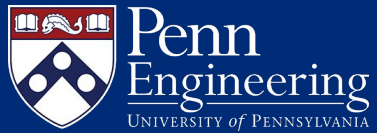
Security, Scaling, Bridges

Web3 Builders workshop series #4



Disclaimer

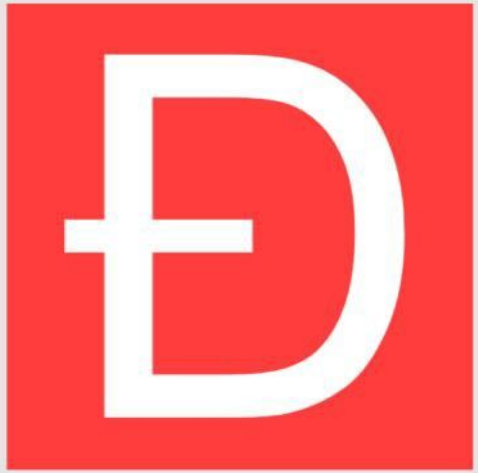
- This workshop series is **not** designed to teach you everything about blockchain, but it serves as a starting point for you to do your own research
- We will not be going into too much details, but feel free to discuss more about it with us after the main workshop!
- Feel free to interrupt us anytime you want
-
- Enjoy :)

Web3 Security

The DAO

DAO FAILURE

- One of the first ICOs of investment funds on Ethereum
- Collected 11,5 mln ethers (now it is ~ $1 bln)
- Smart contract wasn't properly audited by Slock.it team (the creators), as a result, there was a critical money-draining bug
- The smart contract checked balance after sending coins, this lead to the DAO failure.
- A lot of Ethereum tokens were under the control of hackers, which could be a problem for the community
- In order to save investors and punish hackers, Ethereum foundation made a hardfork. Ethereum classic was created.



Message from the “Attacker”-

To the DAO and the Ethereum community,

I have carefully examined the code of The DAO and decided to participate after finding the feature where splitting is rewarded with additional ether. I have made use of this feature and have rightfully claimed 3,641,694 ether, and would like to thank the DAO for this reward.

Message from the “Attacker”-

I am disappointed by those who are characterizing the use of this intentional feature as "theft". I am making use of this explicitly coded feature as per the smart contract terms and my law firm has advised me that my action is fully compliant with United States criminal and tort law. For reference please review the terms of the DAO:

"The terms of The DAO Creation are set forth in the smart contract code existing on the Ethereum blockchain at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413. Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO’s code*. Any and all explanatory terms or descriptions are merely offered for educational purposes and do not supercede or modify the express terms of The DAO’s code set forth on the blockchain; to the extent you believe there to be any conflict or discrepancy between the descriptions offered here and the functionality of The DAO’s code at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413, The DAO’s code controls and sets forth all terms of The DAO Creation."*

Message from the “Attacker”-

A soft or hard fork would amount to seizure of my legitimate and rightful ether, claimed legally through the terms of a smart contract. **Such fork would permanently and irrevocably ruin all confidence in not only Ethereum but also the in the field of smart contracts and blockchain technology. Many large Ethereum holders will dump their ether, and developers, researchers, and companies will leave Ethereum. Make no mistake: any fork, soft or hard, will further damage Ethereum and destroy its reputation and appeal.**

I reserve all rights to take any and all legal action against any accomplices of illegitimate theft, freezing, or seizure of my legitimate ether, and am actively working with my law firm. Those accomplices will be receiving Cease and Desist notices in the mail shortly.

I hope this event becomes an valuable learning experience for the Ethereum community and wish you all the best of luck.

Yours truly,

"The Attacker"

The DAO - Aftermath

- 14% of all ether in circulation was in this smart contract
- Hacker siphoned out $50mil (3,641,694)
- ETH dropped 25%
- Hard fork -> Ethereum Classic

Gym Network

Gym network is a **defi aggregator investment system.**

$GYMNET

Gym Network- 2.1Mil lost

The project was audited by both Certik and Peckshield in May, however the faulty code was introduced two days ago.

Why carry out two audits if you're going to change the codebase a month later?

