Elements of DeFi

https://web3.princeton.edu/elements-of-defi/

Professor Pramod Viswanath

Princeton University

Lecture 13

DeFi Attack Vector Space

Last lecture: Flash loans

- Liquidity pools
  - Lending liquidity pools - Unused capital due to overcollateralization
  - Exchange liquidity pools – Locked collateral for margin traders (dydx) – (Check if AMMs also provide liquidity)
- Trust requirements
  - Replace borrower trust with trust on Ethereum (atomic transaction execution)
  - Replace with incentivized trust (margin trading)
- Flash loans
- Applications:
  - Flash loan arbitrage
  - Flash loan liquidation

This Lecture: Attack Space in DeFi

- Attacker can be attacked:
  - Sandwich
  - Poisoned sandwich
- Attacks can be done cheaply:
  - Flash loan attacks
  - Euler labs attack and the dangers of contagion
- Attacks can destabilize the trust platform:
  - Shorting attacks in PoS protocols: **dangers to consensus**
  - Lending vs Staking tradeoff in PoS protocols: danger even without byzantine agents

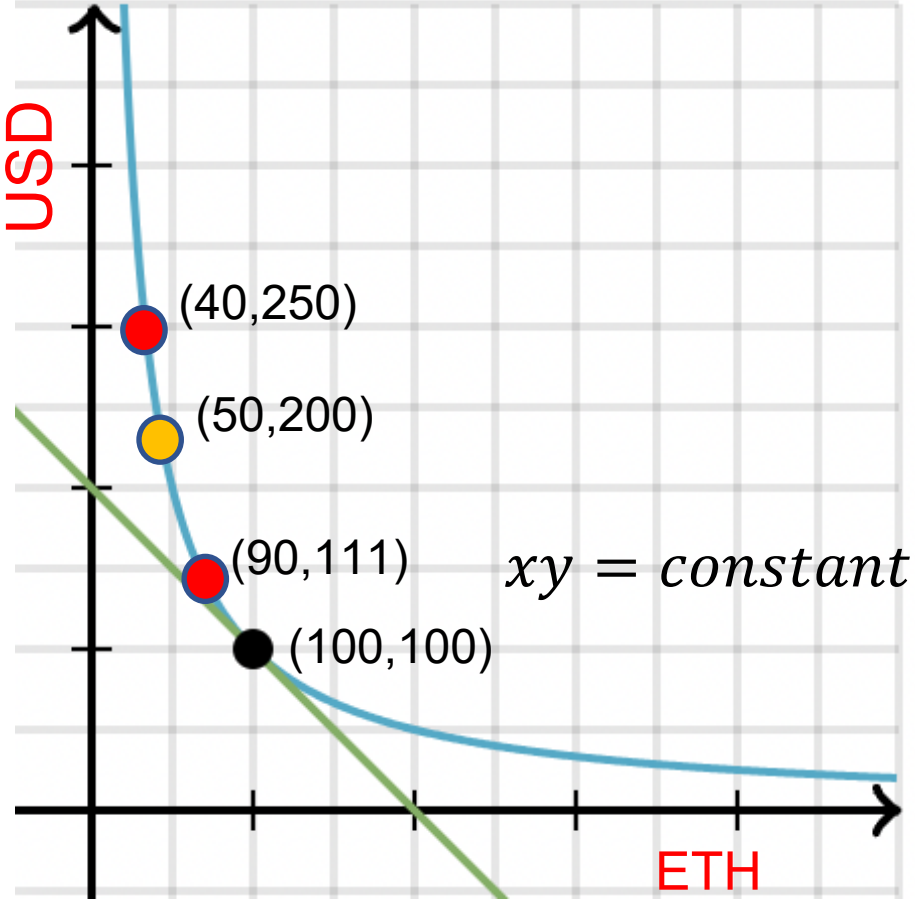
Theme 1: Attackers can be attacked

Recall: Sandwich attack

MEV : Sandwich Attack

- User wants to do a normal trade :
  - Buy 50 ETH, (has to pay 100 USD normally)

- If miner sees a large buy txn,
  - Introduce a buy txn just before it : buy 10 ETH
  - Put the txn
  - Introduce a sell txn just after it : sell 10 ETH
- Miner gets profit with no risk : 39 USD
- User gets a worse price : 139 USD



Poisoned sandwich attack

- If you know what sort of transactions are sandwiched by attackers, maybe you can bait them?
- MEV-bots take the bait in a token you created
- Add non-standard functions in your token implementation to steal the bots' profit
- Poisoned sandwich attack

There's always a BIGGER fish!

