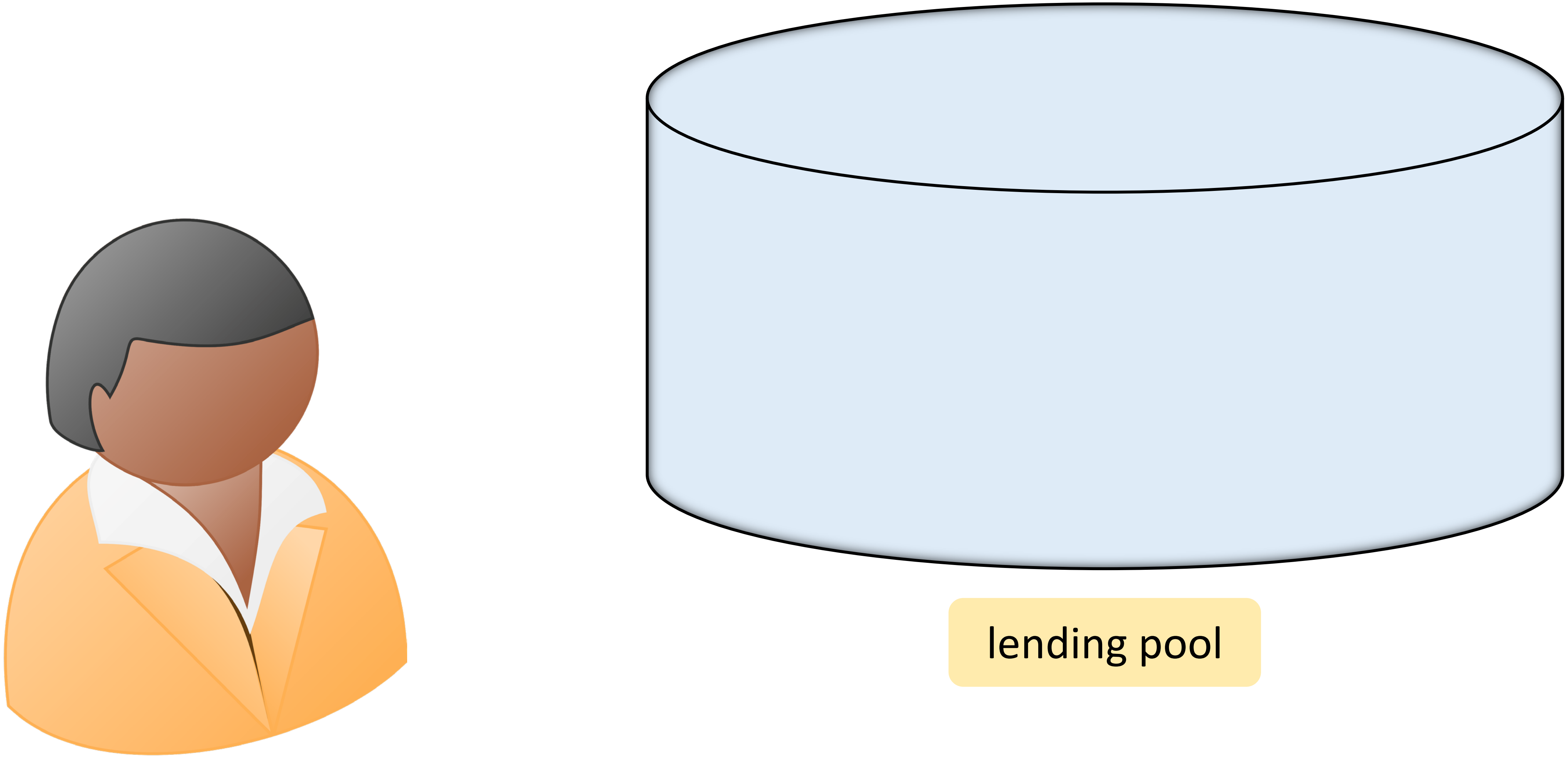
Short Squeeze in DeFi Lending Market: Decentralization in Jeopardy?

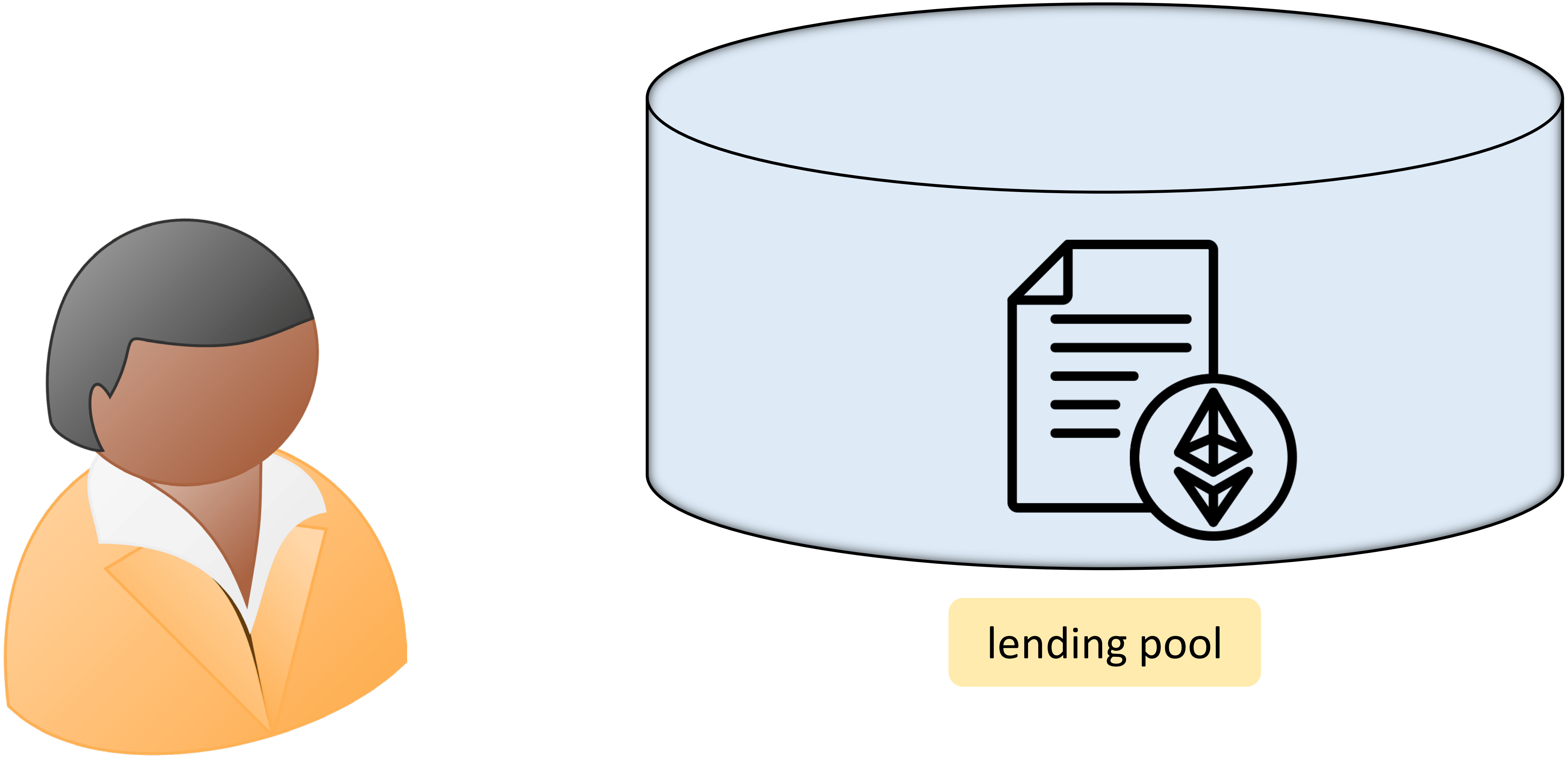
The 3rd Workshop on Decentralized Finance (DeFi)
Lioba Heimbach, Eric Schertenleib and Roger Wattenhofer
ETH Zurich – Distributed Computing – www.disco.ethz.ch

