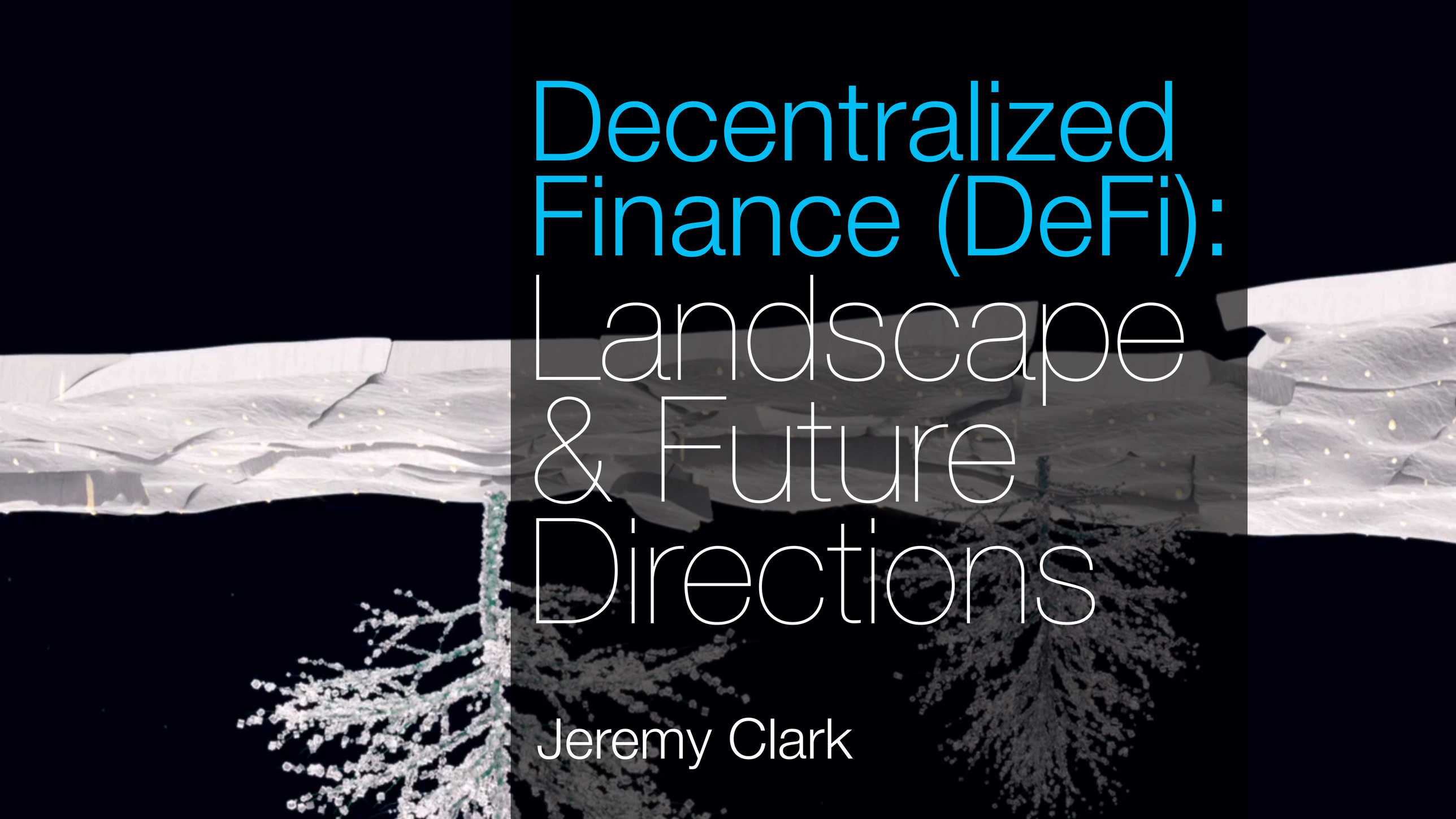


Decentralized Finance (DeFi): Landscape & Future Directions

Jeremy Clark

Jeremy Clark

- Associate Professor at the Concordia Institute for Information Systems Engineering (CIISE) in Montreal
- NSERC / Raymond Chabot Grant Thornton / Catallaxy Industry Research Chair in Blockchain Technologies
- PhD from the University of Waterloo (2009)
- Team of ~10 graduate students
- Numerous academic papers on Bitcoin/Blockchain
- Contributed to courses (Concordia, Princeton, MIT) & textbook on Bitcoin/blockchain
- Testified to Senate and House committees on Bitcoin/blockchain

MADIBA security research group

UNIVERSITÉ Concordia UNIVERSITY

GINA CODY SCHOOL OF ENGINEERING AND COMPUTER SCIENCE

Funding & Partners:

Raymond Chabot Grant Thornton

catallaxy

AUTORITÉ DES MARCHÉS FINANCIERS

Fonds de recherche Nature et technologies Québec

Office of the Privacy Commissioner of Canada

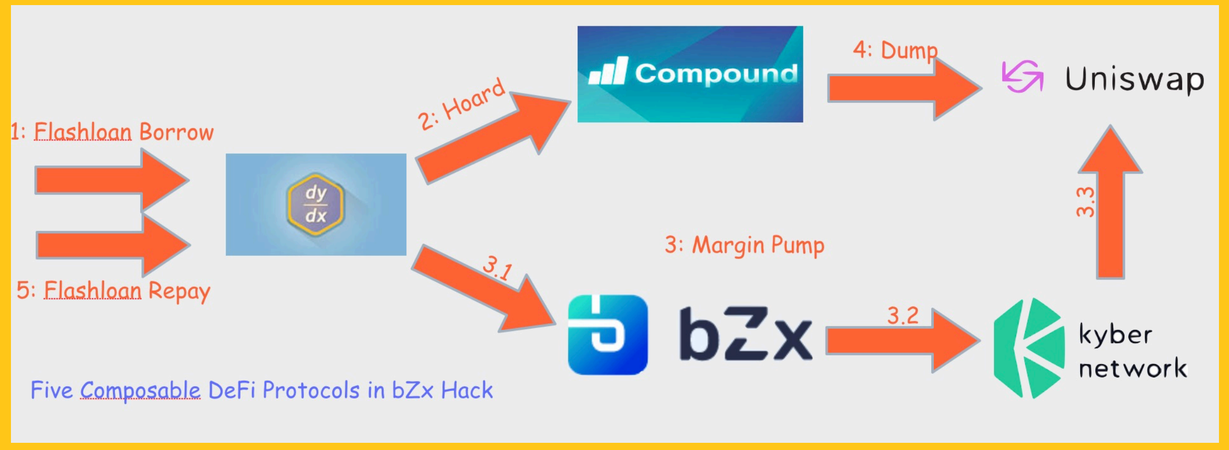
- You code your financial service and push it to a public blockchain like Ethereum
- The Ethereum's global network of servers runs your code for you
- While it is slow and can only run (relatively) simple code, it will run exactly as coded

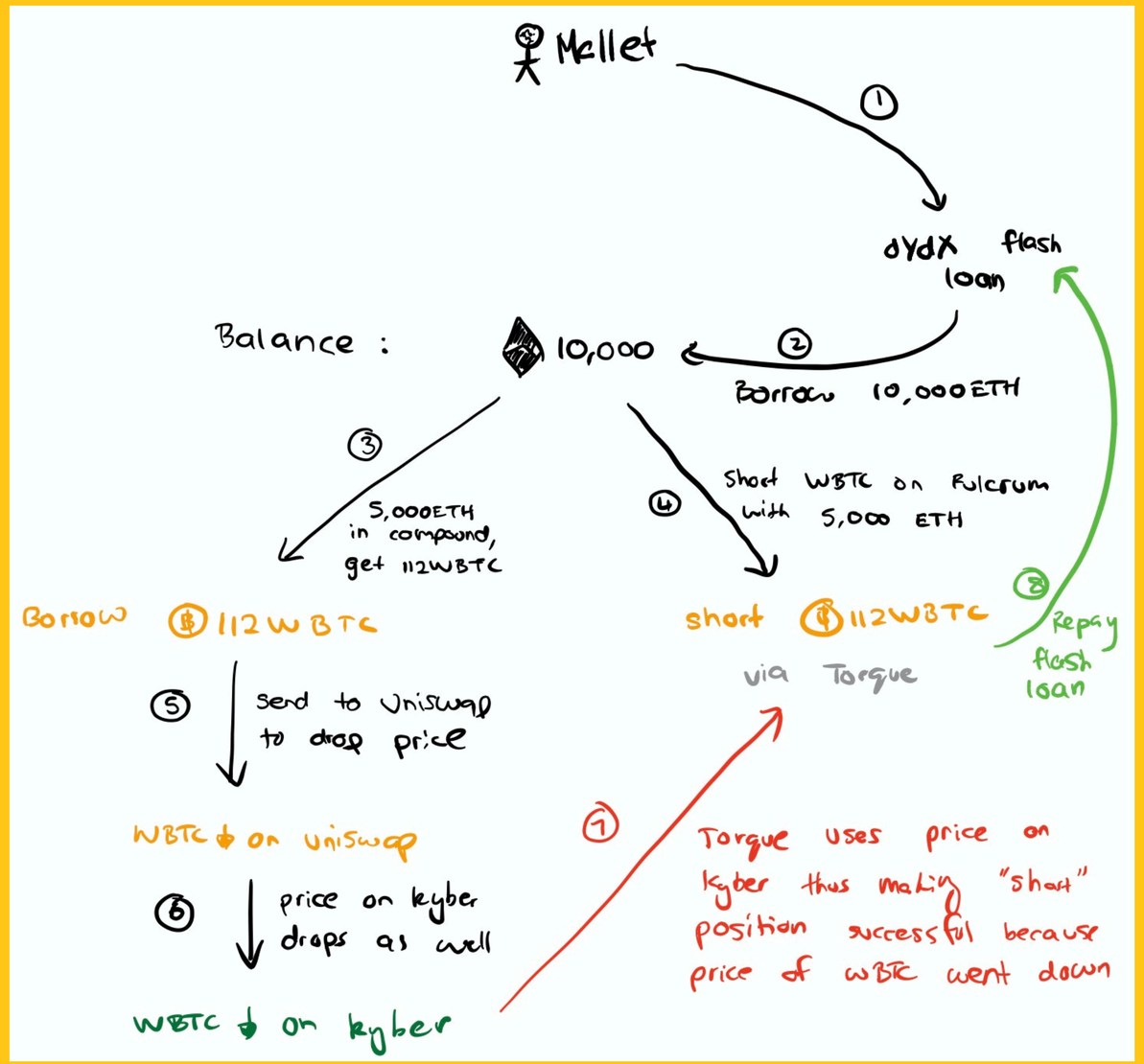
- In 2020, decentralized finance (DeFI) services hold $10B USD on Ethereum