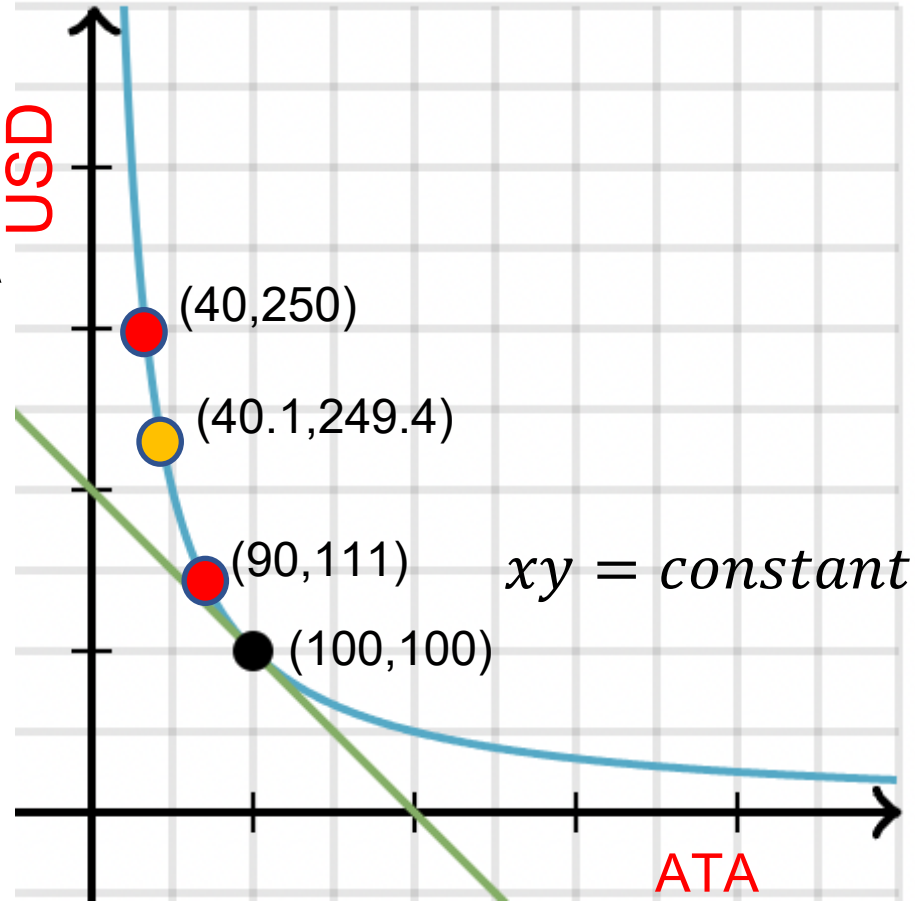
Poisoned sandwich attack

- Idea : create a pool of ATA/USD tokens, where ATA is your attack ERC-20 token

- Modify the “transfer” function of ATA to give only 10% of the transfer tokens to the recipient, rest to you
- Create a bunch of buy/sell ATA transactions
- MEV bots would try to sandwich them
- Because of the “poisoned” transfer, they end up leaving USD in the pool!