DeFi lending



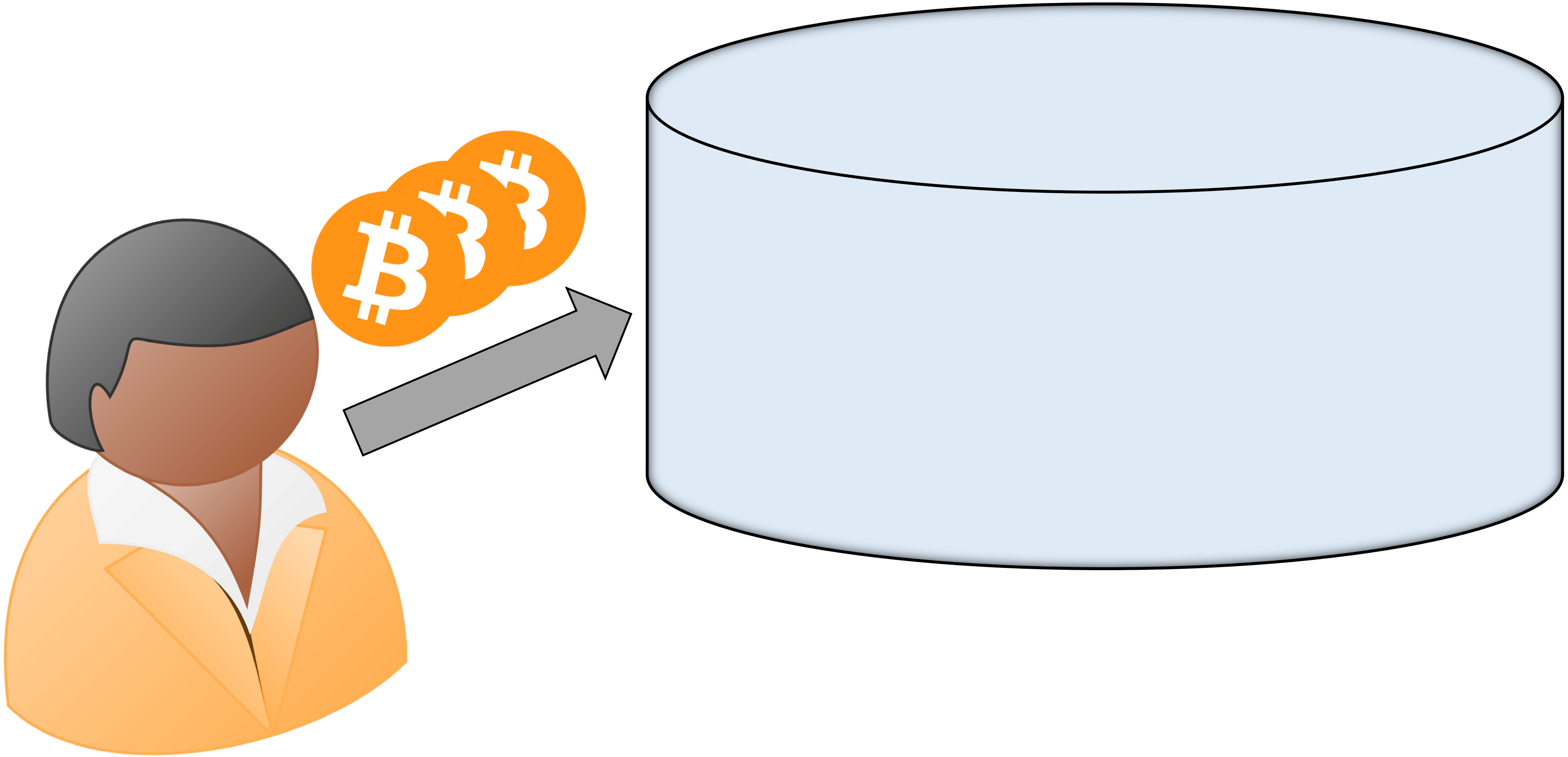
lending pool

DeFi lending

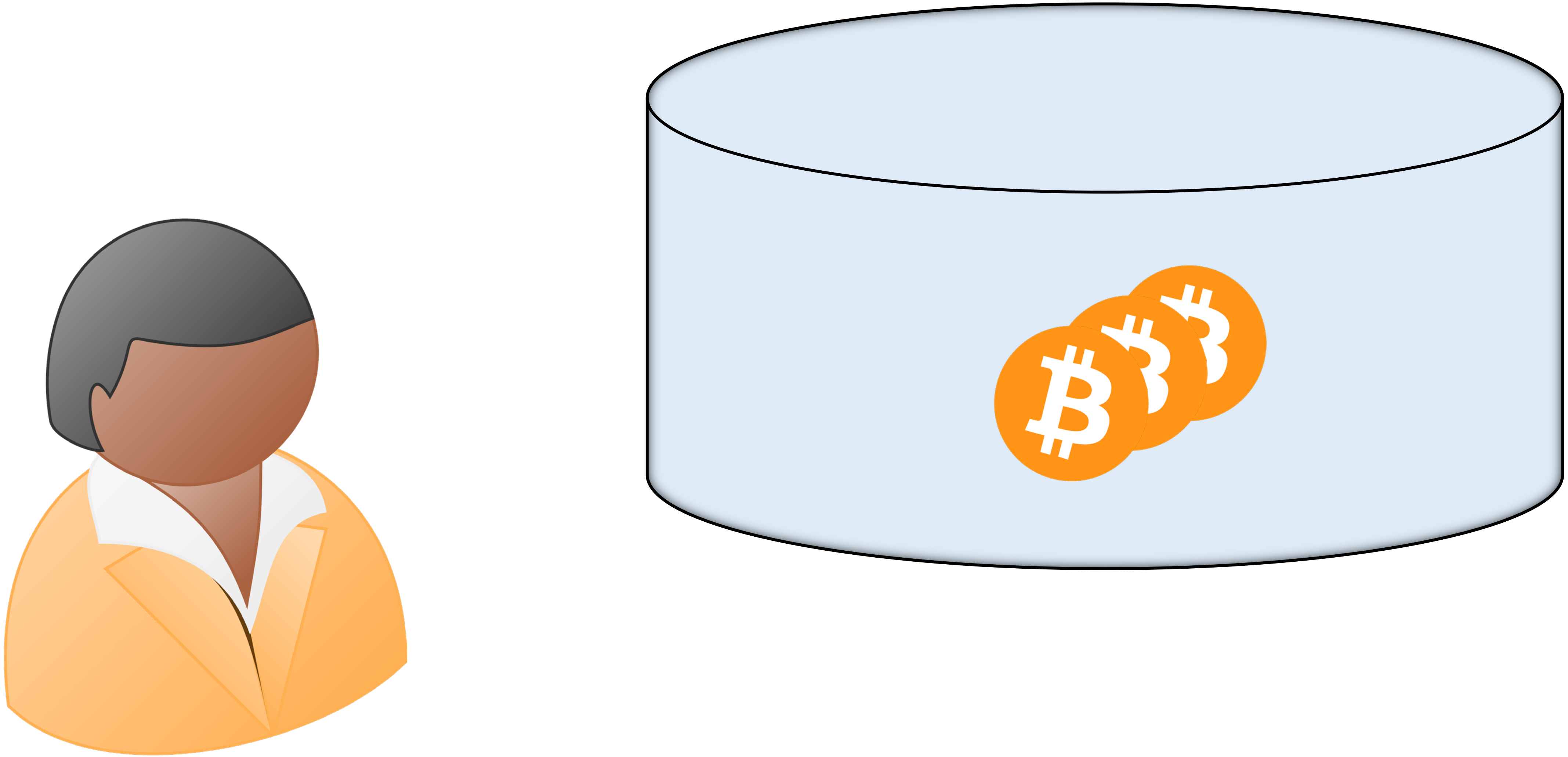


lending pool

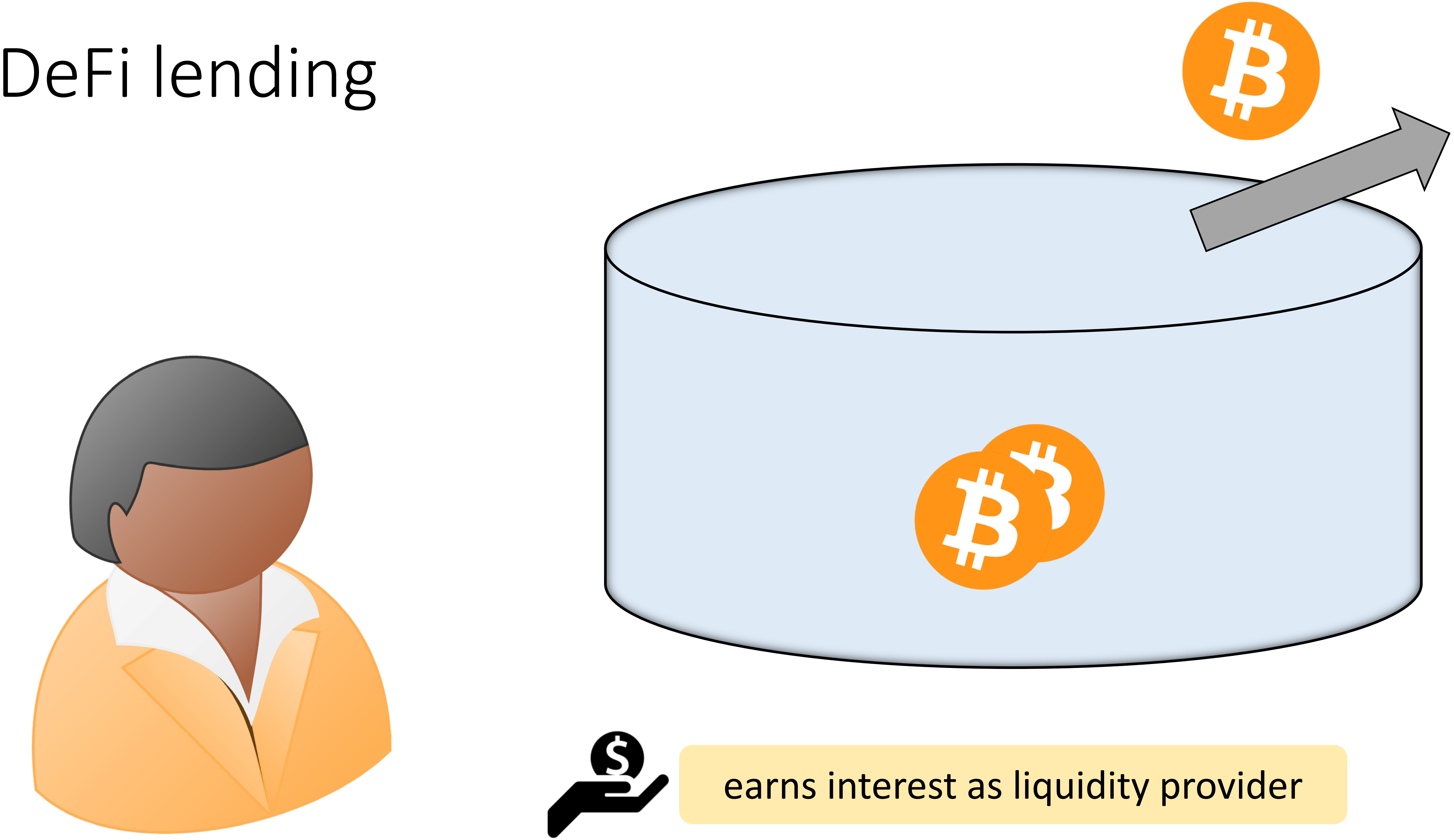
DeFi lending



DeFi lending

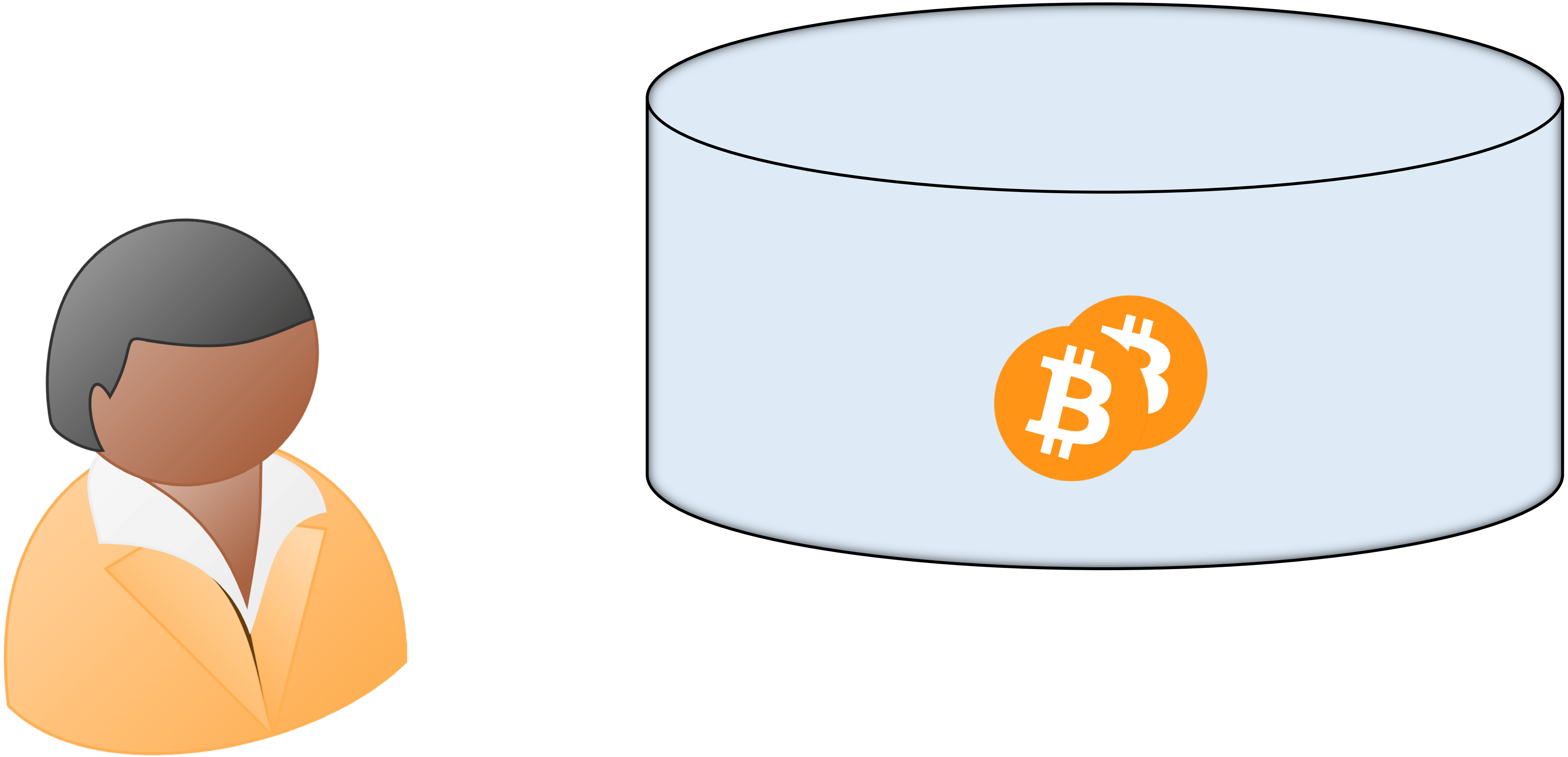


DeFi lending

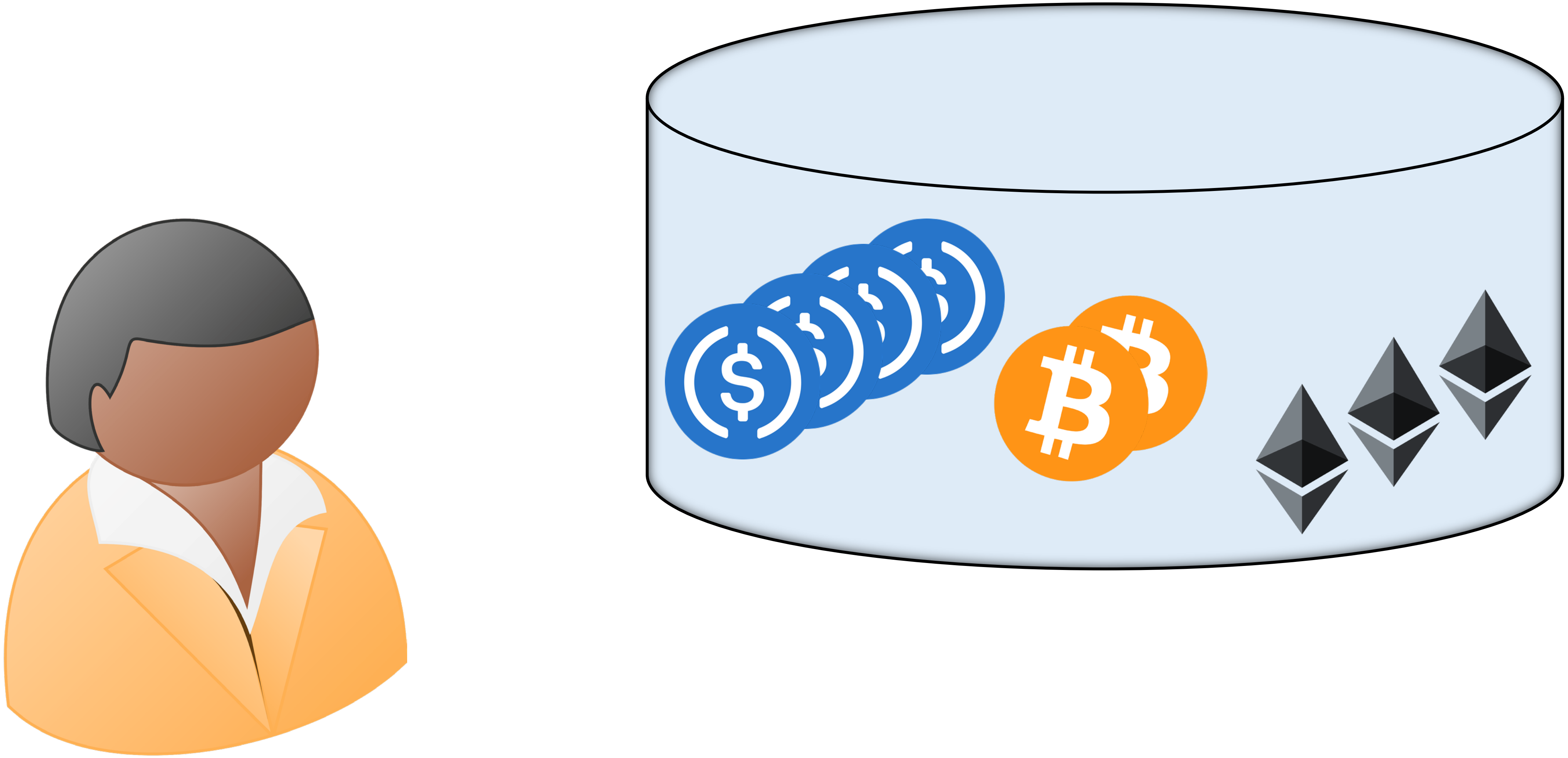


earns interest as liquidity provider

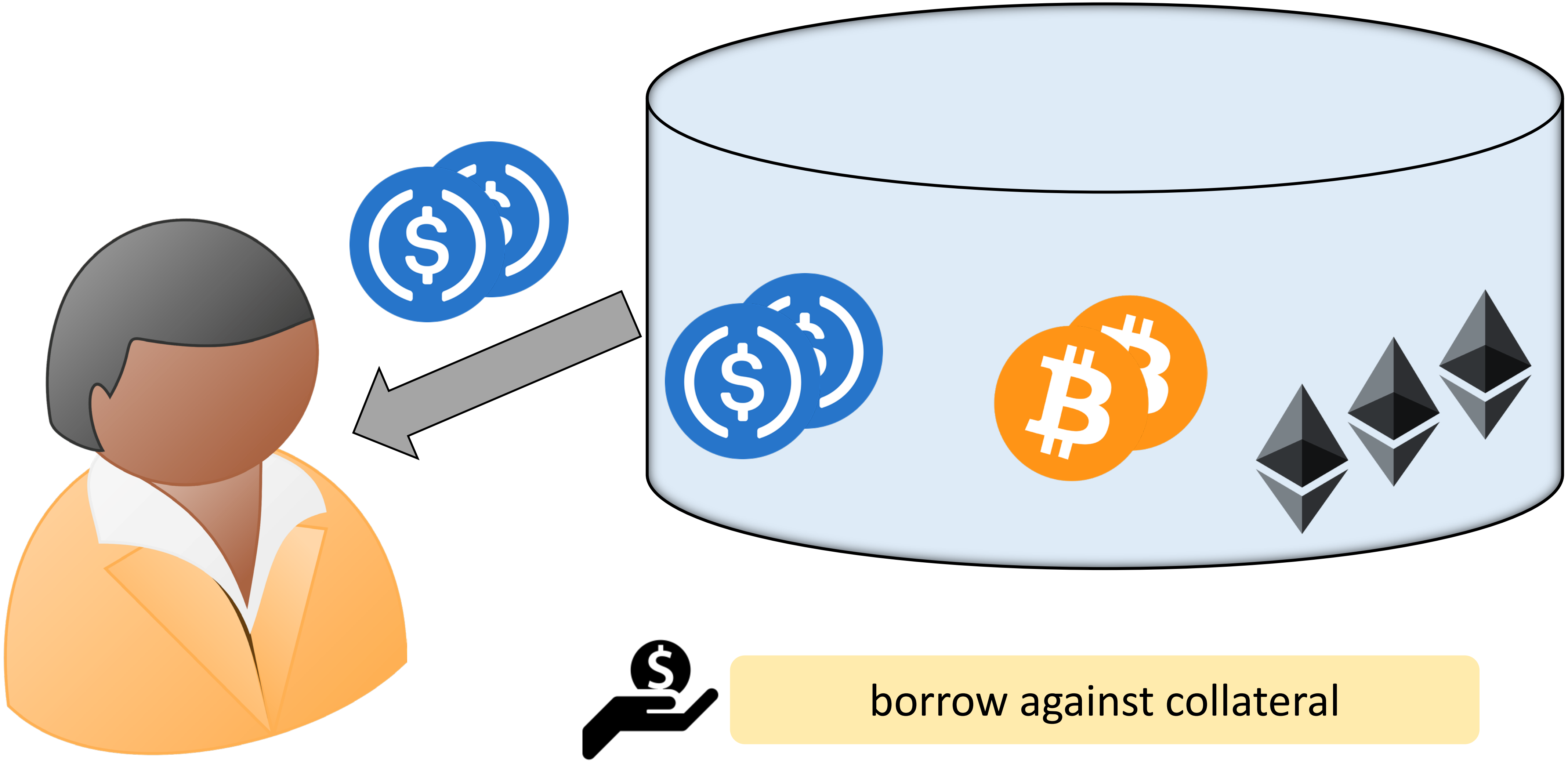
DeFi lending



DeFi lending

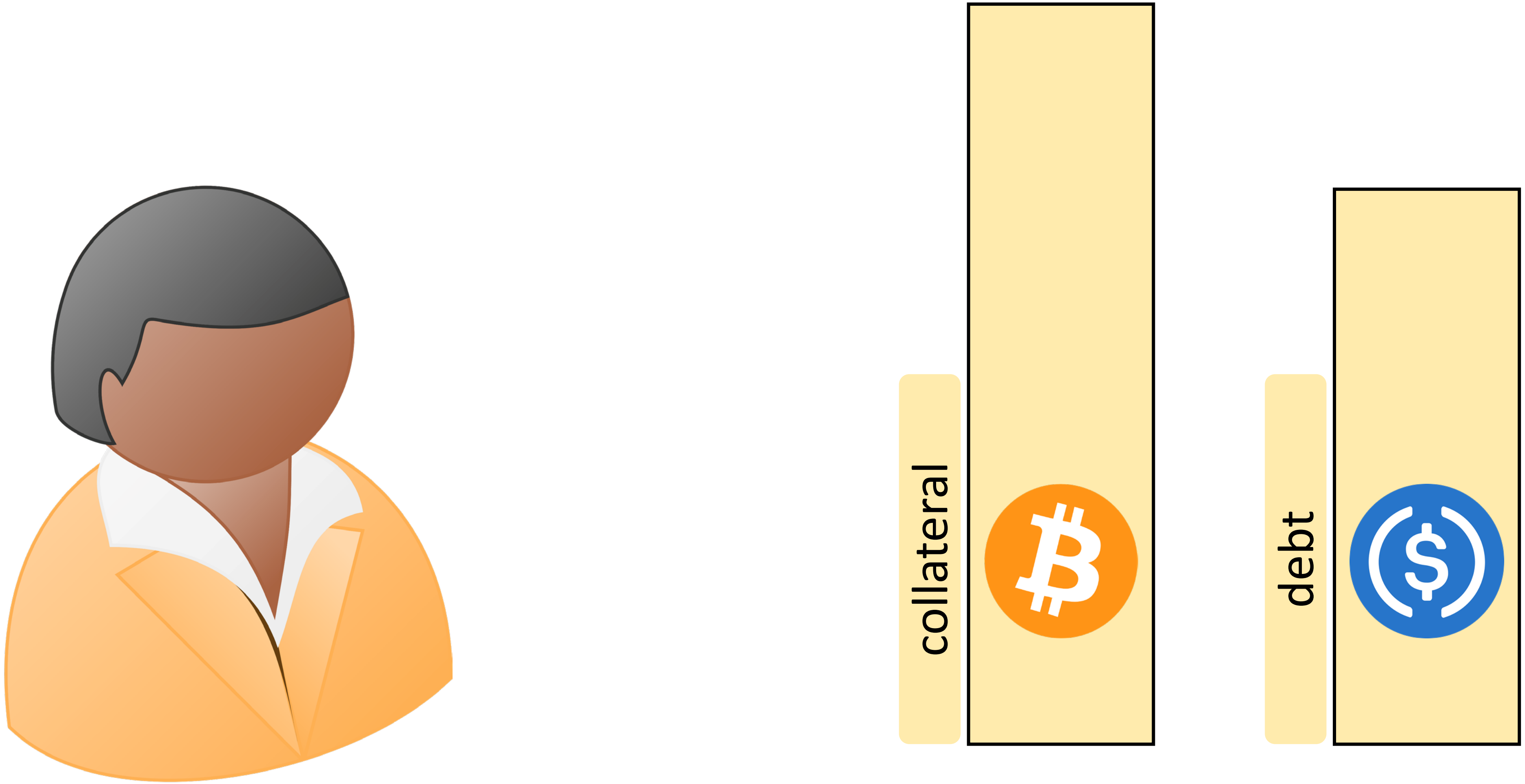


DeFi lending

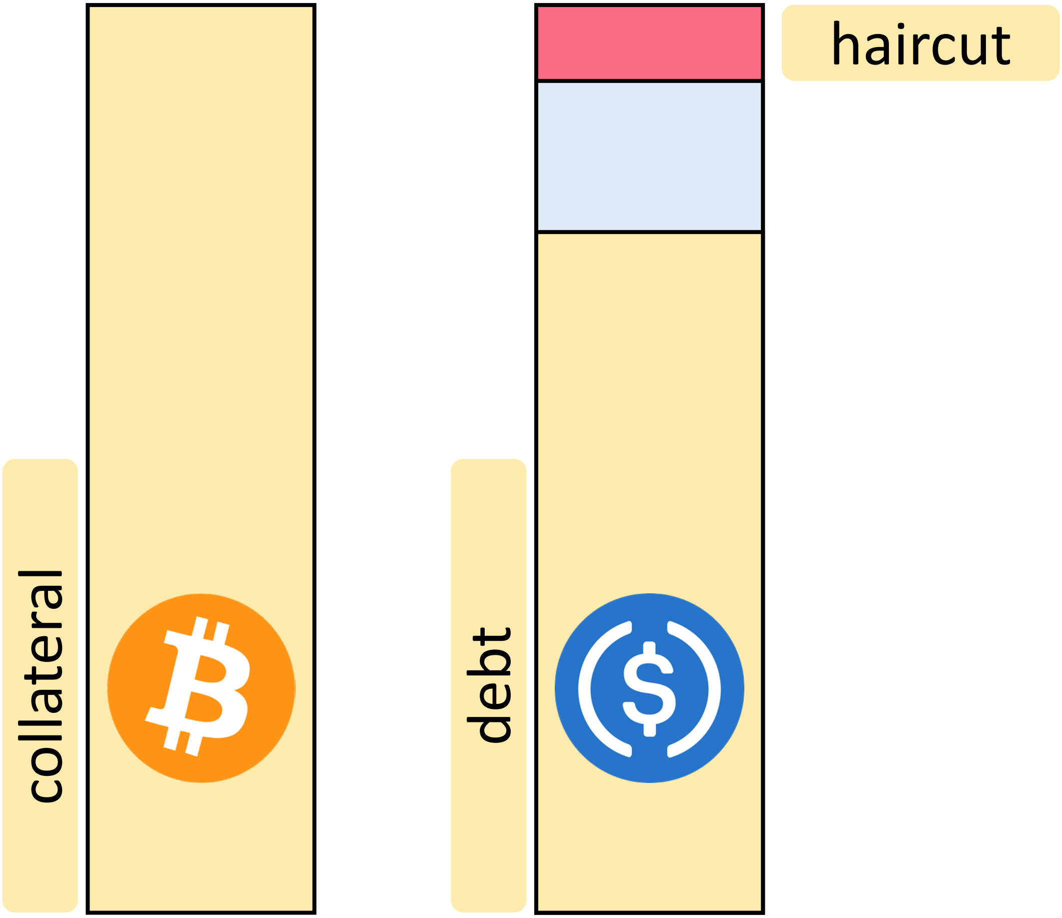


borrow against collateral

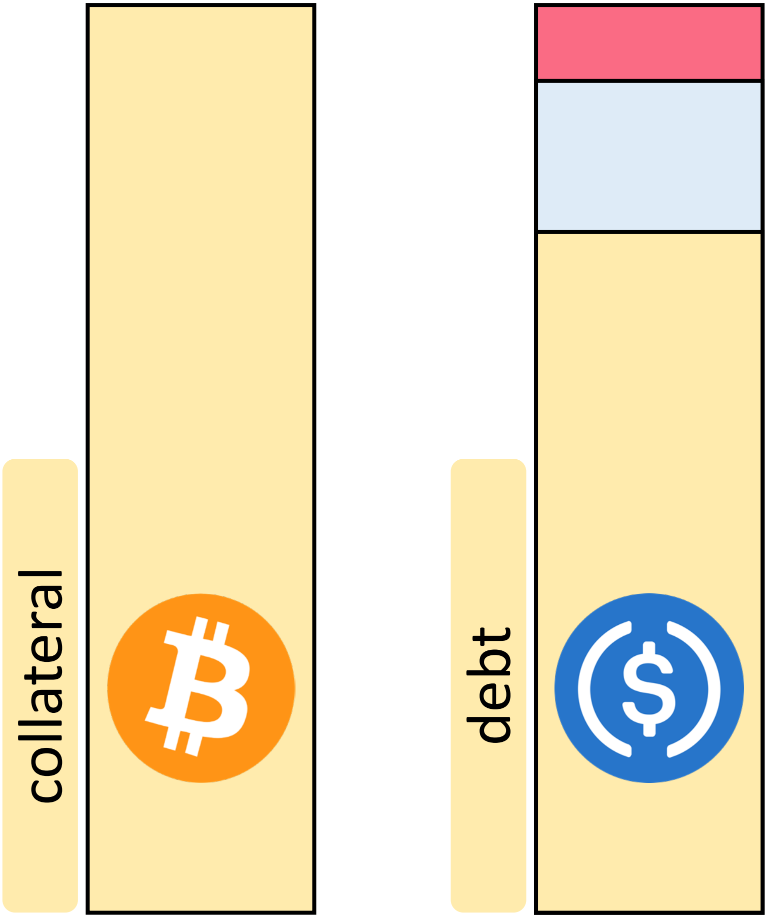
DeFi lending



DeFi lending



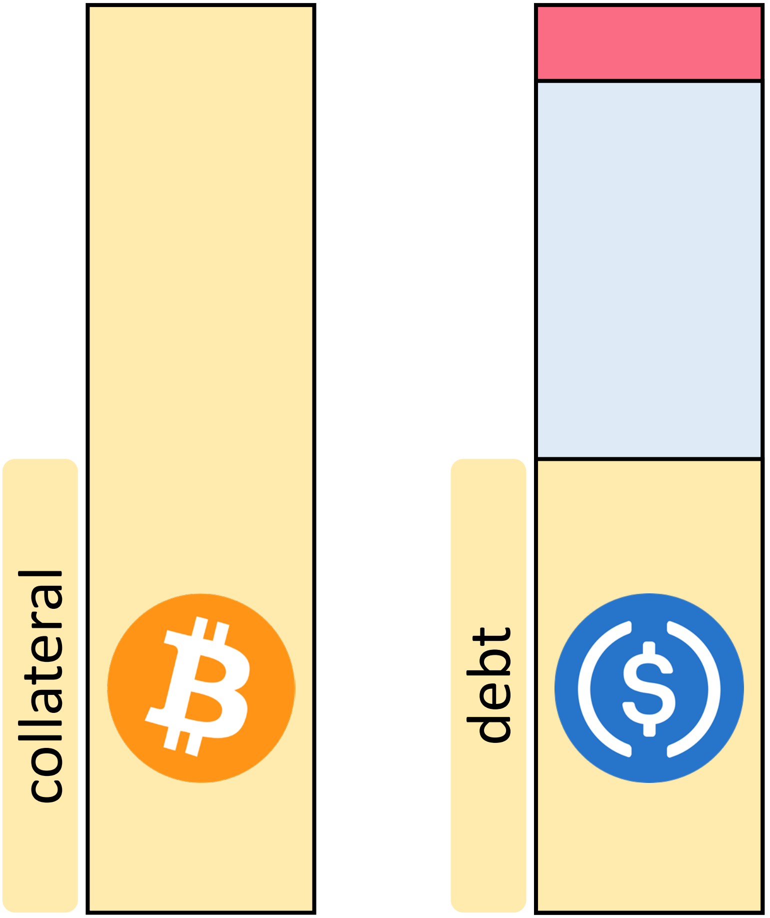
DeFi lending



collateral

debt

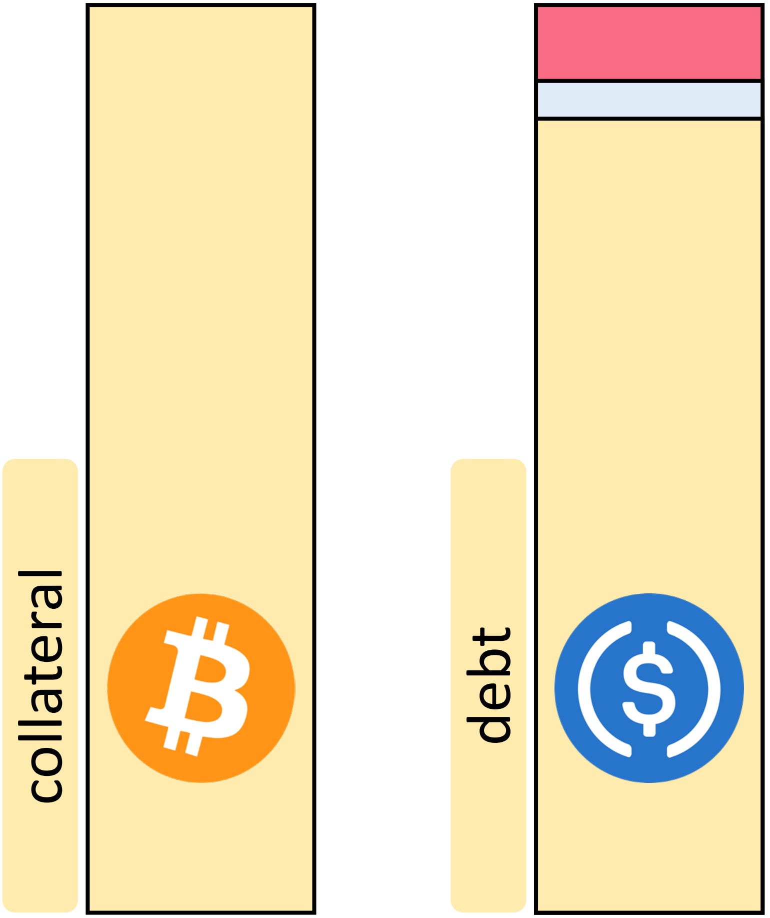
DeFi lending



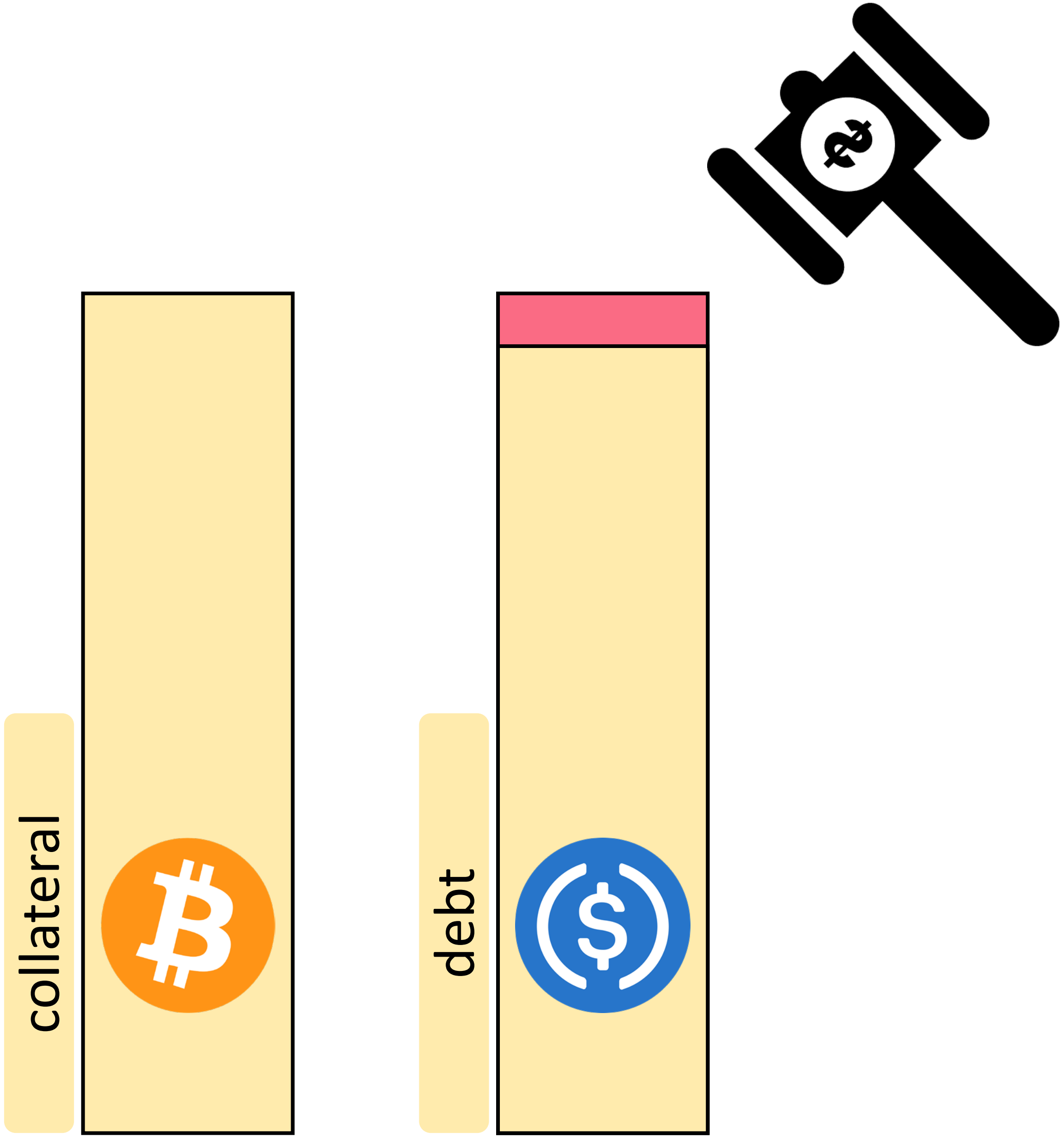
collateral

debt

DeFi lending

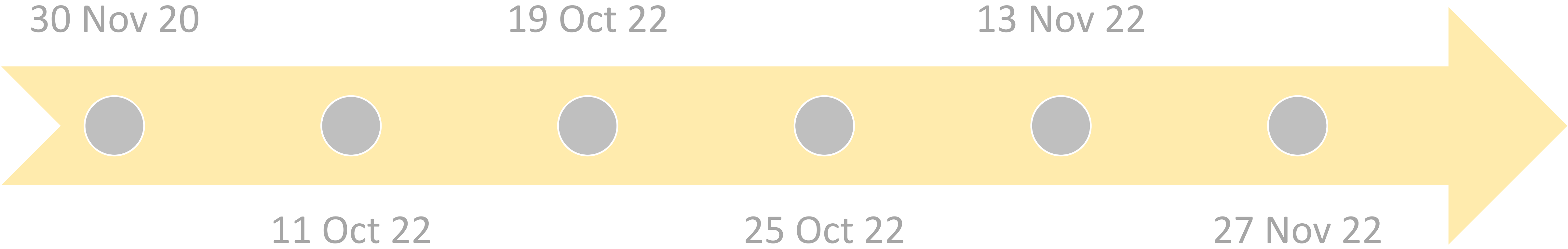


