOMEONE STATES THE DEFINITION

Definition of **Scalability**

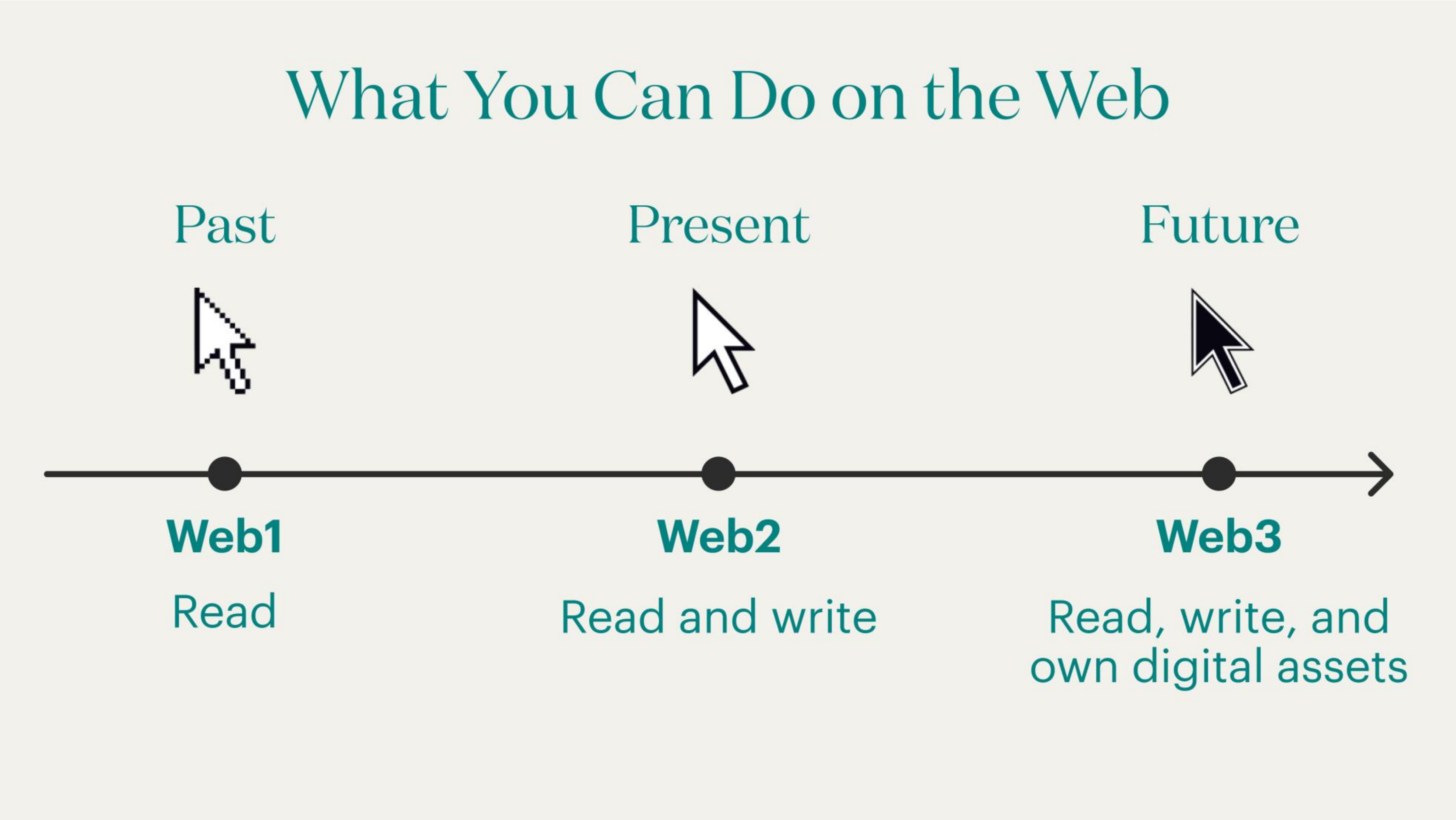
❑ how well a hardware system performs when the number of users is increased

❑ how well **a** database withstands growing numbers of queries

❑ how well **an** operating system performs on different classes of hardware.

Performance vs Resource

Then?



What You Can Do on the Web

Past

Present

Future

Web1

Read

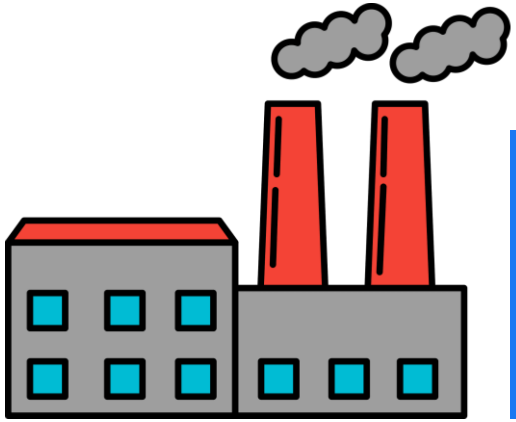
Web2

Read and write

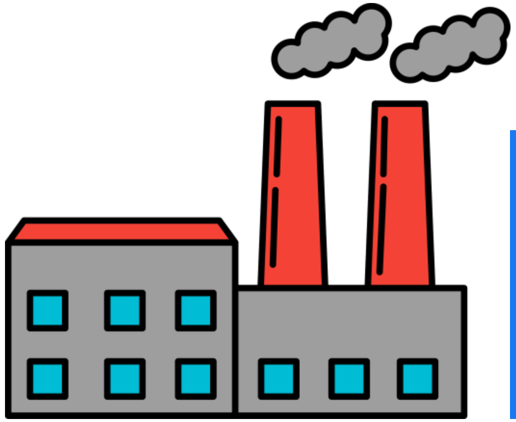
Web3

Read, write, and own digital assets

KEY TAKEAWAYS



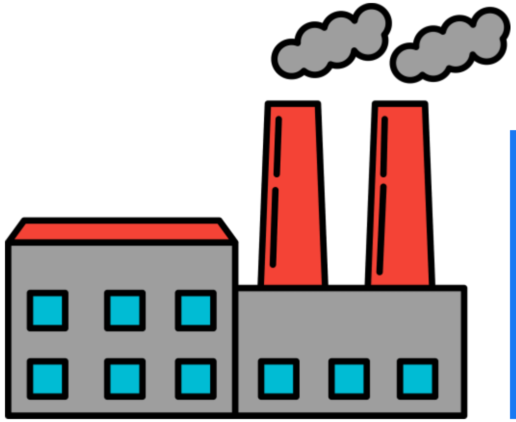
	Past (Traditional)	**Present (Information)**	**Future (Token)**
Key takeaways	Understand the **Production, distribution** and **Consumption**	Understand the new set of variables (**Intangible information, data, asset**)	Understand the new set of variables **(that affects, defines and govern the ecosystem)**



facebook

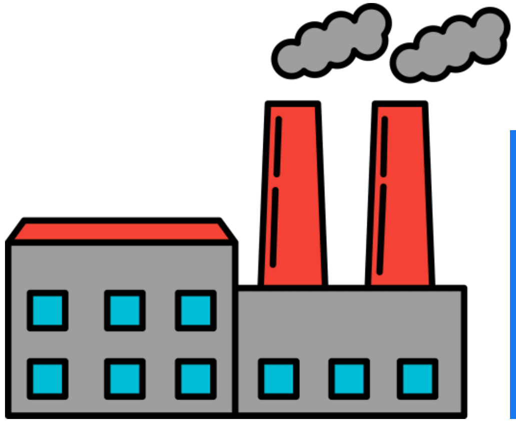
	Past (Traditional)	Present (Information)	Future (Token)
Explanation	Any input to get output in an **system (usually physical)**	Any input to get output in an **system (usually digital)**	**Self-selecting** input to get a **desired** output

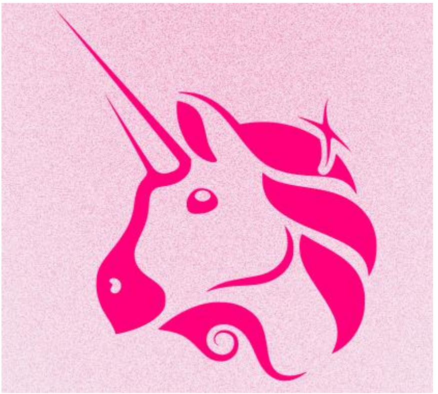
THINK AS SYSTEM THINKER



	Past (Traditional)	Present (Information)	Future (Token)
Goal	To make better decision	Better strategic choices involving information tech	To **affect decision** made by the participant

GOAL OF SYSTEM





	Past (Traditional)	Present (Information)	Future (Token)
Purpose	Efficiency by analyzing when to stop input to get output	To understand the value and how to extract the most value out of ecosystem	To **govern behaviors** by allowing participants to **self-select** and encourage specific behavior

REASONS TO ACHIEVE A GOAL

Look at these two statements again

1) Business needs **real-time transactions**

2) Business needs **thousands transaction per second**

But These are ONLY true for Web 1 and Web 2 but not always for Web3

Look at these two statements again

1) Business needs **real-time transactions**

2) Business needs **thousands transaction per second**

Business delegates obligation to scale to user

The metrics using must be in the same zone of layer being developed

SCALABILITY IN INFRASTRUCTURE LAYER !== IN APPLICATION LAYER

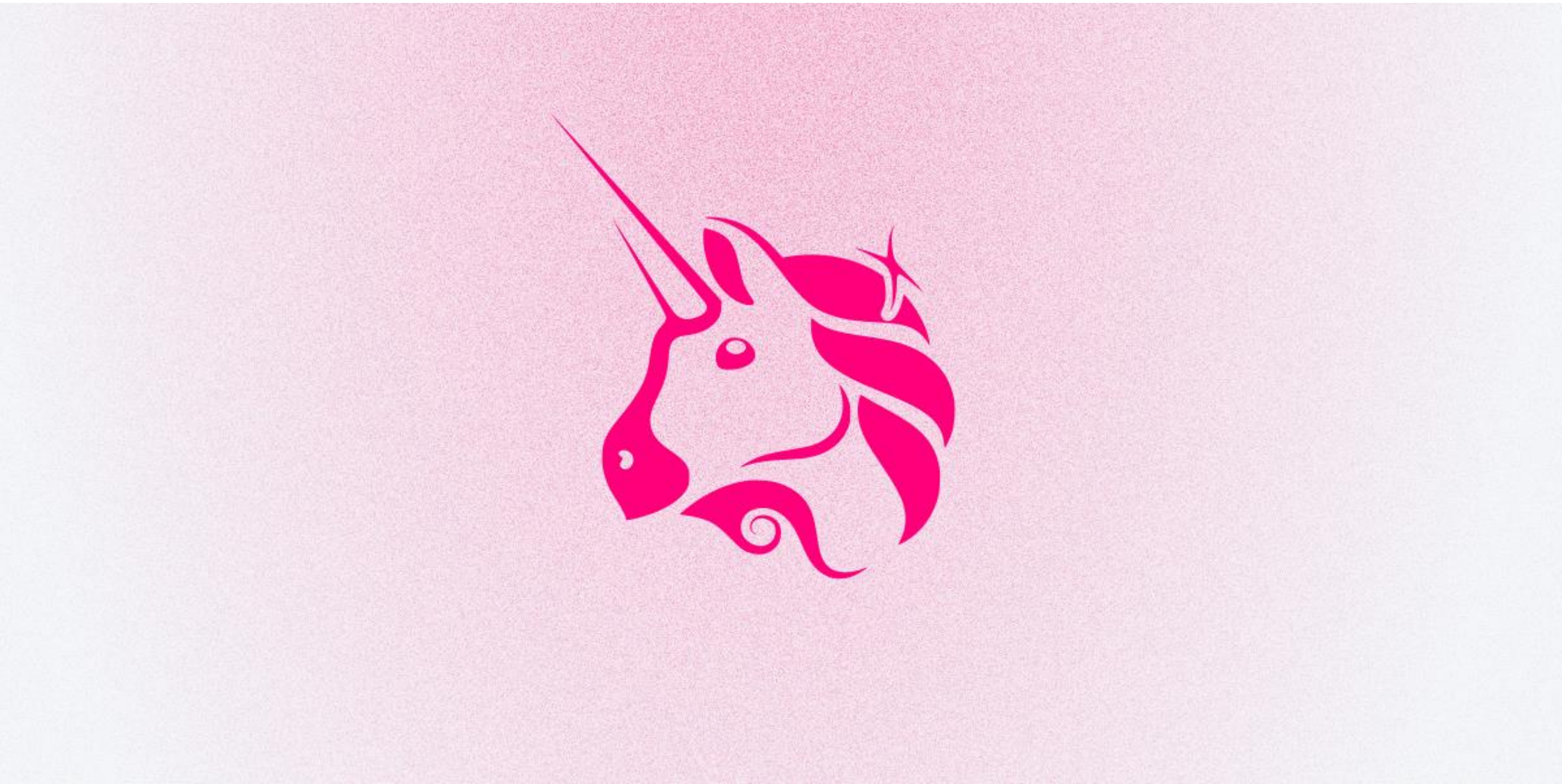
Scalability in Blockchain ?