Poisoned sandwich attack: example

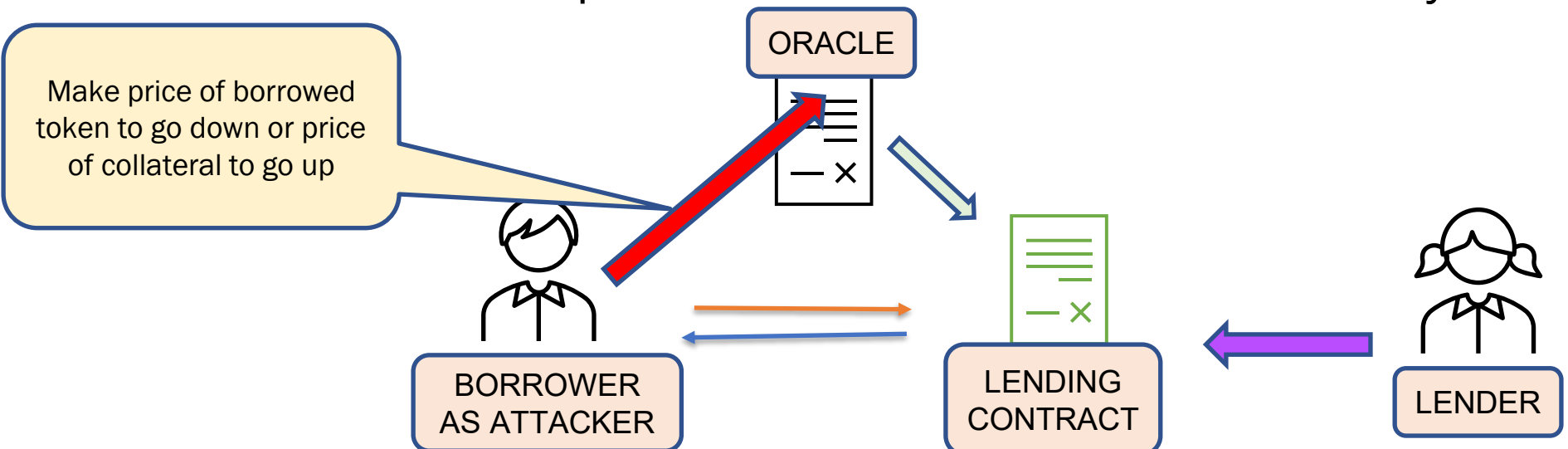
- Attacker puts normal trade :
  - Buy 50 ATA, (has to pay 100 USD normally) – but attacker is the LP itself
- If bot sees a large buy txn,
  - Introduces a buy txn just before it : buy 10 ATA
  - Puts the txn
  - Introduces a sell txn just after it : sell 1 ATA
- Bot suffers loss : ~ 10 USD
- Attacker gets a profit : ~ 10 USD
- https://github.com/Defi-Cartel/salmonella



Theme 2: Attacking is cheap

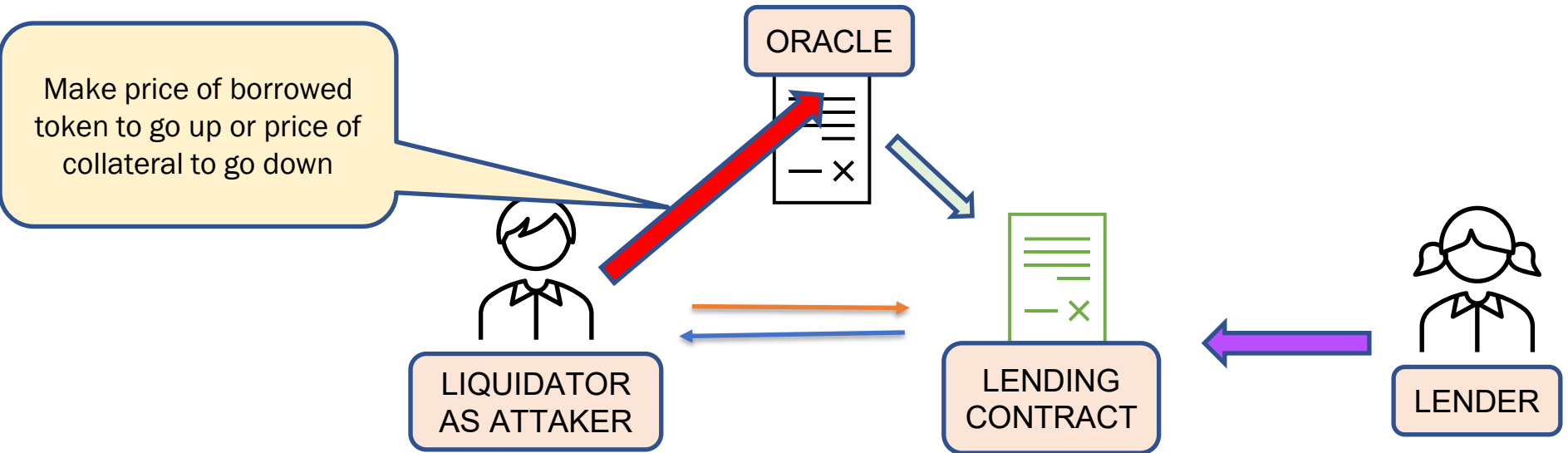
Flash loan attacks: overvalued collateral