DeFi lending



collateral

debt



30 Nov 20

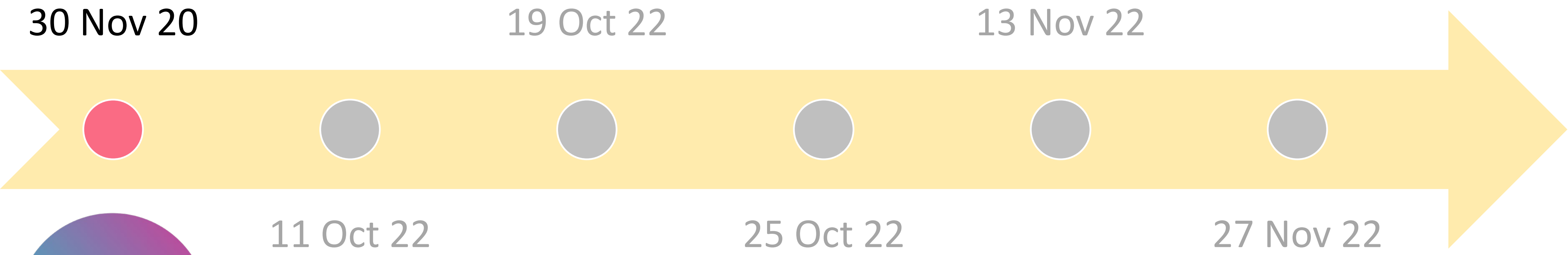
11 Oct 22

19 Oct 22

25 Oct 22

13 Nov 22

27 Nov 22



30 Nov 20

11 Oct 22

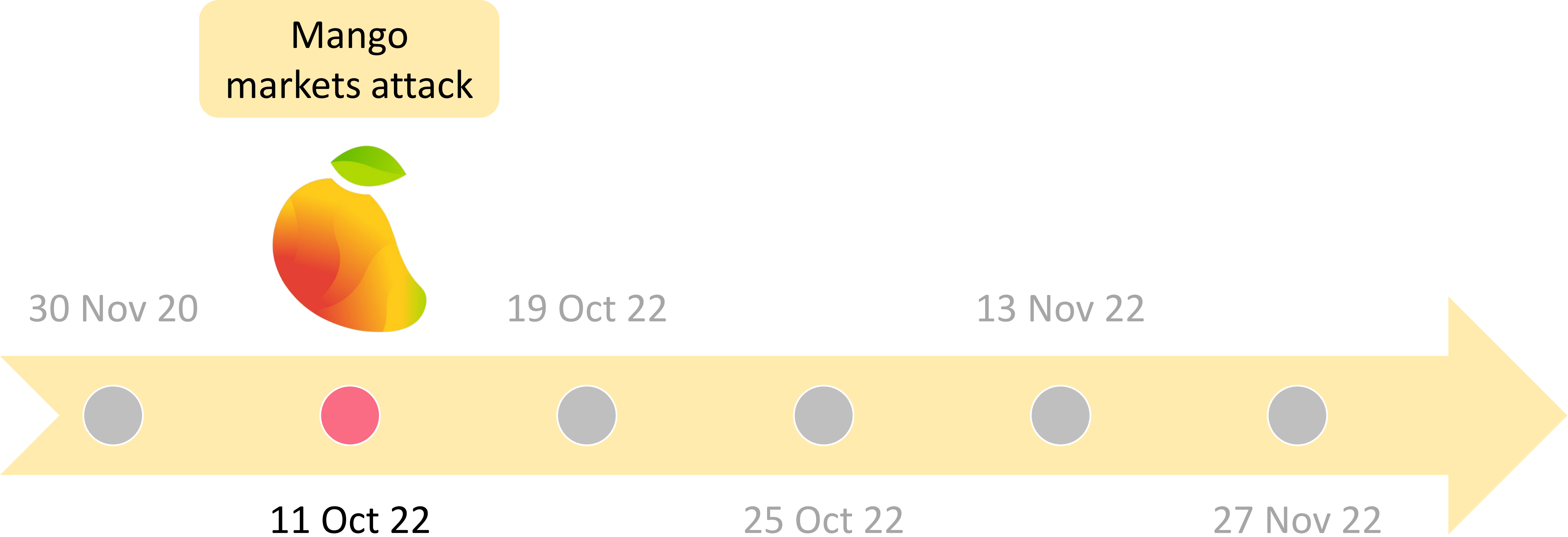
19 Oct 22

25 Oct 22

13 Nov 22

27 Nov 22

AAVE V2 launch



Mango
markets attack

30 Nov 20

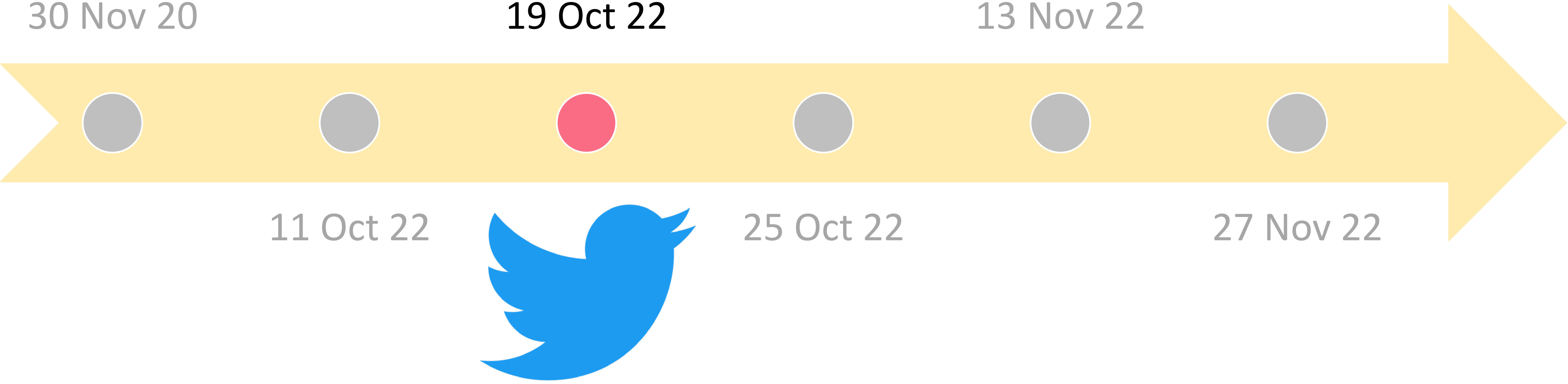
11 Oct 22

19 Oct 22

25 Oct 22

13 Nov 22

27 Nov 22



30 Nov 20

11 Oct 22

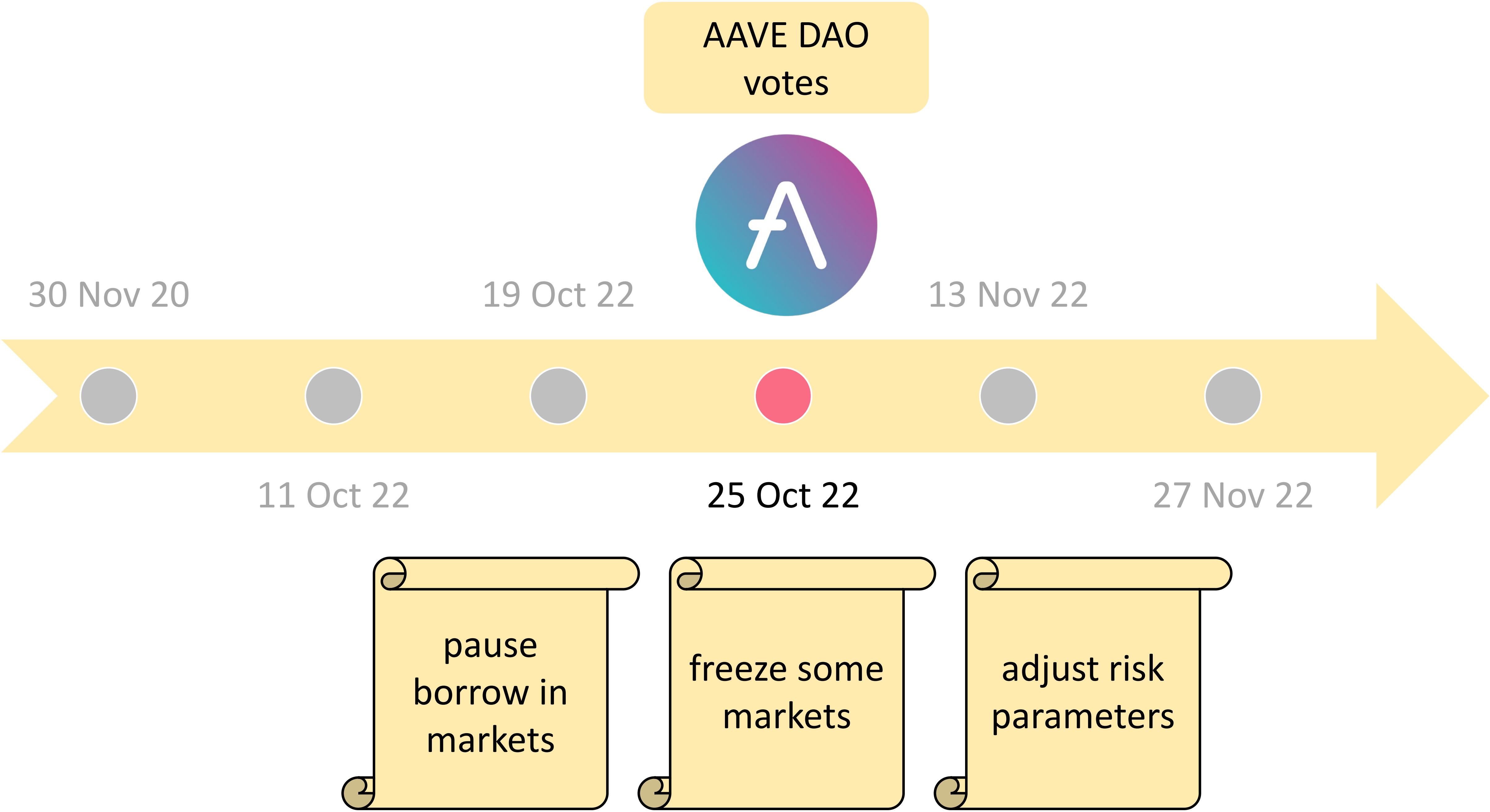
19 Oct 22

25 Oct 22

13 Nov 22

27 Nov 22

Avi Eisenberg tweets



AAVE DAO votes

30 Nov 20

11 Oct 22

19 Oct 22

25 Oct 22

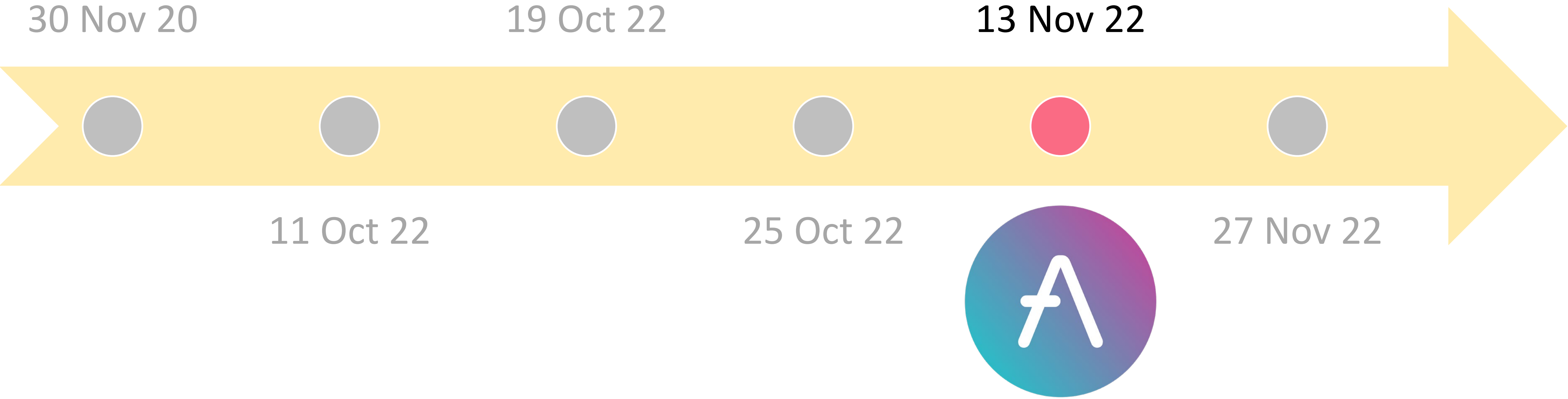
13 Nov 22

27 Nov 22

pause borrow in markets

freeze some markets

adjust risk parameters



30 Nov 20

11 Oct 22

19 Oct 22

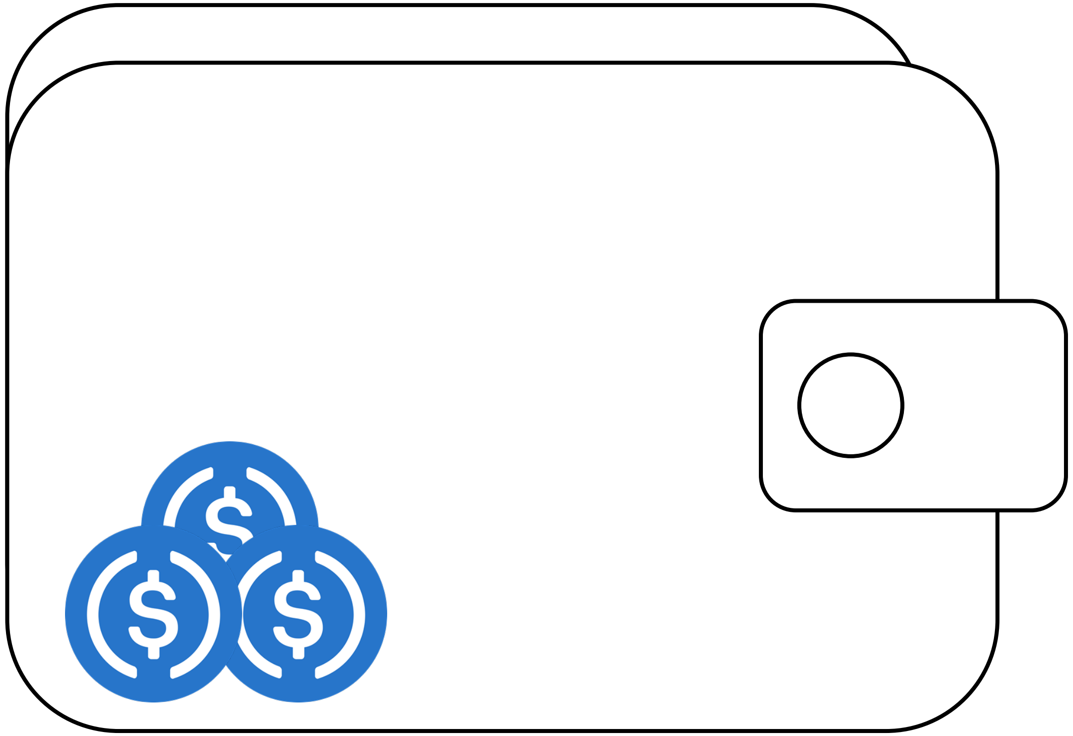
25 Oct 22

13 Nov 22

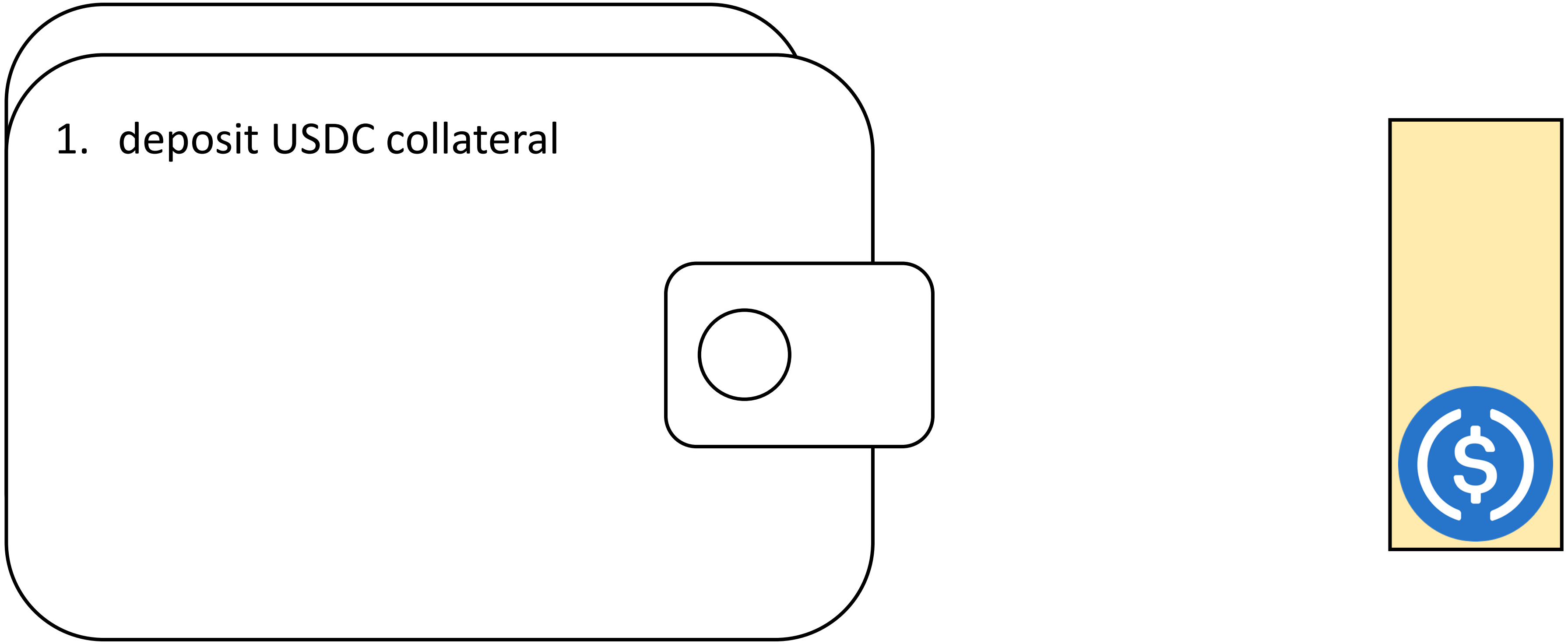
27 Nov 22