Transactions **speed** – average wait time

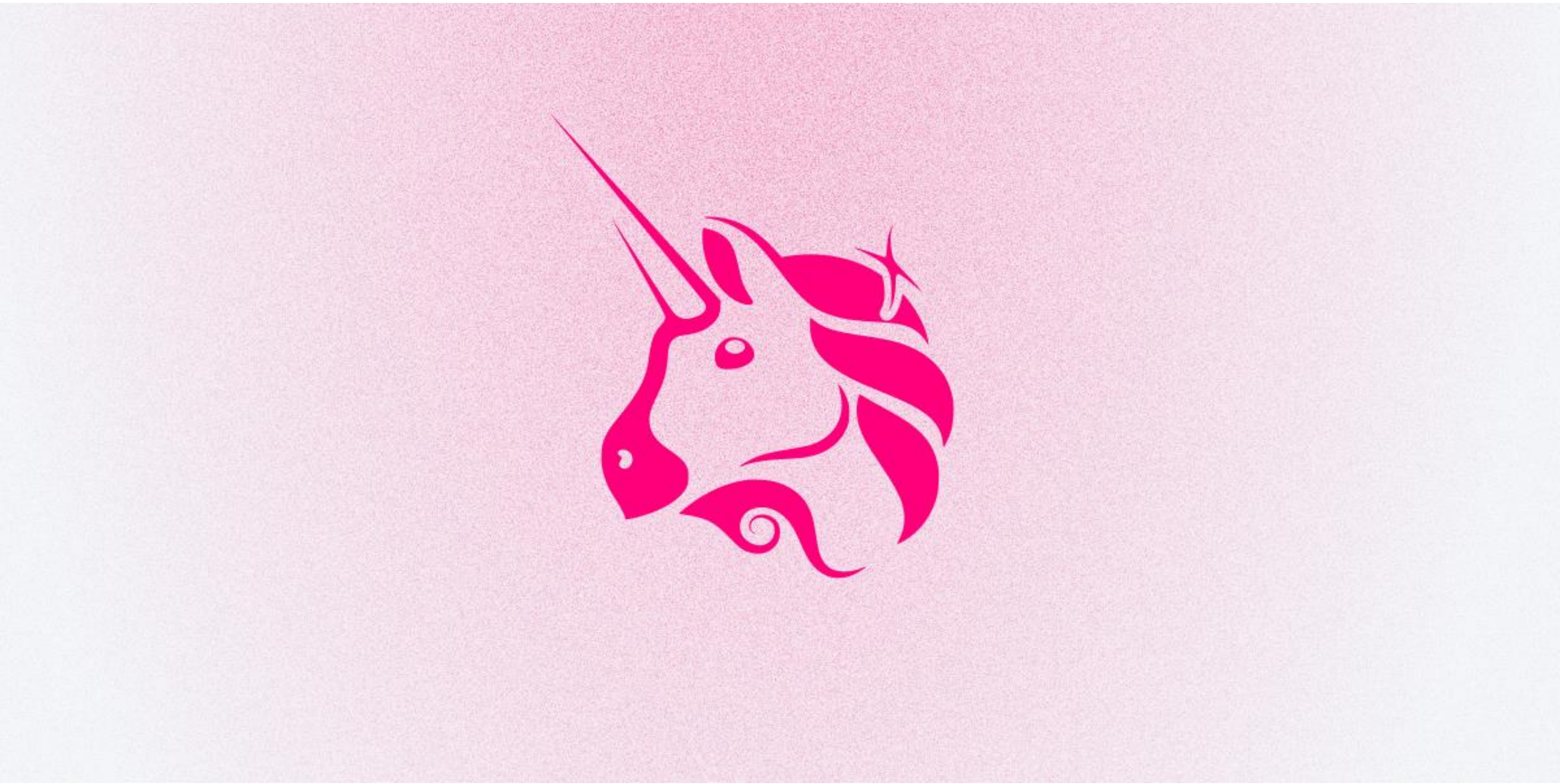
Transactions **throughput** – transactions per second (tps)

These metrics are for settlement layer

Application layer user different metrics



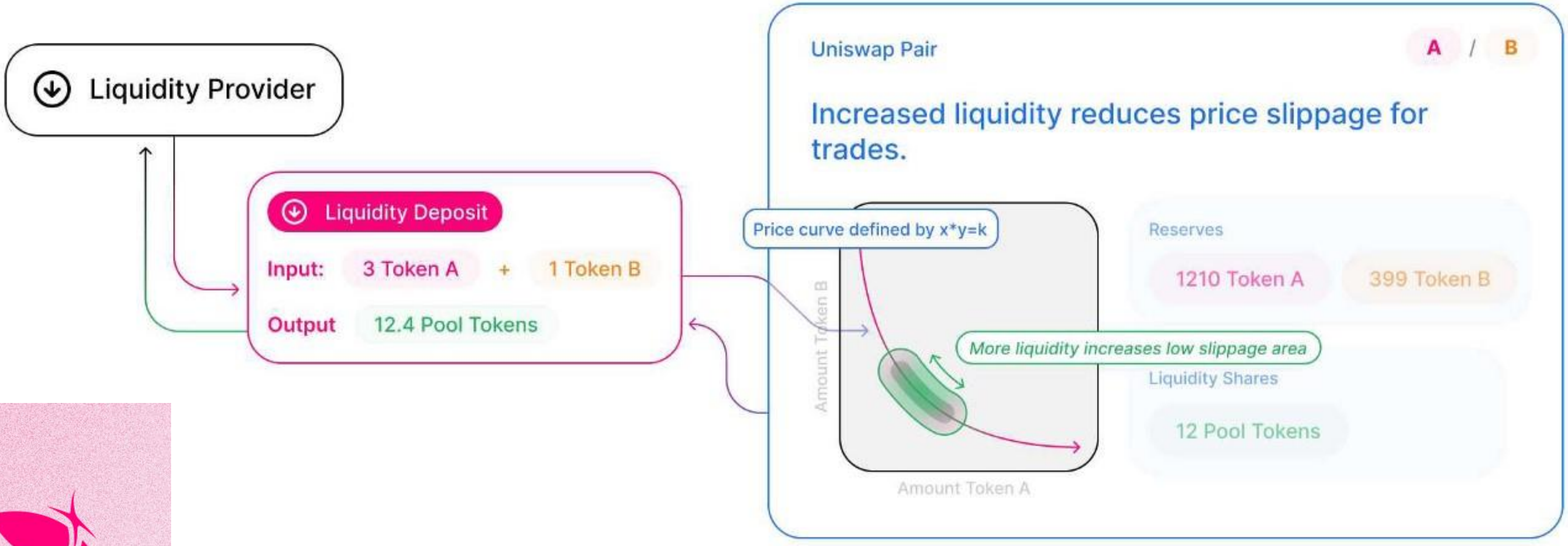
BACK TO UNISWAP AGAIN



2 ASPECTS OF SCALABILITY:

USERS SWAP WITH BETTER PRICE

LIQUIDITY PROVIDERS BECOMES MARKET MAKER FASTER(WITH LOWER COST)



Liquidity Provider

Liquidity Deposit

Input: 3 Token A + 1 Token B

Output 12.4 Pool Tokens

Uniswap Pair

A / B

Increased liquidity reduces price slippage for trades.

Price curve defined by x*y=k

More liquidity increases low slippage area

Reserves

1210 Token A

399 Token B

Liquidity Shares

12 Pool Tokens

XY = K : BIGGER RESERVE, BETTER PRICE (LESS SLIPPAGE)

88.2% OF DEX VOLUME CAME FROM ONLY 3.8% WALLET.

THIS MEANS HIGH GAS ISNT THAT IMPORTANT

Decentralization

Let revisit the definition

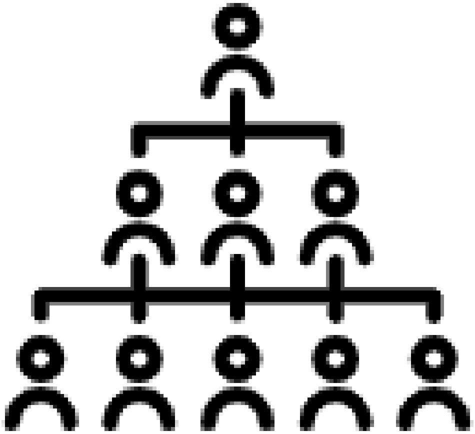
IT IS A LITTLE BIT PHILOSOPHY

Definition of **Decentralization?**

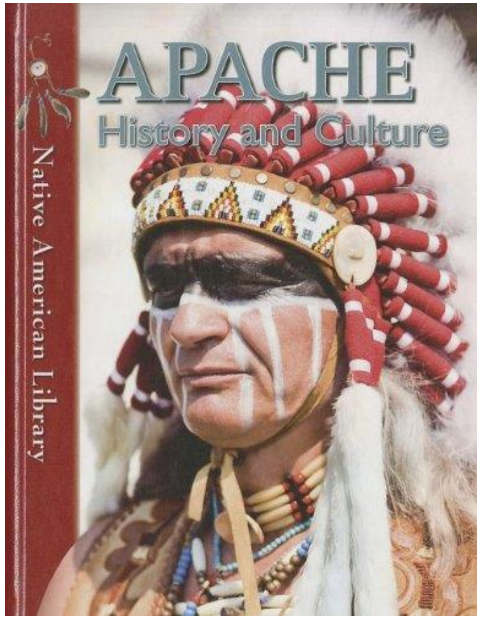
- ❑Is there someone in charge?
- ❑Are there headquarters?
- ❑If you thump it o the head, will it die?
- ❑Is there a clear division of roles?
- ❑If you take out a unit, is the organization harmed?
- ❑Are knowledge and power concentrated or distributed?
- ❑Is the organization flexible or rigid?
- ❑Can you count the employees or participants?
- ❑Are working groups funded by the organization, or are they self-funding?