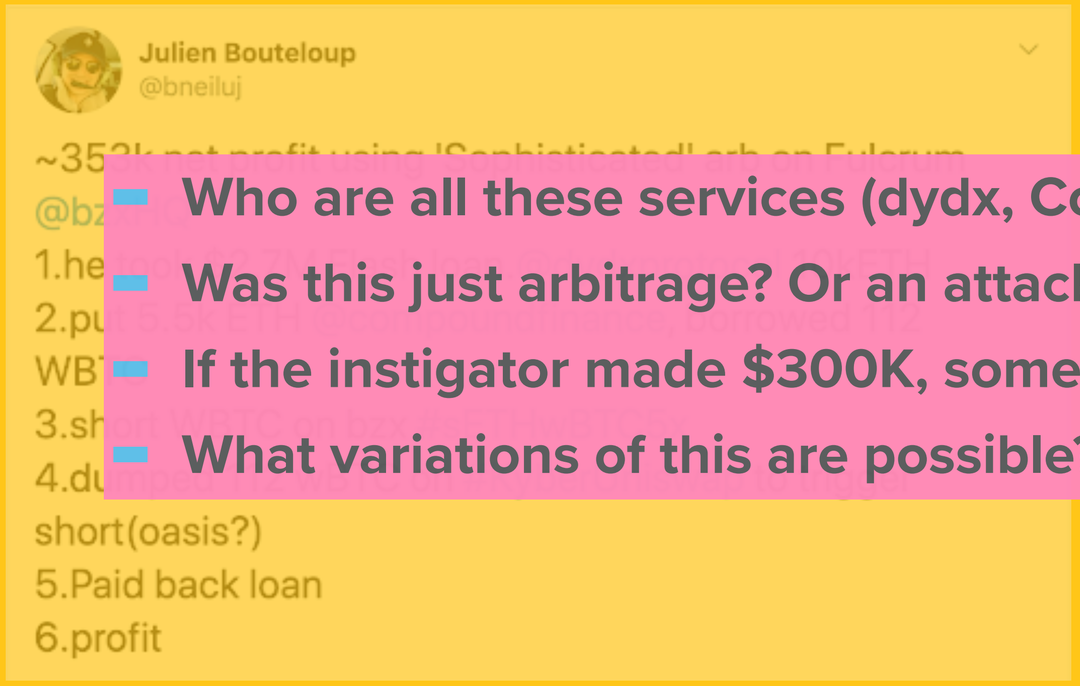
FEB 2020

Julien Bouteloup
@bneiluj

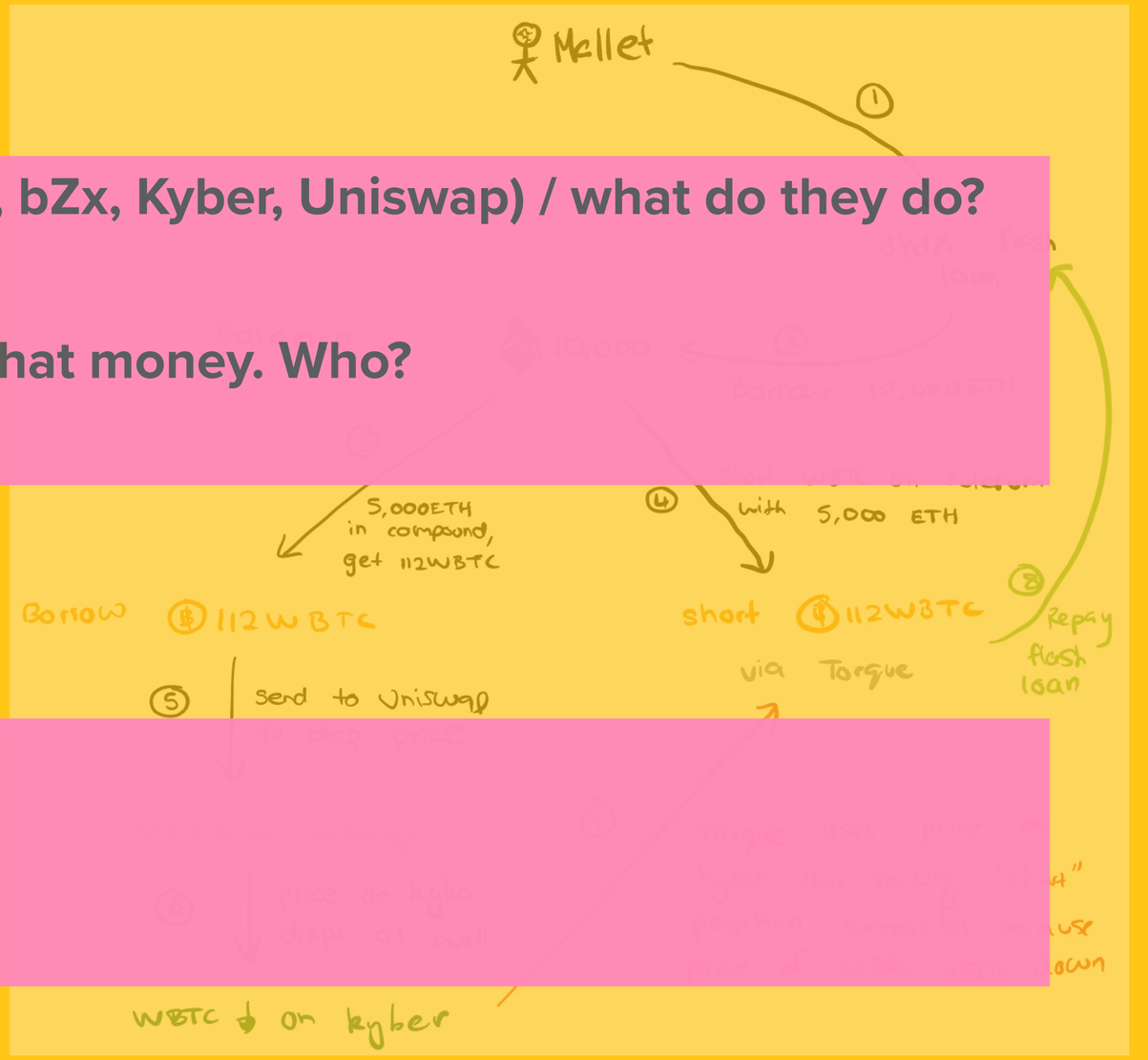
~353k net profit using 'Sophisticated' arb on Fulcrum @bzxHQ
1.he took $2.7M Flash loan.@dydxprotocol 10kETH
2.put 5.5k ETH @compoundfinance, borrowed 112 WBTC
3.short WBTC on bzx #sETHwBTC5x
4.dumped 112 wBTC on #KyberUniswap to trigger short(oasis?)
5.Paid back loan
6.profit



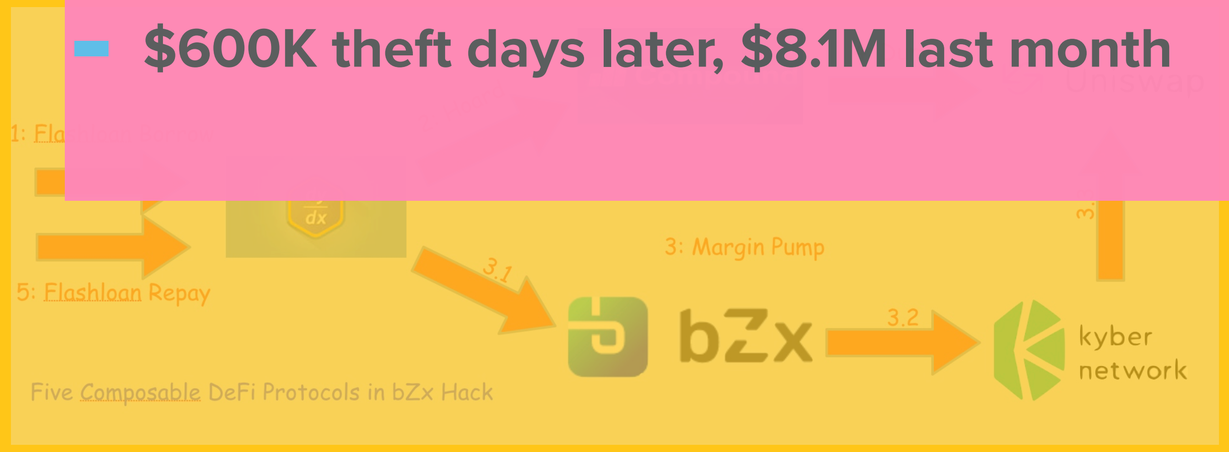




- Who are all these services (dydx, Compound, bZx, Kyber, Uniswap) / what do they do?
- Was this just arbitrage? Or an attack?
- If the instigator made $300K, someone lost that money. Who?
- What variations of this are possible?



- $300K is (relatively) small
- $600K theft days later, $8.1M last month



STABLECOINS

- Cryptocurrencies like ETH (Ether) and BTC (Bitcoin)
- Stablecoins like USDT

- Cryptocurrencies like ETH (Ether) and BTC (Bitcoin)
- Stablecoins like USDT

- Article in Communications of the ACM

BY JEREMY CLARK, DIDEM DEMIRAG, AND SEYEDEHMAHSA MOOSAVI

Demystifying Stablecoins

THE FIRST WAVE of cryptocurrencies, starting in the 1980s, attempted to digitize government-issued currency (or *fiat currency*, as cryptocurrency enthusiasts say).[8] The second wave, represented prominently by Bitcoin,[7] provide their own separate currency—issued and operated independently of any existing currencies, governments, or financial institutions. Bitcoin's currency (BTC) is issued in fixed quantities according to a hard-coded schedule in the protocol.

In the words of Bitcoin's pseudonymous inventor: *"There is nobody to act as a central bank... to adjust the money supply... that would have required a trusted party to determine the value because I don't know a way for software to know the real world value of things. If there was some clever way, or if we wanted to trust someone to actively manage the money supply to peg it to something, the rules could have been programmed for that. In this sense, it's more typical of a precious metal. Instead the supply changing to keep the value, the supply is predetermined*

Without active management, the exchange rate of BTC with governmental currencies has been marked by extreme volatility. Figure 1 shows a comparison of fiat currencies and bitcoin. The values were retrieved daily between Jan. 1, 2016 and Jan. 1, 2019. (Note that 1,000 mBTC = 1 BTC). Squint at the chart to notice how the GBP (British pound) drops around June 2016: This mild-looking pinch is actually the so-called "sharp decline" and "severe swing" that followed the Brexit referendum in the U.K. It is completely overshadowed, however, when pl
beside BTC's large fluc

ETHEREUM LENDING

- First type of loan
  - Bob borrows 80 ETH because he has a good reputation / credit rating / income / etc
-

- First type of loan
  - Bob borrows 80 ETH because he has a good reputation / credit rating / income / etc

- Does not exist on Ethereum

- Second type of loan
  - Alice deposits 100 ETH into a “decentralized bank” to earn interest
  - Bob wants to borrow 80 ETH from the bank (80 ETH = $30K)

- Second type of loan
  - Alice deposits 100 ETH into a “decentralized bank” to earn interest
  - Bob wants to borrow 80 ETH from the bank (80 ETH = $30K)

  - Bob deposits $40K in BTC
  - Bob repays with interest, which is partially passed onto Alice
  - Any credit event: the bank sells his $40K collateral to repay the loan

- Bank is autonomous. It is just code.

- Third type of loan

- Flash loan
- Not possible in the real world!

- Third type of loan

- Flash loan
- Not possible in the real world!

```
{

  TRANSACTION:

    RUN FUNCTION 1
    RUN FUNCTION 2
    RUN FUNCTION 3
    RUN FUNCTION 4

}
```

- Third type of loan

- Flash loan
- Not possible in the real world!

```
{

  TRANSACTION:

    RUN FUNCTION 1
    RUN FUNCTION 2
    RUN FUNCTION 3 => FAILS
    RUN FUNCTION 4

}
```

- Third type of loan

- Flash loan
- Not possible in the real world!

```
{

  TRANSACTION:

    RUN FUNCTION 1
    RUN FUNCTION 2
    RUN FUNCTION 3 => FAILS
    RUN FUNCTION 4

}
```

```
SKIP: 1, 2, 4
```

- Third type of loan

- Flash loan
- Not possible in the real world!

```
{

  TRANSACTION:

    RUN FUNCTION 1
    RUN FUNCTION 2
    RUN FUNCTION 3 => FAILS
    RUN FUNCTION 4

}
```

```
SKIP: 1, 2, 4
ABORT: 1, 2
```

- Third type of loan

- Flash loan
- Not possible in the real world!

```
{

  TRANSACTION:

    RUN FUNCTION 1
    RUN FUNCTION 2
    RUN FUNCTION 3 => FAILS
    RUN FUNCTION 4

}
```

```
SKIP: 1, 2, 4
ABORT: 1, 2
REVERT: NONE
```

- Third type of loan

- Flash loan
- Not possible in the real world!

- One transaction at a time

```
{

  TRANSACTION:

    RUN FUNCTION 1
    RUN FUNCTION 2
    RUN FUNCTION 3 => FAILS
    RUN FUNCTION 4

}
```

```
SKIP: 1, 2, 4
ABORT: 1, 2
REVERT: NONE
```

- Third type of loan

- Flash loan
- Not possible in the real world!