Avi Eisenberg
starts attack

Avi Eisenberg’s attack

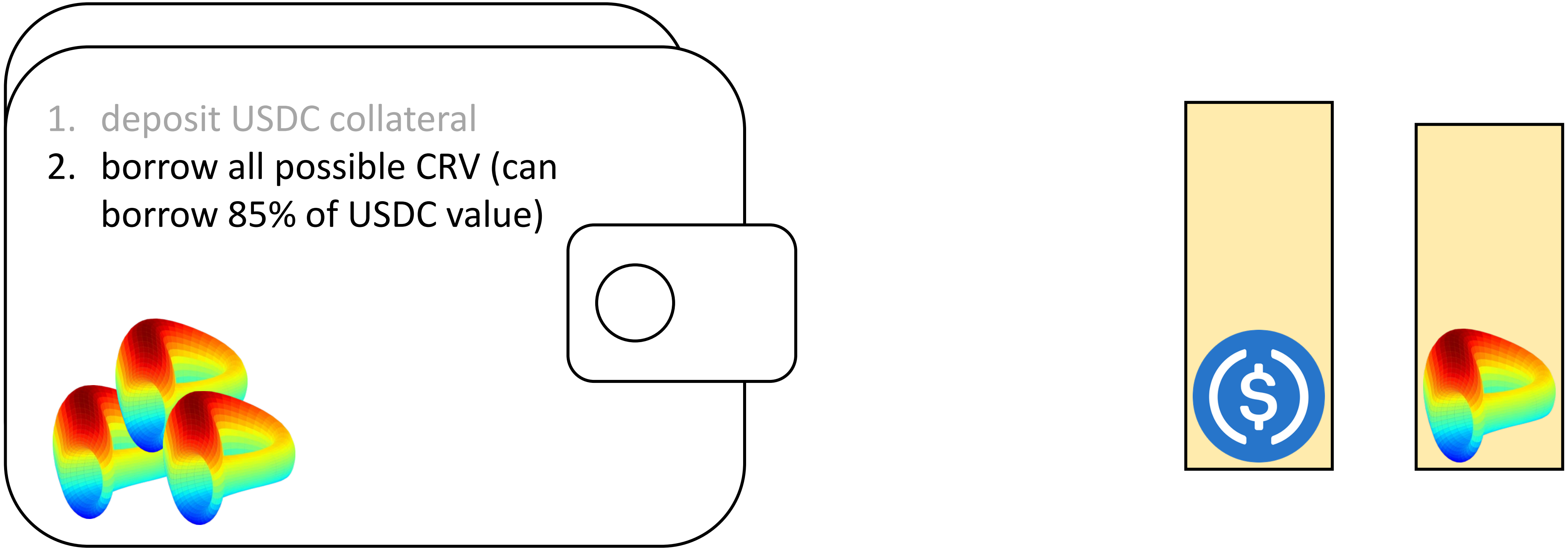


Avi Eisenberg’s attack



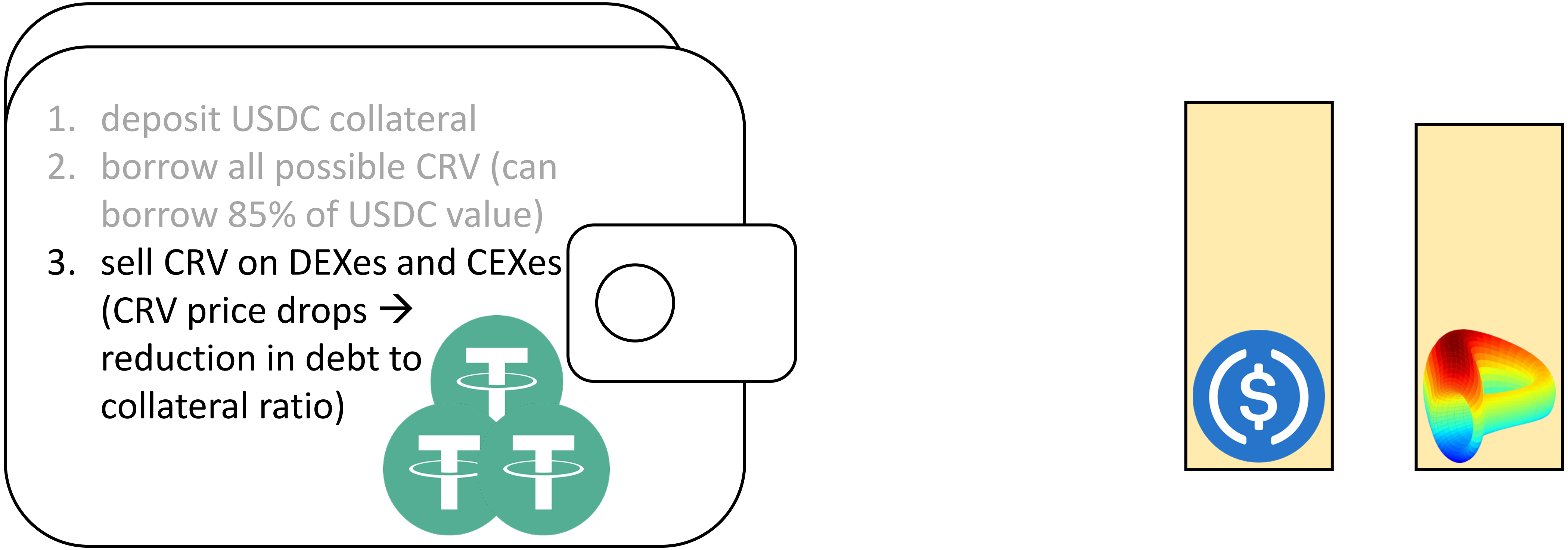
1. deposit USDC collateral

Avi Eisenberg’s attack



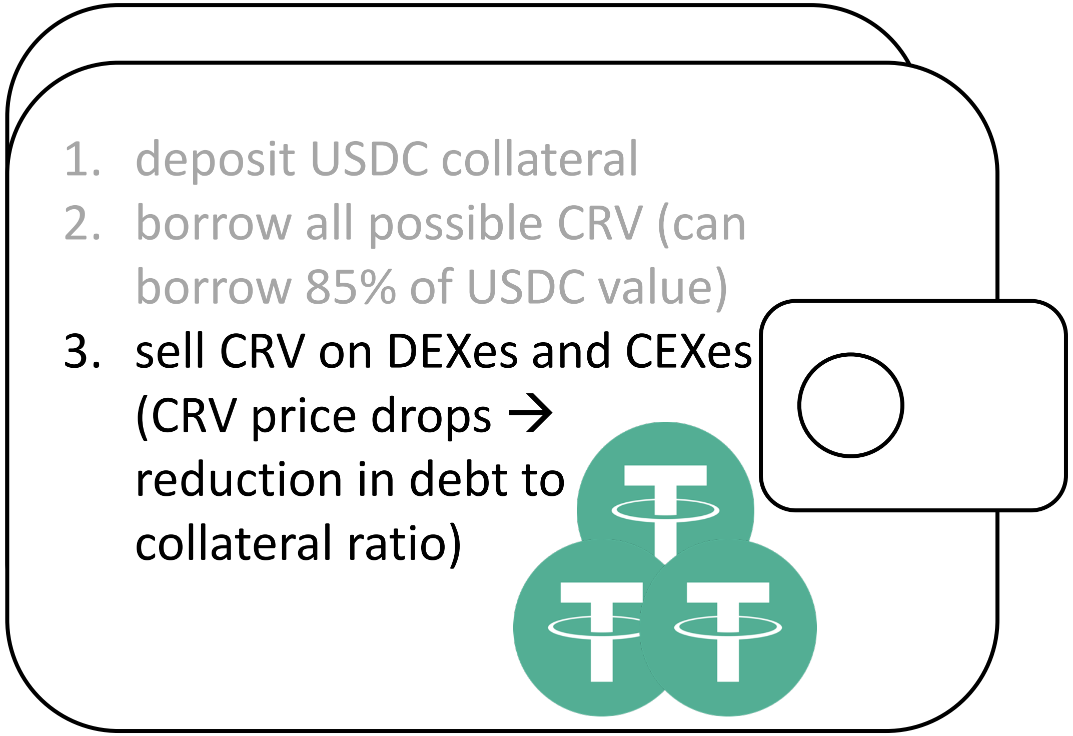
1. deposit USDC collateral
2. borrow all possible CRV (can borrow 85% of USDC value)

Avi Eisenberg’s attack

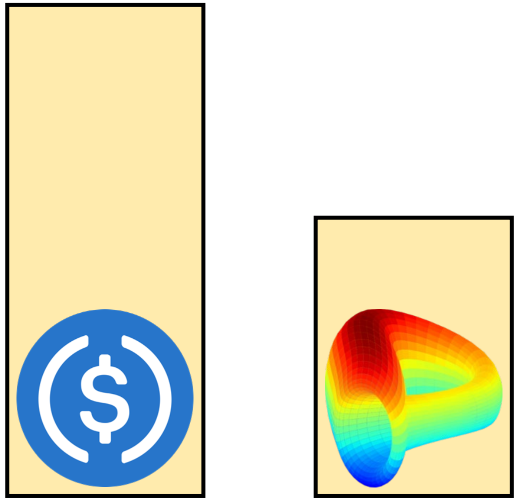


1. deposit USDC collateral
2. borrow all possible CRV (can borrow 85% of USDC value)
3. sell CRV on DEXes and CEXes (CRV price drops → reduction in debt to collateral ratio)

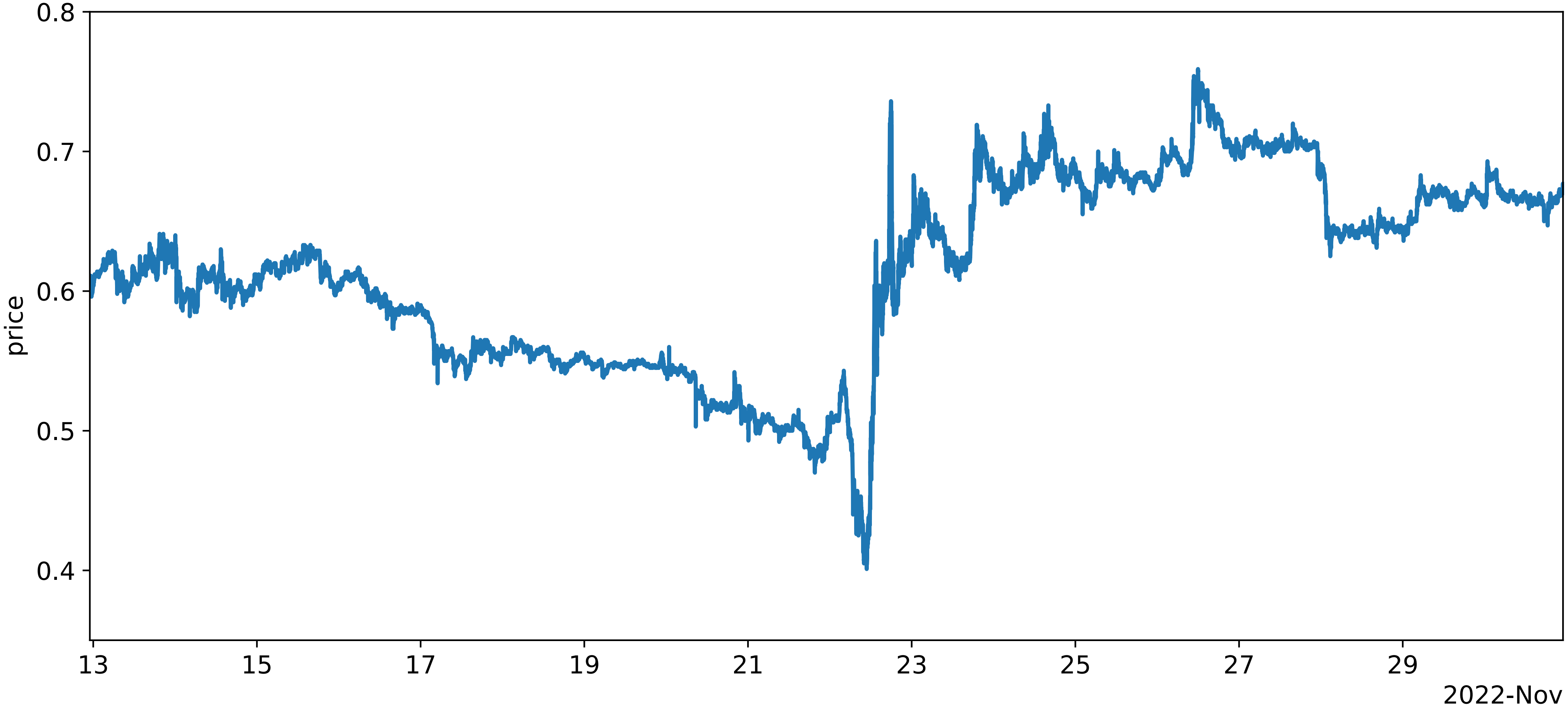
Avi Eisenberg’s attack



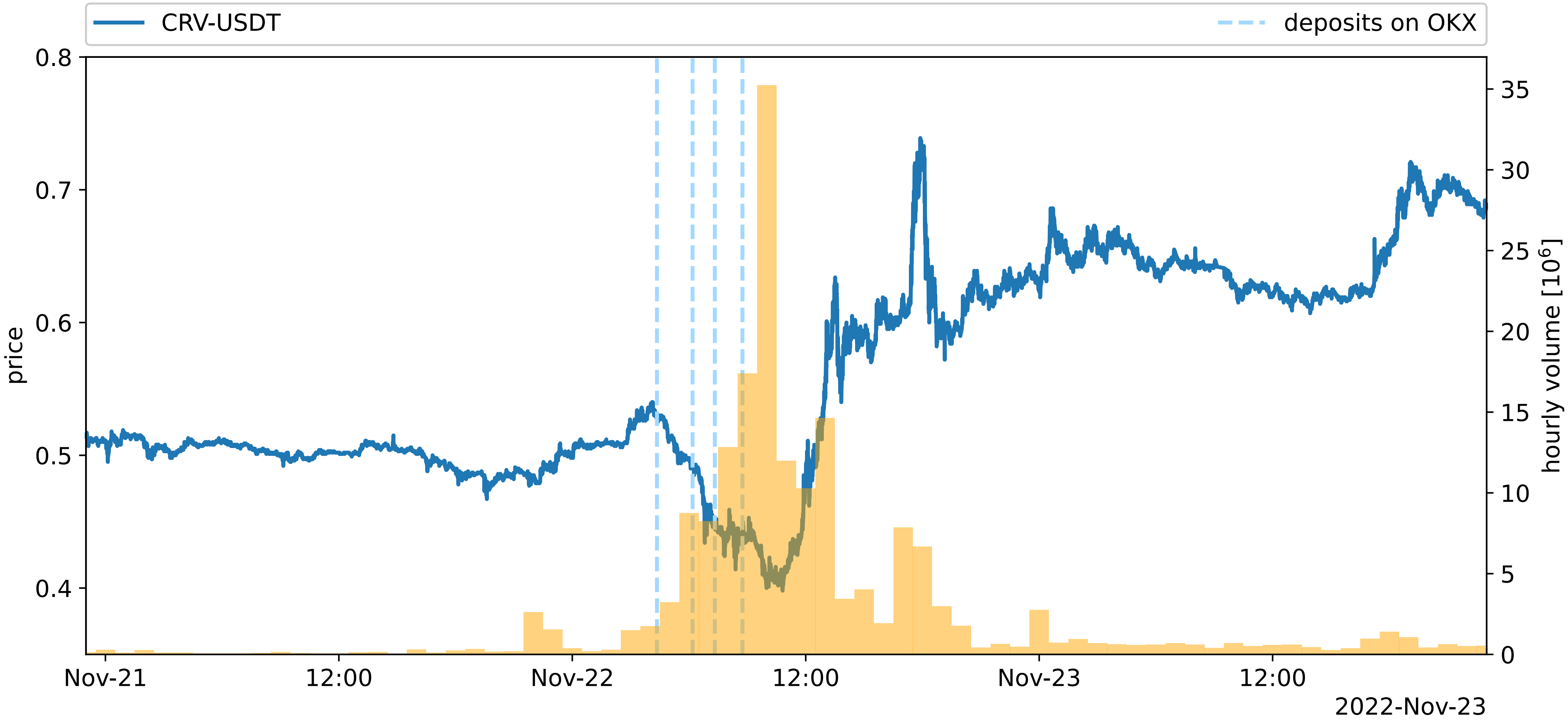
1. deposit USDC collateral
2. borrow all possible CRV (can borrow 85% of USDC value)
3. sell CRV on DEXes and CEXes (CRV price drops → reduction in debt to collateral ratio)