AkuAuction

- 45mil locked in the contract
- Founded by retired MLB player

Penn Engineering
University of Pennsylvania

Wharton
University of Pennsylvania

AkuAuction

```
function processRefunds() external {
  // Removed logic for simplicity
  for (uint256 i=_refundProgress; gasUsed < 5000000 && i < _bidIndex; i++) {
      bids memory bidData = allBids[i];
      if (bidData.finalProcess == 0) {
        uint256 refund = (bidData.price - price) * bidData.bidsPlaced;
        uint256 passes = mintPassOwner[bidData.bidder];
        if (passes > 0) {
            refund += mintPassDiscount * (bidData.bidsPlaced < passes ? bidData.bidsPlaced : passes);
        }
        allBids[i].finalProcess = 1;
        if (refund > 0) {
            (bool sent, ) = bidData.bidder.call{value: refund}("");
            require(sent, "Failed to refund bidder");
        }
      }
```

```
receive() external payable {
    require(false);
}
```

Penn Engineering University of Pennsylvania

Wharton University of Pennsylvania

AkuAuction

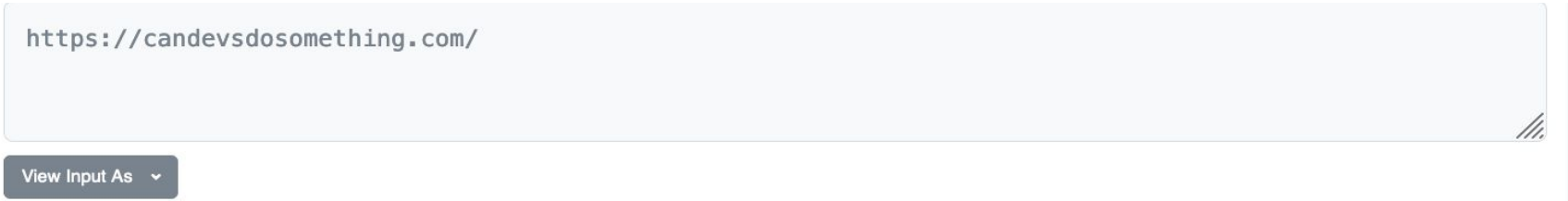
```
Hey, if you start processing refunds and a bidData.bidder.call fails and refunds get stuck, the people who have already been refunded, won't be able to retrieve the rest of their funds using emergencyWithdraw and you guys can't use claimProjectFunds() either because of require(refundProgress >= totalBids, "Refunds not yet processed");. Please do bug bounty on your contracts or have them audited at least.
```

View Input As

Penn Engineering
University of Pennsylvania

Wharton
University of Pennsylvania

AkuAuction



Penn Engineering
University of Pennsylvania

Wharton
University of Pennsylvania

AkuAuction

https://imgflip.com/i

View Input As

Penn Engineering
University of Pennsylvania

Wharton
University of Pennsylvania

AkuAuction

```
contract exploit {
    bool blocked;
     function unblock() external {
         blocked = false;
    }
   receive() external payable {
       require(blocked);
    }
}
```

AkuAuction

Well, this was fun, had no intention of actually exploiting this lol. Otherwise I wouldn't have used coinbase. Once you guys publicly acknowledge that the exploit exists, I will remove the block immediately. - USER221

View Input As

It's unlocked now

View Input As

How to prevent this

1. Study classes of vulnerabilities
    a. Know what to look out for!
2. Write specs and run automated tooling
3. Get audited!
4. Bug bounties

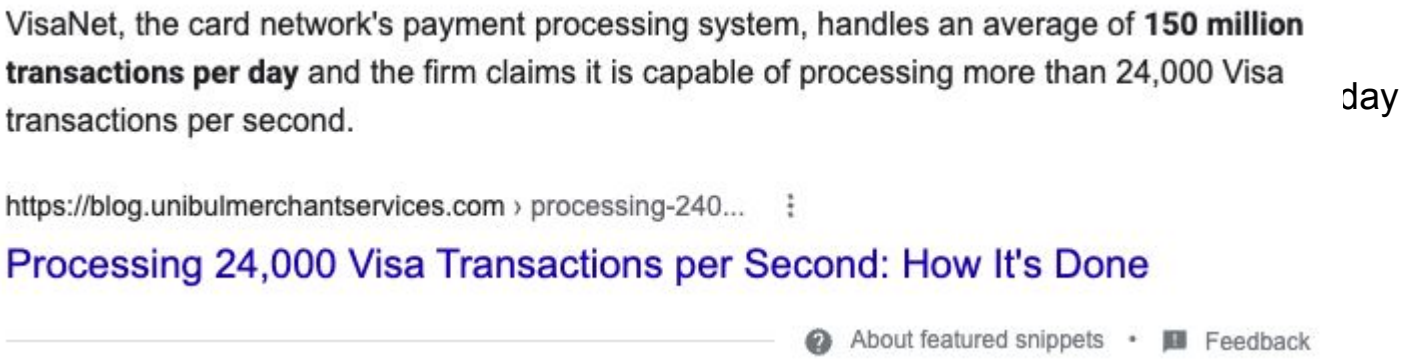
Scaling

Why do we need to scale?

day

Why do we need to scale?