- Flash loans can be used by malicious attackers to manipulate oracle prices
- We have already seen the bZx attack that
  - Used a flash loan to manipulate oracle prices by a lot
  - This caused a certain token to be extremely overvalued as collateral
  - Attacker deposits overvalued token and runs away with loan



Flash loan attacks: trigger liquidations

- Flash loans can be also used to trigger liquidations
- Here, the attacker does the following
  - Manipulate oracle price of a collateral to make it undervalued
  - This puts many lending position underwater
  - Liquidate all such positions and make a huge profit

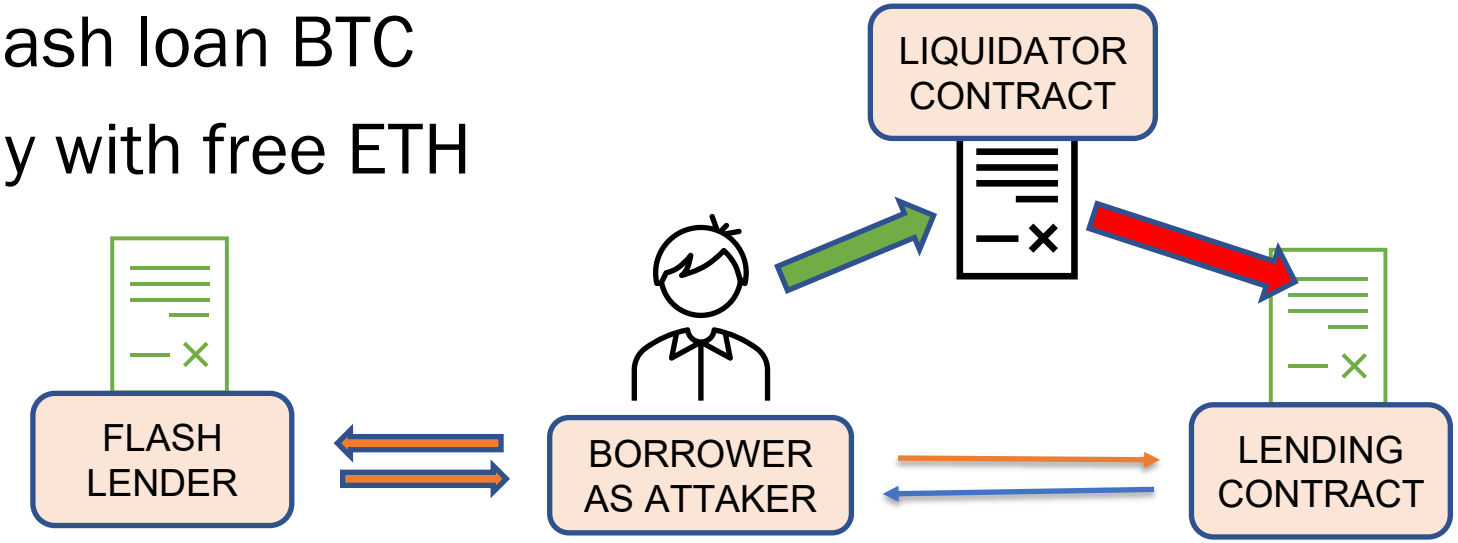


Euler Labs attack

- Mar 13, 2023
- Flash loan was used to exploit a bug in a lending protocol
- The bug allowed a borrower to effectively push their own positions underwater and hence liquidate themselves and obtain a large profit
- Normally, this is not allowed – you can only withdraw collateral up to the point where your health factor is 1