Definition of **Decentralization?**

- ❑ Is there someone in charge?
  - ➢ Order
  - ➢ Hierarchy
  - ➢ Accountability
  - ➢ Communicate via intermediaries



VS



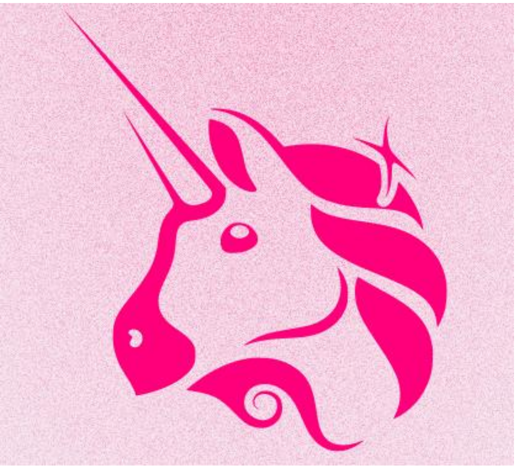
take-the-gold-and-kill-the-leader-strategy

NANT'AN

Definition of **Decentralization?**

❑ Are there headquarters?

- ➢ Permanent Address
- ➢ Physical Location



UNISWAP

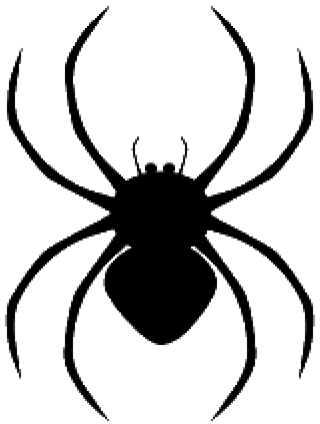
VS

BINANCE

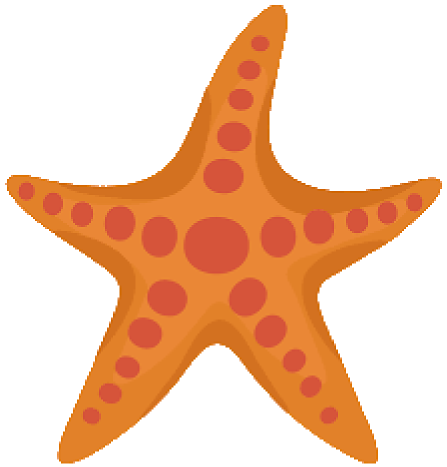
Definition of Decentralization?

❑ If you thump it on the head, will it die?

- ➢ Headquarter



VS

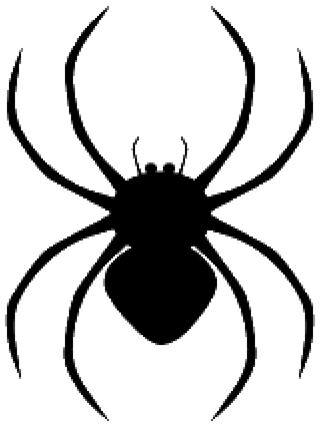


Spider

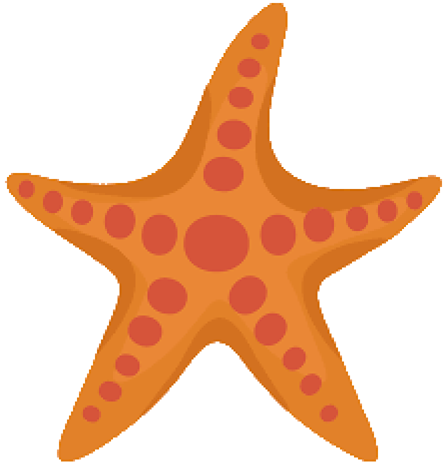
STARFISH

Definition of Decentralization?

- ❑ Is there a clear division of roles?
  - ➢ Own responsibility vs
  - ➢ Anyone can do anything



VS

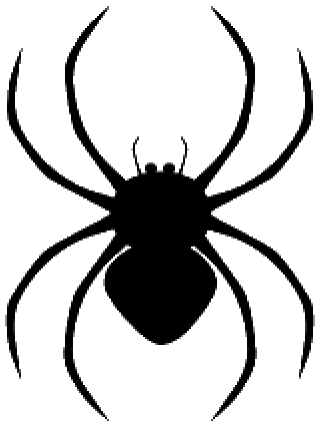


Spider

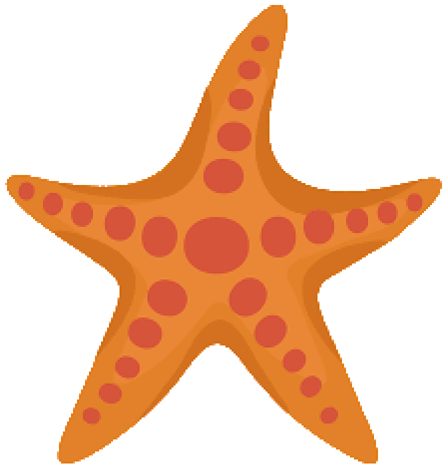
STARFISH

Definition of Decentralization?

- ❑ If you take out a unit, is the organization harmed?
  - ➢ Irreparable vs
  - ➢ Autonomous Units



vs



Spider

STARFISH

Definition of **Decentralization?**

- ❑ Are knowledge and power concentrated or distributed?
  - ➢ Person in charge vs
  - ➢ Each group can decide

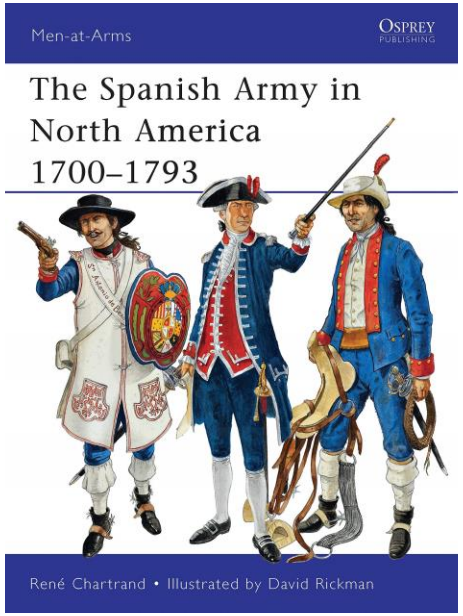
CZ

VS

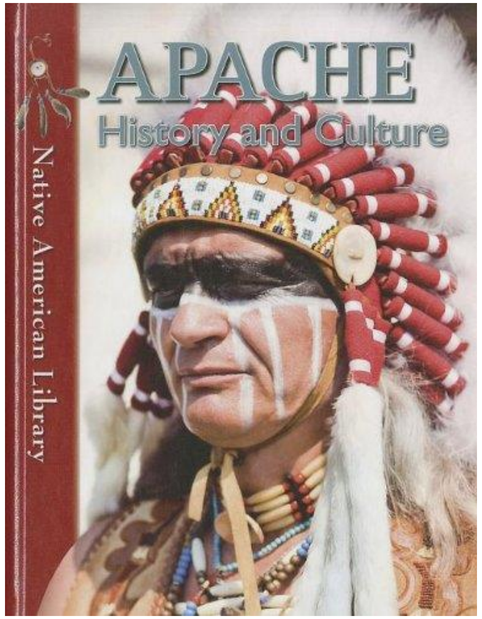
VITALIK

Definition of **Decentralization?**

- ❑ Is the organization flexible or rigid?
  - ➢ Spreading
  - ➢ Growing
  - ➢ Shrinking
  - ➢ Dying off
  - ➢ Re-emerging


Men-at-Arms
OSPREY PUBLISHING
The Spanish Army in North America 1700–1793
René Chartrand • Illustrated by David Rickman

VS

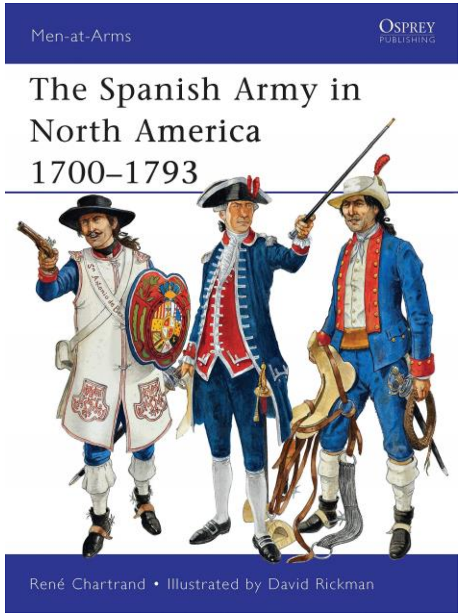


take-the-gold-and-kill-the-leader-strategy

NANT'AN

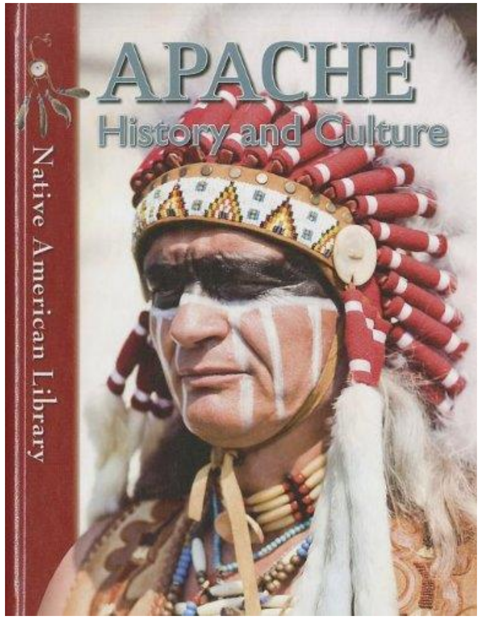
Definition of **Decentralization?**

- ❑ Can you count the participants
  - ➢ (/The Employees)?
  - ➢ Access to Record vs
  - ➢ Open membership


Men-at-Arms
OSPREY PUBLISHING
The Spanish Army in North America 1700–1793
René Chartrand • Illustrated by David Rickman