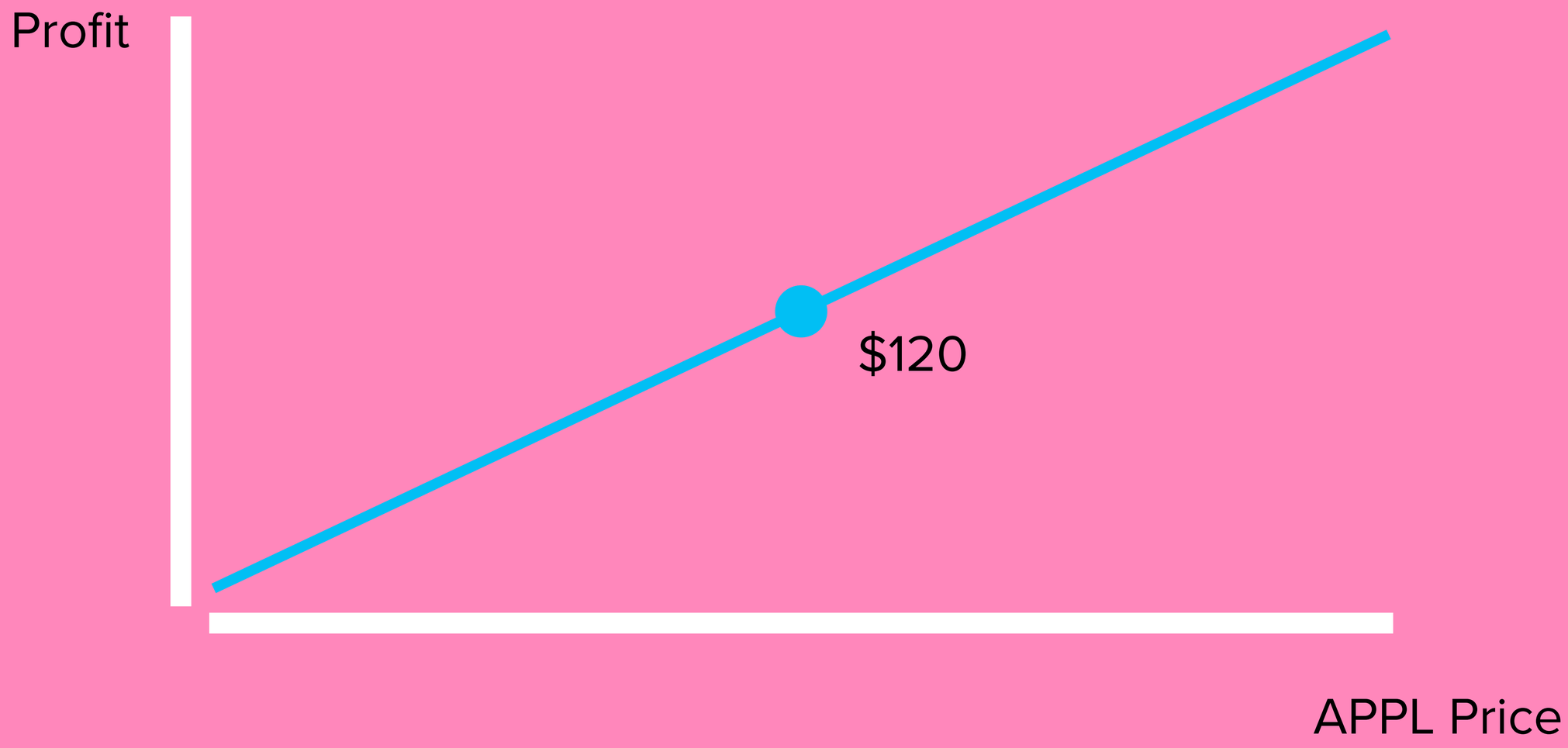
- One transaction at a time

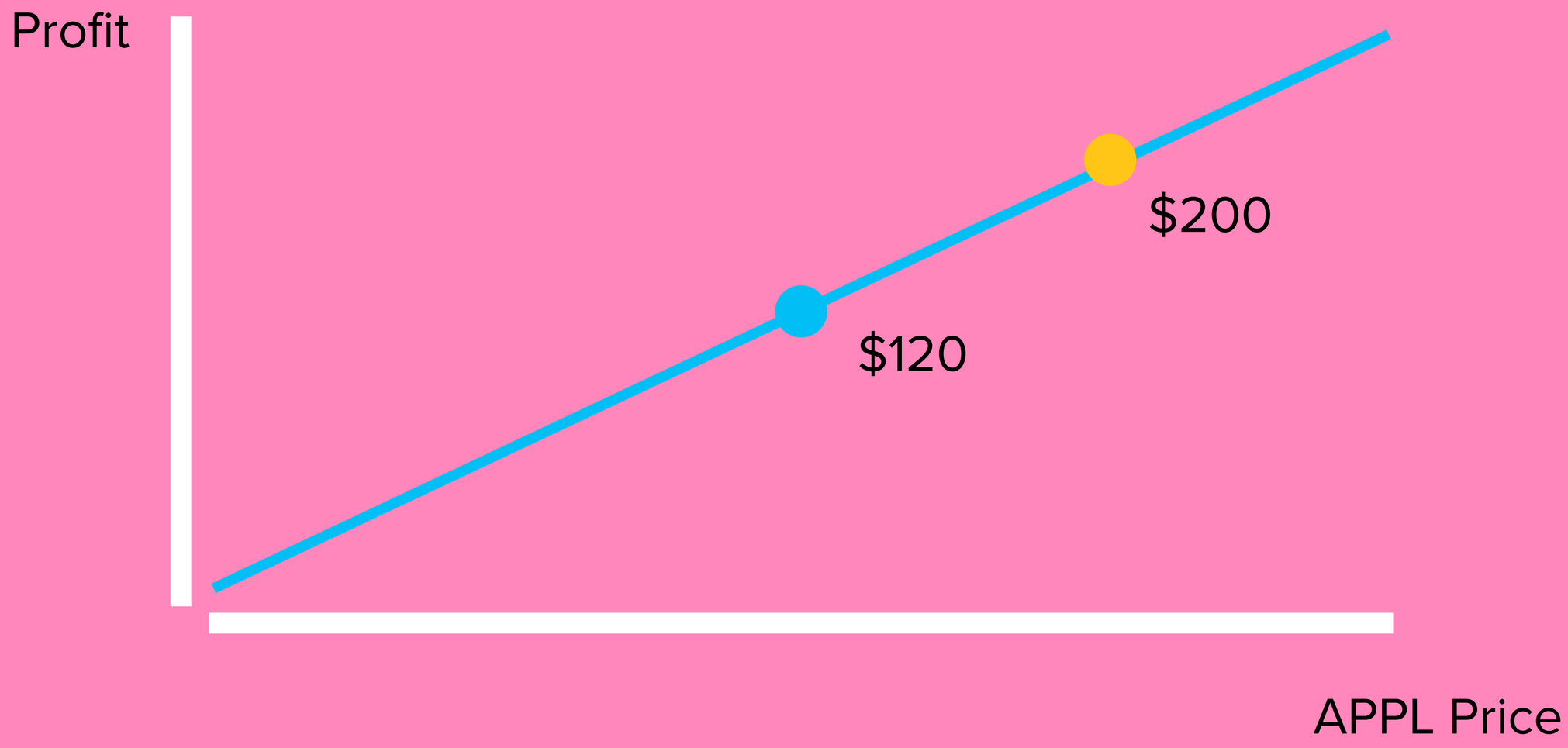
```
{

  TRANSACTION:

    BORROW XXX ETH
    DO WHATEVER YOU WANT
    REPAY XXX ETH
    REPAY COMPLETE? => REVERT IF FAIL

}
```

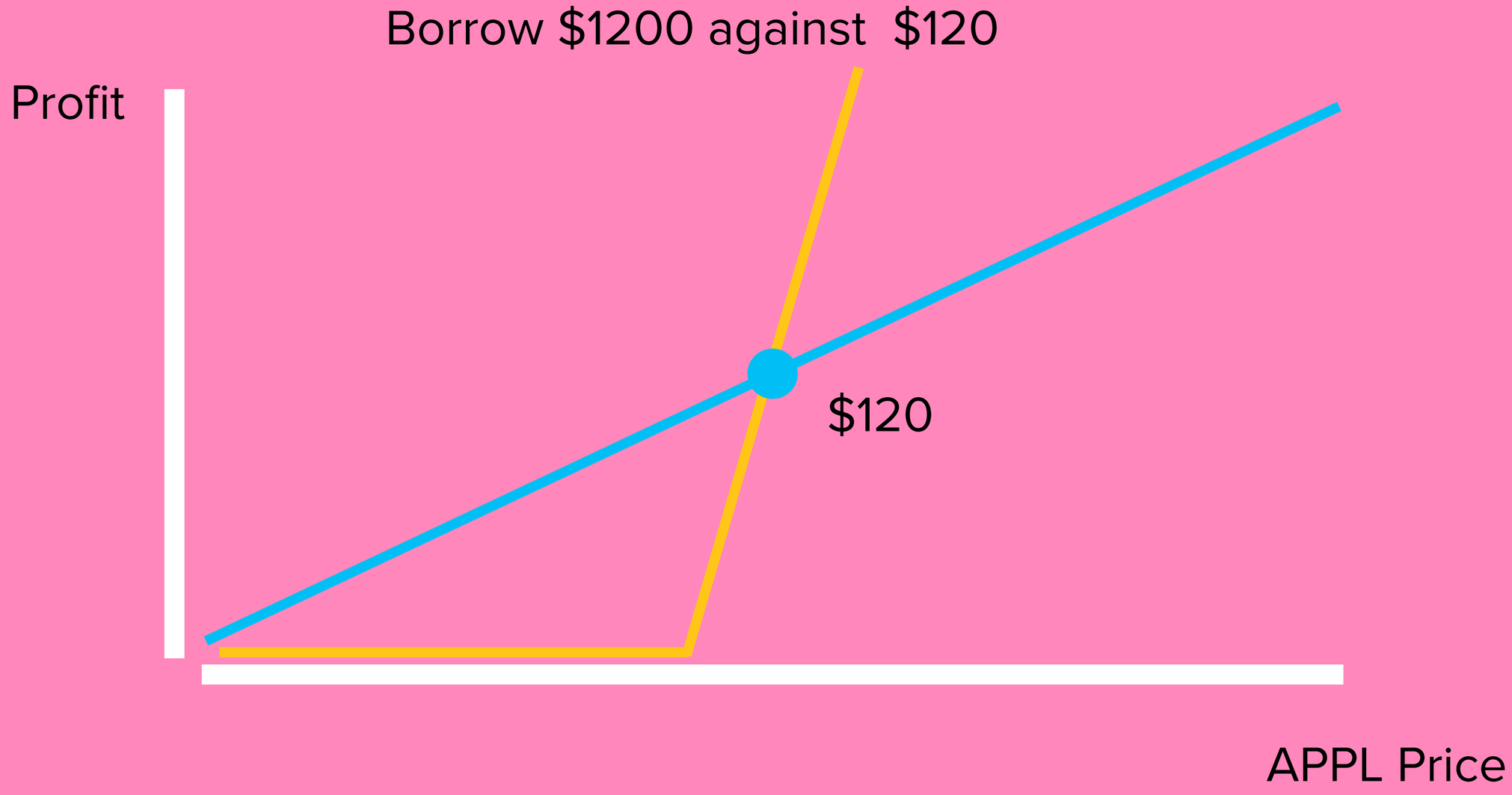
- Third type of loan
- Flash loan
- Not possible in the real world!
- One transaction at a time
- No risk, no collateral, anonymous, borrow maximum amount available (no one can use it while your transaction is running)

```
{

  TRANSACTION:

    BORROW XXX ETH
    DO WHATEVER YOU WANT
    REPAY XXX ETH
    REPAY COMPLETE? => REVERT IF FAIL

}
```