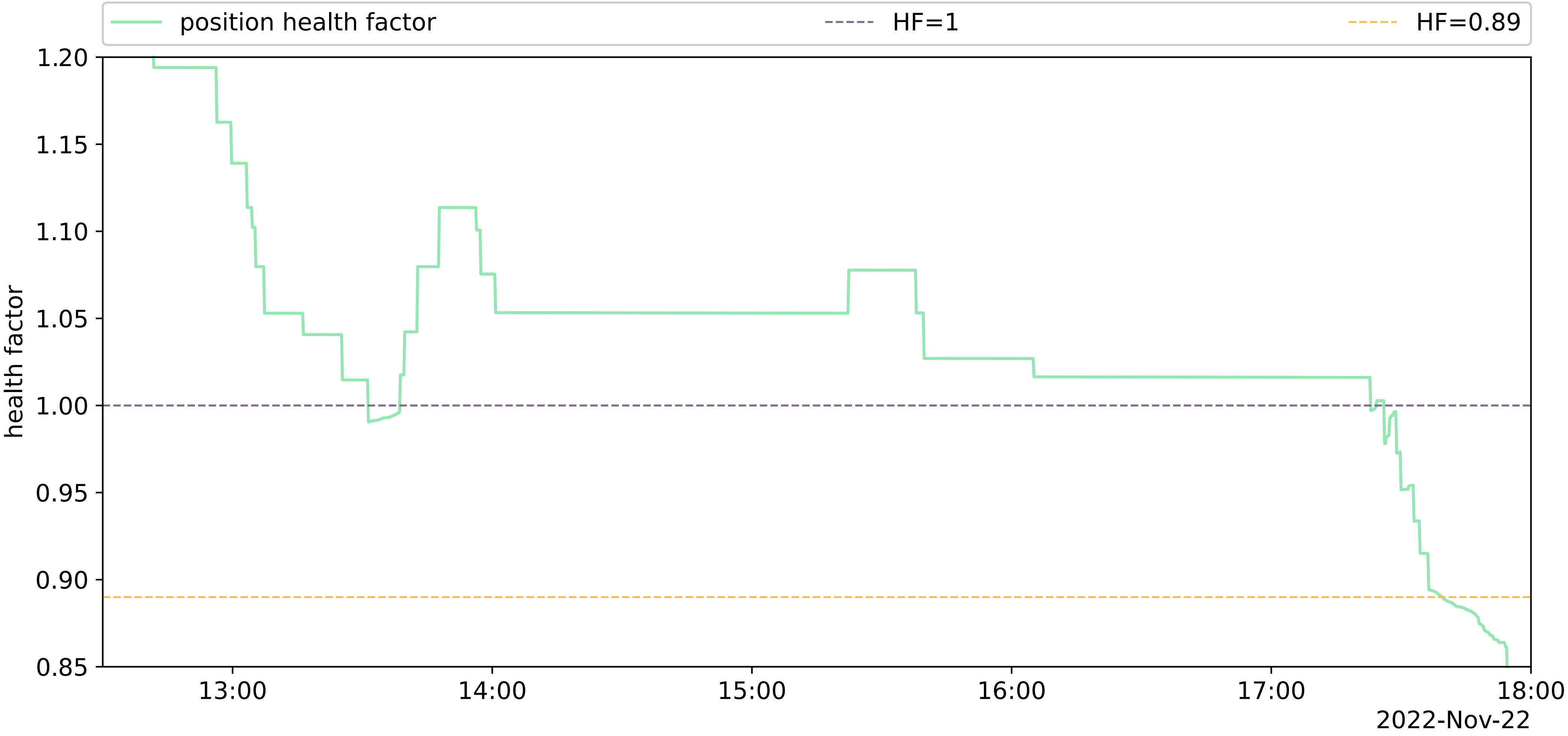
CRV price



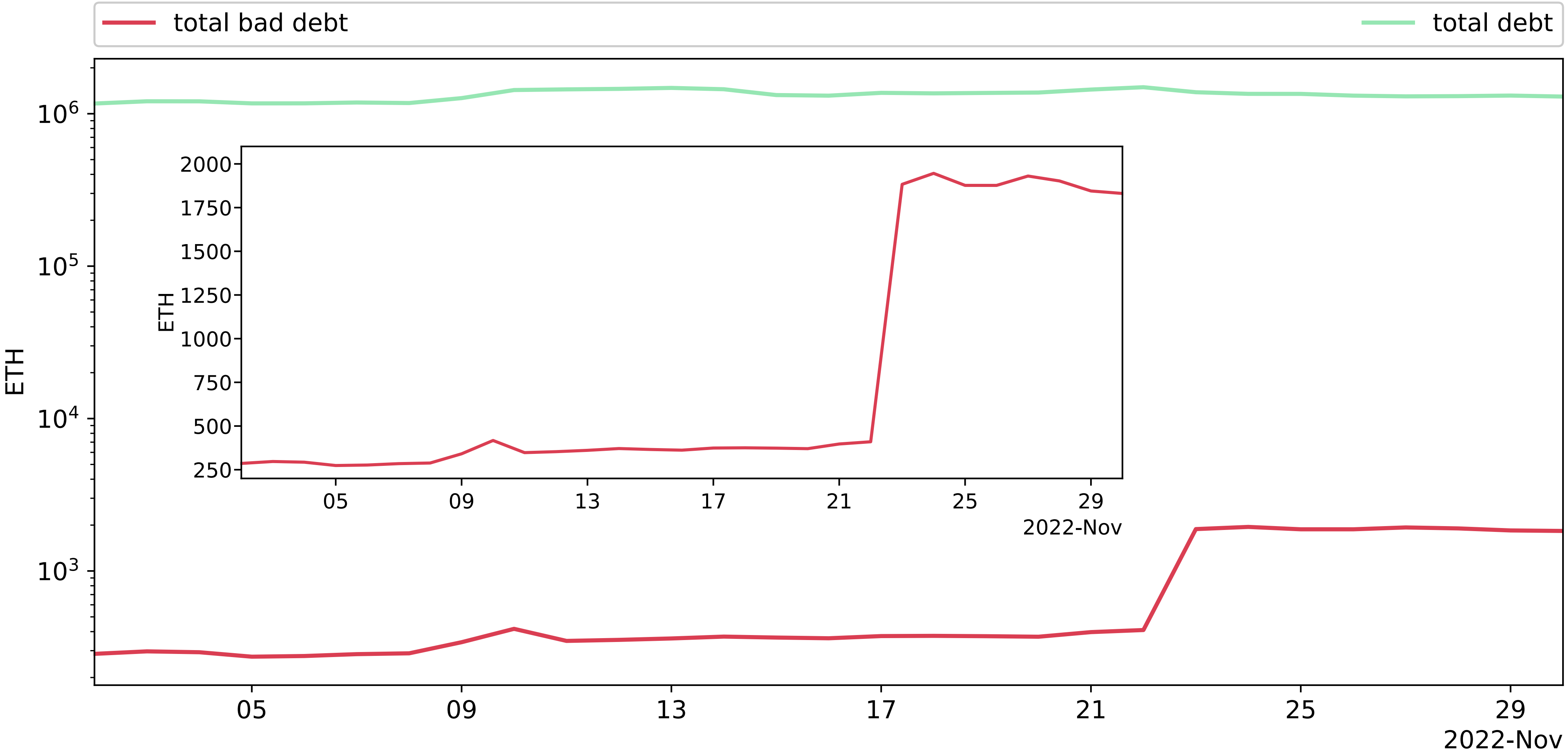
CRV price and volume on OKX

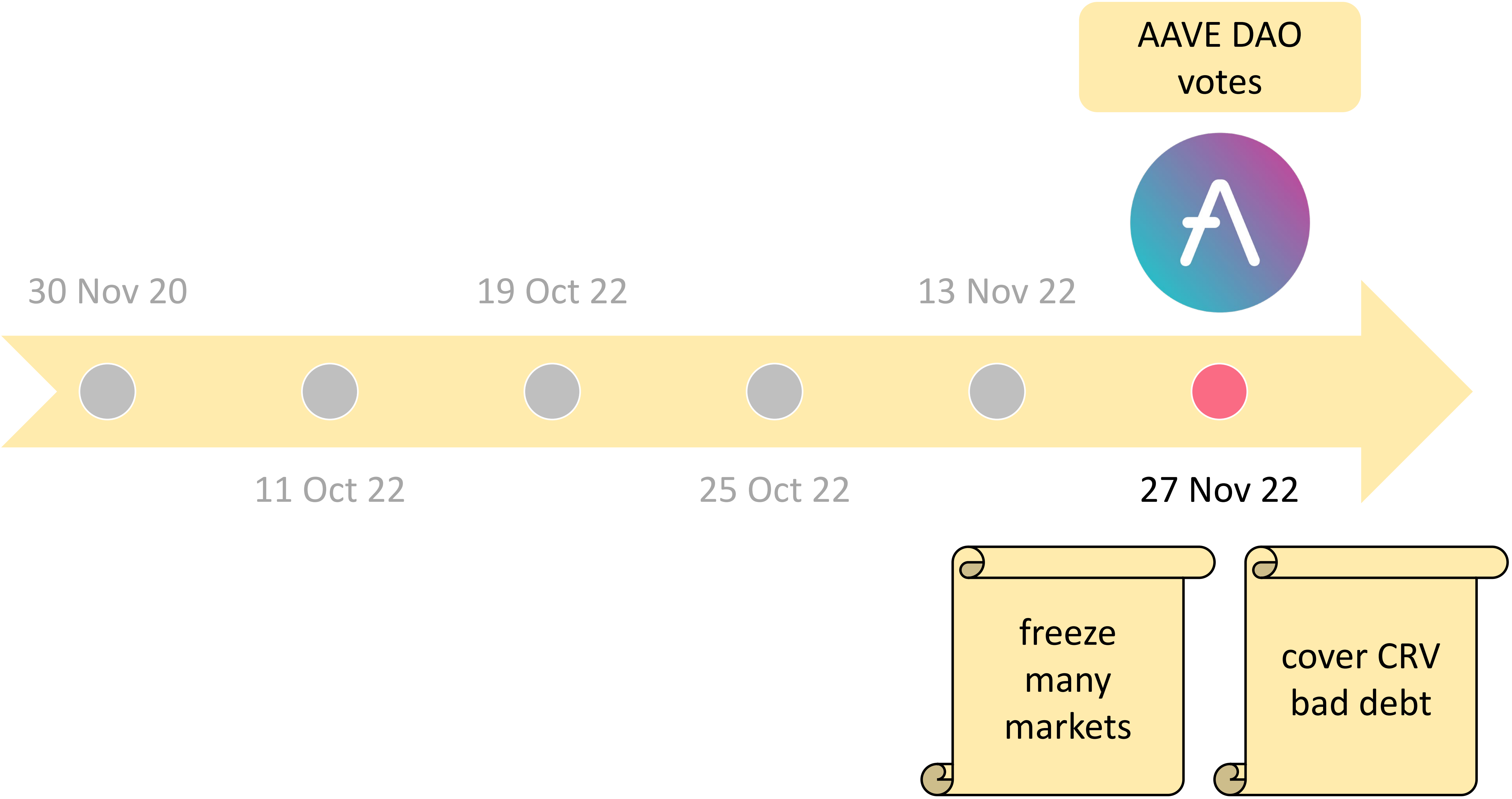


Avi Eisenberg’s position



Bad debt on Aave





AAVE DAO votes

30 Nov 20

11 Oct 22

19 Oct 22

25 Oct 22

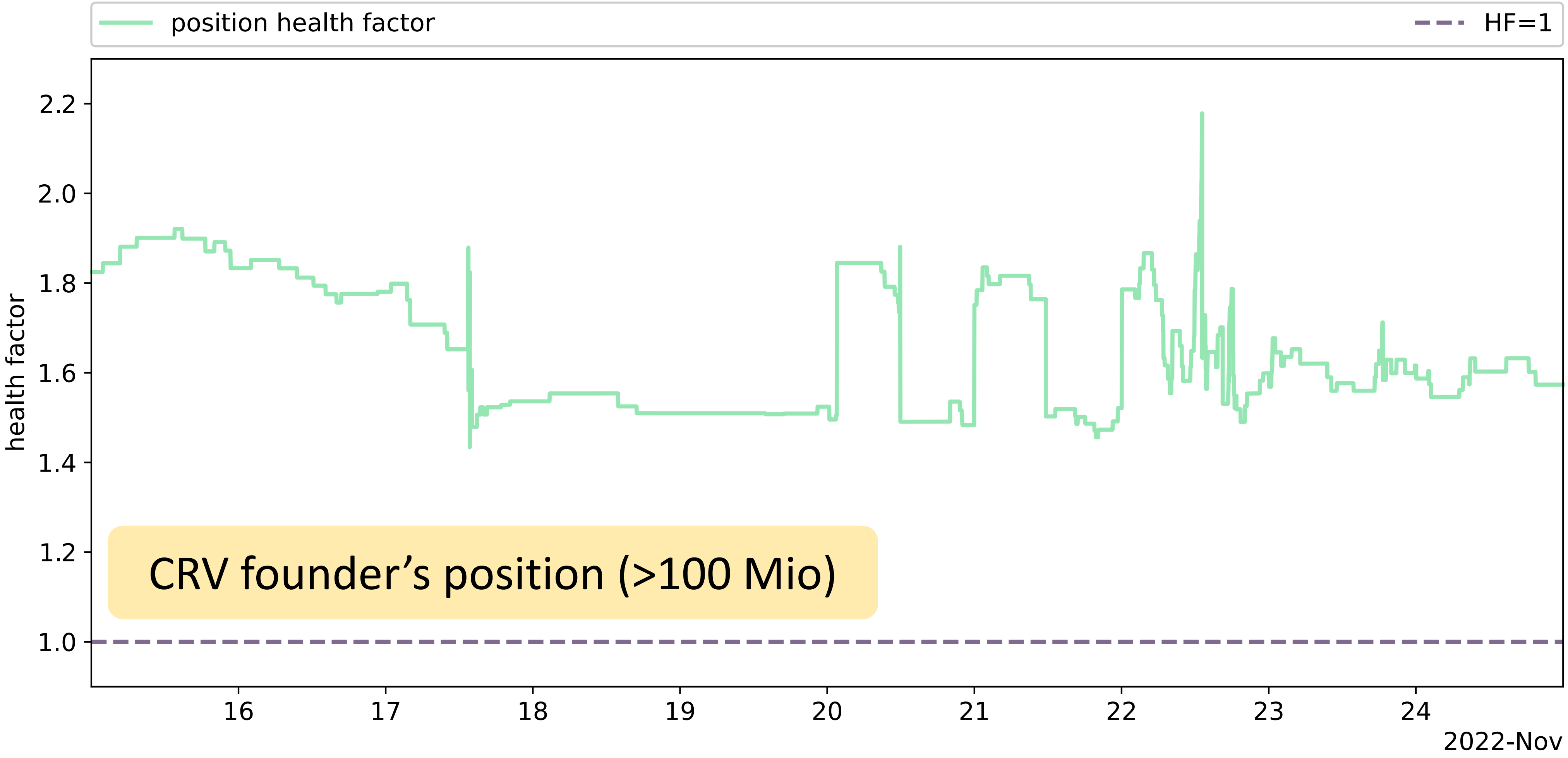
13 Nov 22

27 Nov 22

freeze many markets

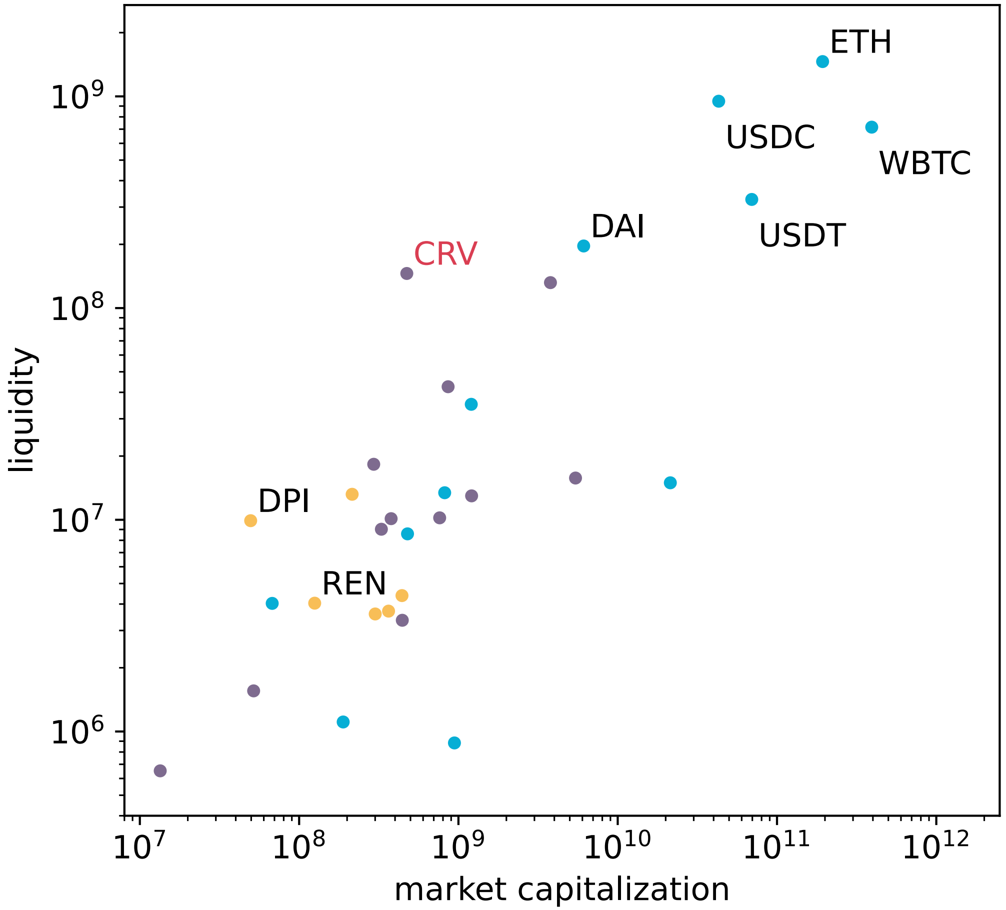
cover CRV bad debt

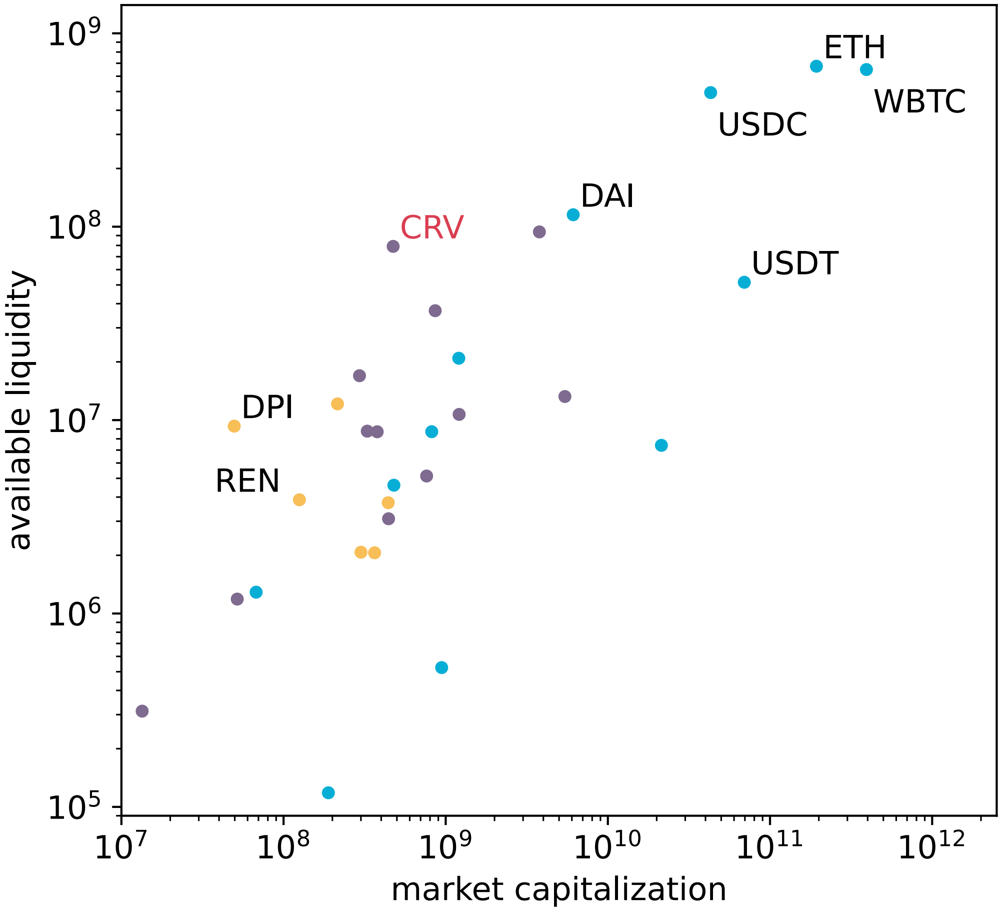
Why CRV?



CRV founder’s position (>100 Mio)

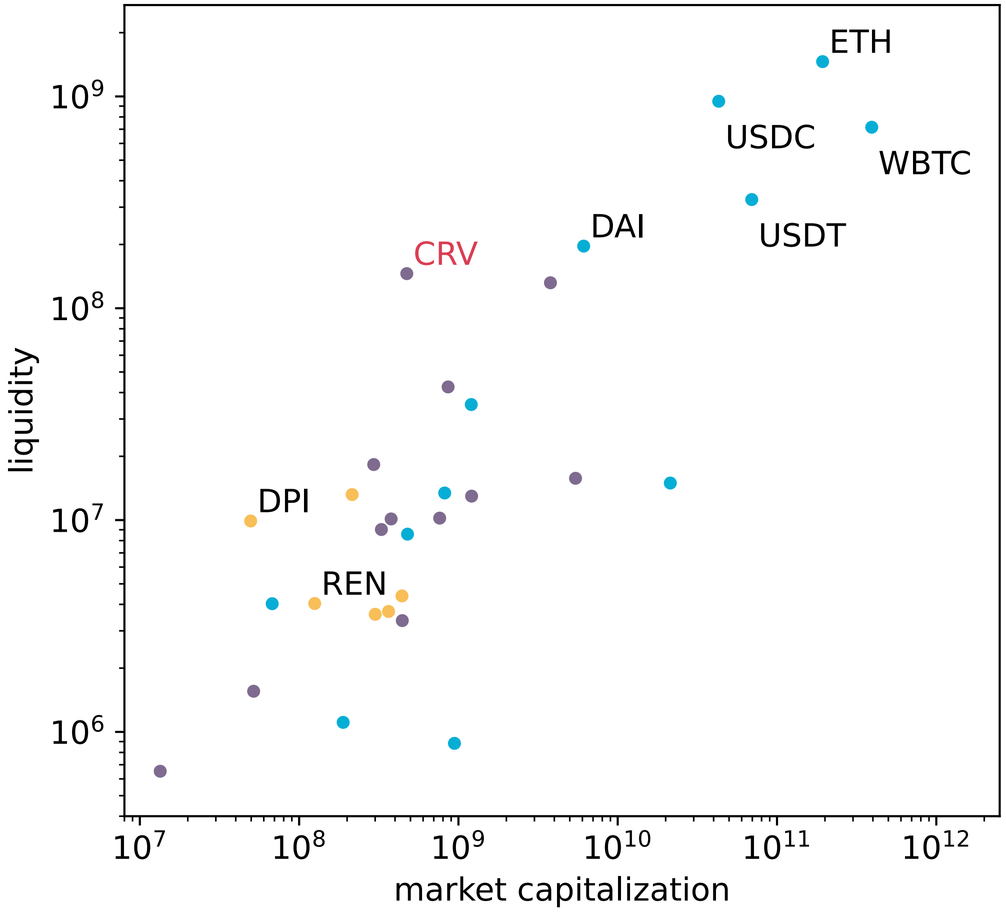
Why CRV?

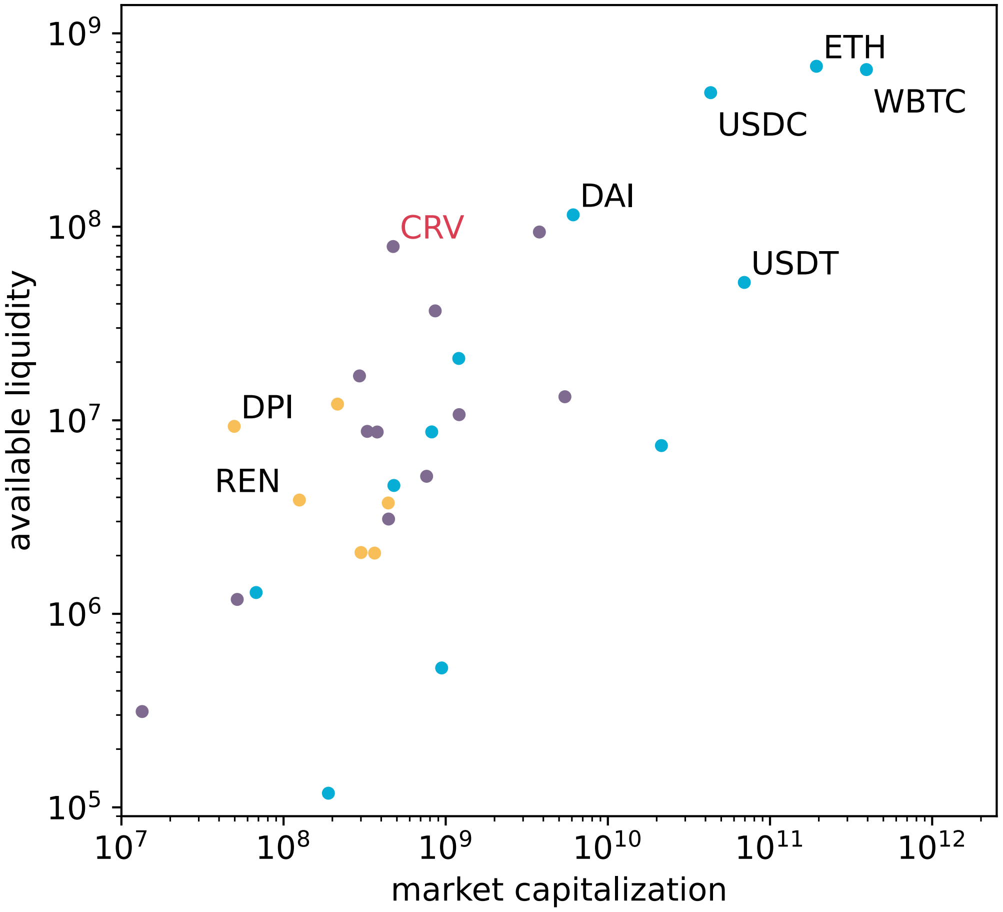

ETH
USDC
WBTC
USDT
DAI
CRV
DPI
REN
liquidity
10^9
10^8
10^7
10^6
10^7
10^8
10^9
10^{10}
10^{11}
10^{12}
market capitalization


ETH
WBTC
USDC
DAI
CRV
USDT
DPI
REN
available liquidity
10^9
10^8
10^7
10^6
10^5
10^7
10^8
10^9
10^{10}
10^{11}
10^{12}
market capitalization

Why CRV?