- Ethereum is so much more than just payment
- Gaming, banking, other apps…
- We need more capacity for our blockchain computer



Penn Engineering University of Pennsylvania
Wharton University of Pennsylvania

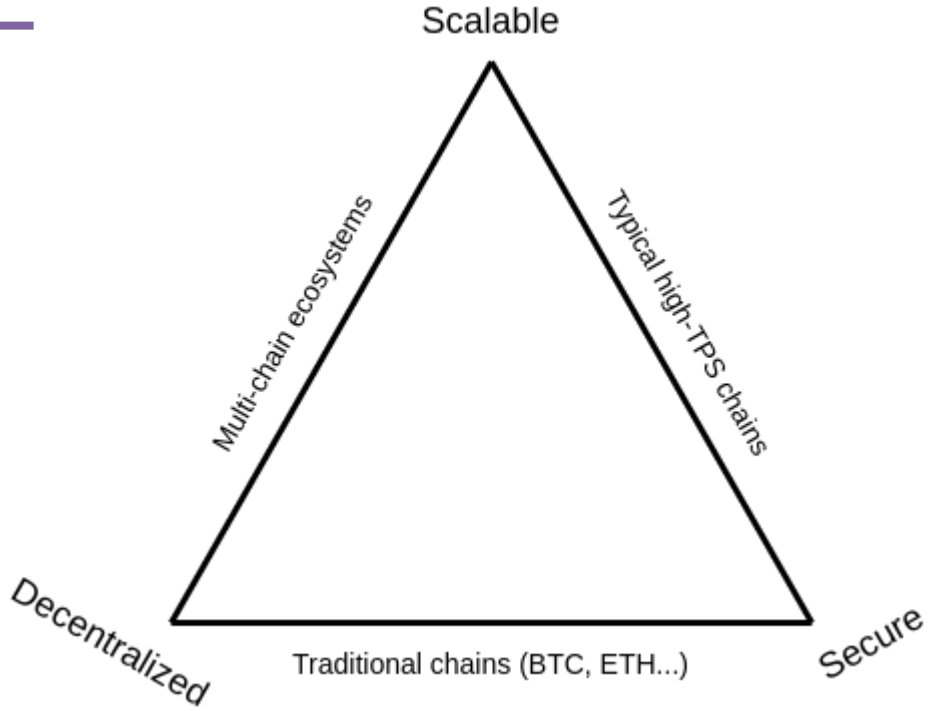
Are we bottlenecked by Ethereum's throughput?

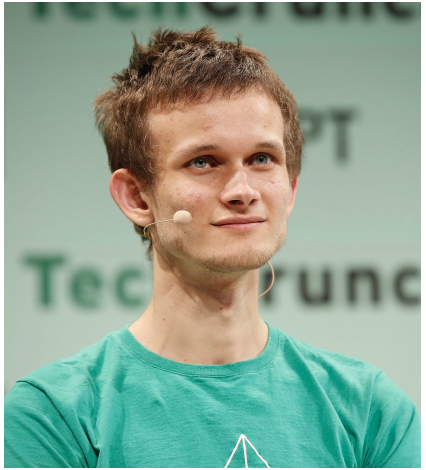
- Current: ~11
- Max recorded: 93.01 -> what happens when there's a lot of demand?
- Our target (Visa):
  - **150x** to reach average TPS
  - **2400x** to reach theoretical top TPS
  - Prob **10000x** to replace financial infrastructure
- Positive feedback loop
  - More throughput/capacity means?

What is stopping Ethereum from going faster

- Consensus -> Security
  - We want to make sure people all agree on the correctness of the blockchain
  - **If we don't** -> blockchain loses its purpose, no one will use Ethereum
- Distributed System -> Decentralization
  - To achieve consensus, we need to have many nodes all talk to each other. The communication is done via the Internet.
  - Speed of Internet is limited by the speed of light
  - **We are limited my physics**