Spanish Army

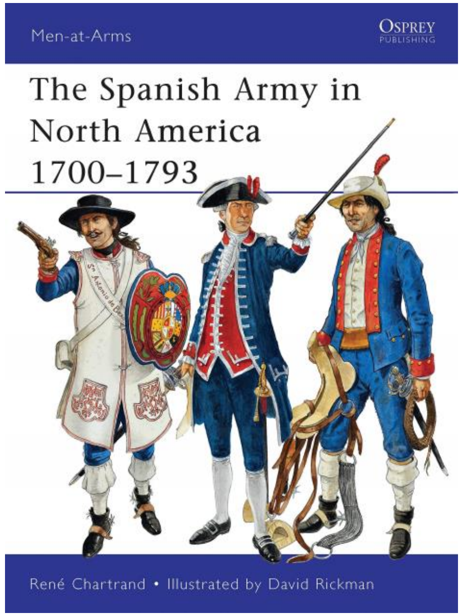
VS



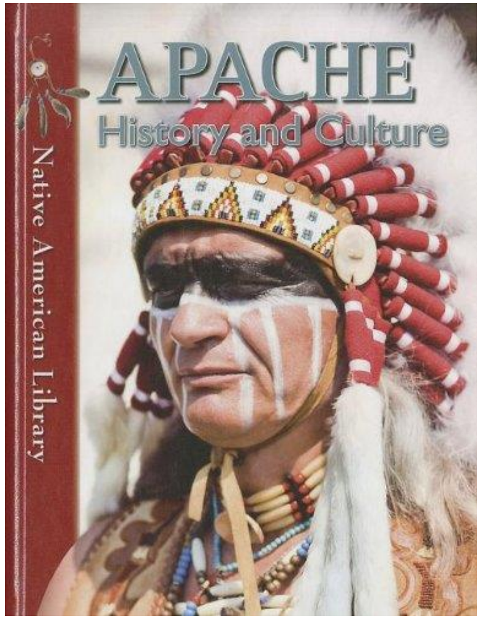
NANT'AN

Definition of **Decentralization?**

- ❑ Are units self-funding?
  - ➢ Re-distribute Revenue vs
  - ➢ Receive funding from outside


Men-at-Arms
OSPREY PUBLISHING
The Spanish Army in North America 1700–1793
René Chartrand • Illustrated by David Rickman

VS



Spanish Army

NANT'AN

3 Reasons for **Decentralization?**

Immutability

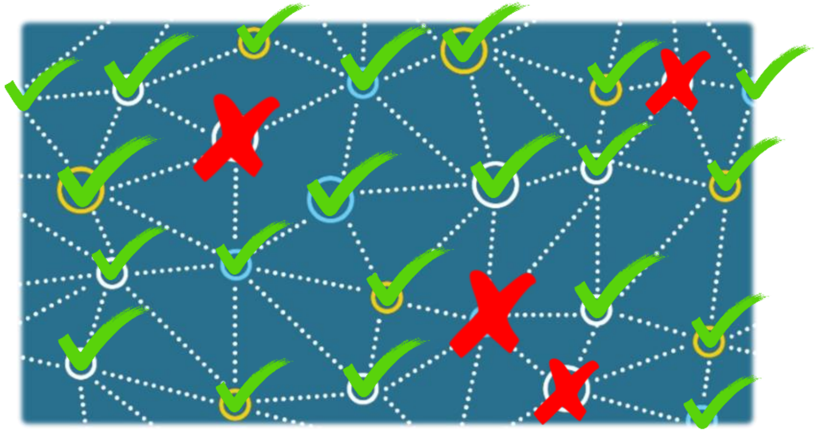
- Once data is stored, it cannot be manipulated later
- Much harder to collude and to act in fraudulent way

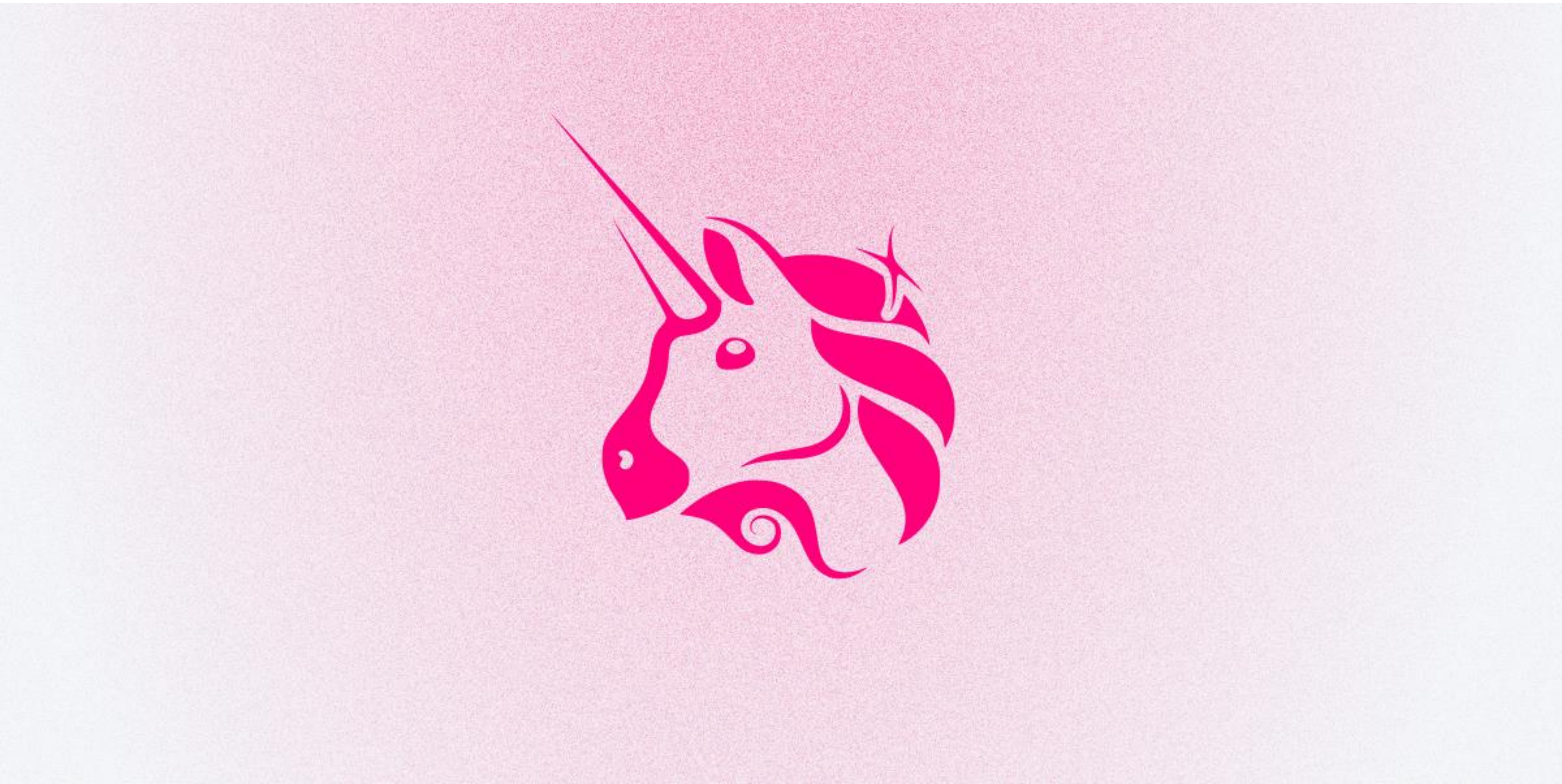
Fault tolerance

- Less likely to fail accidentally

Attack resistance

- More expensive to attack





BACK TO UNISWAP AGAIN

Yes, must think differently on different layers

DECENTRARISATION IN INFRASTRUCTURE LAYER !== IN APPLICATION LAYER

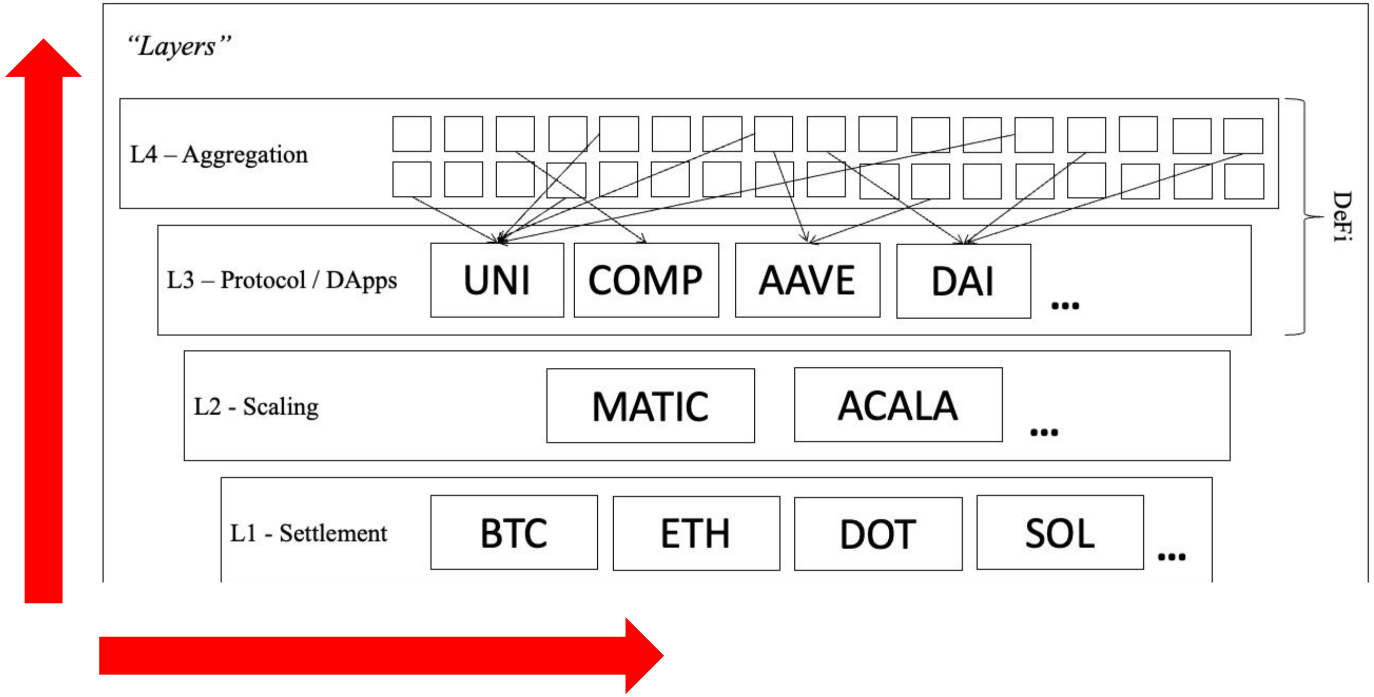
Security

Security in Blockchain ?