15% CRV available to borrow

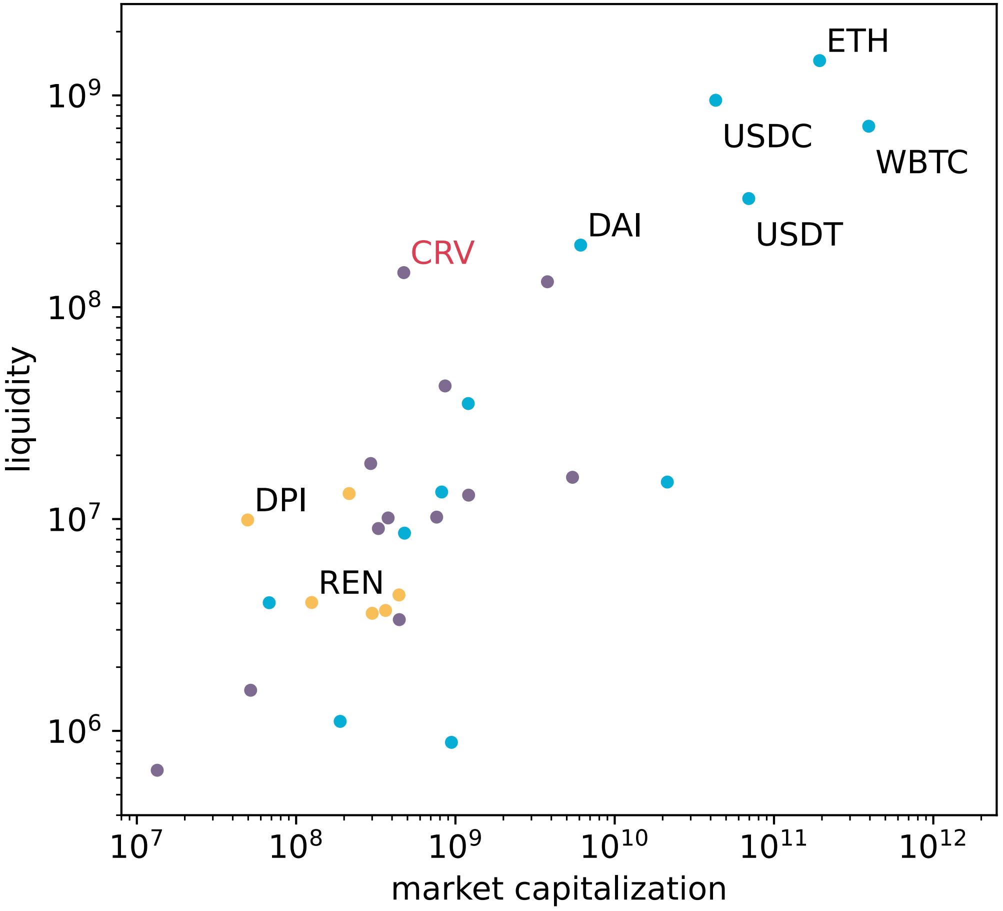


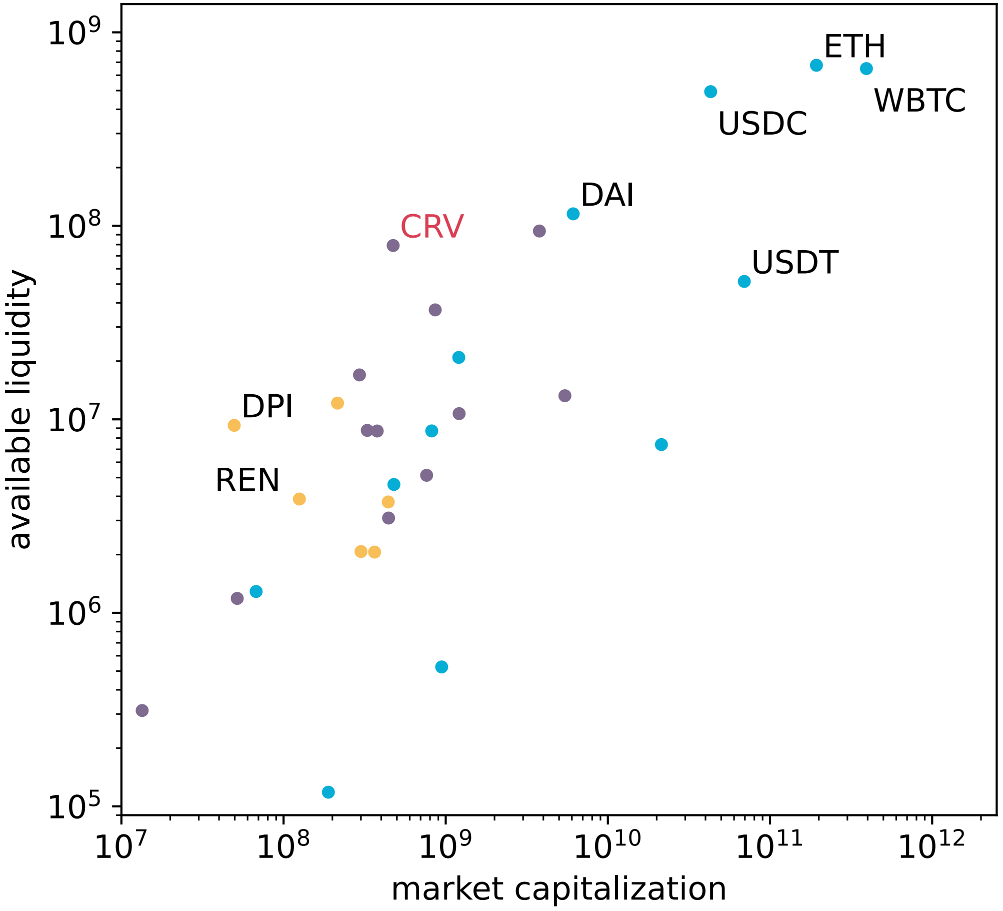


Why CRV?

15% CRV available to borrow

purple assets frozen after the attack





Conclusion

limit scope

increase margin requirement

compromise decentralization

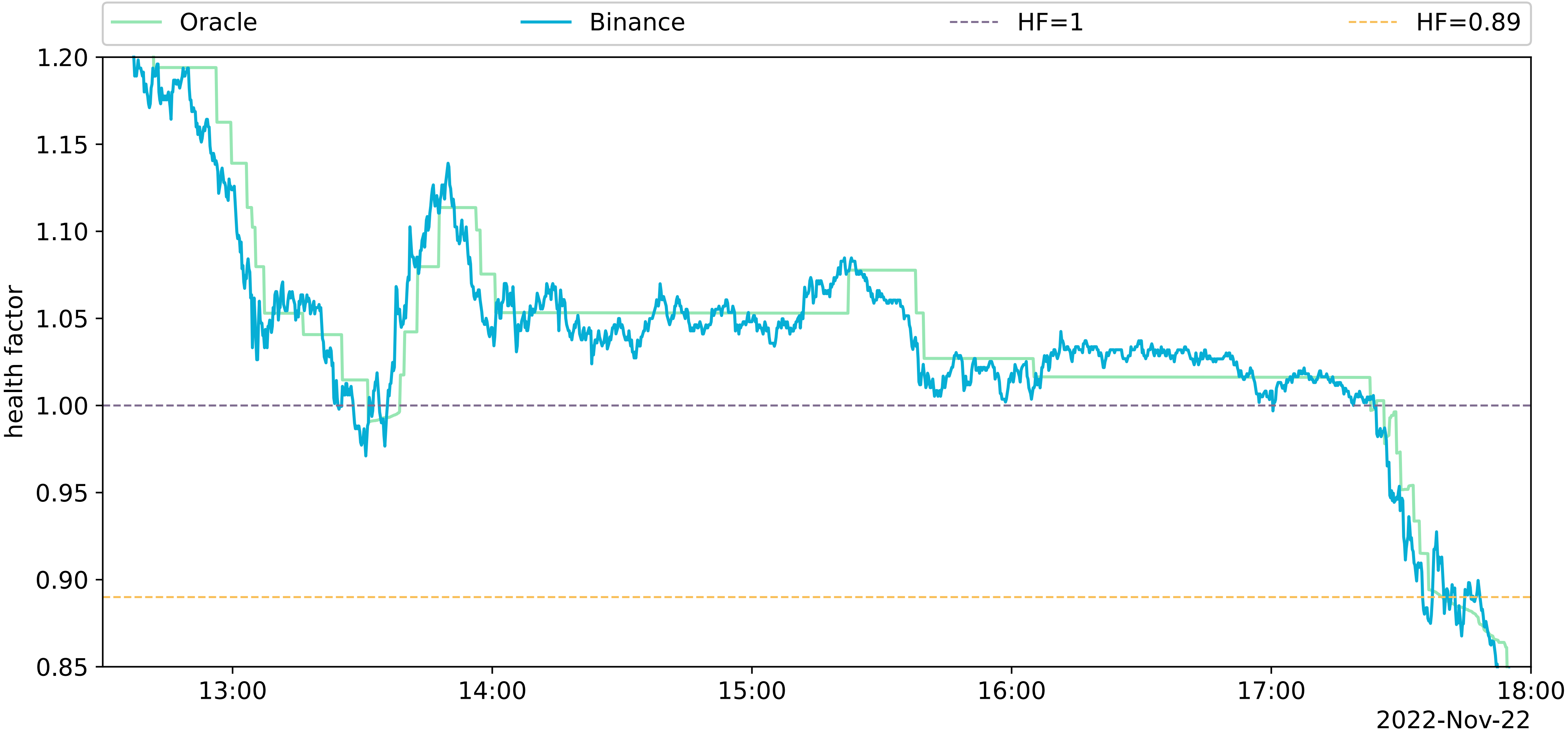
Thank You!

Questions & Comments?

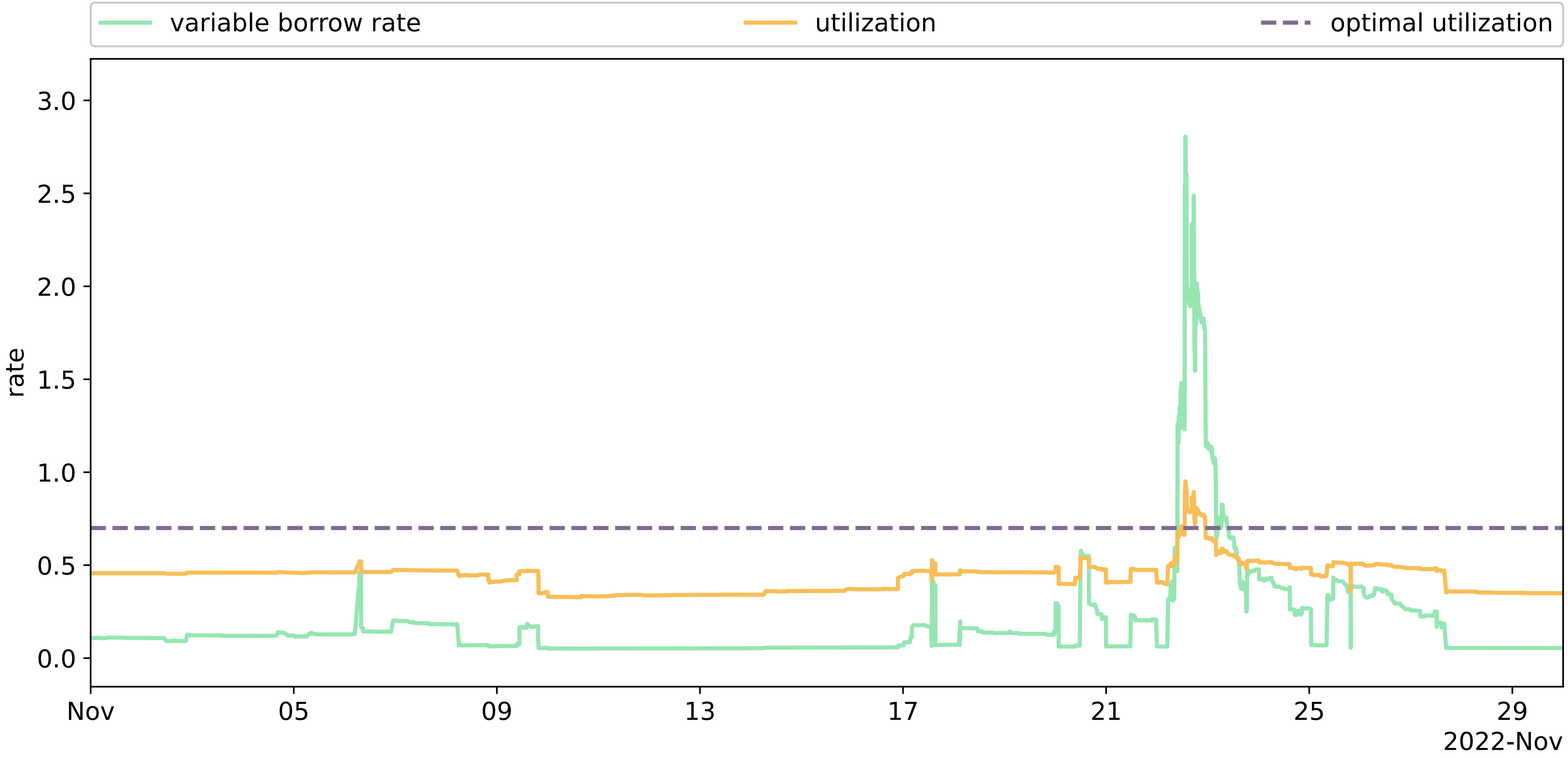
@liobaheimbach

hlioba@ethz.ch

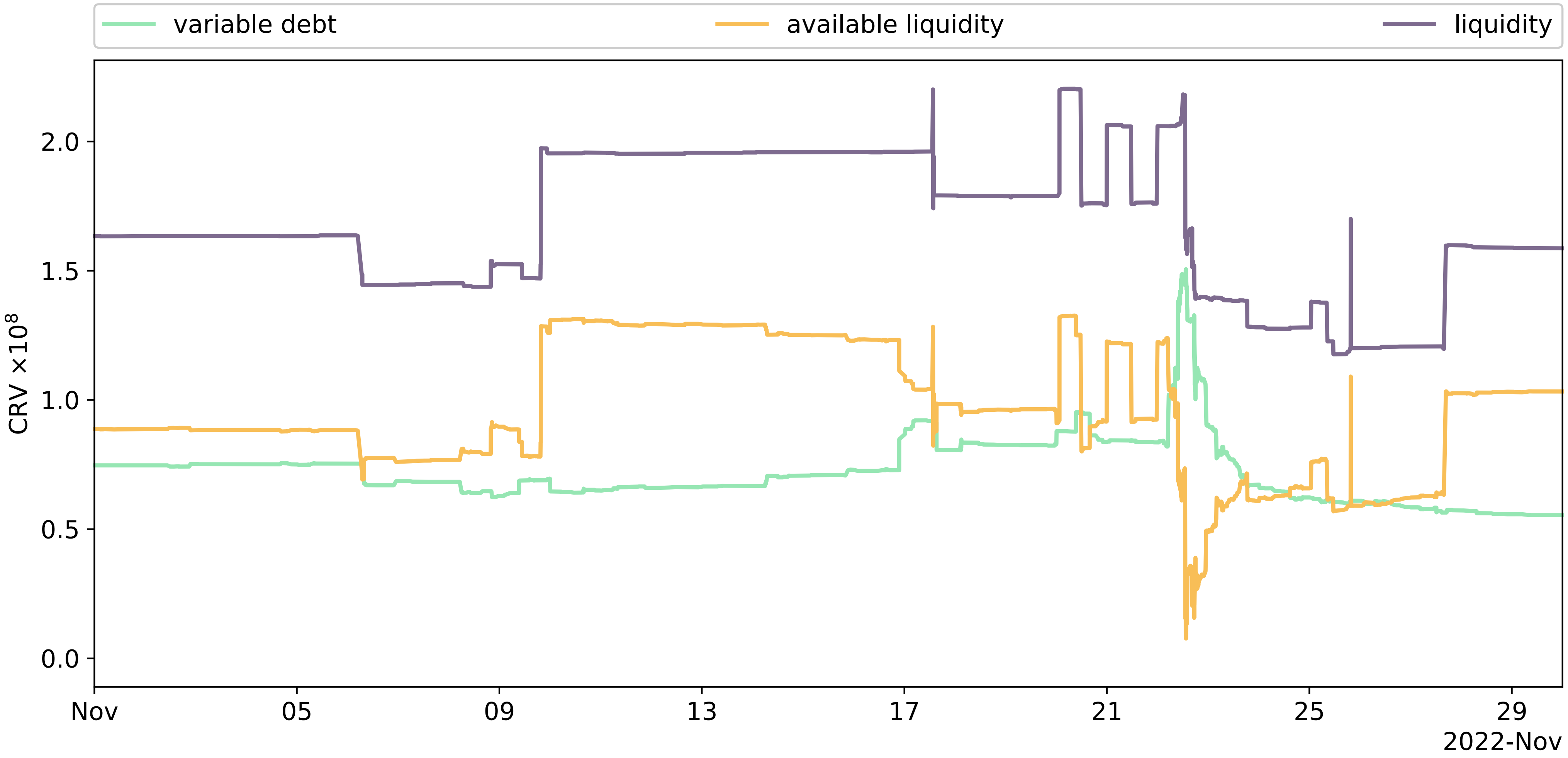
Avi Eisenberg’s position



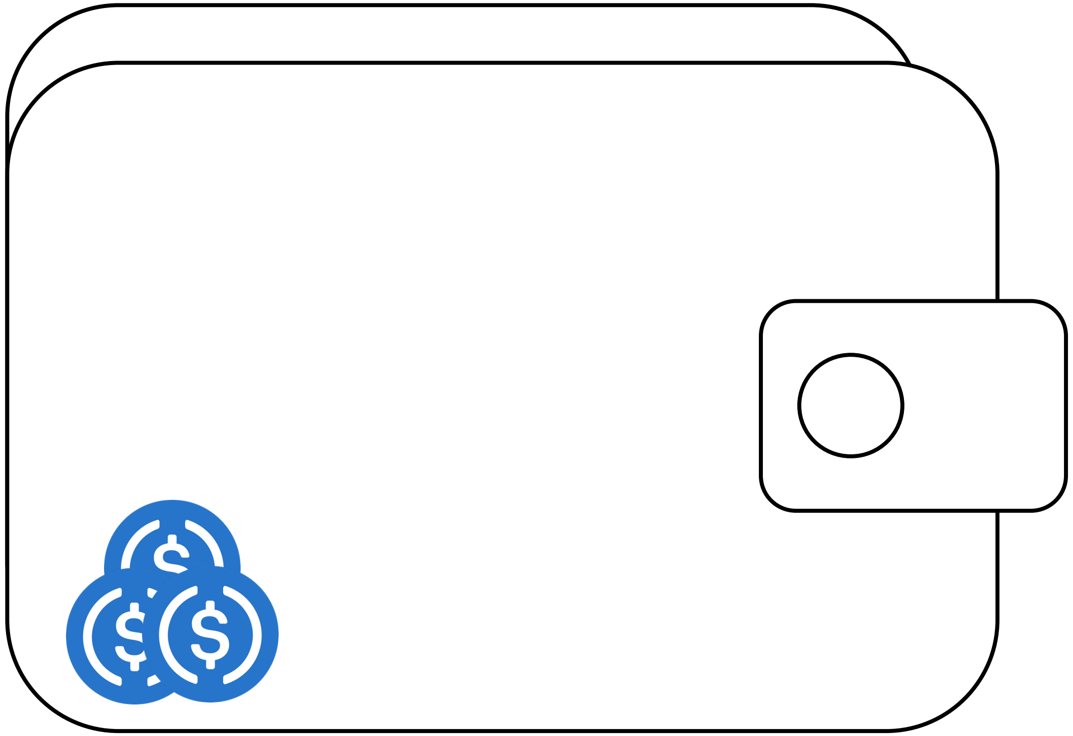
AAVE rates and utilization



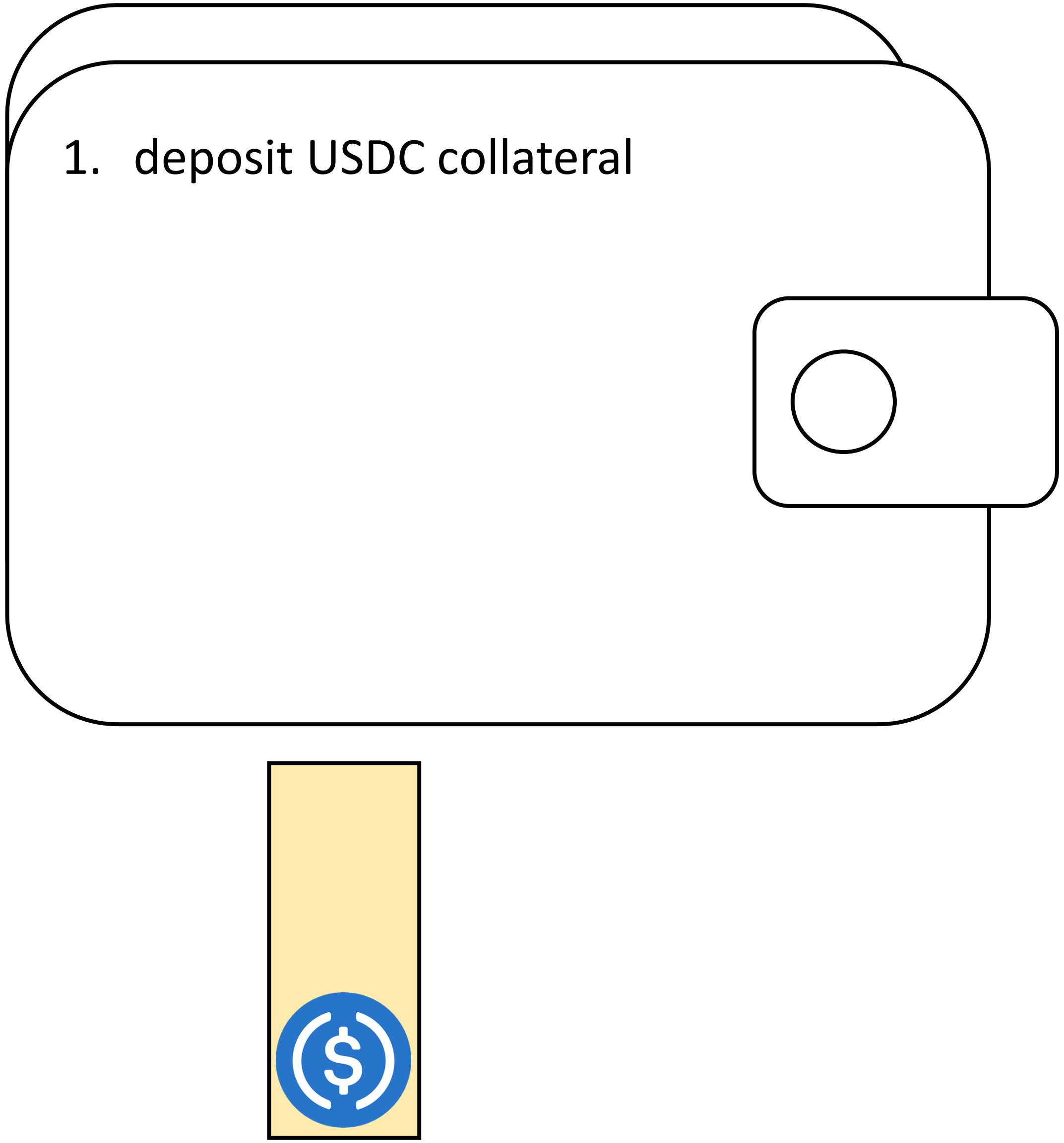
AAVE rates


variable debt
available liquidity
liquidity
CRV ×10^8
0.0
0.5
1.0
1.5
2.0
Nov
05
09
13
17
21
25
29
2022-Nov