Blockchain Trilemma





Penn Engineering
University of Pennsylvania

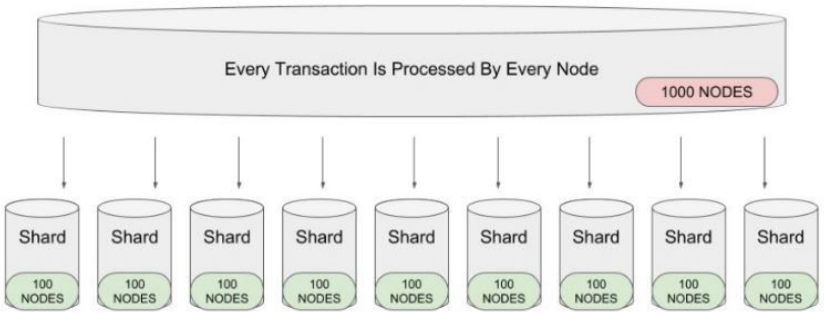
Wharton
University of Pennsylvania

Ethereum Future Upgrades - PoS

- PoS-> done
- Benefits
  - More green
  - Predictable blocktime
  - Removes computation overhead

Ethereum Future Upgrades - Sharding

- Sharding
  - Turn one network into multiple shards
  - Imagine you want 1000 students to vote

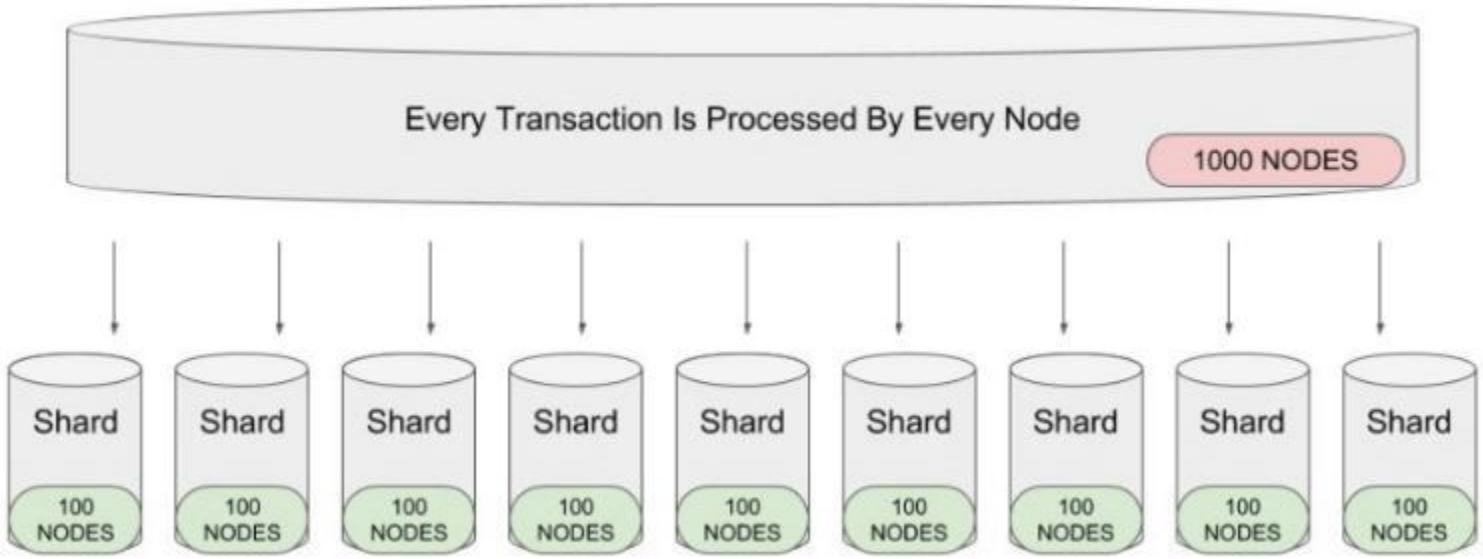


1000 nodes can be divided into 10 shards (100 nodes each) to achieve 10x performance.