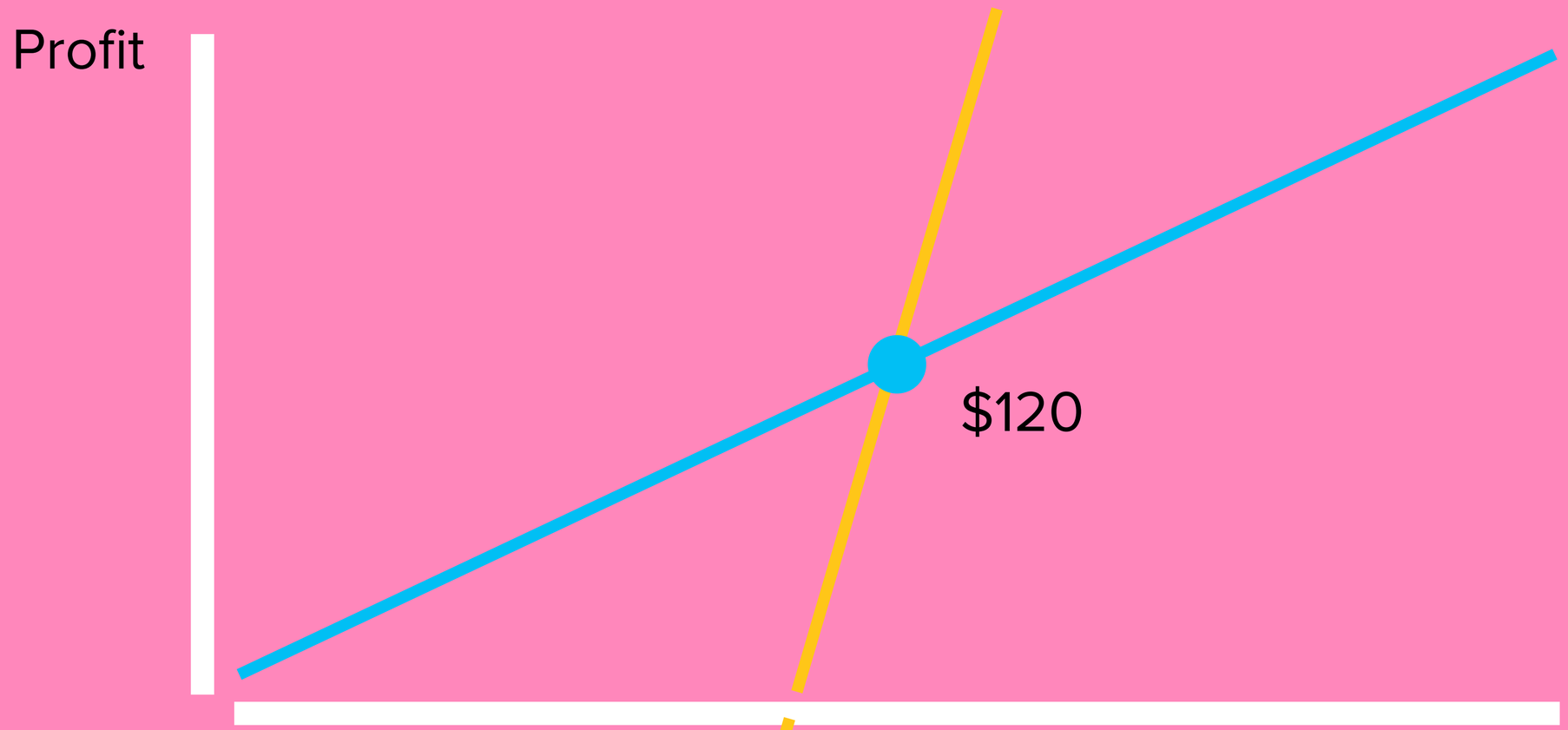
MARGIN LENDING


Profit
$120
APPL Price


Profit
$200
$120
APPL Price


Borrow $1200 against $120
Profit
$120
APPL Price

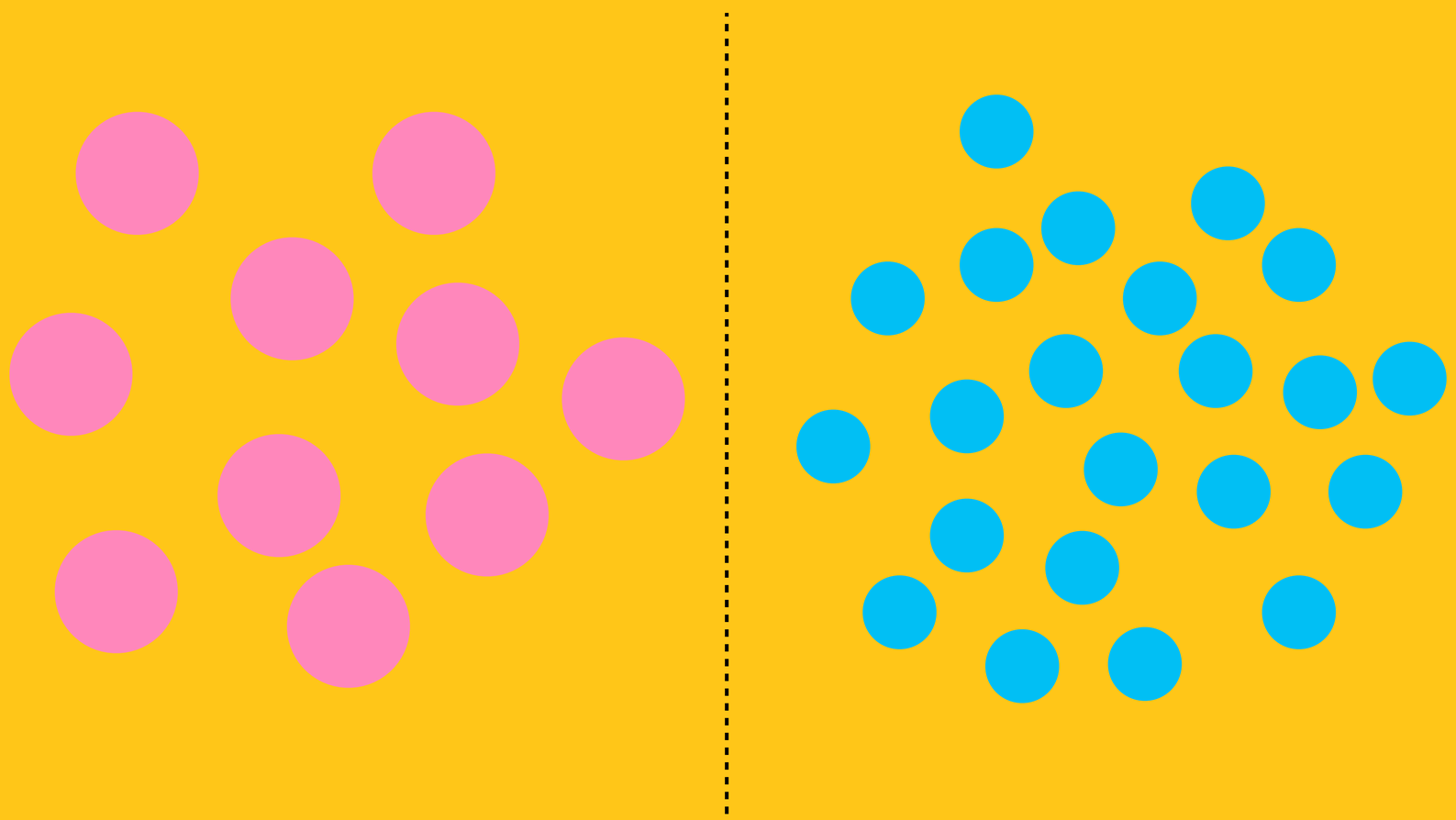
Borrow $1200 against $120

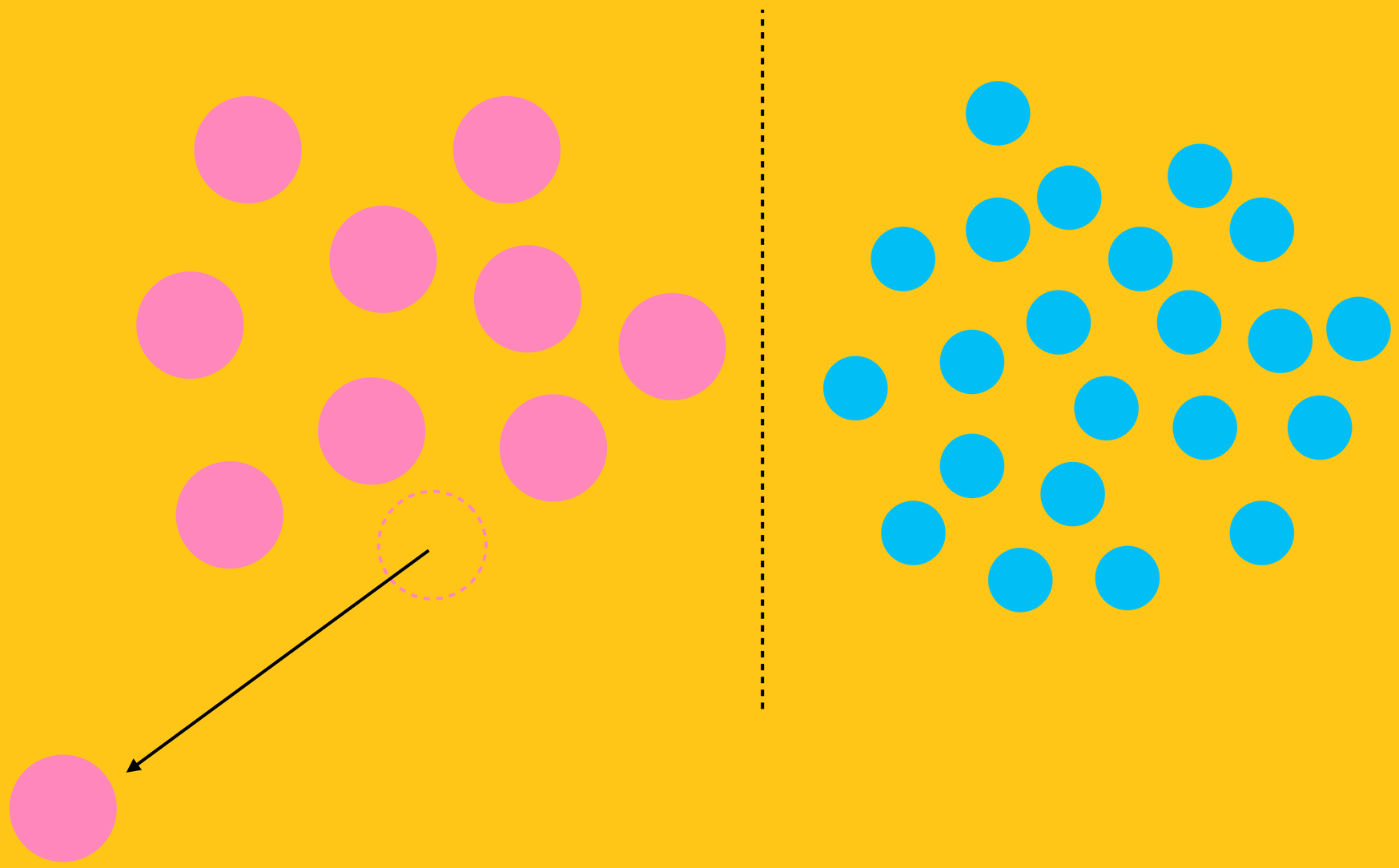


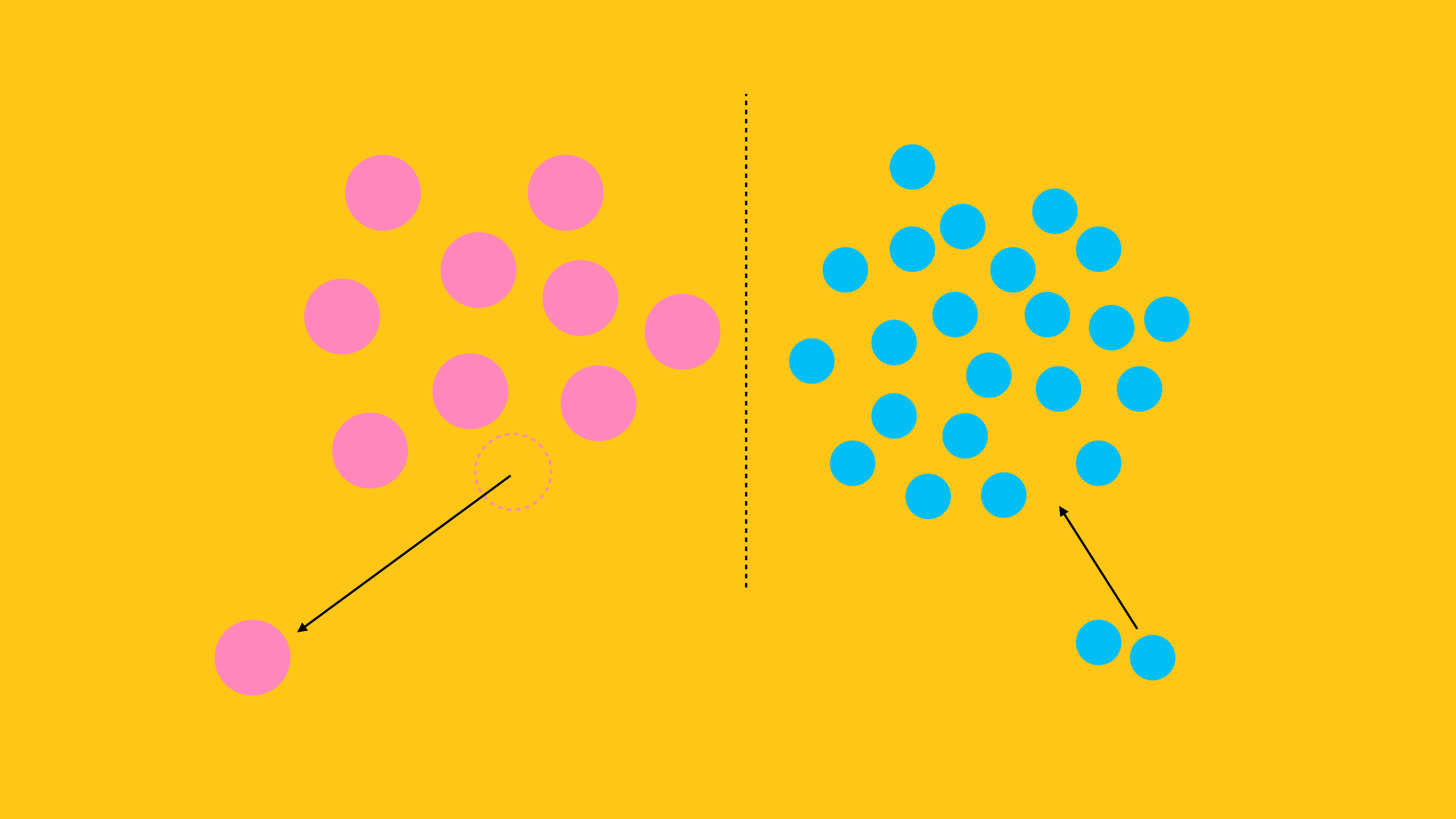
APPL +$10: make $100
APPL +$120: make $1200
APPL -$10: lose $100
APPL -$12: broke

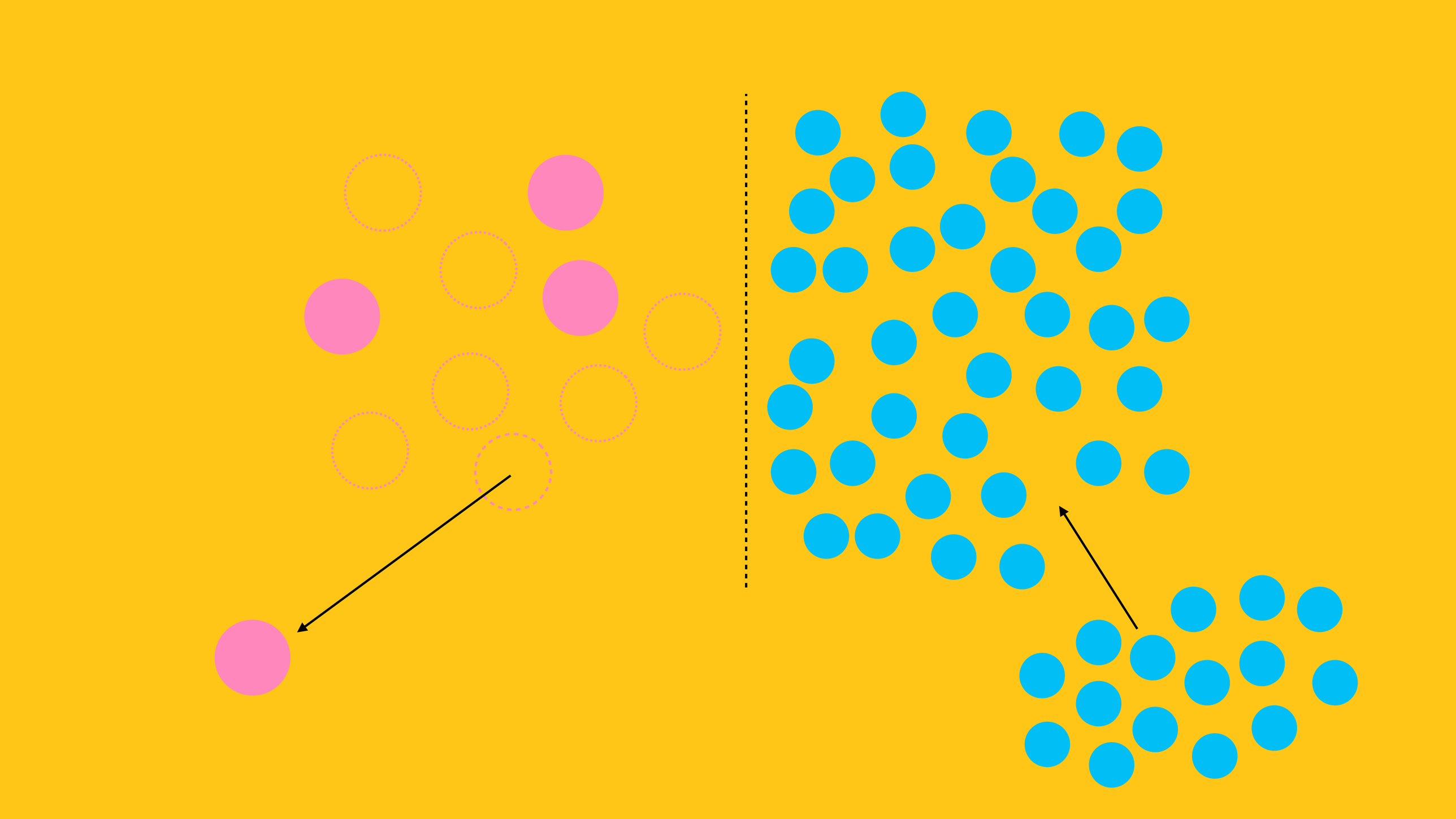
TOKEN EXCHANGES

- Normally you go off-chain for exchange
- For instant exchange, you can use an Automated Market Maker (AMM)



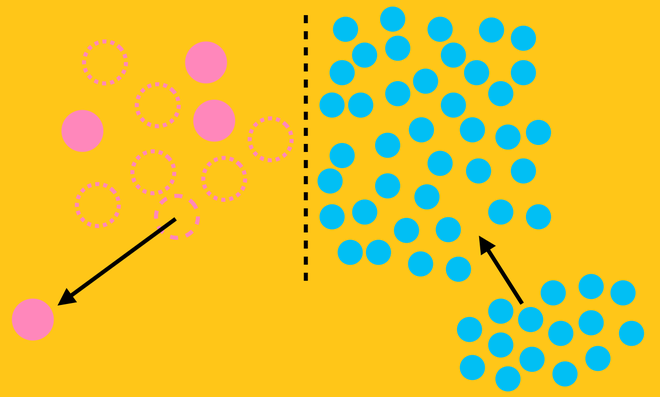






