DeFi

AND THE

Future of Finance

Course IV:

DeFi Risks and Opportunities

3. Scaling Risk

(i) Alternative Consensus

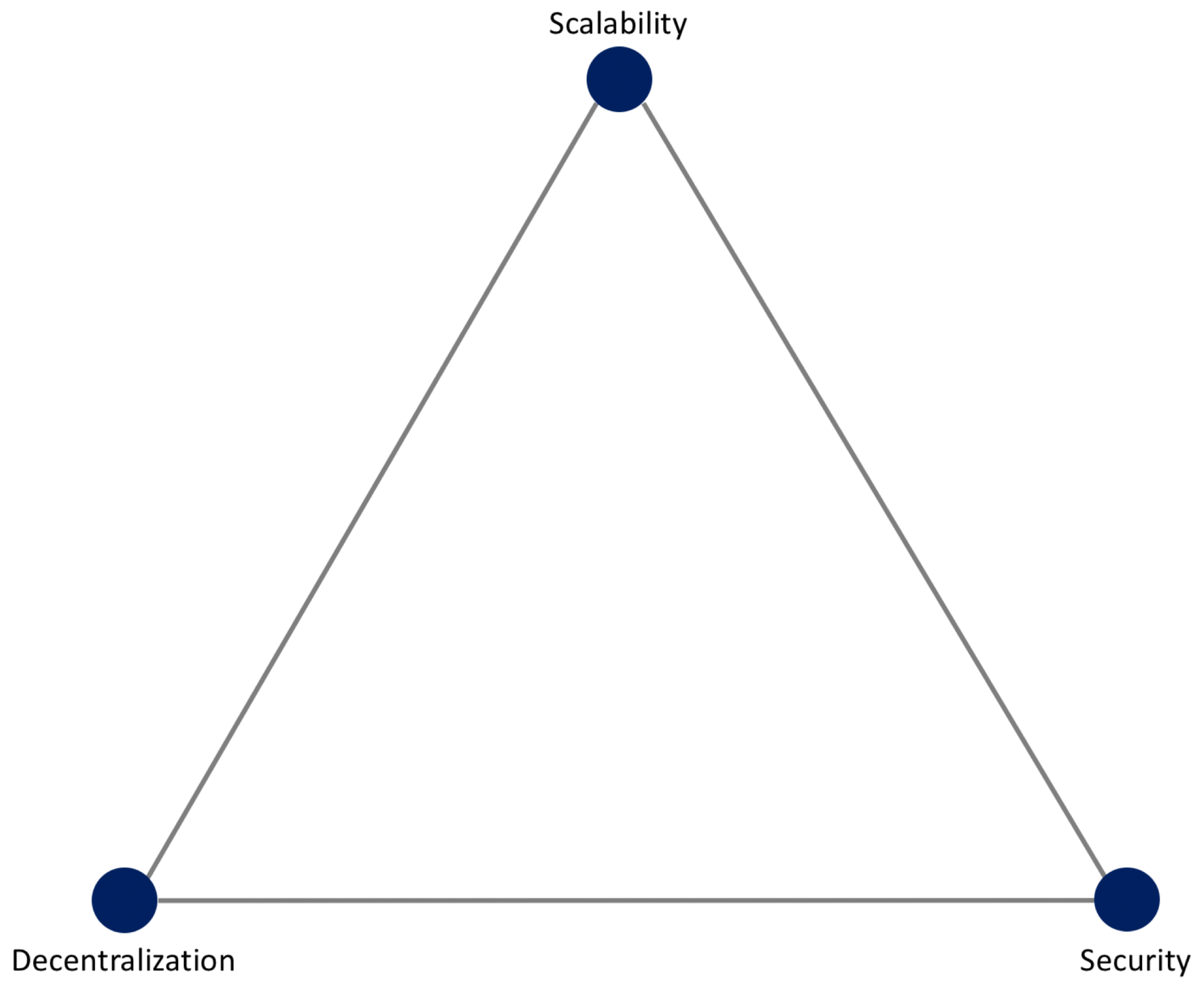
Risks: Scaling risk

Blockchain trilemma

- Vitalik Buterin introduced this term which refers to the key tradeoffs that developers need to consider when developing a blockchain
  - Decentralized (no central point of control)
  - Scalable (handle increasing number of transactions per second)
  - Secure (operate as expected and resilient to attacks)
- Tradeoffs refers to the inability to achieve all three. For example, more centralized blockchains are much more scalable

Risks: Scaling risk

Blockchain trilemma



Risks: Scaling risk

What is scaling risk?

- As we have discussed, Ethereum and other “Proof of Work” (the consensus mechanism) blockchains have a fixed block size.
- For a block to become part of the chain, every Ethereum miner must execute all of the included transactions on their machine.
- To expect each miner to process all of the financial transactions for a global financial market is unrealistic.

Risks: Scaling risk

What is scaling risk?

- Ethereum is currently limited to a maximum of 15 TPS.
- Yet, almost all of DeFi today resides on this blockchain.
- Compared to Visa, which can handle upward of 65,000 transactions per second, Ethereum is capable of handling less than 0.1% of the throughput.
- Ethereum's lack of scalability places DeFi at risk of being unable to meet requisite demand.

Risks: Scaling risk

What is scaling risk?

- Much effort is focused on increasing Ethereum’s scalability or replacing Ethereum with an alternative blockchain that can more readily handle higher transaction volumes.
- To date, all efforts have proven unsuccessful.

Risks: Scaling risk

Proof of Stake

- One actively pursued solution to the problem is a new consensus algorithm, *Proof of Stake*.
- Proof of Stake simply replaces mining of blocks (which requires a probabilistic wait time), with staking an asset on the next block, with majority rules similar to PoW.
- *Staking*, an important concept in cryptocurrencies and DeFi, means a user escrows funds in a smart contract and is subject to a penalty (*slashed funds*) if they deviate from expected behavior.

Risks: Scaling risk

Proof of Stake risks

- An example of malicious behavior includes voting for multiple candidate blocks.
- This action shows a lack of discernment and skews voting numbers, and thus is penalized.
- The security in PoS is based the idea that a malicious actor would have to amass more of the staked asset (ether in the case of Ethereum) than the entire rest of the stakers on that chain.
- This is infeasible in Ethereum and hence results in strong security properties similar to PoW.