Penn Engineering
University of Pennsylvania

Wharton
University of Pennsylvania

Ethereum Future Upgrades

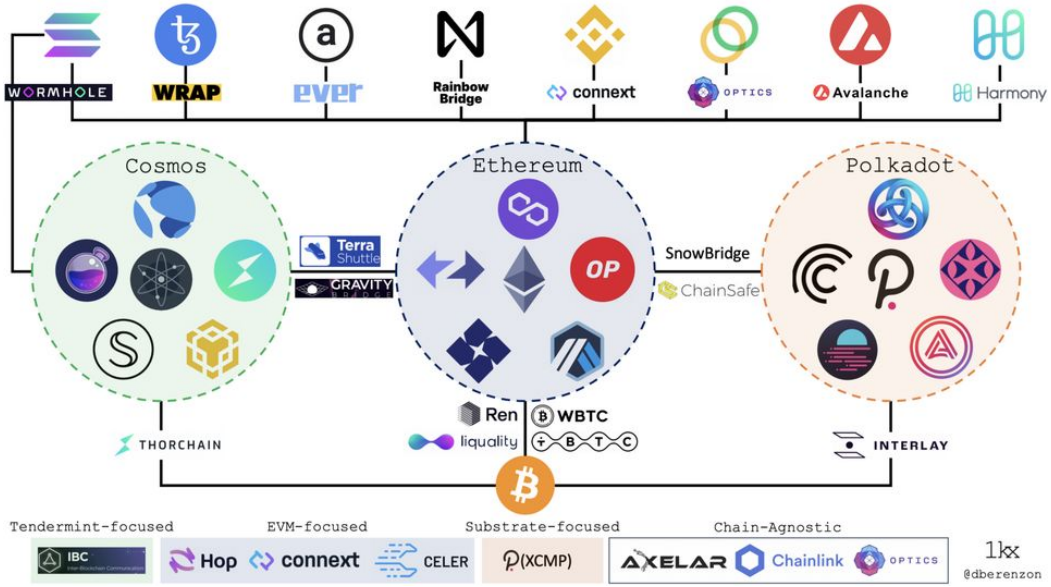


1000 nodes can be divided into 10 shards (100 nodes each) to achieve 10x performance.

Ethereum Future Upgrades - DAS

- Data Availability Sampling
  - Make it easier to prove block integrity without downloading
- Separate compute and storage

Off-chain scaling

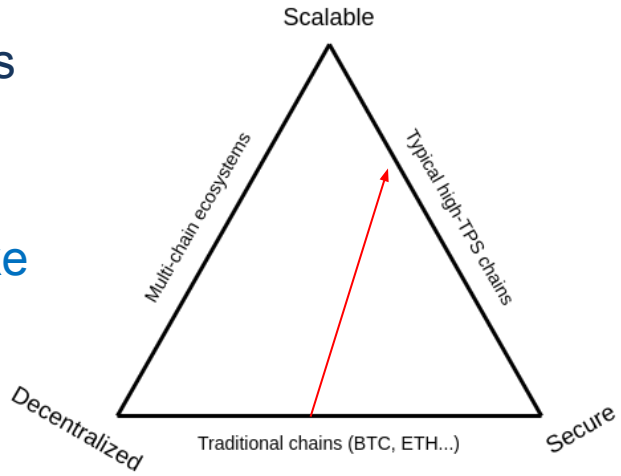


Rollups

- If Ethereum can only accommodate 100 tx, what if we “compress” 100 tx in to 1tx -> then we get 100x scaling.
- How do you pack 100 tx into 1?
  - You buy another computer, have it process the 100 tx.
  - Then you store the result onto Ethereum via 1 tx.
  - Ex. you have 100 requests to increment A by 1
    - Aggregate somewhere else -> ETH increment A by 100
  - Less secure
    - Why?

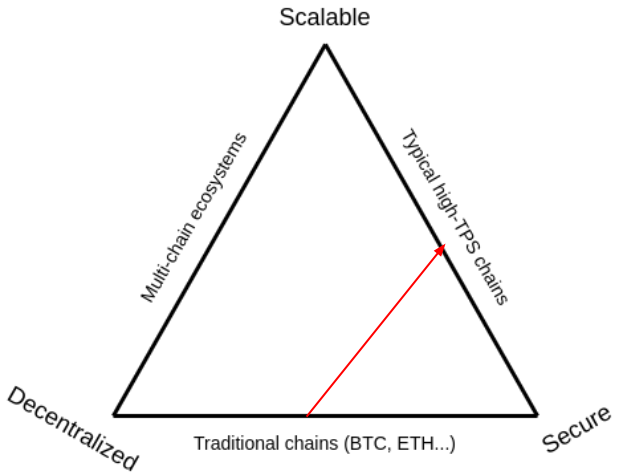
Solution 1- Roll up - Optimistic

- SO… we have one computer rather than the entire Ethereum network to handle transactions on roll ups
- What if that computer makes one mistake?
- Optimistic
  - We assume the computer doesn't make mistake
  - We have a small group of people watching the computer
  - They get rewarded if they catch a mistake
  - Then we fix the mistake