Avi Eisenberg’s proposed attack

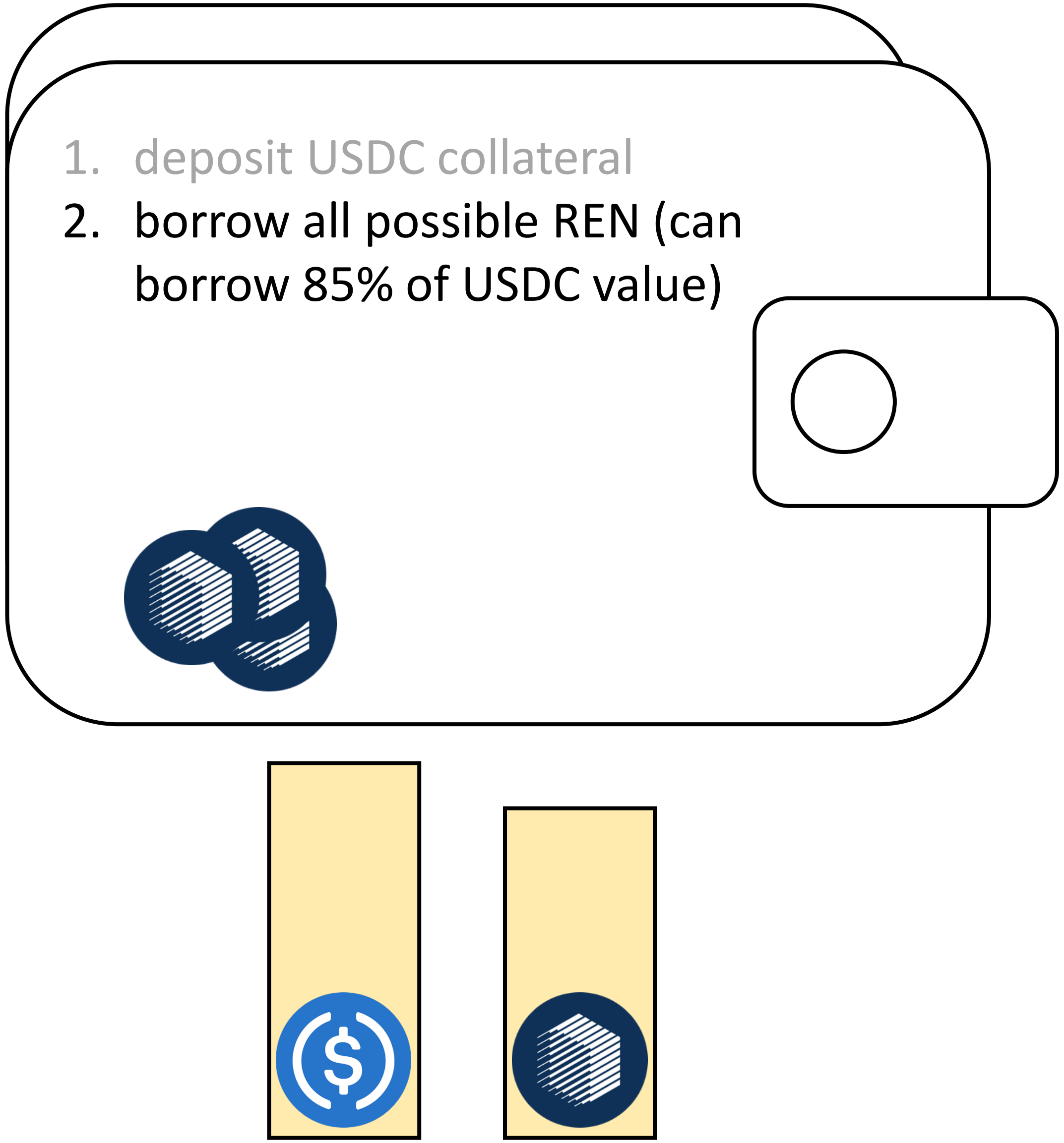


Avi Eisenberg’s proposed attack



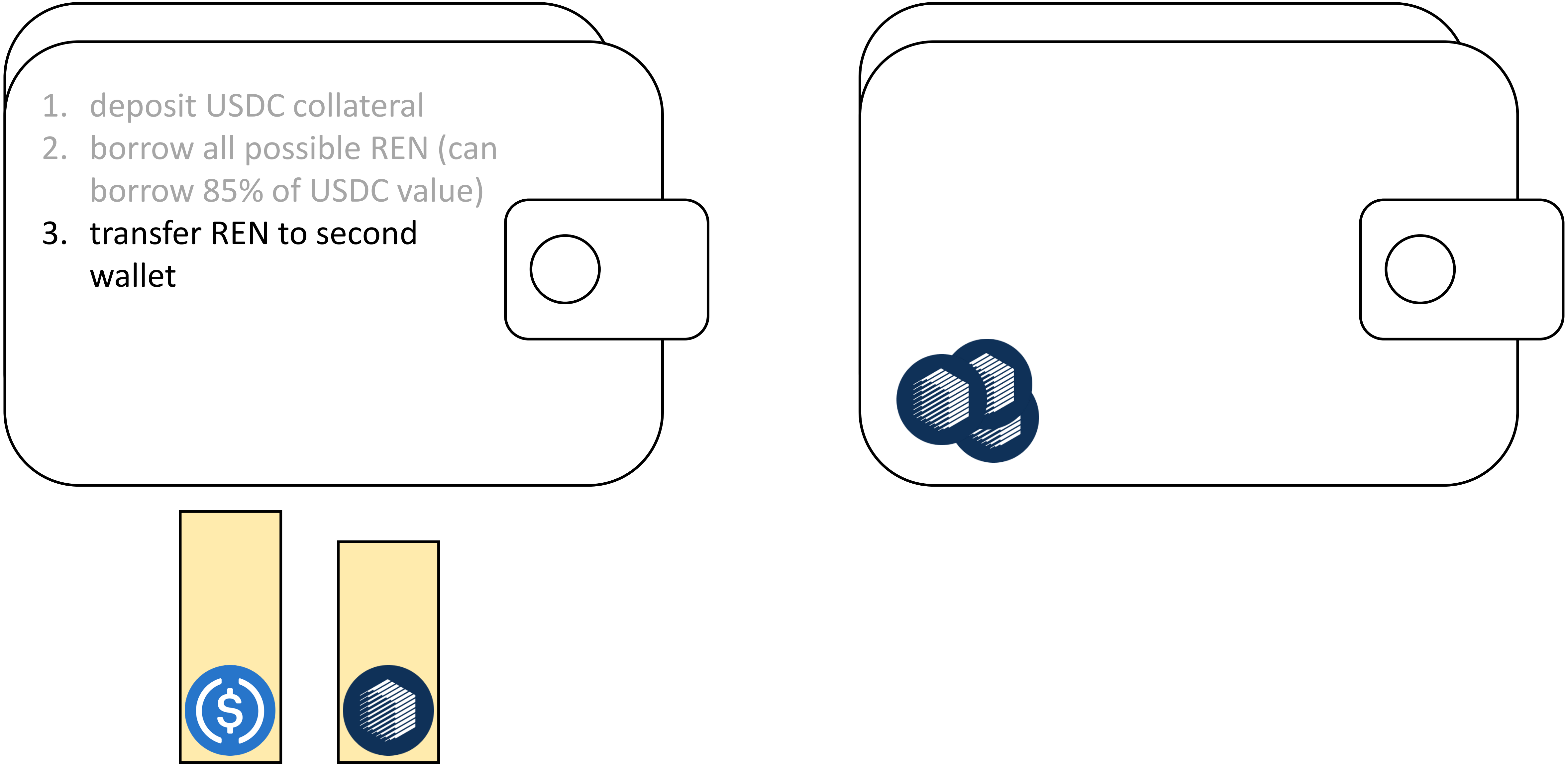
1. deposit USDC collateral

Avi Eisenberg’s proposed attack



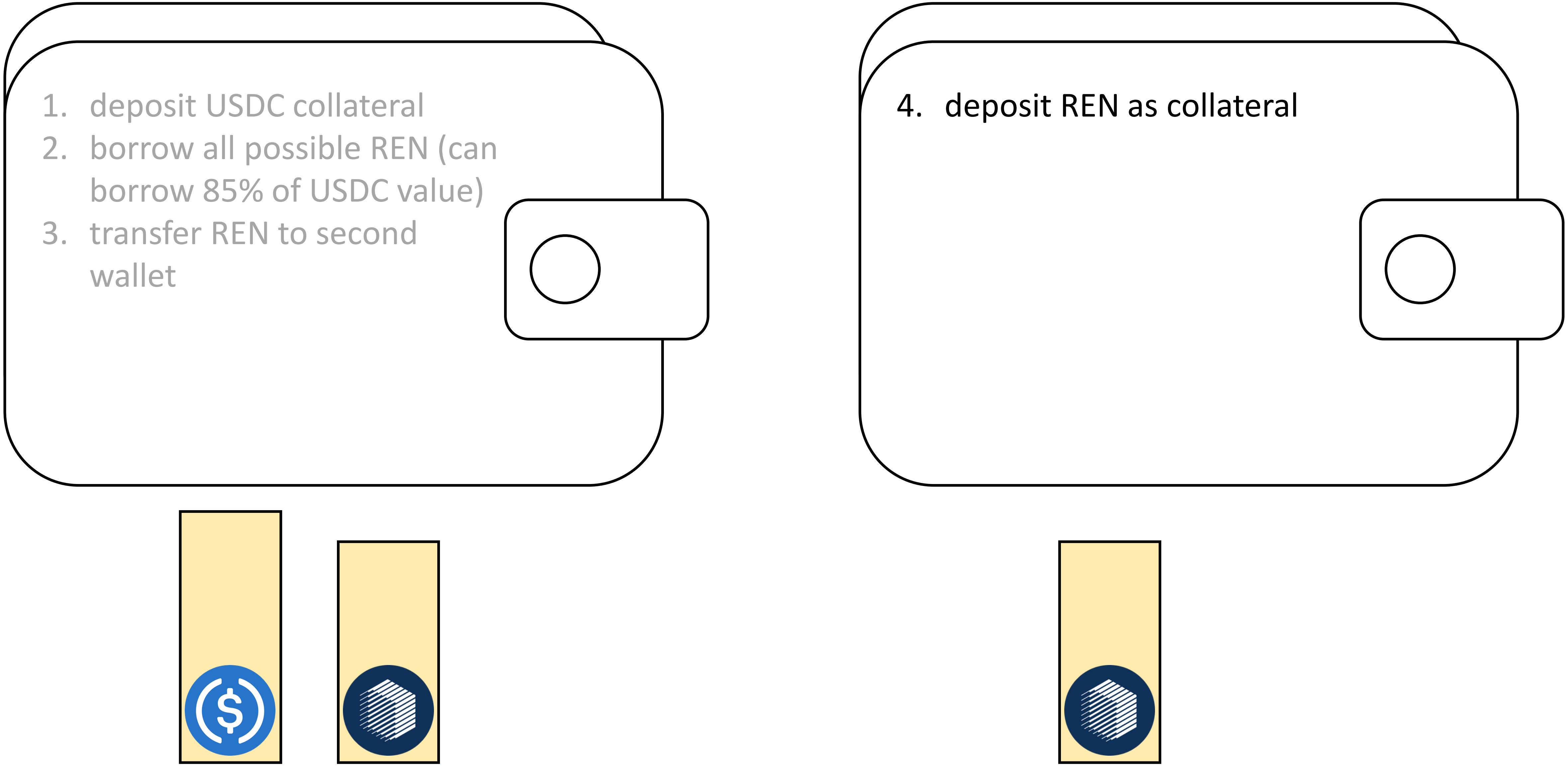
1. deposit USDC collateral
2. borrow all possible REN (can borrow 85% of USDC value)

Avi Eisenberg’s proposed attack



1. deposit USDC collateral
2. borrow all possible REN (can borrow 85% of USDC value)
3. transfer REN to second wallet

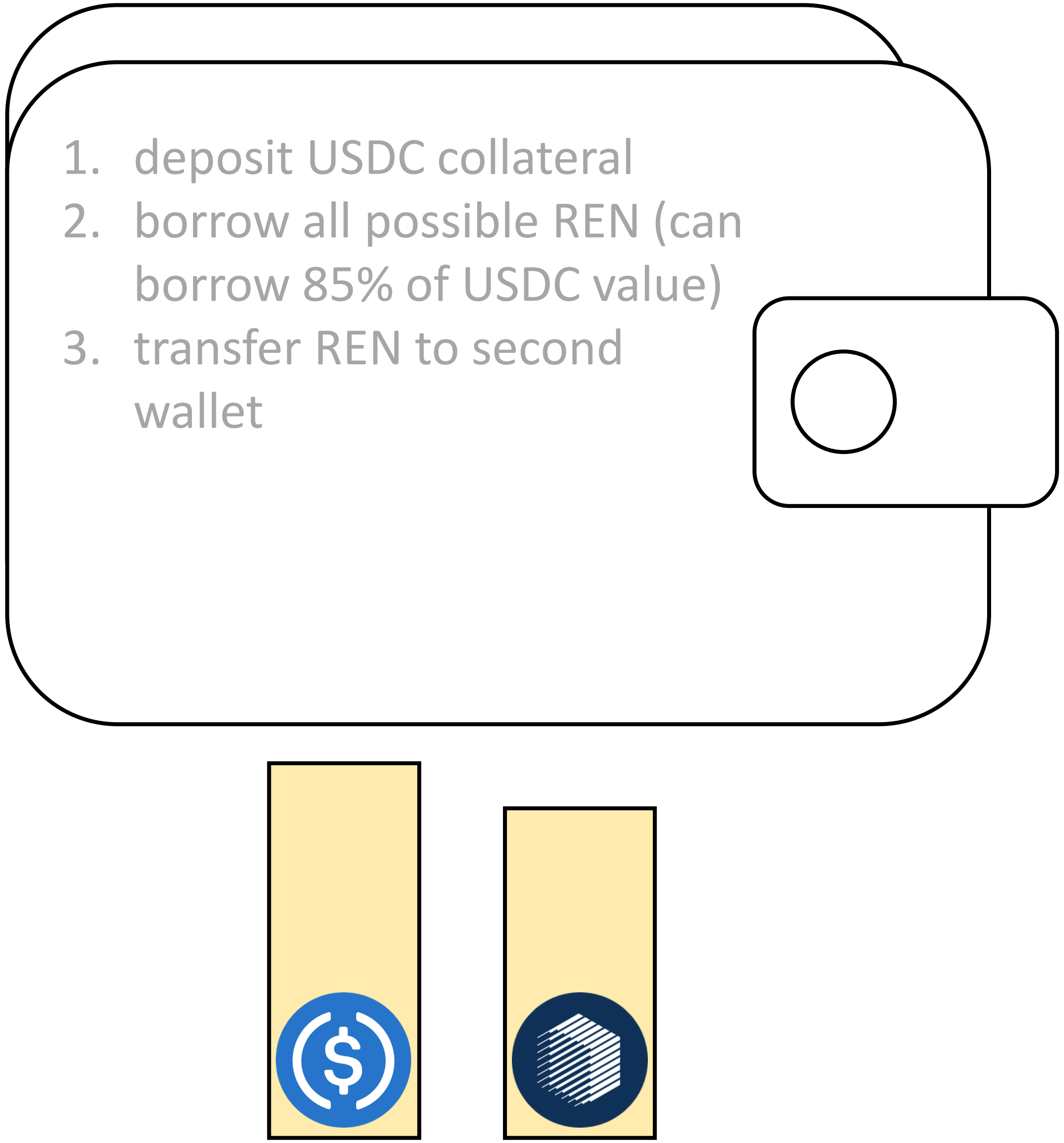
Avi Eisenberg’s proposed attack



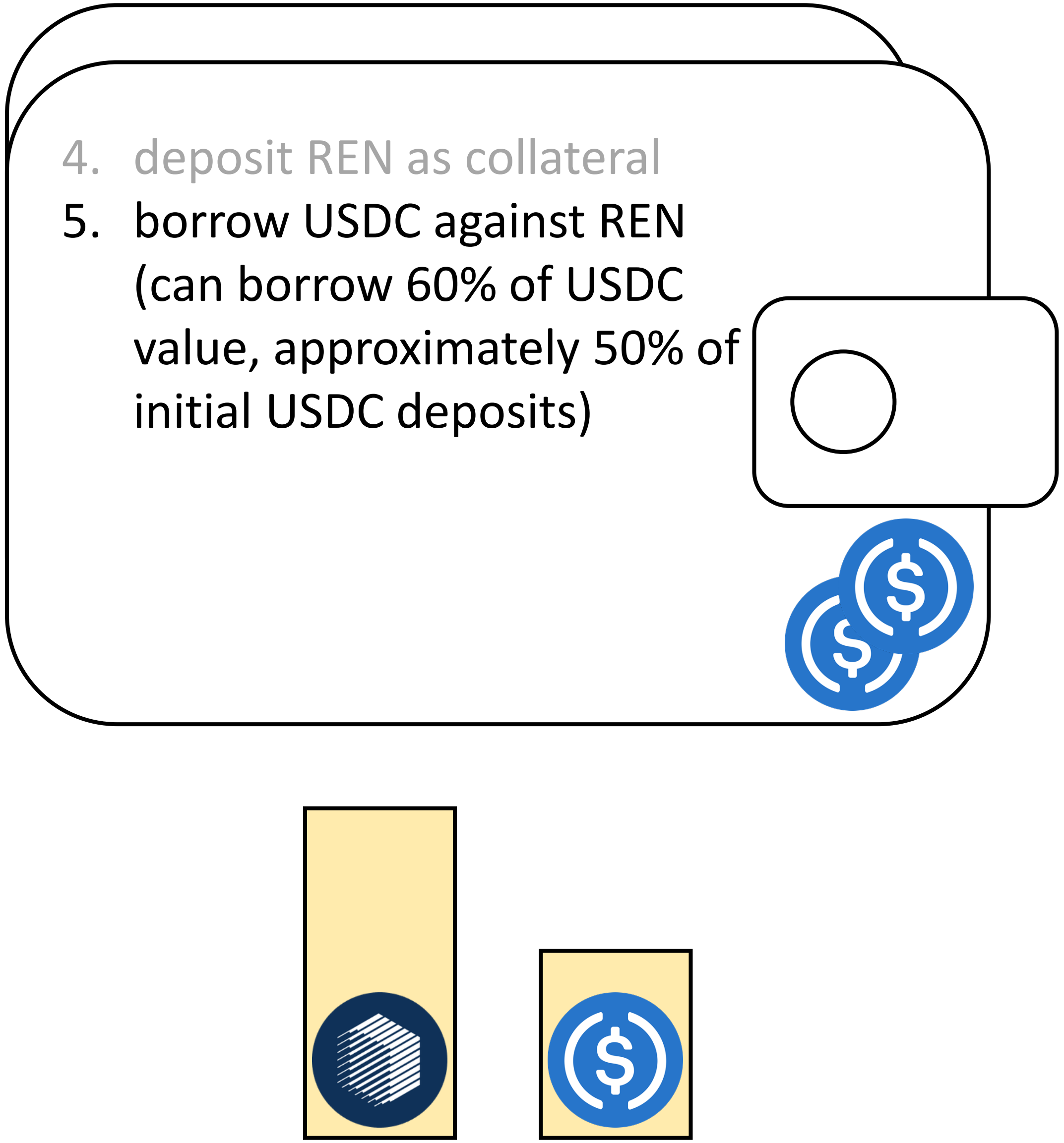
1. deposit USDC collateral
2. borrow all possible REN (can borrow 85% of USDC value)
3. transfer REN to second wallet

4. deposit REN as collateral

Avi Eisenberg’s proposed attack

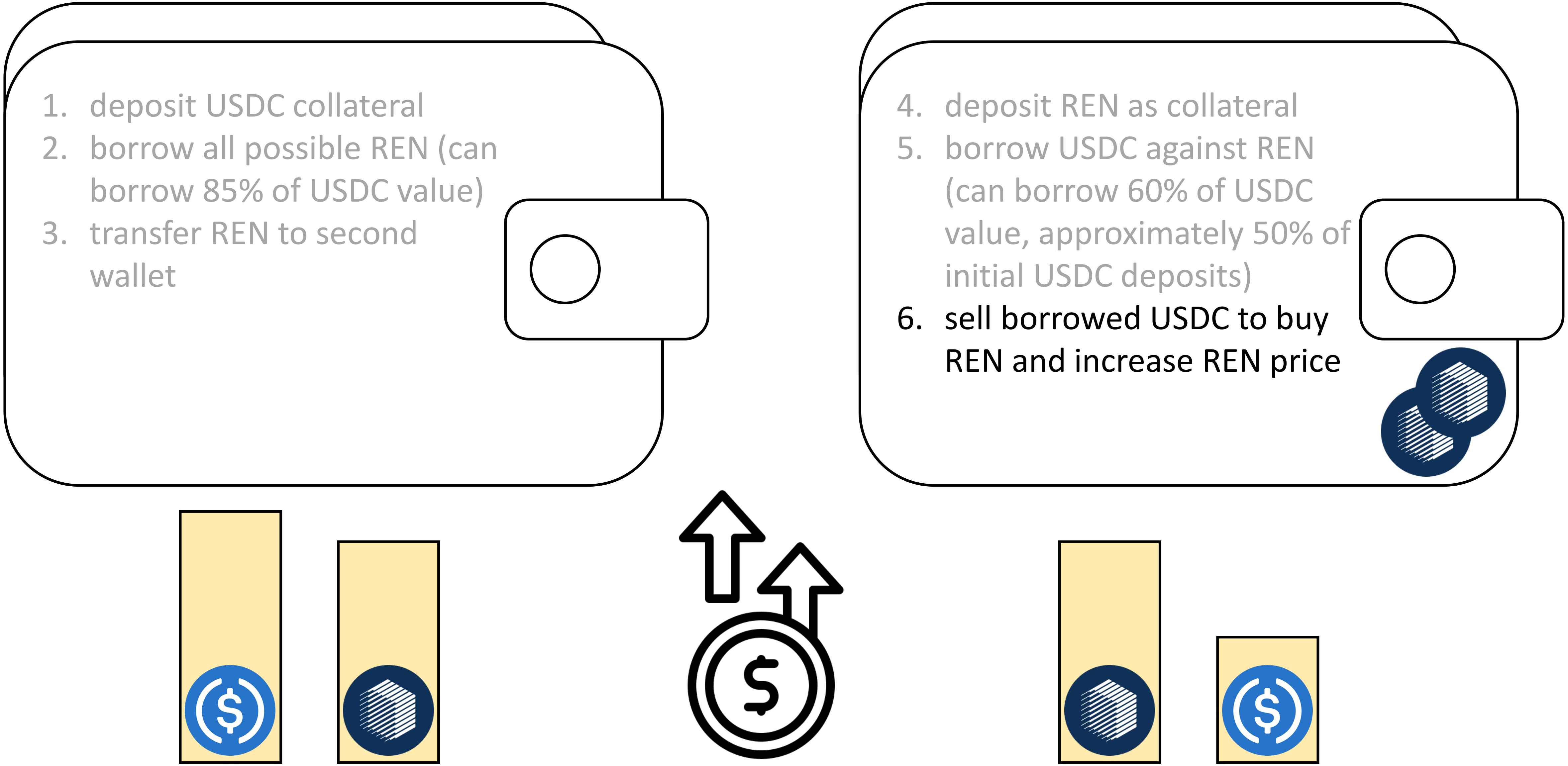


1. deposit USDC collateral
2. borrow all possible REN (can borrow 85% of USDC value)
3. transfer REN to second wallet