❑ Integrity

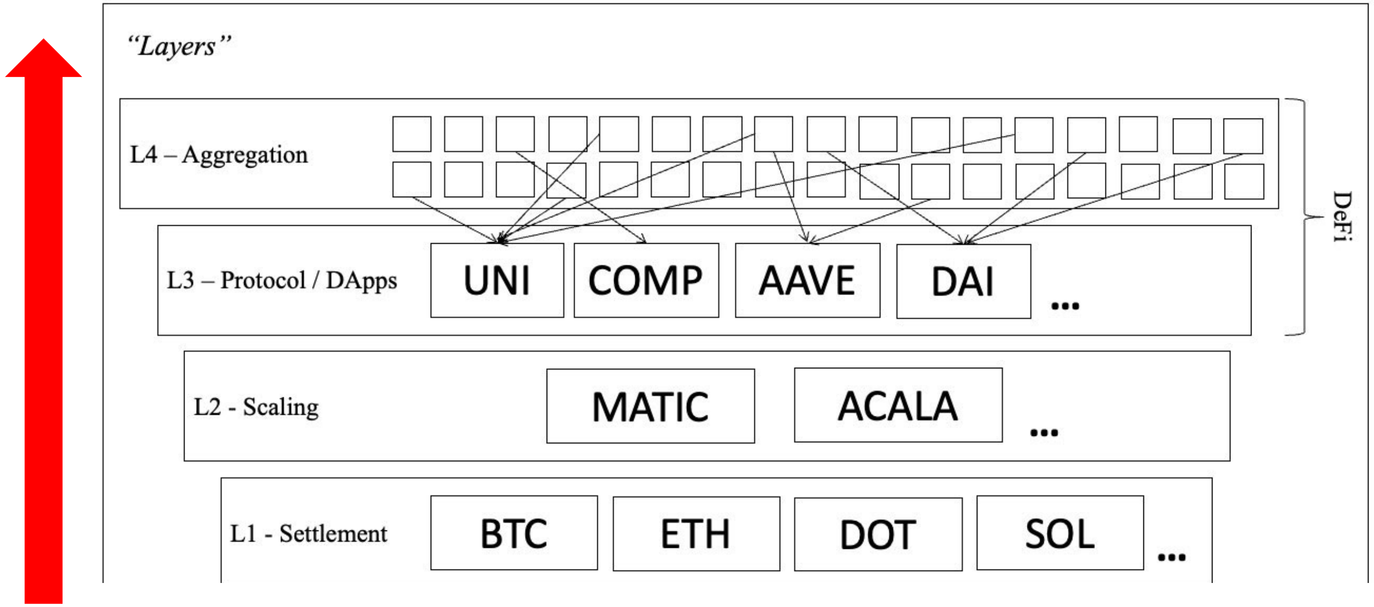
❑ Availability

❑ Confidentiality ✗



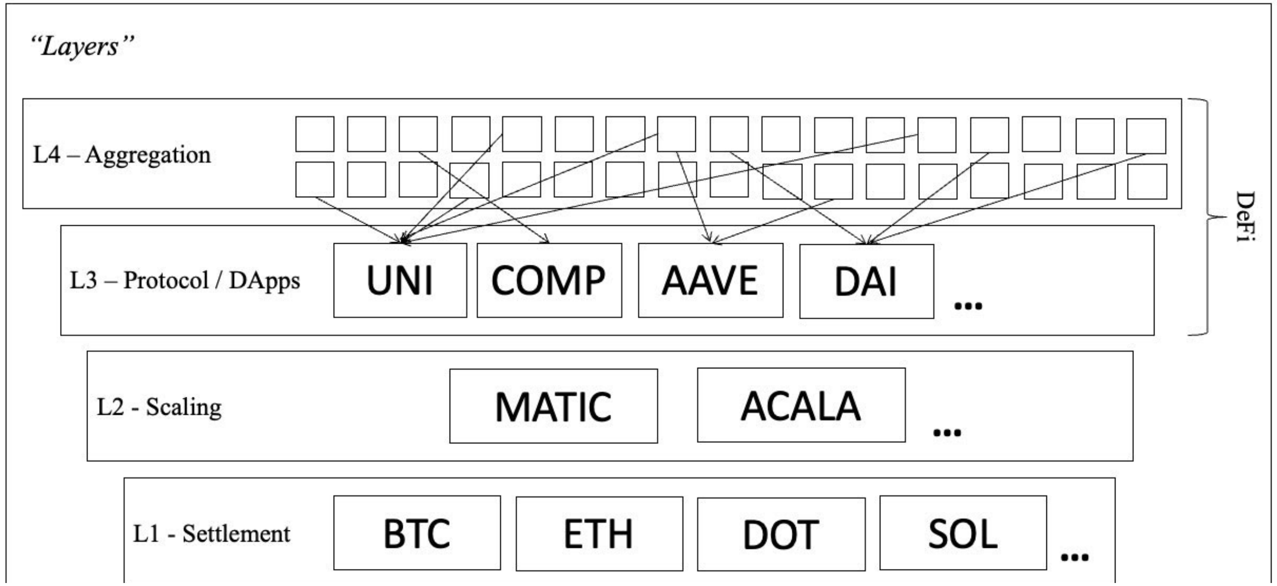
Security propagates through all different layers

DIFFERENT FROM SCALABILLITY/DECENTRALIZATION



Vertically: Inherit security risk from below layers

DEVELOPING OWN DAPP ON OWN CHAIN



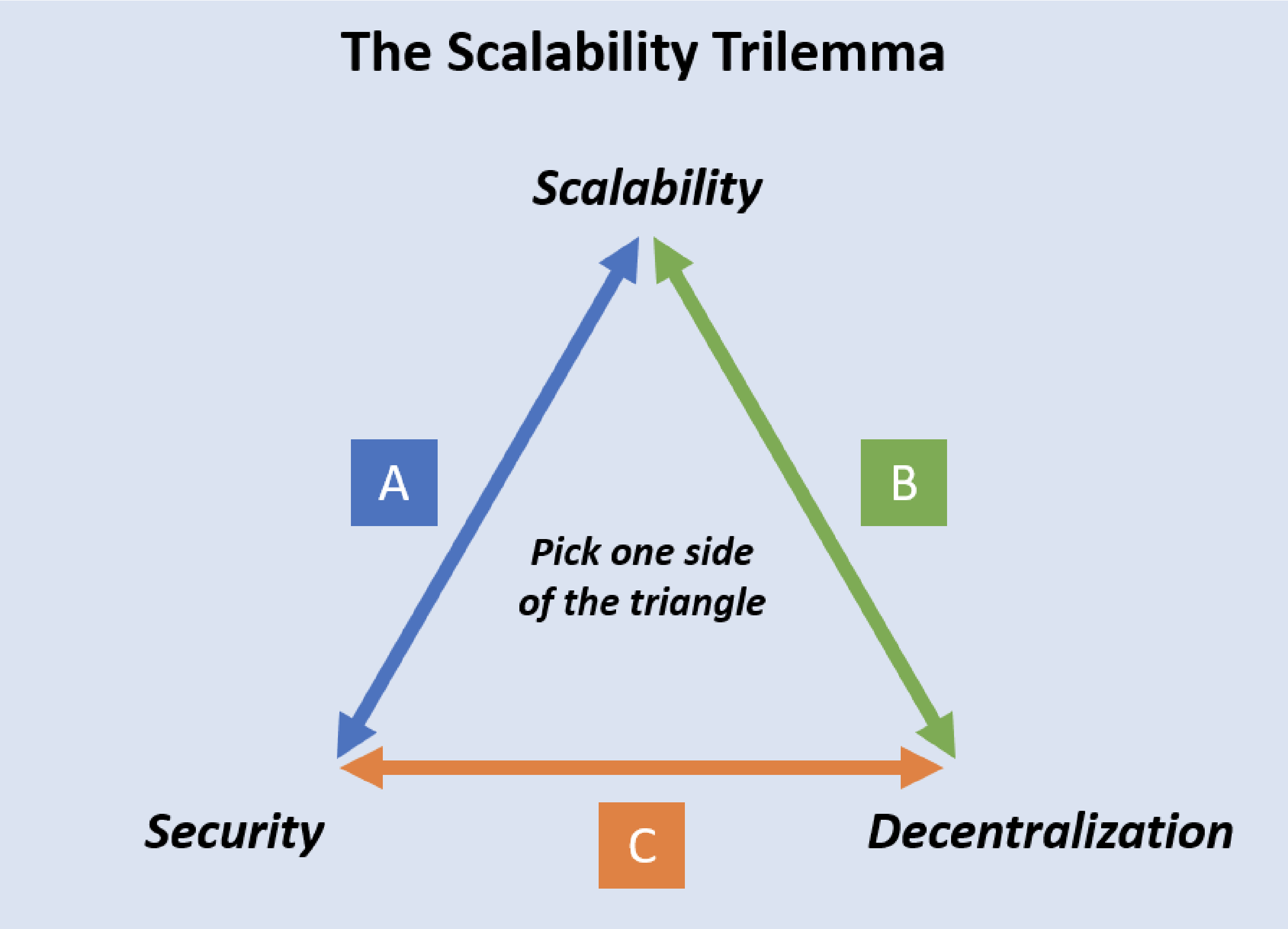
Horizontally: More Surfaces to Attack

BRIDGES FROM DIFFERENT L1

Let back to the question

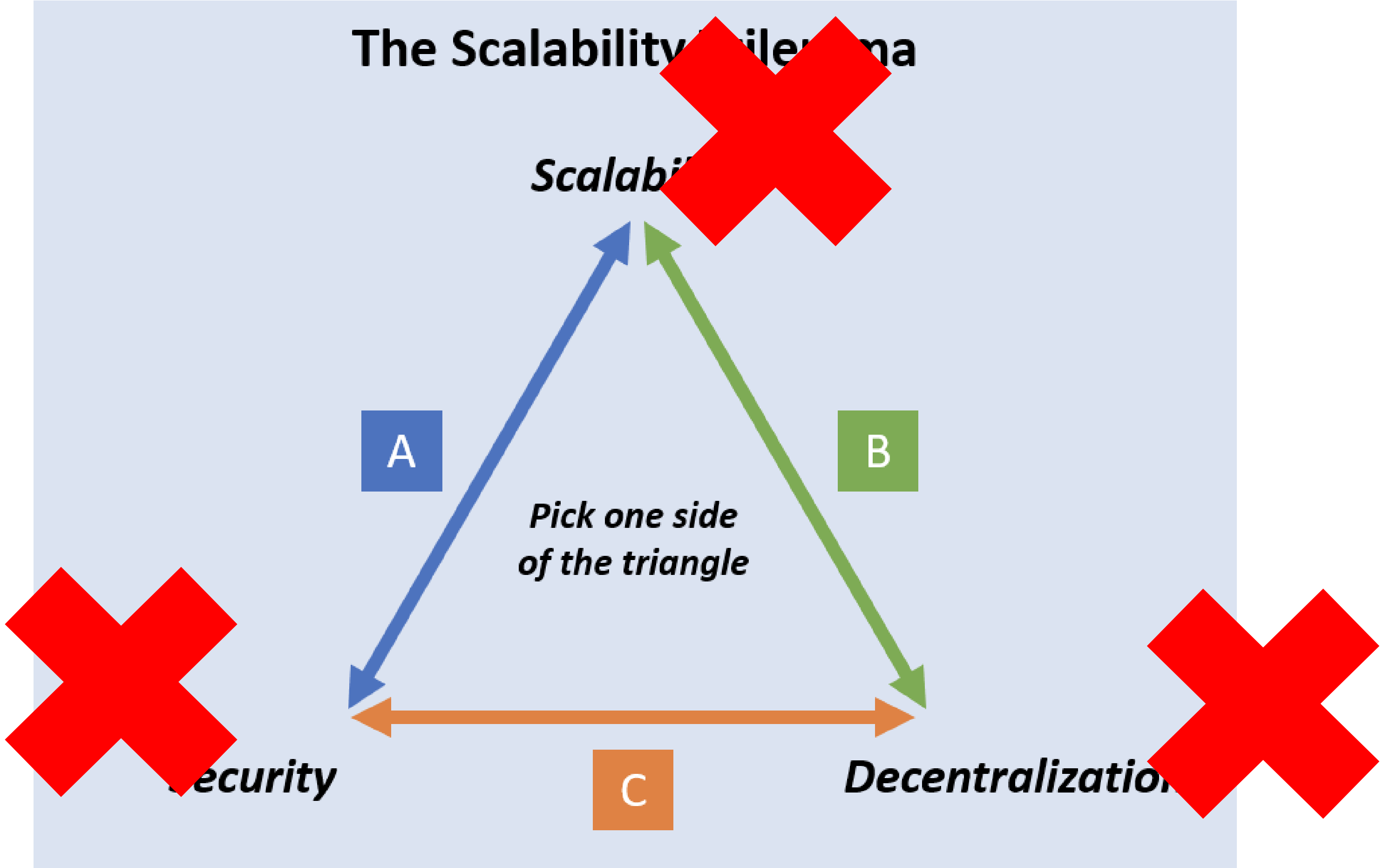
SOMEONE STATES THE DEFINITION

What is the hardest part of blockchain development?