- More tokens you buy, more you pay (slippage)
- Buy a lot of tokens, you will pay way too much

- Next person can get blue coins for cheap



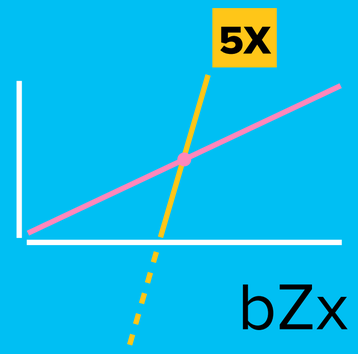
FEB 2020 INCIDENT

- Mallory tricks Alice into overpaying for something with Alice's money

Note: simplified and re-ordered

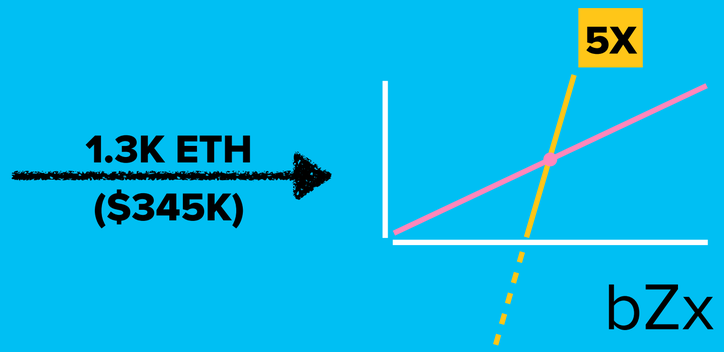
- Mallory tricks Alice into overpaying for something with Alice's money
- Mallory sells to Alice

Note: simplified and re-ordered

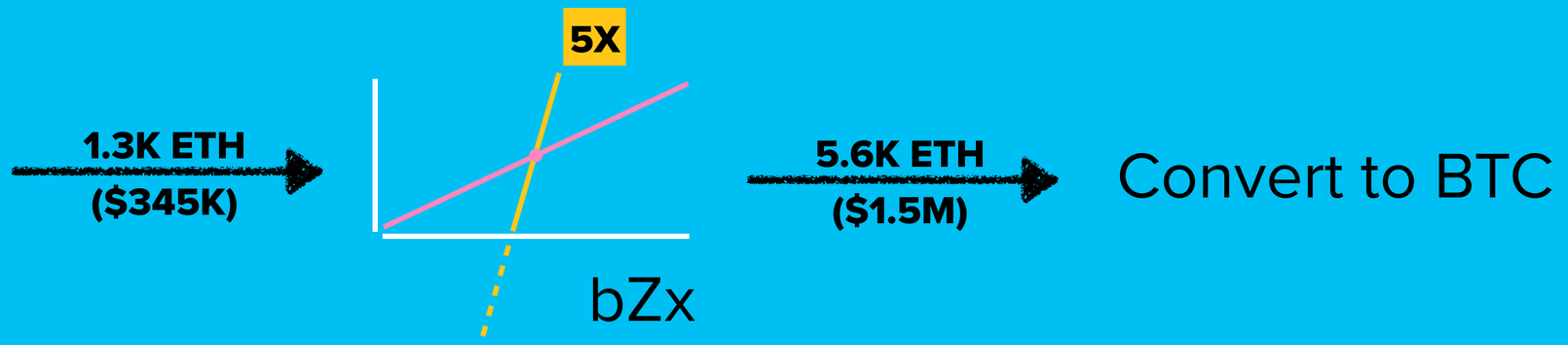


- Mallory tricks Alice into overpaying for something with Alice's money
- Mallory sells to Alice