Euler Labs attack: toy version

- Use flash loan to post $150 in BTC, get $100 in ETH
- Use a buggy function to withdraw $60 BTC collateral – now $90 BTC backs $100 ETH – this would not be allowed normally
- Deploy and trigger the liquidator contract – get $90 BTC at a discount by posting just $80 ETH
- Return flash loan BTC
- Run away with free ETH



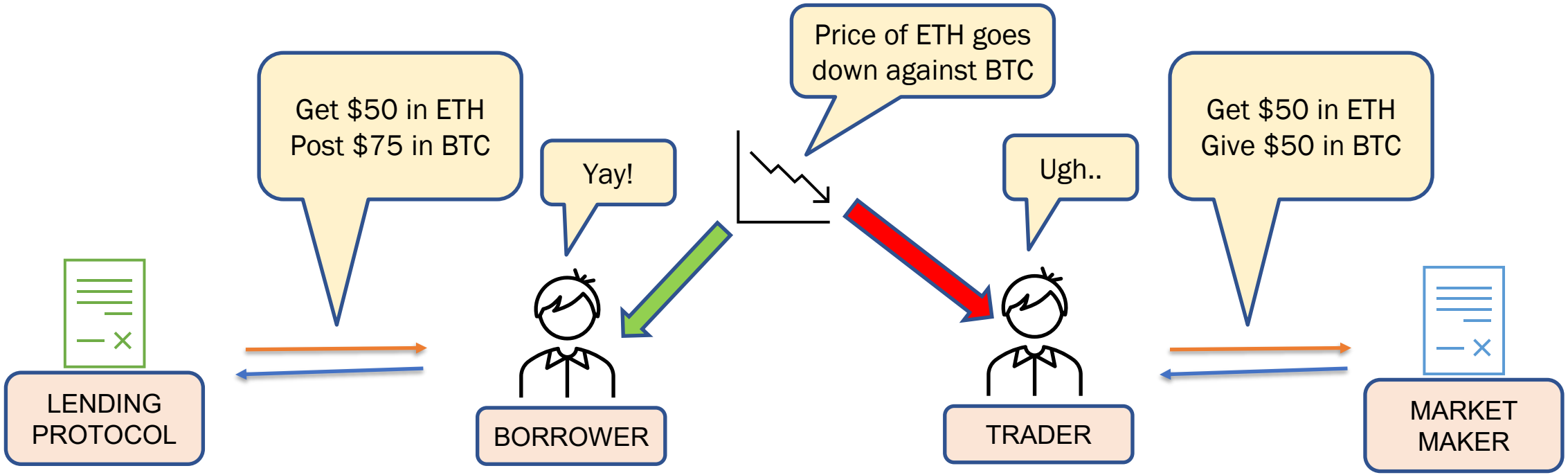
Euler Labs attack: contagion

- Around $200M stolen from Euler in various tokens: DAI, WBTC, stETH,
- More than 11 major DeFi protocols suffered additional losses of $40M
- E.g. Balancer, Yearn finance, Angle
- We see the downside of composability – contagion risk in DeFi
- Calls for better insurance provision and audits in DeFi