The answer is …

What is the hardest part of blockchain development?



The answer is understanding the **trade-offs**

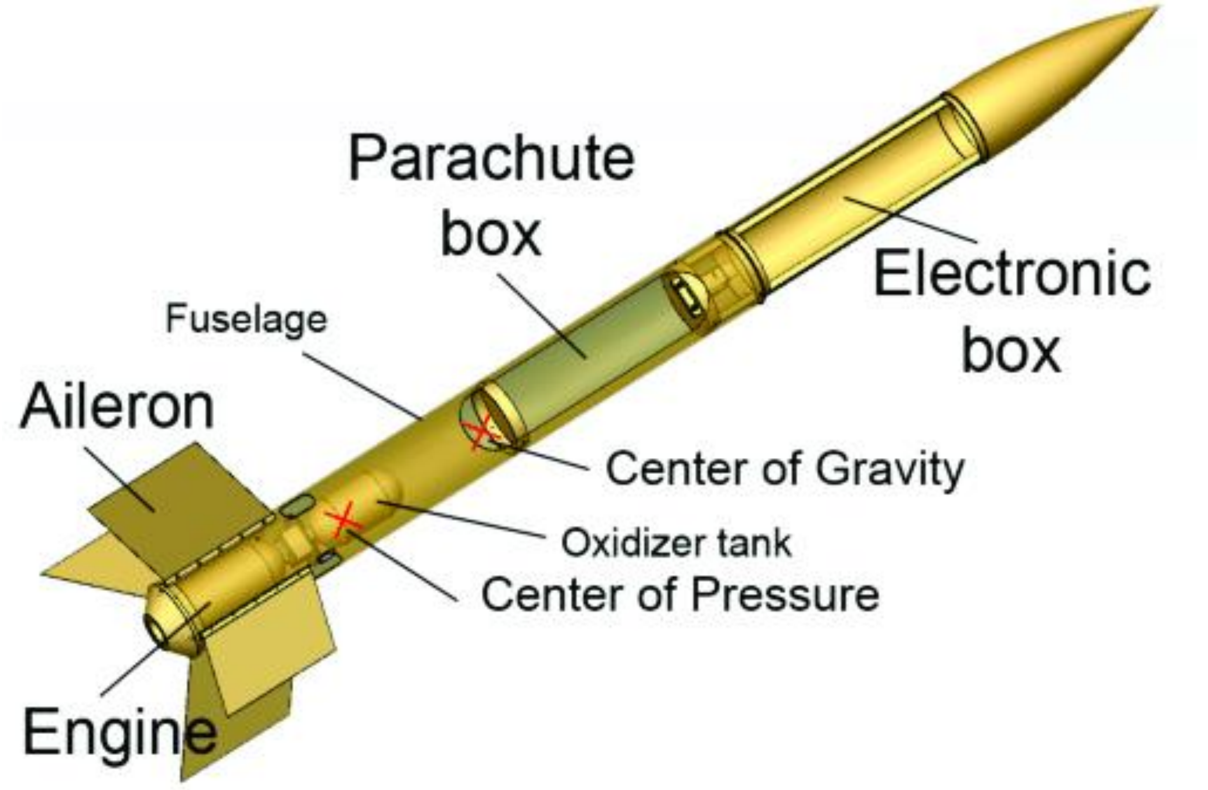
Any choices you make, any mistake can have unforeseen, potentially devastating consequences and it is **irreversible**

Blockchain Stuff is a mission critical application

- It is an extremely adversarial environment
- It is like Rocket Launch
- It is like complex system

Complex System

- Systems Thinking
  - Linkages and Interactions
- Emergence / Emergency
  - Functionality is > sum of entities



The answer is understanding the **trade-offs**

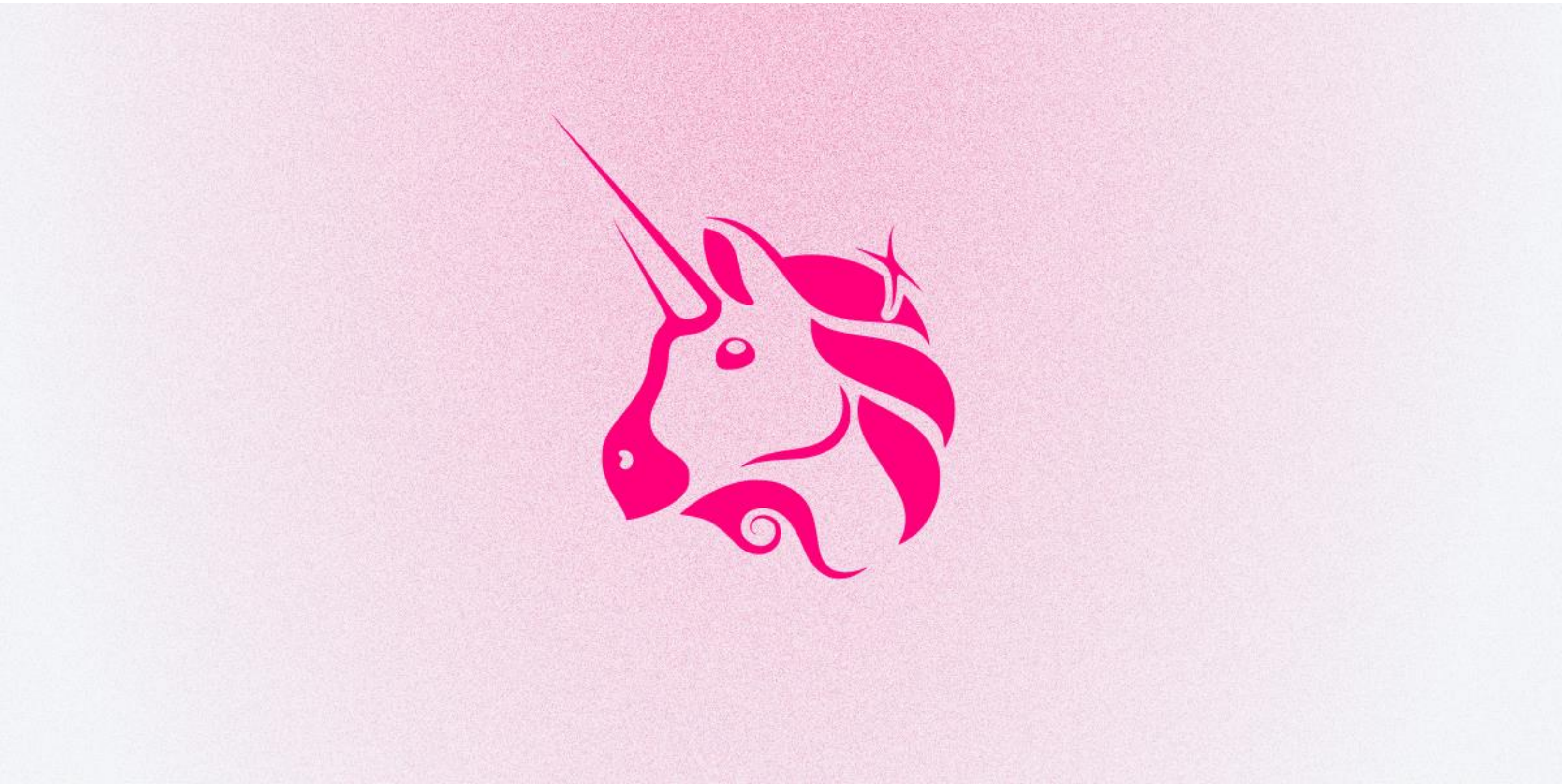
KNOWING TRADE-OFF OF ROCKET BEFORE LAUNCHING,

SO WE CAN DECIDE APPROPRIATE ARCHITECTURE

Before you develop blockchain, do you understand what do you want to solve?

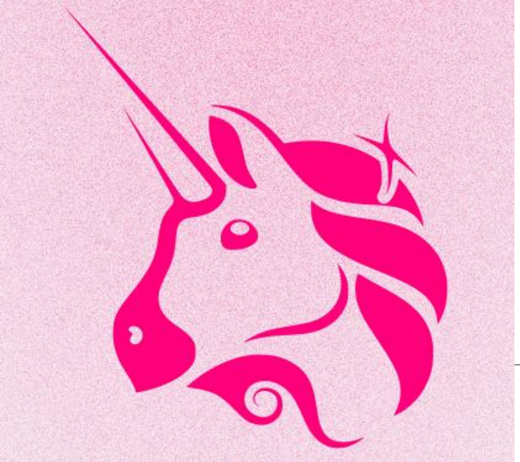
Ask yourself before building web3 DApp

- ❑ Does it really need a blockchain?
- ❑ Do users lose something when deploying traditionally?
- ❑ Does emergence add a real benefit to your idea?
  - ➢ Real Benefit as Emergence of complex system



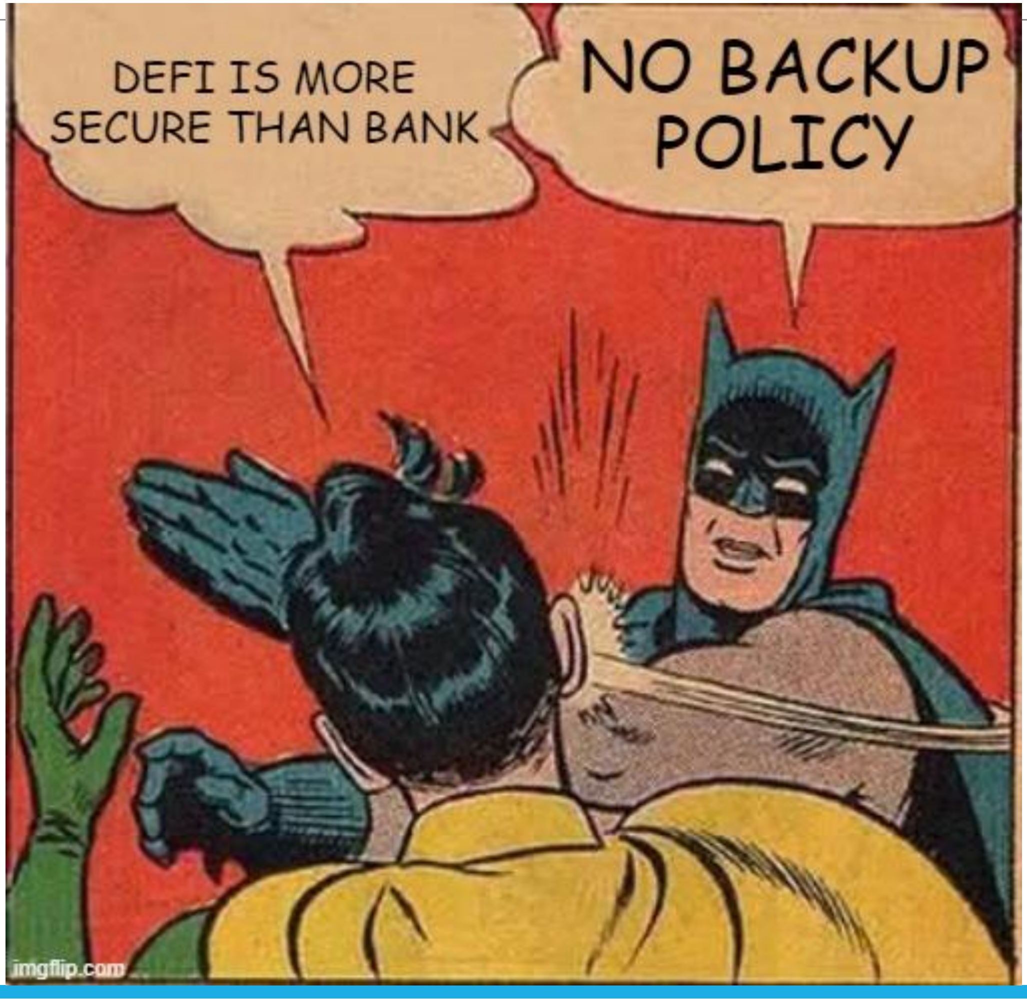
BACK TO UNISWAP AGAIN

Emergences of UNISWAP



- Does it really need a blockchain?
  - Yes
- Do users lose something when deploying traditionally?
  - Yes
- Does emergence add **a real benefit** to your idea?
  - Decentralization & Scalability (of broker as middleman)on Application layer