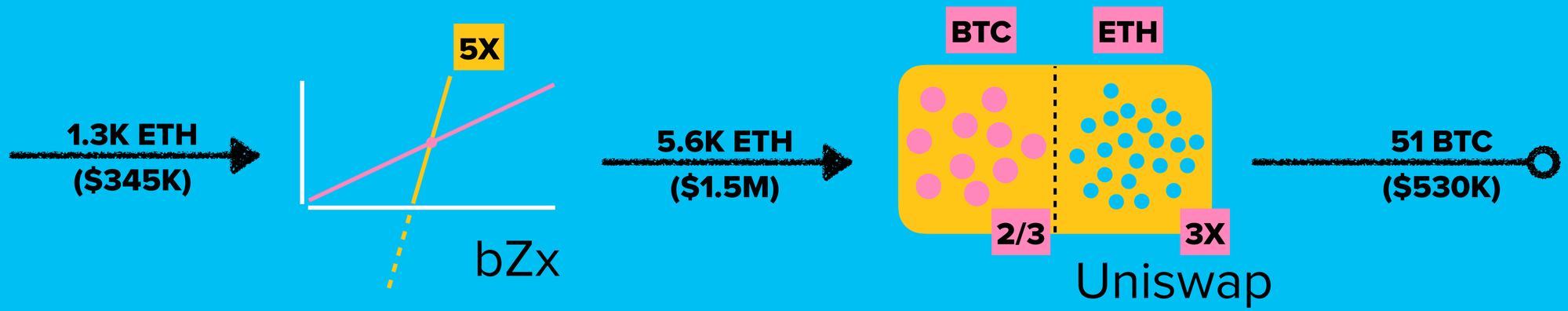
Note: simplified and re-ordered



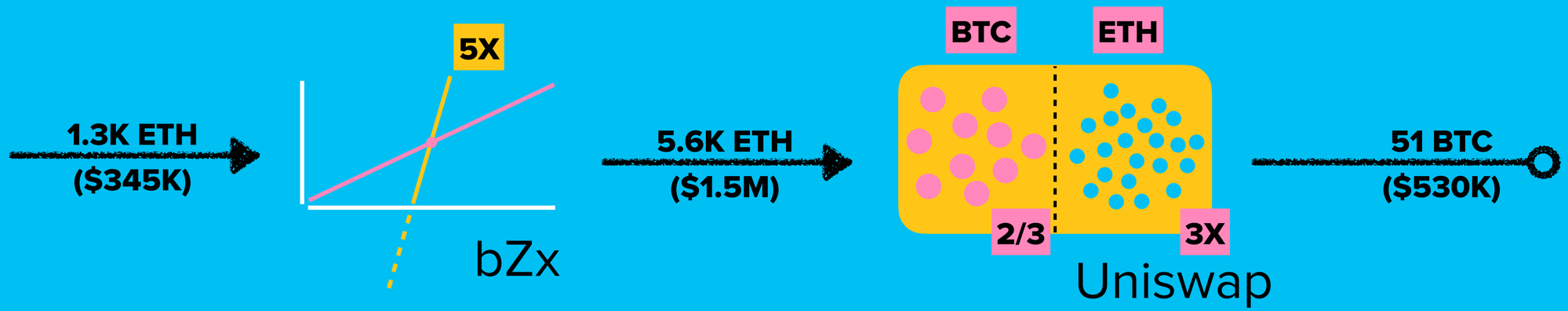
Note: simplified and re-ordered



Note: simplified and re-ordered

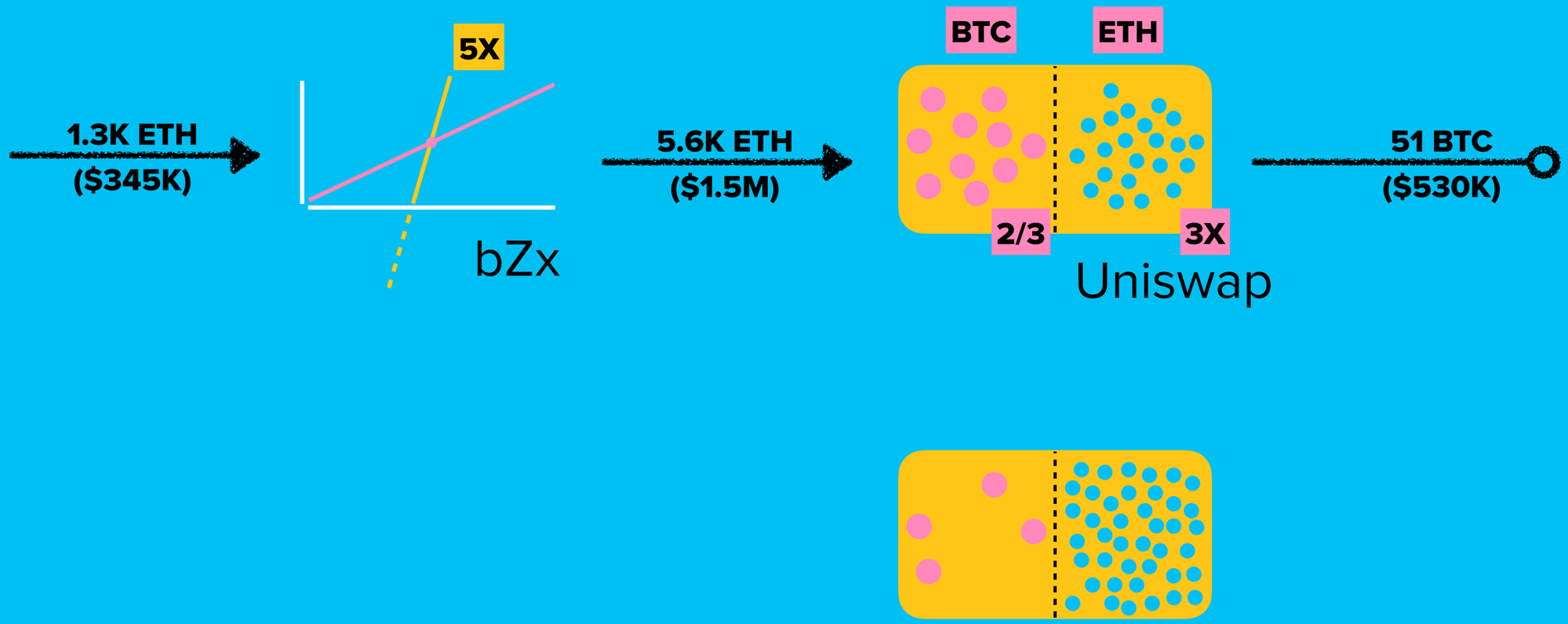


Note: simplified and re-ordered

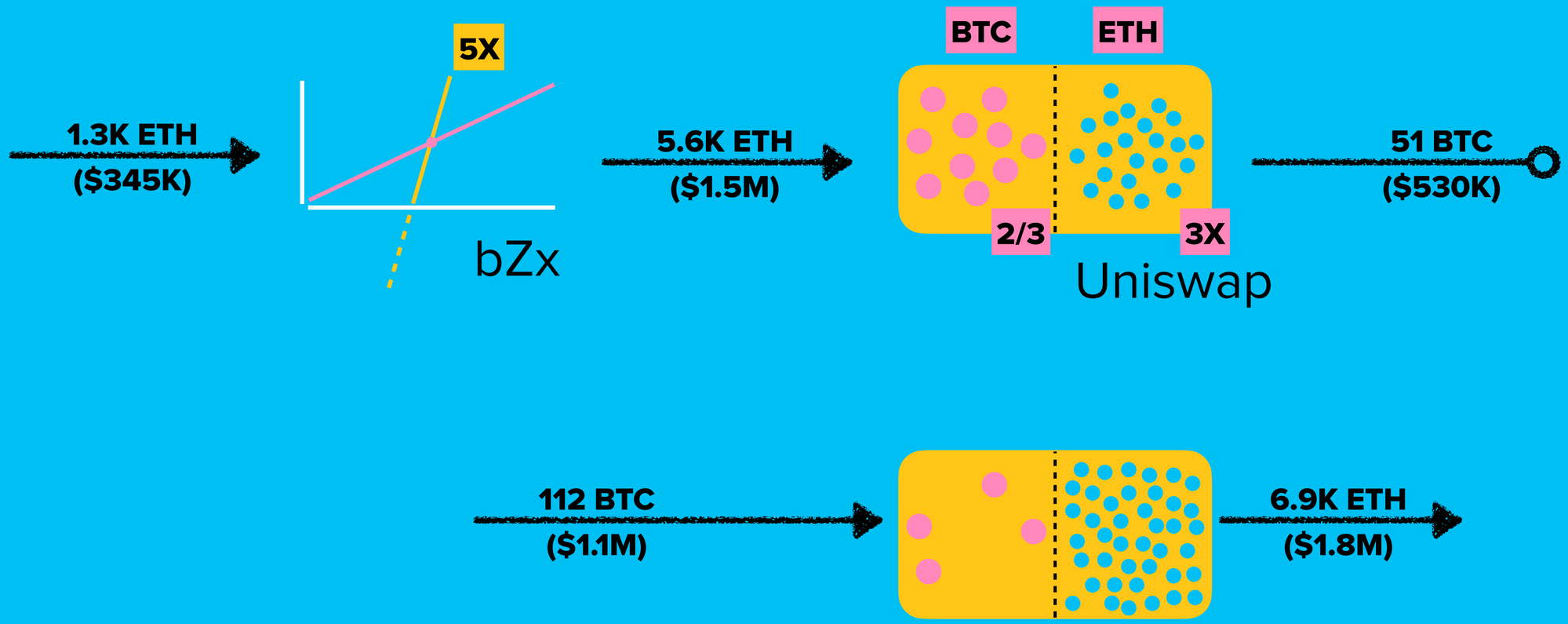


- Trade itself causes a price drop
- After price drop, all collateral is gone and borrowed money too
- Software error in bZx