Theme 3: Dangers to consensus

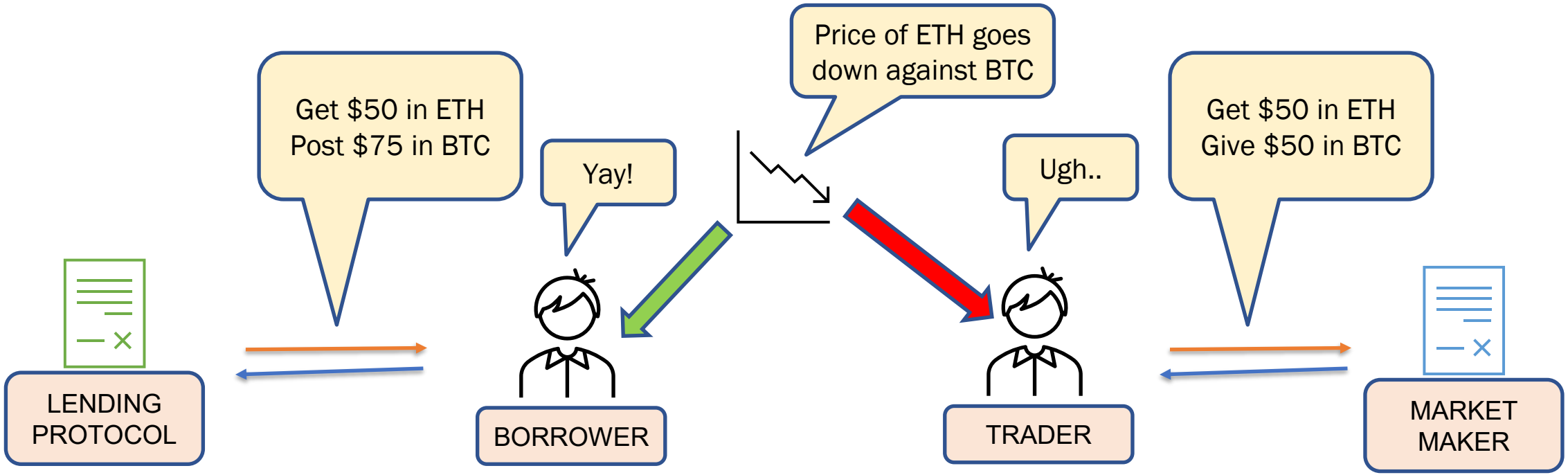
Borrowing vs Swapping

- Why borrow a token A by posting collateral token B when you can just swap A for B on AMM?
- Think about what happens when price of A goes down



Recall: Lending enables shorting

- Lending protocols enables traders to **short** tokens, do margin trading
- However, need to make sure expected cost incurred from interest rate and posting collateral < expected profit from price falling