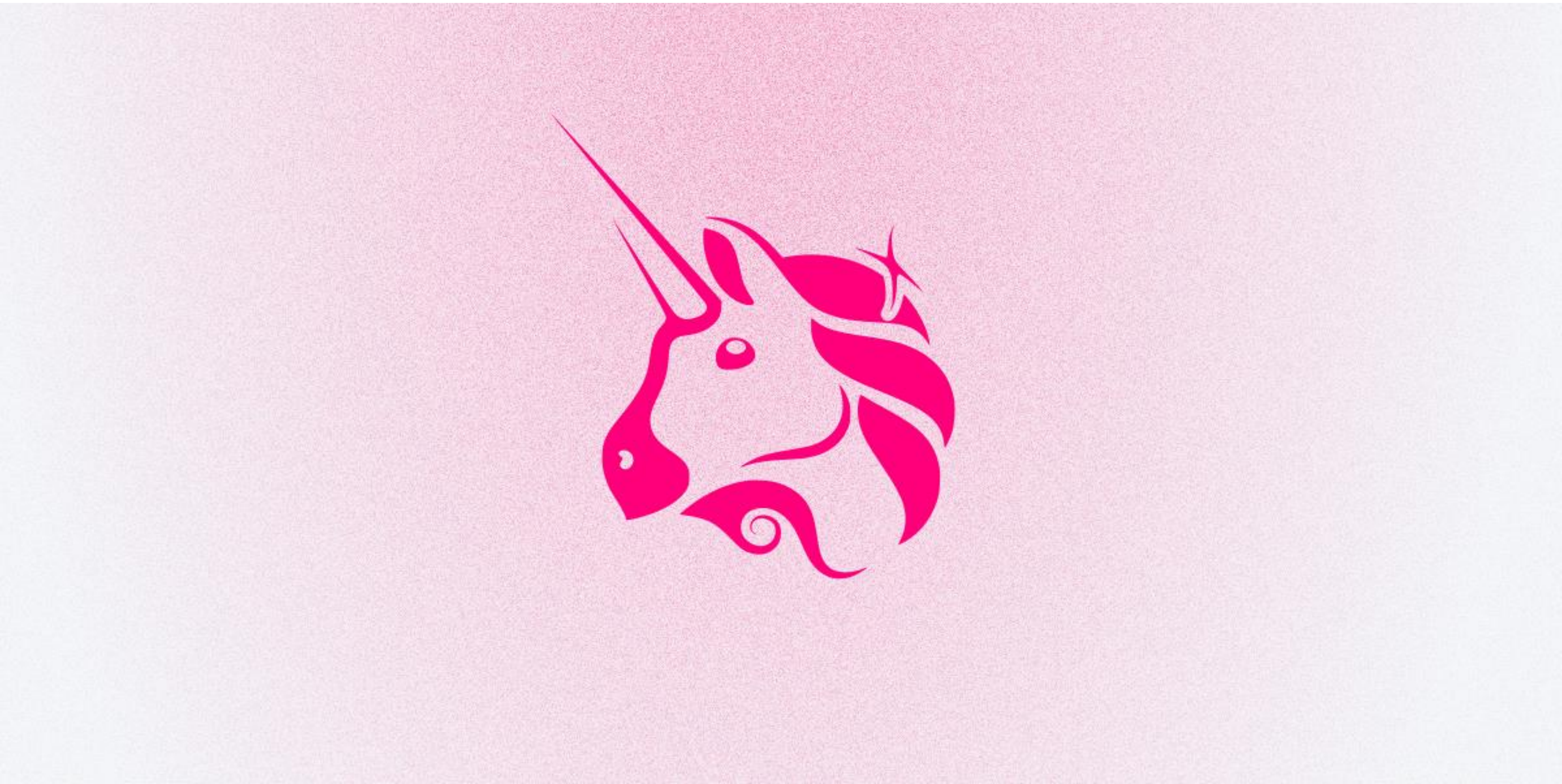
Security vs (De)Centralization



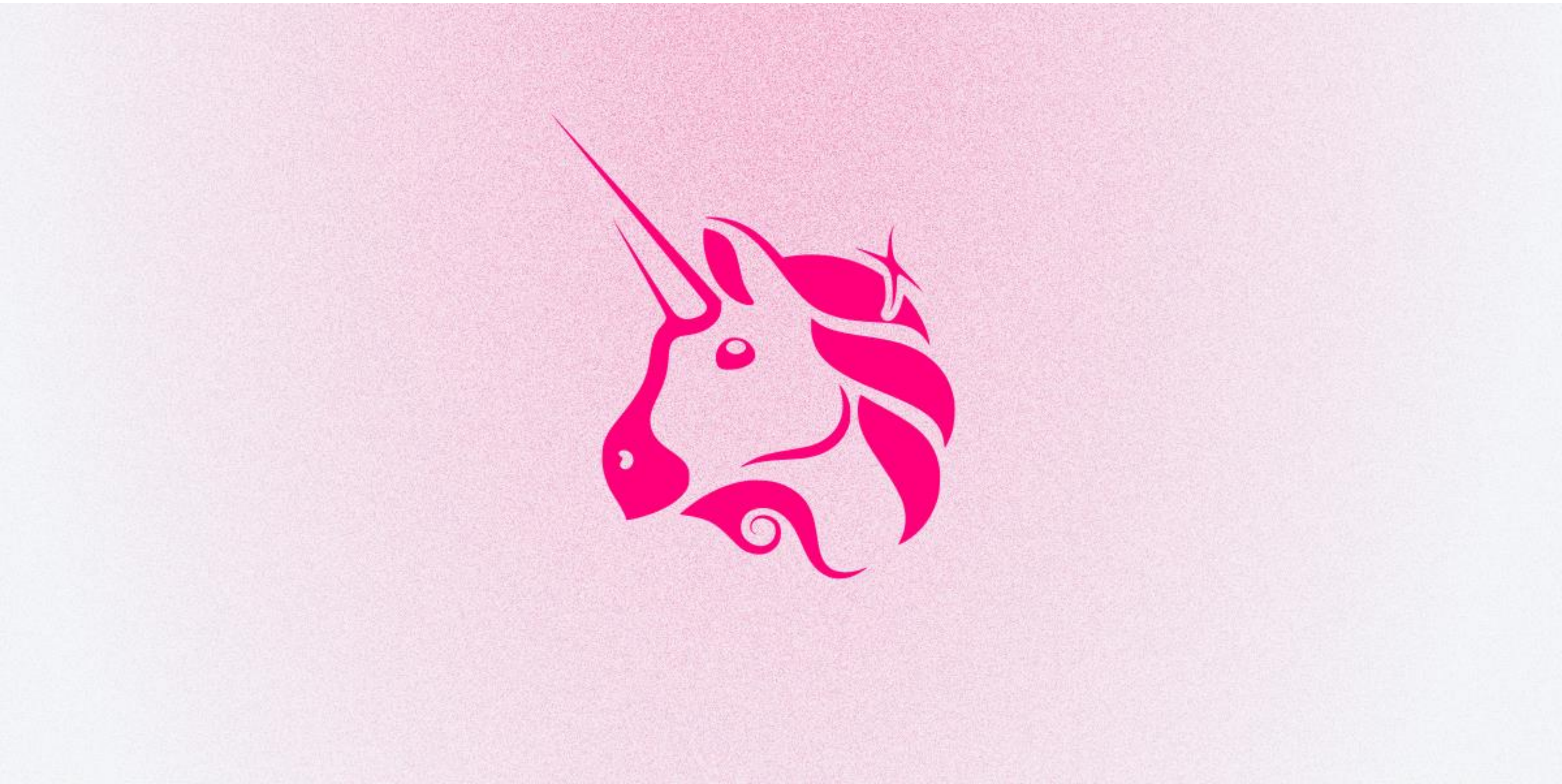
After you understand what do you want to solve, what is the next challenge?