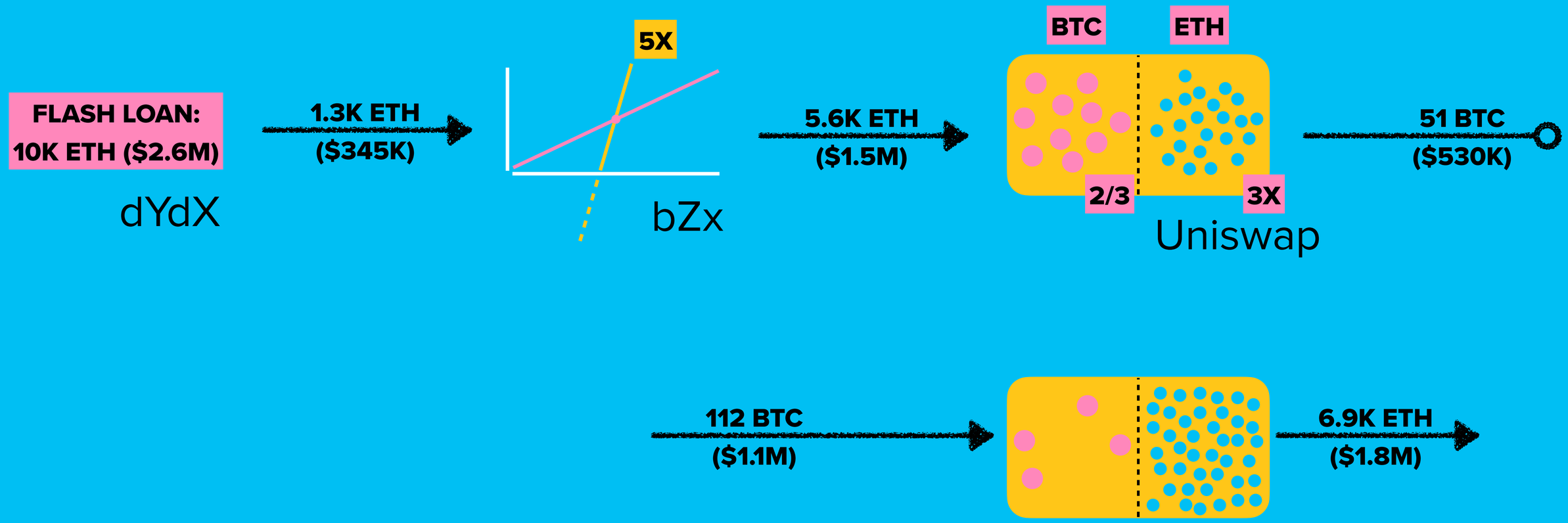
Note: simplified and re-ordered



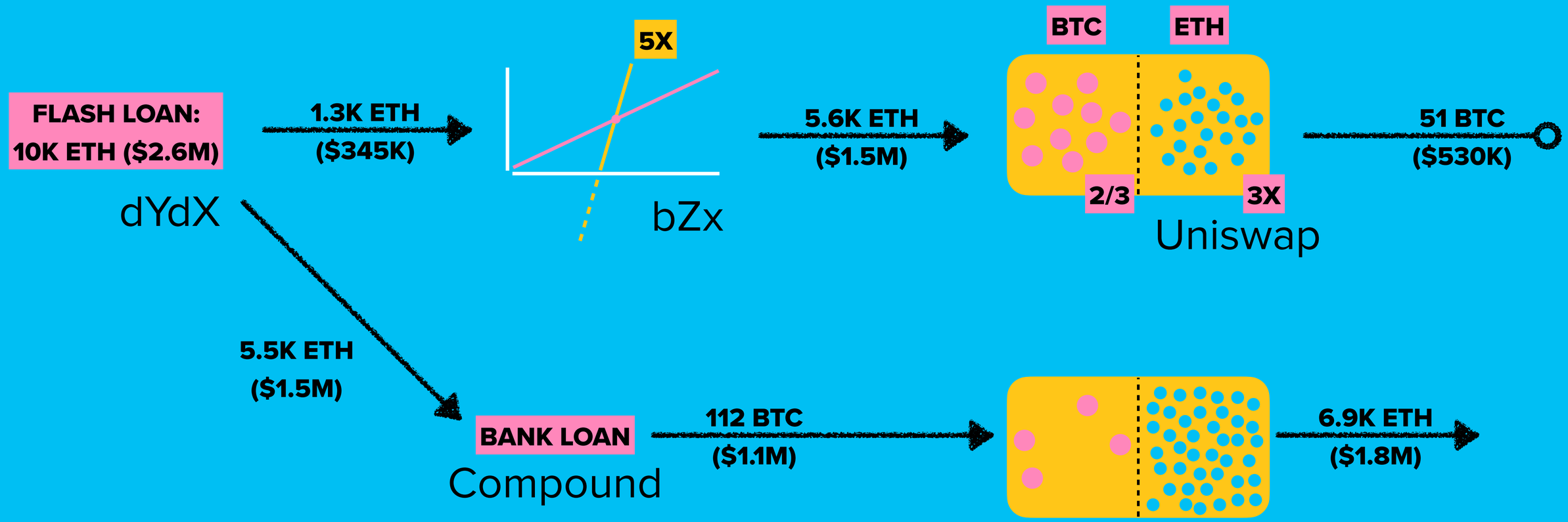
Note: simplified and re-ordered



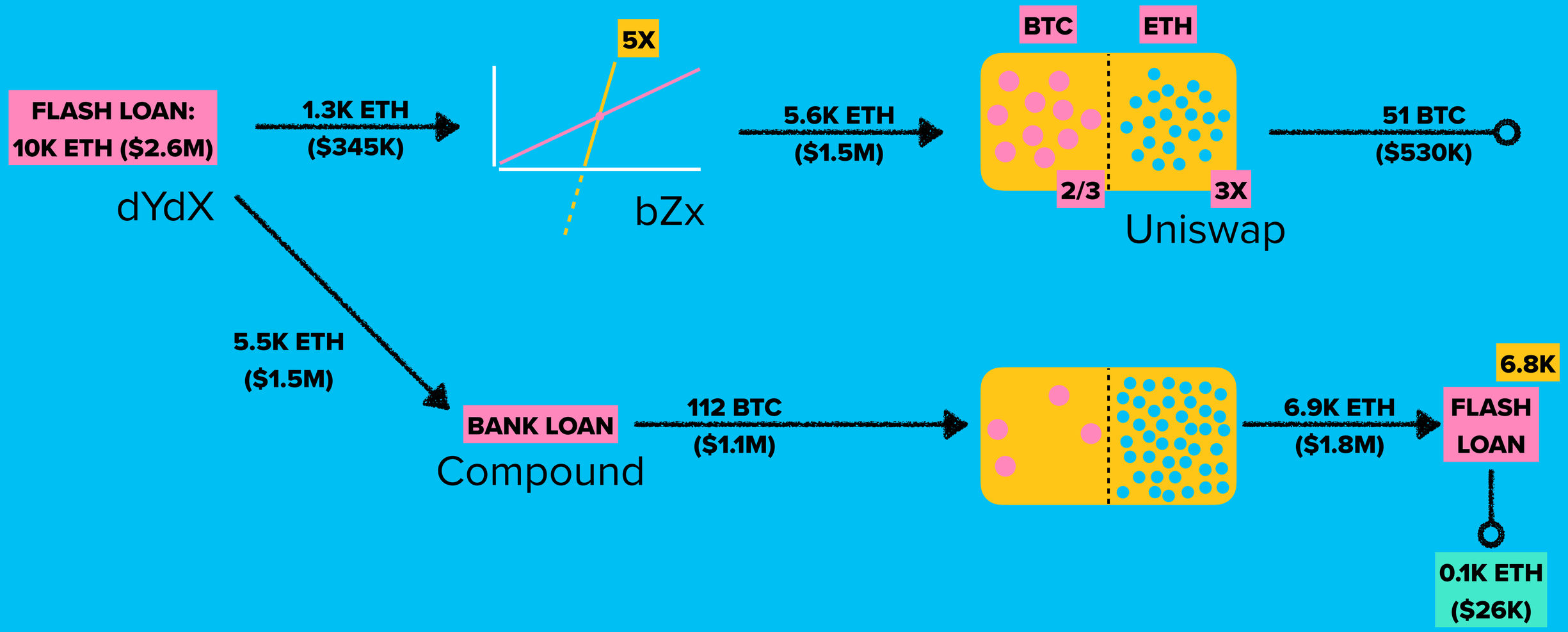
Note: simplified and re-ordered



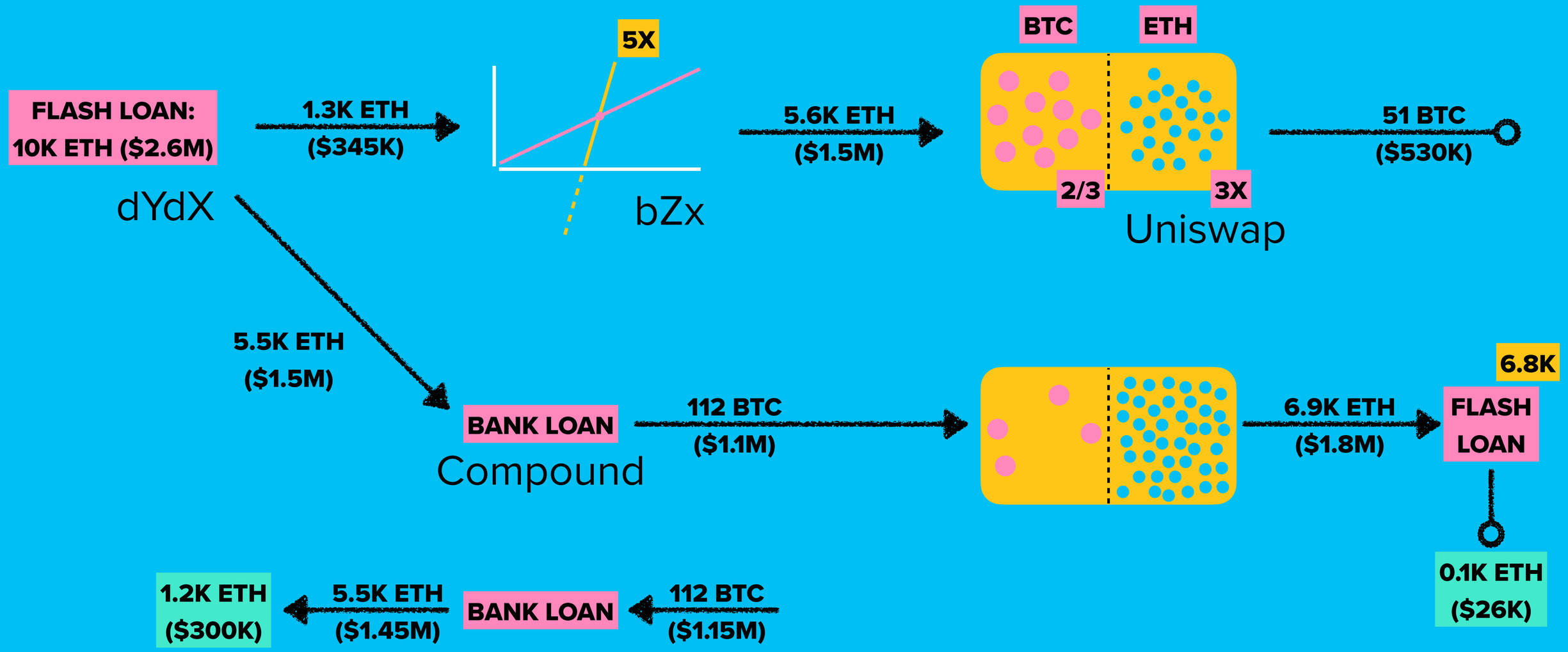
Note: simplified and re-ordered



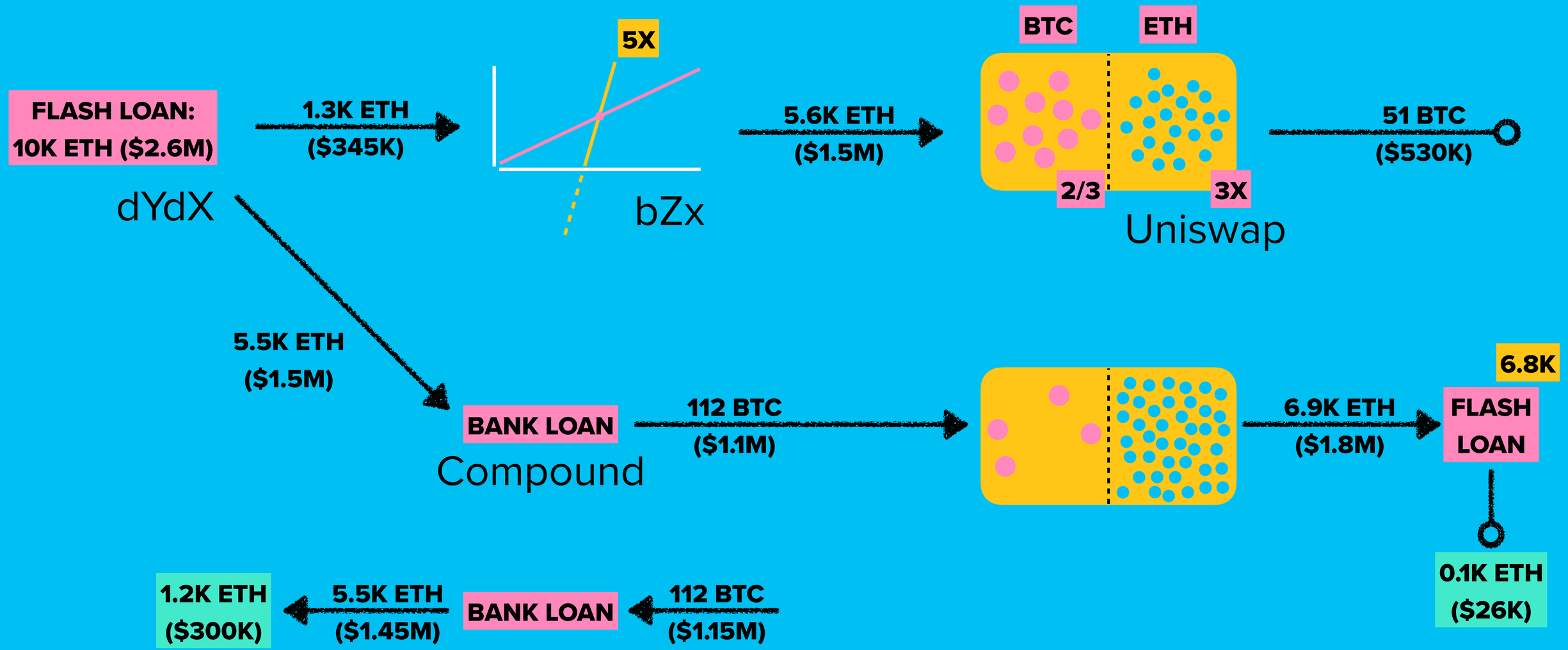
Note: simplified and re-ordered



Note: simplified and re-ordered



Note: simplified and re-ordered



Note: simplified and re-ordered

WRAP-UP

- A mistake left free tokens in Uniswap. When a researcher tried to redeem them, a miner automatically noticed it was profitable and modified the transaction and stole the tokens.