Solution 2- Roll up - Zero-knowledge

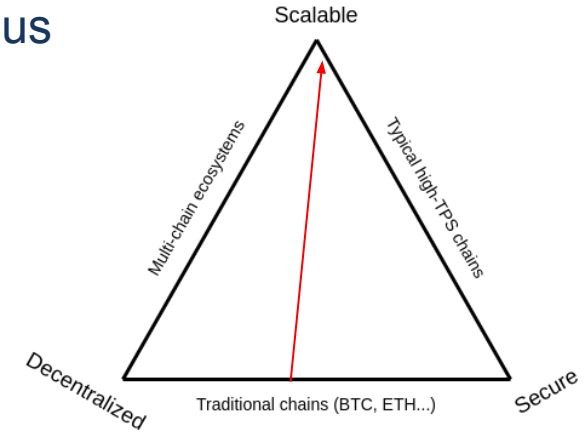
- What if that computer makes one mistake?
- ZK
  - For each batch of 100 tx, I submit a mathematical proof that I computed all 100 correctly. The proof is verified on Ethereum(-> so we know the verifying part won't have a mistake)
  - How? Super-duper complicated math
  - In fact, until recently, we can only batch "transfers" and not what Ethereum really needs - which is arbitrary computation.



Penn Engineering University of Pennsylvania
Wharton University of Pennsylvania

Solution 3 - Sidechain

- Let’s make a copy of Ethereum
- Except we use a less secure/ decentralized consensus
  - But it’s faster
  - Which way do we move on the trilemma?
- Last step, we connect this copy to Ethereum
- Now we have more TPS, and cheaper
  - Like 1000x + cheaper
  - And faster too



Problems

- Optimistic roll up
  - Centralized, potentially less secure
  - **What if a mistake is made?**
- ZK roll up
  - Centralized but not at the expense of security
  - **We don’t have the tech yet**
- Sidechain
  - Centralized, potentially less secure
  - **Basically a separate blockchain**

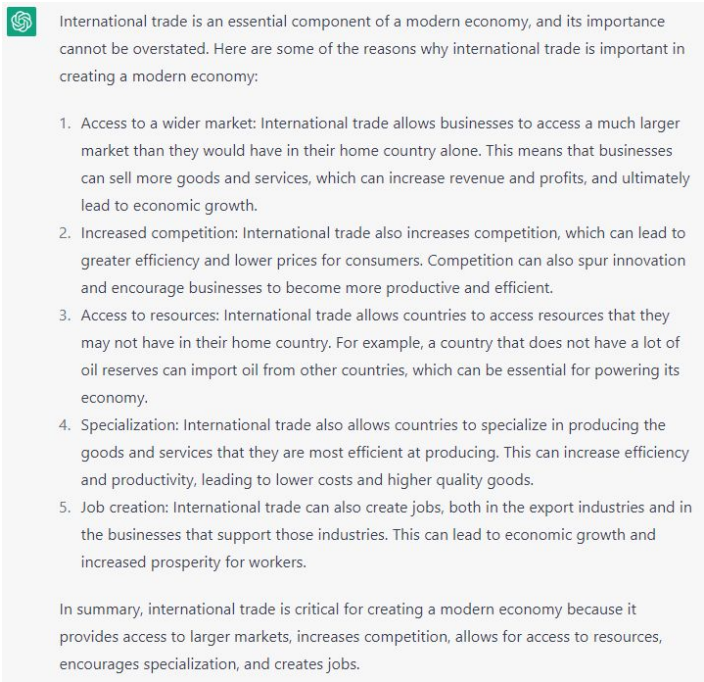
Industry directions

- Let’s just make a lot of sidechains
  - -> Cosmos
- We don’t actually care about decentralization and thus security
  - -> Optimistic roll-up services e.g. Constellation
- I have a novel consensus algorithm that solves all problems
  - -> Algorand
- ZK is the future
  - -> zkEVM e.g. Polygon, zkSync, Starknet, Scroll.
- …

Bridges

Imagine a world without airplanes and sea ships…

- A closed ecosystem within each continent
- Resources cannot flow freely between continents
- Inefficiencies everywhere
- International trade is important! (chatGPT agrees)



International trade is an essential component of a modern economy, and its importance cannot be overstated. Here are some of the reasons why international trade is important in creating a modern economy:

1. Access to a wider market: International trade allows businesses to access a much larger market than they would have in their home country alone. This means that businesses can sell more goods and services, which can increase revenue and profits, and ultimately lead to economic growth.
2. Increased competition: International trade also increases competition, which can lead to greater efficiency and lower prices for consumers. Competition can also spur innovation and encourage businesses to become more productive and efficient.
3. Access to resources: International trade allows countries to access resources that they may not have in their home country. For example, a country that does not have a lot of oil reserves can import oil from other countries, which can be essential for powering its economy.
4. Specialization: International trade also allows countries to specialize in producing the goods and services that they are most efficient at producing. This can increase efficiency and productivity, leading to lower costs and higher quality goods.
5. Job creation: International trade can also create jobs, both in the export industries and in the businesses that support those industries. This can lead to economic growth and increased prosperity for workers.