The answer is neutrality

It ‘s all about balancing the user-selected inputs in complex system



BACK TO UNISWAP AGAIN

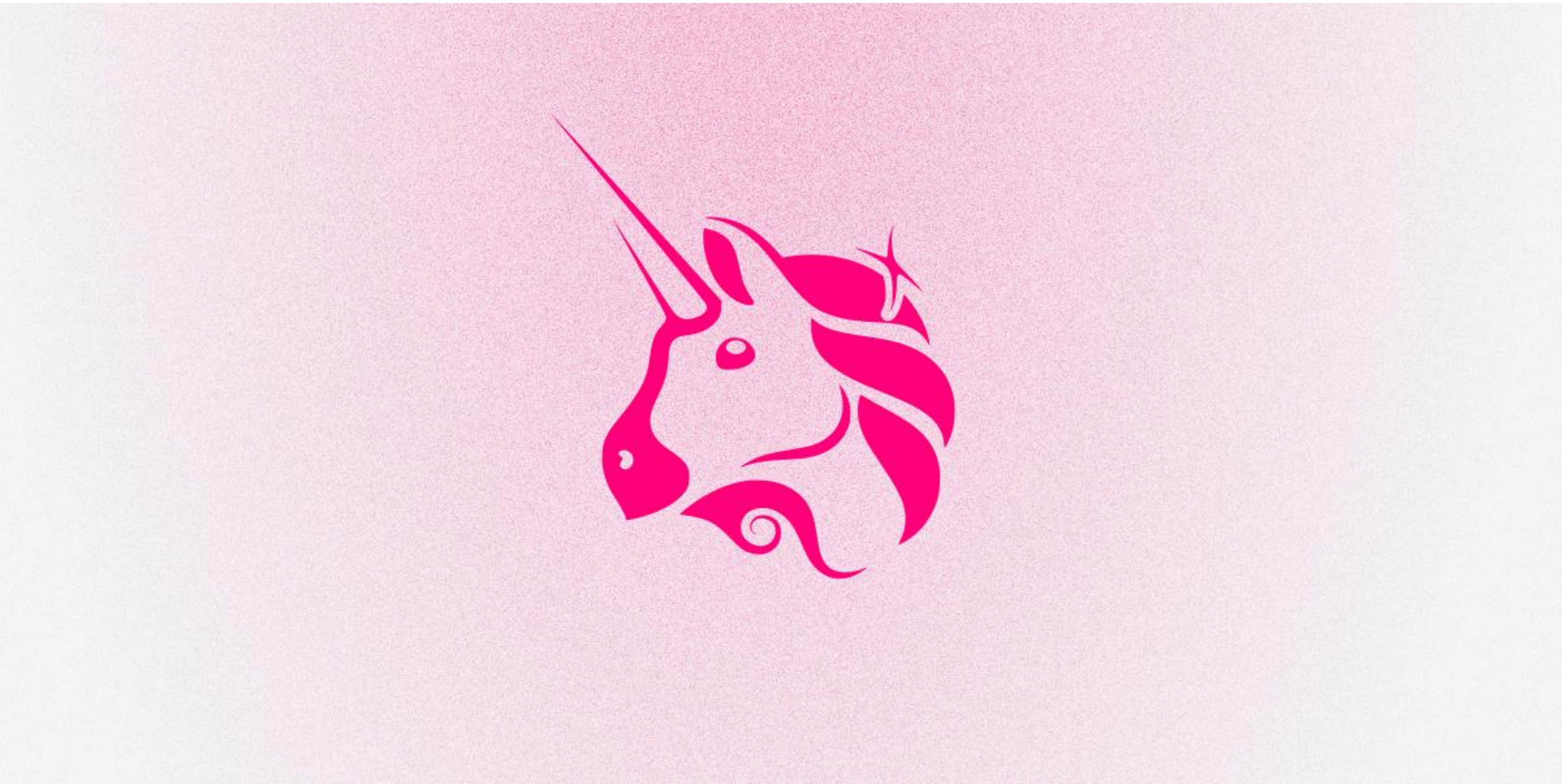


PROBLEM: TRADITIONAL ORDERBOOK

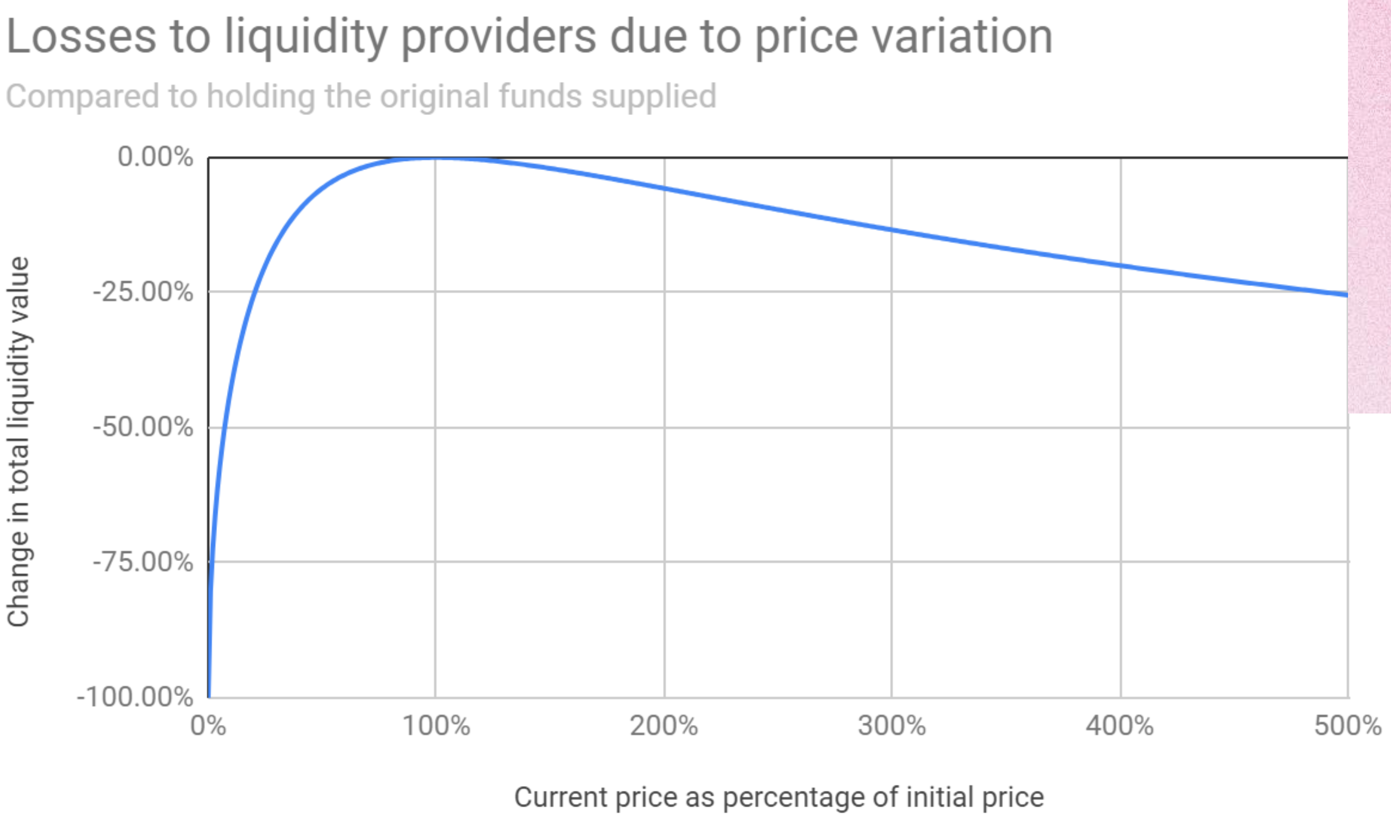
DIFFICULT TO BOOTSTRAP LIQUIDITY

(SELL & BUY ORDERS ARE **IMBALANCED**)

Orderbook vs AMM



SOLUTION: X*Y = K (BALANCING BY CONSTANT)



NEW PROBLEM: IMPERMANENT LOSS

WHEN A LIQUIDITY PROVIDER HAS A TEMPORARY LOSS OF FUNDS BECAUSE OF VOLATILITY IN A TRADING PAIR.

Squeeth

POLYNOMIAL DERIVATIVE FINANCIAL INSTRUMENT

Composable without Permission

DO YOU REMEMBER THIS?

Think Blockchain world as complex system

NEED TO INNOVATE NEW SOLUTIONS TO SOLVE EMRGING PROBLEMS

Squeeth

PROBLEM: HARD TO HEDGE AGAINST IMPERMANENT LOSS

DIFFICULT TO ESTIMATE THE RISK WHEN THE PRICES OF PAIRED ASSETS ARE VOLATILE

RISK BETWEEN DOWNSIDE AND UPSIDE ARE **IMBALANCED**

Squeeth

Solution: Y = X^2
(balance short and long positions)

Squeeth

NEW PROBLEM: LIQUIDITY BOOTSTRAPPING

DIFFICULT TO GOVERN ITSELF

SHORT AND LONG POSITIONS ARE **IMBALANCED**

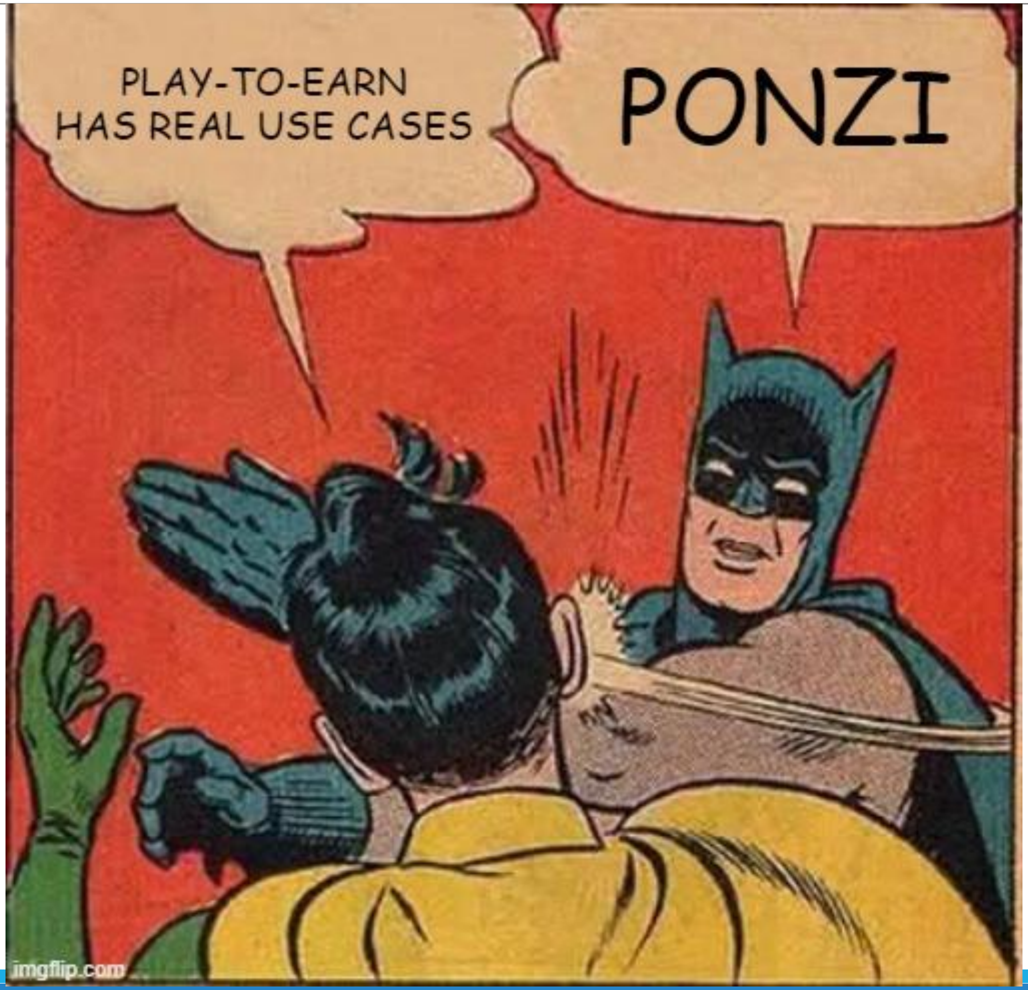
Squeeth

Solution: Funding Mechanism
(balance short and long positions by paying short positions fee)

Composable without Permission

IT MUST BE BUILT ON TOP OF REAL PRODUCT

Truth about Play-to-Earn



How ponzinomics works

DRIVE FOMO FOR SHORT-TERM GAINS WITHOUT LONG-TERM RESULTS

PROBLEM: CANT ESCAPE PONZINOMICS

MOST OF REVENUE COMES FROM INVESTMENT, NOT REAL USE CASE

(DEMAND & SUPPLY ARE **IMBALANCED**)

Axie INFINITY

Solution: make inflation in line with real growth as long as possible (balance inflation and real growth) (not solve real problem btw)

AGENT SMITH: THE **DIFFERENCE** BETWEEN US, TOM?

ANYONE COULD HAVE BEEN YOU.

WHEREAS I’VE **ALWAYS** BEEN ANYONE.

Thank you