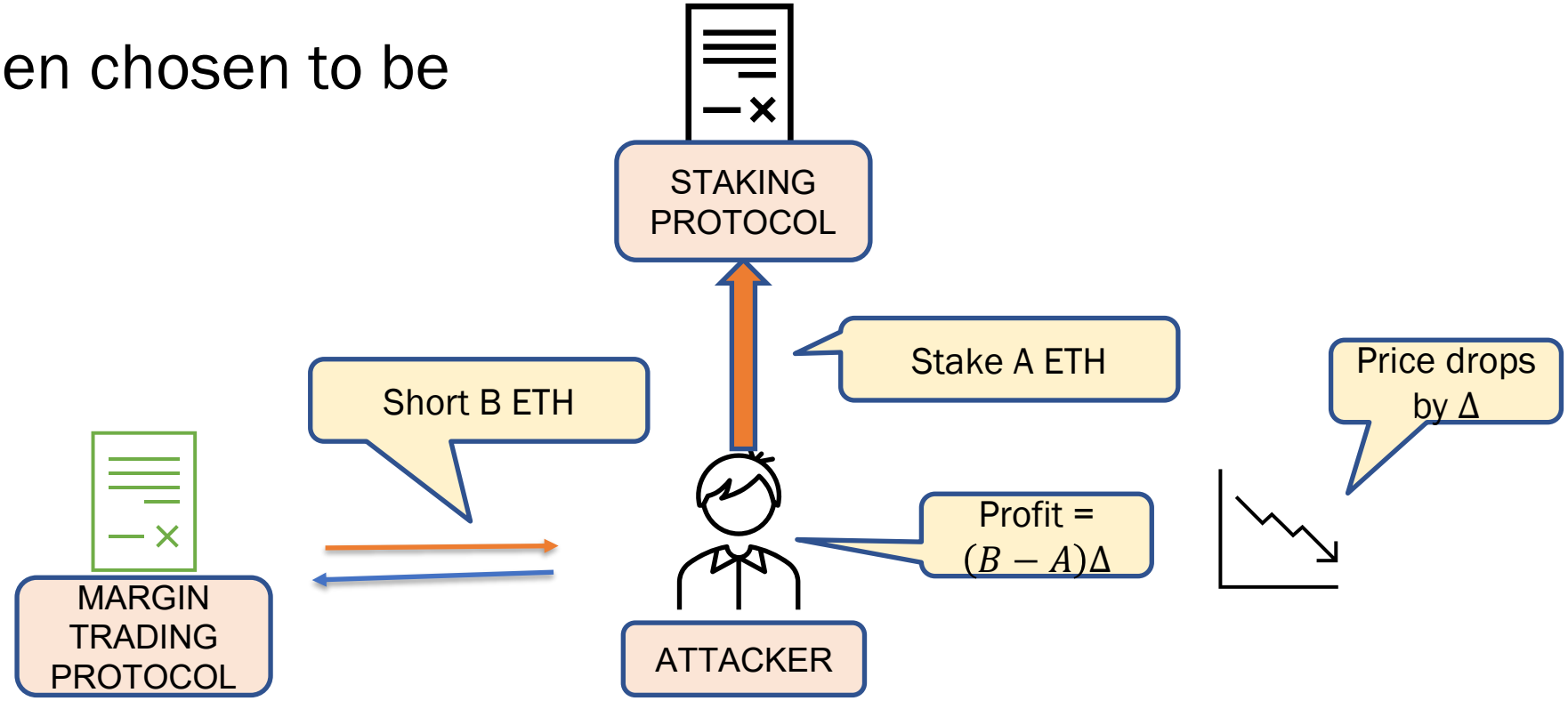


Shorting Attack on PoS

- PoS protocol – Proof-of-stake implies that a miner or block proposer is chosen with probability proportional to stake
- Usually, if a staker chooses to attack the protocol, the token loses value and is bad for the staker
- But, what if staker benefits from token losing value?
- i.e. Staker shorts the token

Shorting Attack on PoS

- Stake the token
- Short the token
- Attack when chosen to be proposer



Shorting Attack on PoS

Exchange	Volume ($)	Derivatives	Margin Trading
BitMex	886,007,632	✓	up to 100x
Bybit	716,387,848	✓	up to 100x
Coinfloor	347,269,026		up to 100x
PrimeXBT	90,115,864	✓	up to 100x
Kraken	33,180,001		up to 5x
HitBTC	14,066,926		up to 3x
Poloniex	9,940,037		up to 100x
bitFlyer	9,141,821	✓	up to 100x
BitMax	5,233,272	✓	up to 10x
Bibox	2,225,506		up to 50x
OKCoin	634,708	✓	up to 100x

Large amounts can be shorted via margin trading

The shorting attack is usually prevented by "slashing"
Rest of the validators agree on the attacker address and penalize it

Fall in prices because of an attempt at 51% attack

Coin	P_{MAX} date/price(USD)	P_{DAM} date/price(USD)	Δ
ETH	June 17 2016 13:19:22 21.49	June 16 2016 13:19:22 14.29	34%
ETC	Jan 07 2019 09:04:03 5.50	Jan 08 2019 13:19:22 4.92	11%
BTG	May 24 2018 14:34:17 47.62	May 25 2018 14:34:17 47.18	1%
VTC	Dec 06 2018 14:49:00 0.316917	Dec 07 2018 14:49:00 0.238420	25%
XVG	April 04 2018 04:34:04 0.075580	April 05 2018 04:34:04 0.059703	21%

Lending vs Staking

- Staking is incentivized by a stake reward that goes to validators and proposer
- However, the same staked token (e.g. ETH) can also be lent out by financial protocols built on top of the blockchain (e.g. Aave, Compound)
- Validator needs to decide whether to stake or lend
- What if validators simply choose the one with the higher yield?