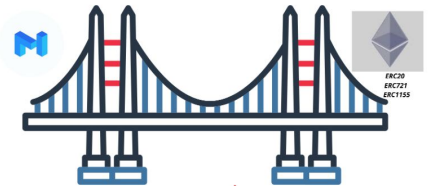
In summary, international trade is critical for creating a modern economy because it provides access to larger markets, increases competition, allows for access to resources, encourages specialization, and creates jobs.

Independent blockchains are like continents

Penn Engineering University of Pennsylvania

Wharton University of Pennsylvania

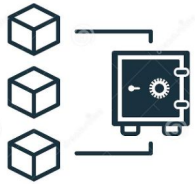
Cross-chain Bridges



- Oracle: entities that connect blockchains to external systems
  - thereby enabling smart contracts to execute based upon inputs and outputs from the real world
- Cross-chain Bridges enable interactions between separate blockchains
  - Transfer of value
  - Smart Contract calls
  - NFT ownership transfer across chains
- Oracles observe events on source and destination chains, and facilitates the cross-chain interaction between source and destination chains

Main Types of Bridges

Native Cross-chain Validation



Proof of Stake (PoS) / Multi Party Computation (MPC) Bridges

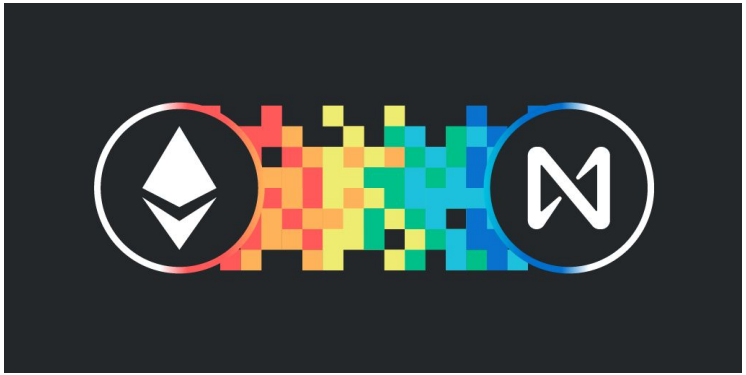
1:1 Bridges

Penn Engineering University of Pennsylvania

Wharton University of Pennsylvania

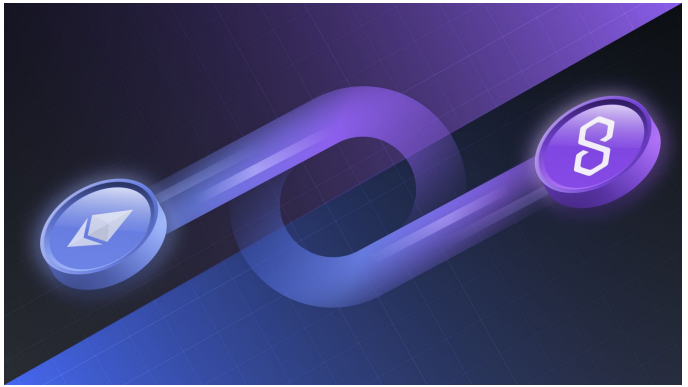
Native Cross-chain Validation

- Source and destination chains have protocols designed to integrate with each other
- Ex: Rollups, Near Rainbow Bridge
- Validate source chain data in destination chain natively
- Trust minimized
- Can have high cost of integration
- Can be slow for rollup exits



Proof of Stake / Multi Party Computation Bridges

- 3rd-party sets of validators act as oracle
- Ex: Polygon PoS Bridge, Thorchain
- Can either be centralized or decentralized
- Have to trust the 3rd-party validators, the larger and decentralized the validator set the safer
- Normally have lower cost
- Can either be fast or slow depending on how centralized the infrastructure is
- **Works on mostly any chain!**



1:1 Bridges

- A 2-party swap system facilitated by the demander and supplier of the token
- Tokens first get locked in escrows on both source and destination chains, then released at the same time
- Ex: Connext Bridge, Liquality
- Trust-minimized
- Low cost
- Requires liquidity pools on both source and destination chains
- Fast confirmation
- Works on mostly any chains
- **The net transfer of value across chain is near zero**

connext

Penn Engineering
University of Pennsylvania

Wharton
University of Pennsylvania

Do bridges work?