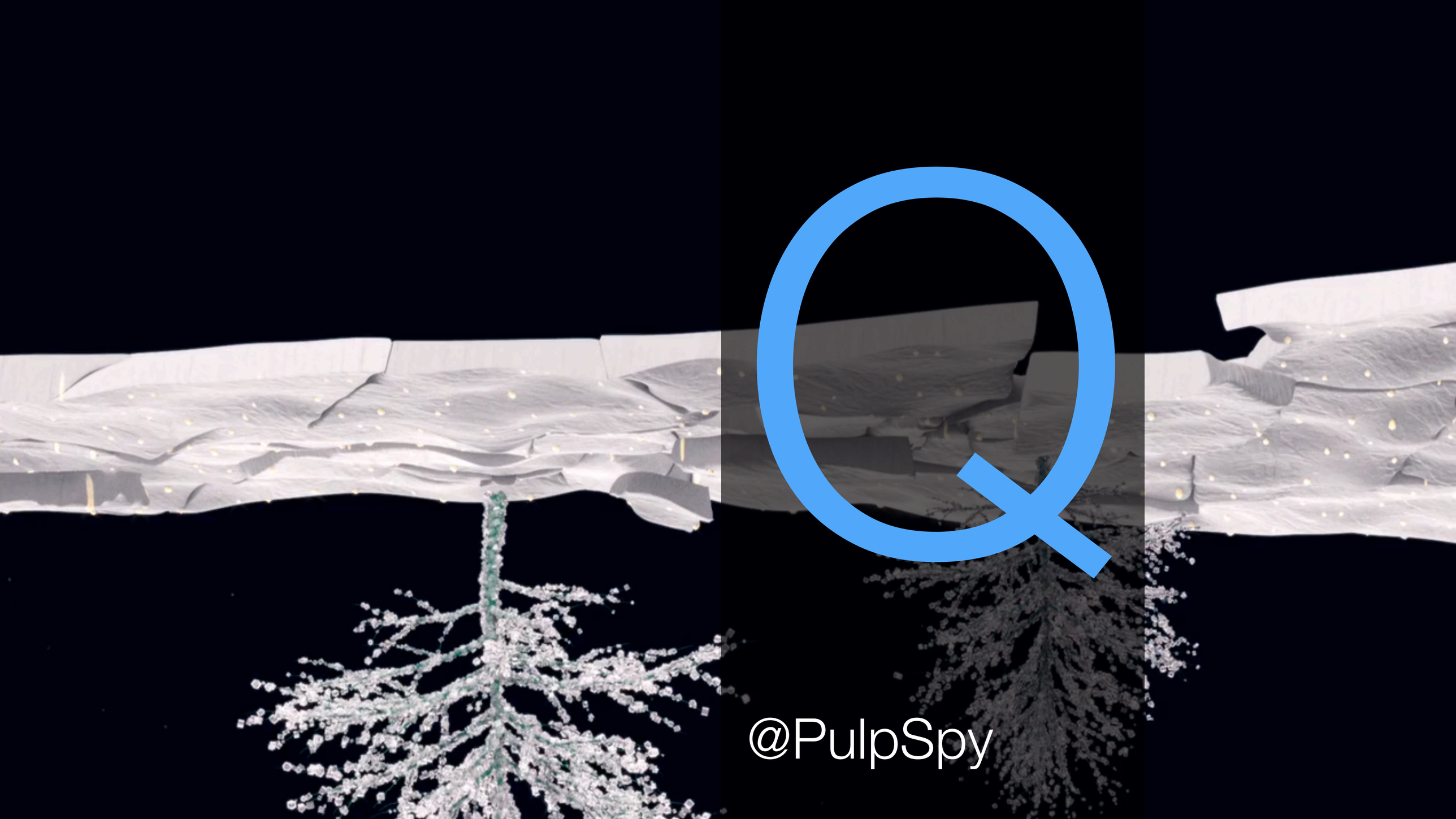
- Celebrity developer pushed unannounced pre-launch code to Ethereum and users noticed it. They used it immediately (despite not knowing what it did exactly), buying up $15M in tokens. It was then hacked.

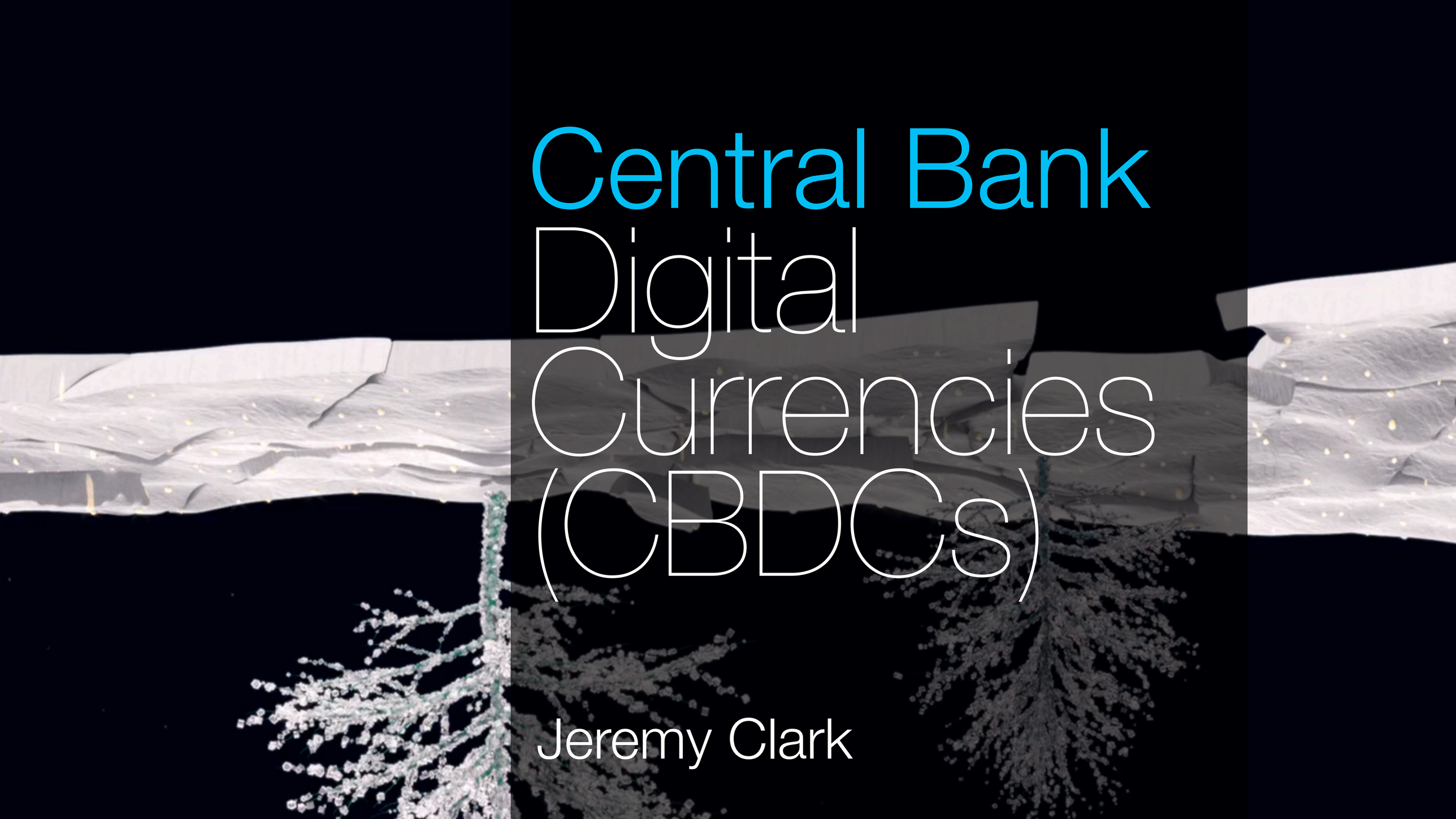
- “Unaudited” is a selling feature for getting in on the ground floor. A single wrong line in Yam (v2.0) locked $450K tokens.

- Novel techniques
- Size of losses are material
- Size of losses are growing

- No takeaways or conclusions… yet

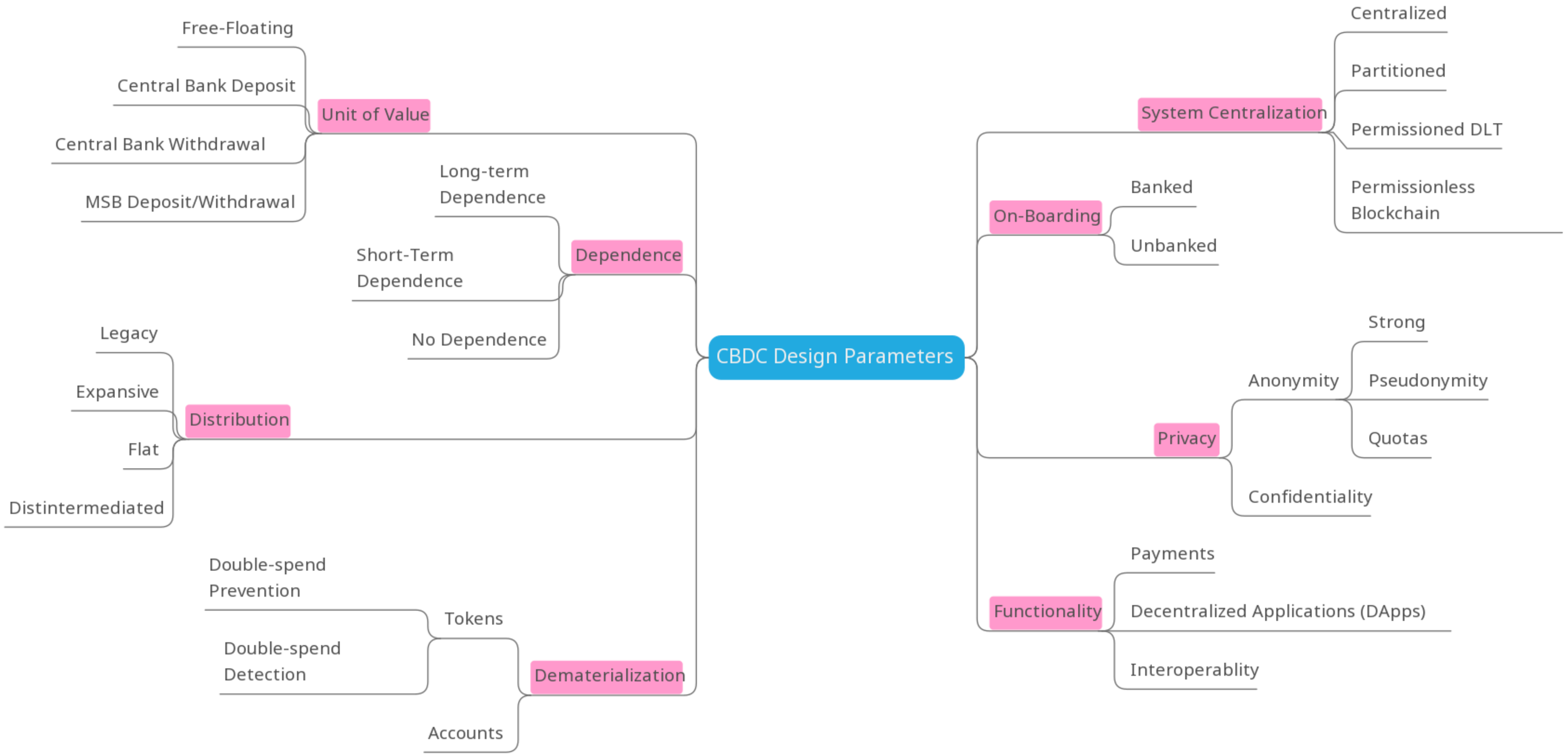
-


Q
@PulpSpy



Central Bank Digital Currencies (CBDCs)

Jeremy Clark


CBDC Design Parameters
Unit of Value
Free-Floating
Central Bank Deposit
Central Bank Withdrawal
MSB Deposit/Withdrawal
Dependence
Long-term Dependence
Short-Term Dependence
No Dependence
Distribution
Legacy
Expansive
Flat
Distintermediated
Dematerialization
Double-spend Prevention
Tokens
Double-spend Detection
Accounts
System Centralization
Centralized
Partitioned
Permissioned DLT
Permissionless Blockchain
On-Boarding
Banked
Unbanked
Privacy
Anonymity
Strong
Pseudonymity
Quotas
Confidentiality
Functionality
Payments
Decentralized Applications (DApps)
Interoperablity

- Would you use a CBDC personally?
- Which stakeholders do you expect would want CBDCs? Which do not want one?
- What do you expect in terms of privacy?

- Any other thoughts…?