Lending vs Staking: model

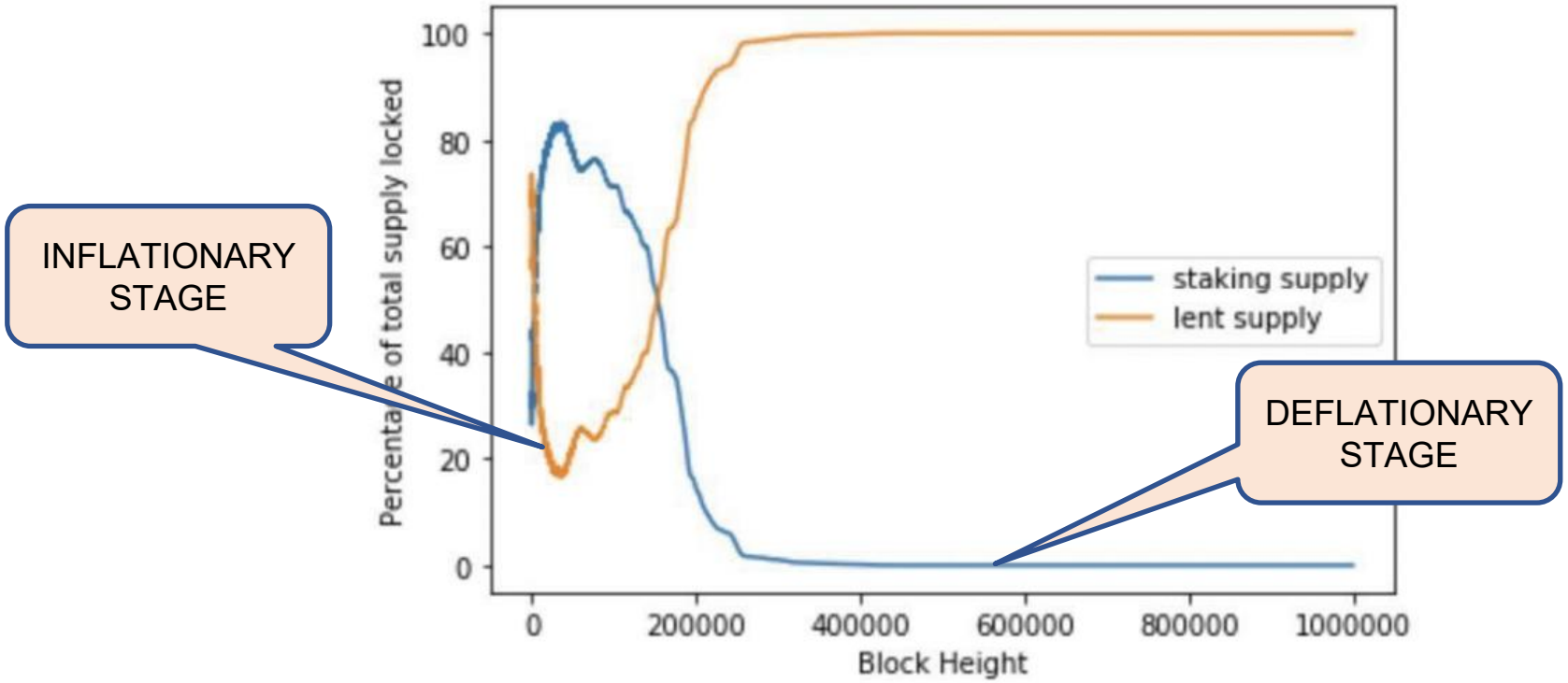
- Assume lending yields react to borrow/lend demand –
  - When borrowing increases, rates go up
  - When lending increases, rates go down

- Assume different schedules for block rewards (staking rewards)
  - Constant or decreasing supply (gas fees burnt, no block reward) - deflation
  - Linear increase in supply (constant block reward)
  - Exponential increase in supply (constant relative reward) – inflation

- Assume each agent chooses better yielding action (lending vs staking)

Lending vs Staking

- As the lending ecosystem around the staked token evolves, they will end up cannibalizing the staked token supply
- Less amount of token staked makes protocol easier to attack



Lending vs Staking

- Monetary policy is critical to solving this tradeoff
- New tokens minted after each block and given to the validators should be inflationary enough to deter too much lending
- At the same time, not so inflationary that token loses value and is volatile
- Open Questions:
  - Automate monetary policy to minimize instability?
  - Decentralized monetary policy?

Conclusion

- DeFi offers

atomicity, composability, programmability, permission-less access

- The same features also increase the attack surface