Mostly, but…

The aftermath of Axie Infinity's $650M Ronin Bridge hack

Since the hack of Axie Infinity's Ronin bridge, developers behind the game have raised $150 million to reimburse the affected users.

Wormhole token bridge loses $321M in largest hack so far in 2022

The token bridge between Ethereum and Solana saw 120,000 wETH tokens removed from the platform and distributed between the hacker's Solana and ETH wallets.

Nomad crypto bridge loses $200 million in 'chaotic' hack

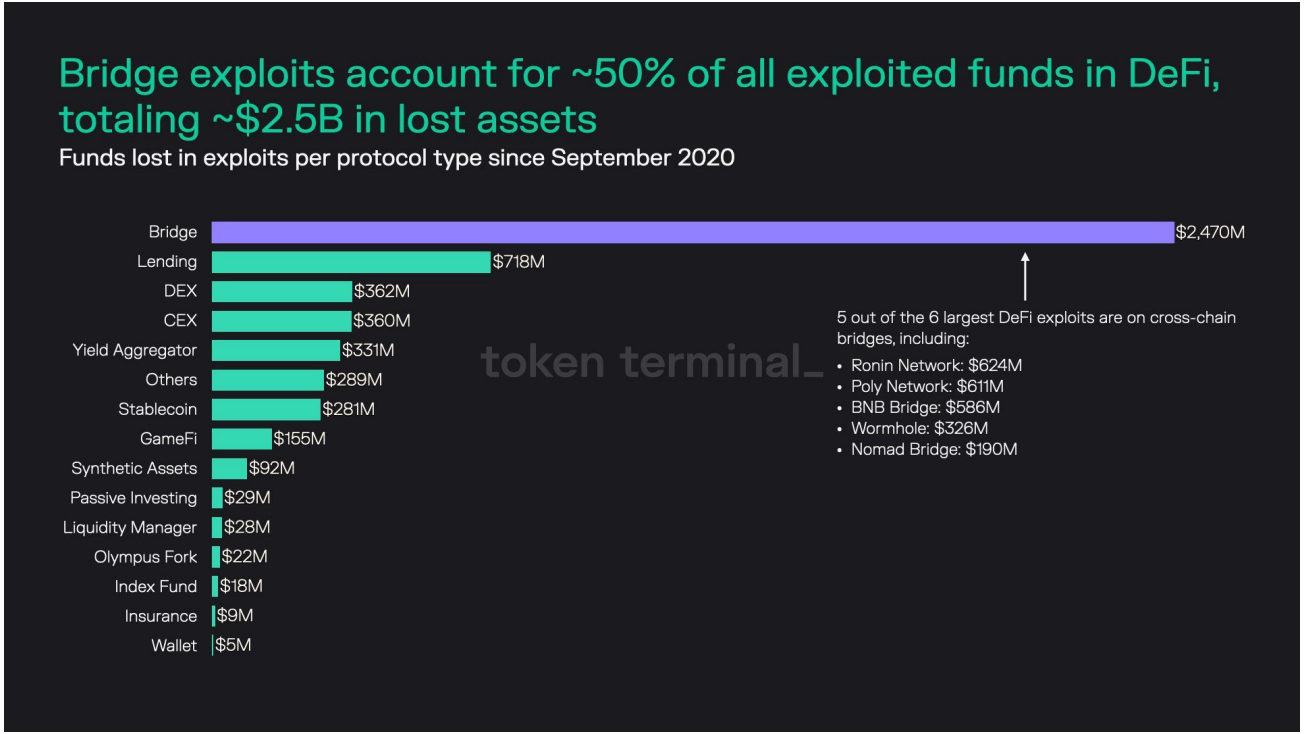
Binance hit by $100 million blockchain bridge hack

Carly Page @carlypage_ / 9:36 AM EDT • October 7, 2022

Comment

Penn Engineering University of Pennsylvania

Wharton University of Pennsylvania



Penn Engineering
University of Pennsylvania

Wharton
University of Pennsylvania

Challenges with designing a secure bridge system

- Needs to ensure all stakeholders have positive incentives in ensuring the security of the bridge
- **Canon** is a very intangible concept
- ***The Hard Fork Problem***
  - Validators are incentivized to collude together and authorize malicious transactions
  - Non-oracle nodes have no clue!
- Difficult to hold decentralized oracles accountable
- Needs good finality time, ease of use/implementation, strong assurance
- Program bugs lol