4. deposit REN as collateral
5. borrow USDC against REN (can borrow 60% of USDC value, approximately 50% of initial USDC deposits)

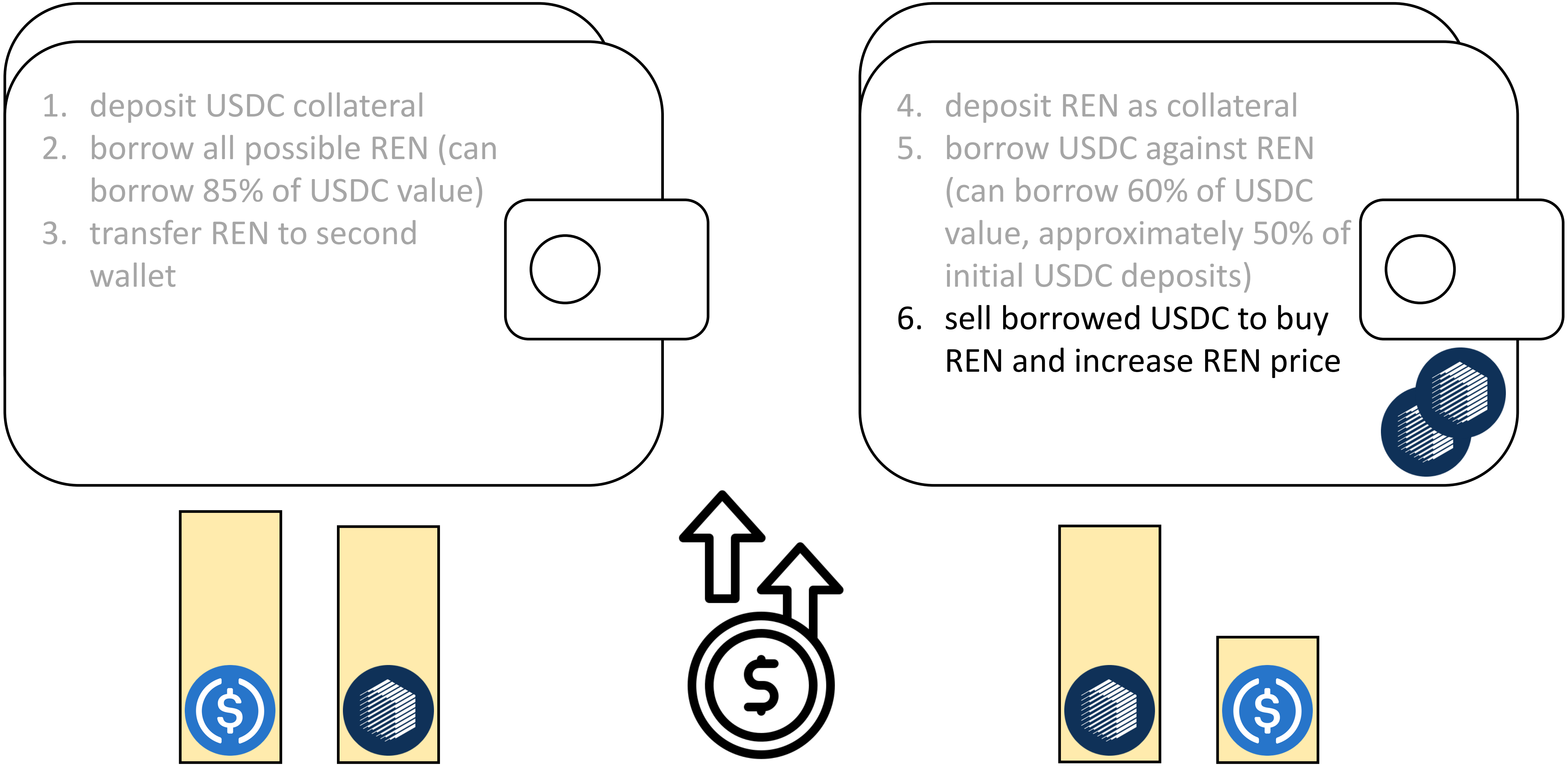
Avi Eisenberg’s proposed attack



1. deposit USDC collateral
2. borrow all possible REN (can borrow 85% of USDC value)
3. transfer REN to second wallet

4. deposit REN as collateral
5. borrow USDC against REN (can borrow 60% of USDC value, approximately 50% of initial USDC deposits)
6. sell borrowed USDC to buy REN and increase REN price

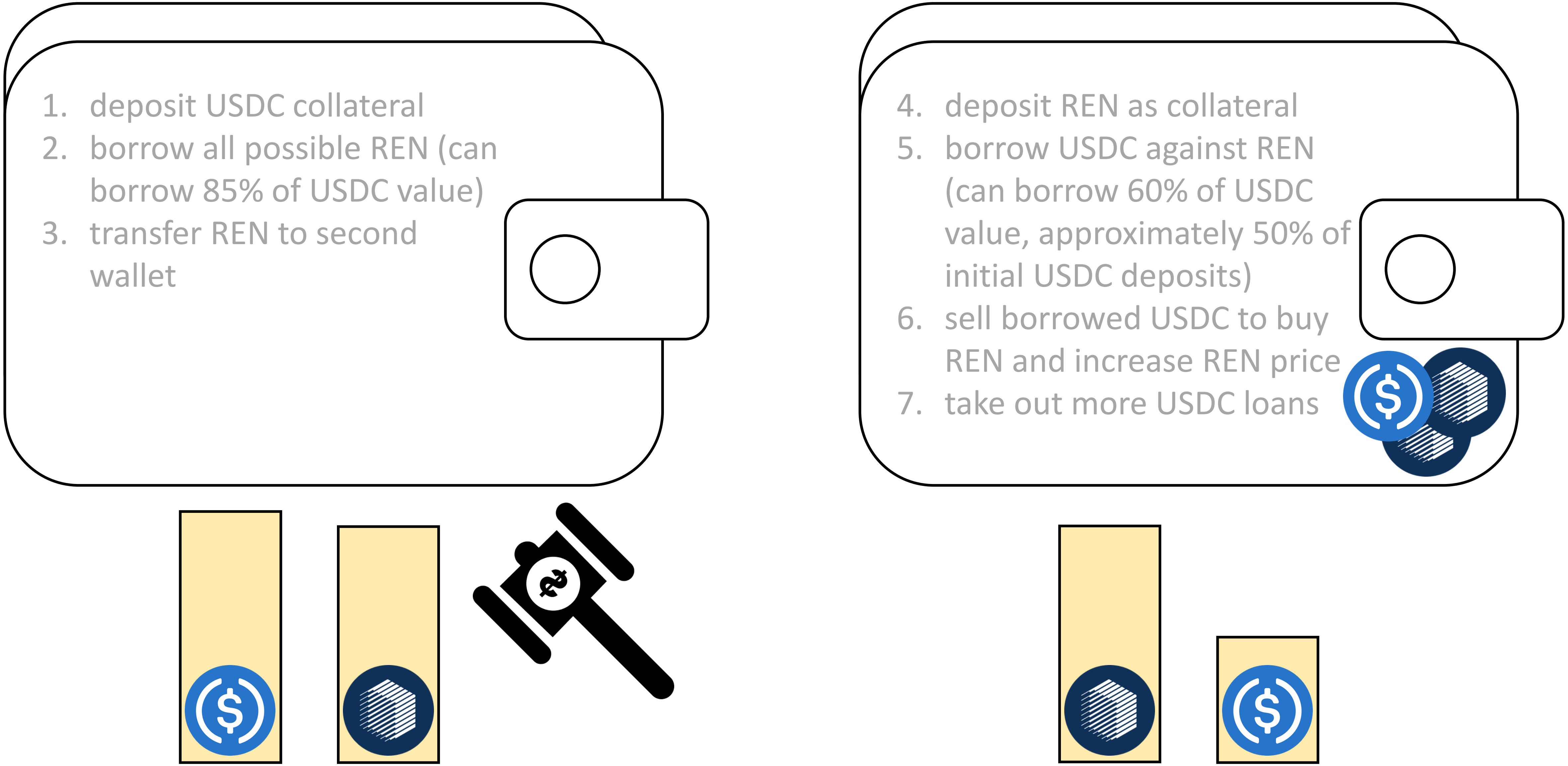
Avi Eisenberg’s proposed attack



1. deposit USDC collateral
2. borrow all possible REN (can borrow 85% of USDC value)
3. transfer REN to second wallet

4. deposit REN as collateral
5. borrow USDC against REN (can borrow 60% of USDC value, approximately 50% of initial USDC deposits)
6. sell borrowed USDC to buy REN and increase REN price

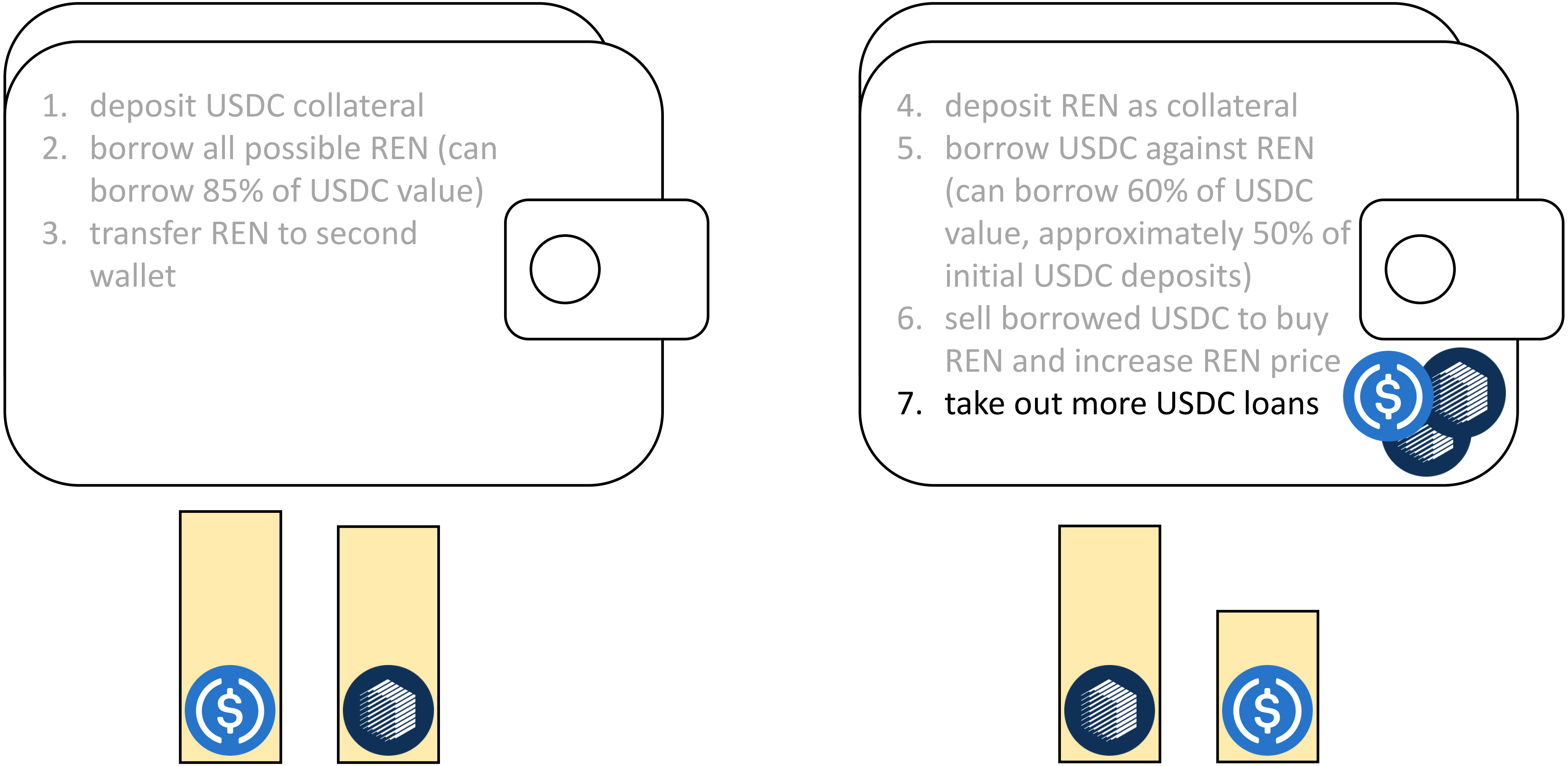
Avi Eisenberg’s proposed attack



1. deposit USDC collateral
2. borrow all possible REN (can borrow 85% of USDC value)
3. transfer REN to second wallet

4. deposit REN as collateral
5. borrow USDC against REN (can borrow 60% of USDC value, approximately 50% of initial USDC deposits)
6. sell borrowed USDC to buy REN and increase REN price
7. take out more USDC loans

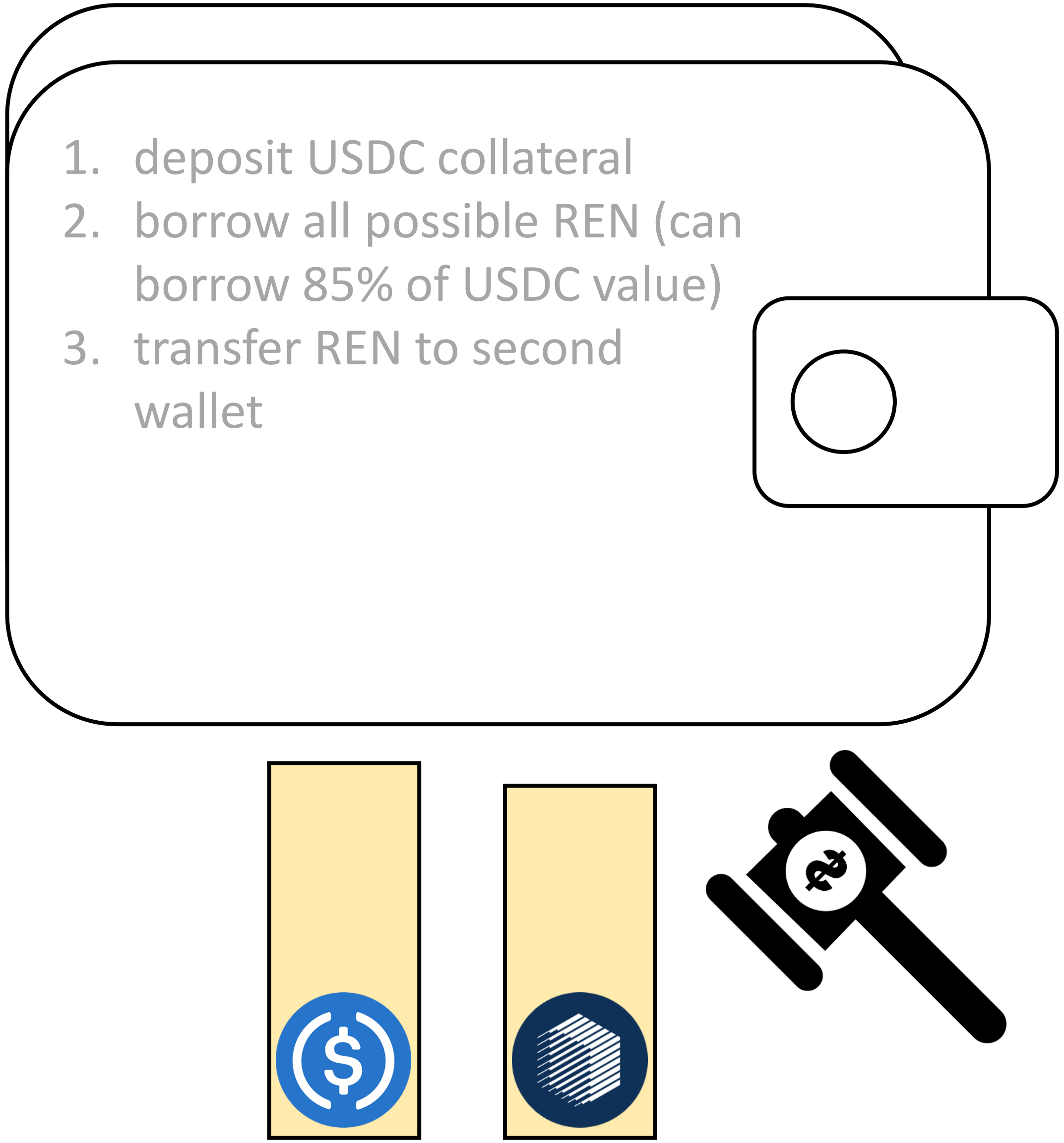
Avi Eisenberg’s proposed attack



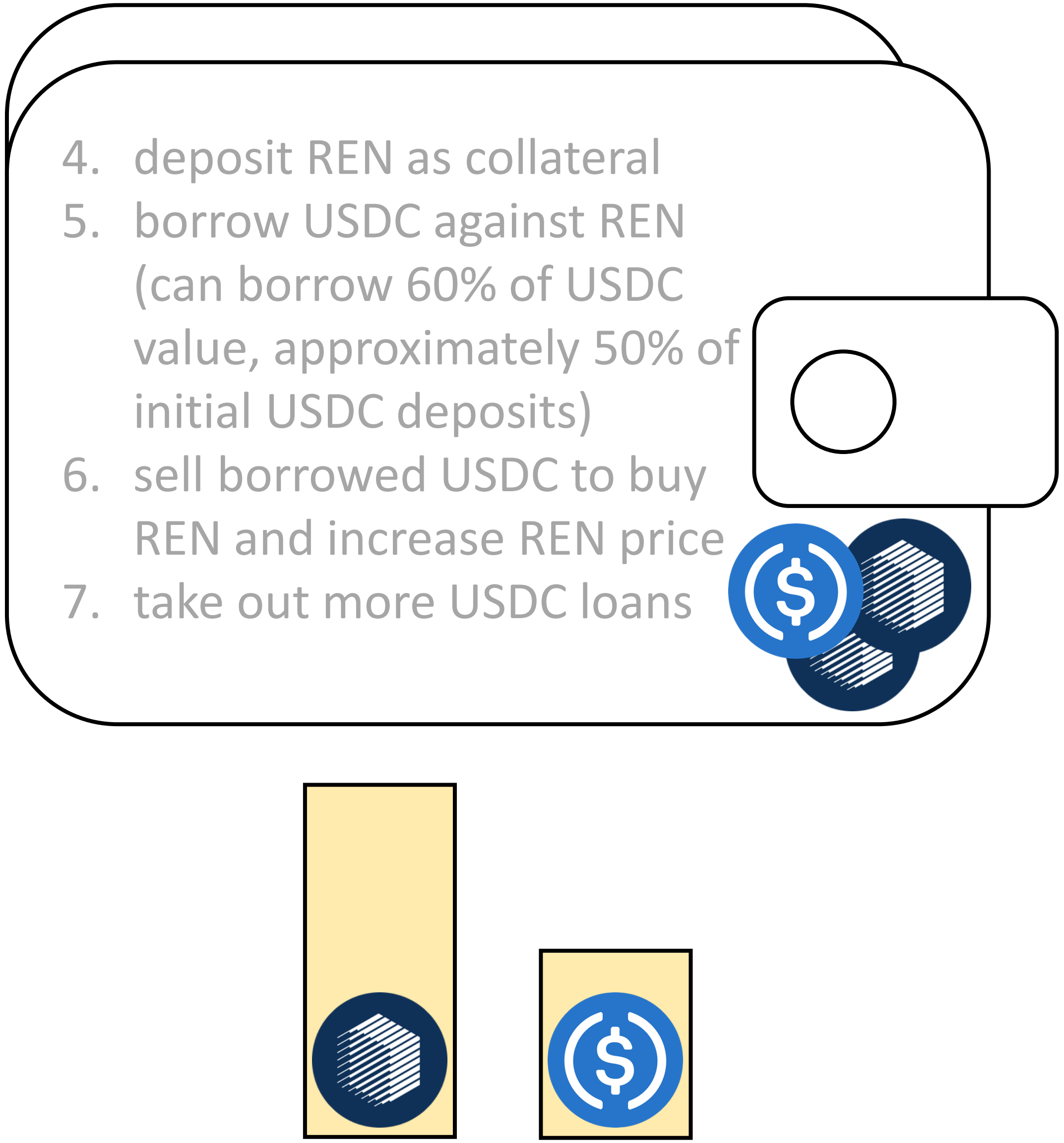
1. deposit USDC collateral
2. borrow all possible REN (can borrow 85% of USDC value)
3. transfer REN to second wallet

4. deposit REN as collateral
5. borrow USDC against REN (can borrow 60% of USDC value, approximately 50% of initial USDC deposits)
6. sell borrowed USDC to buy REN and increase REN price
7. take out more USDC loans

Avi Eisenberg’s proposed attack

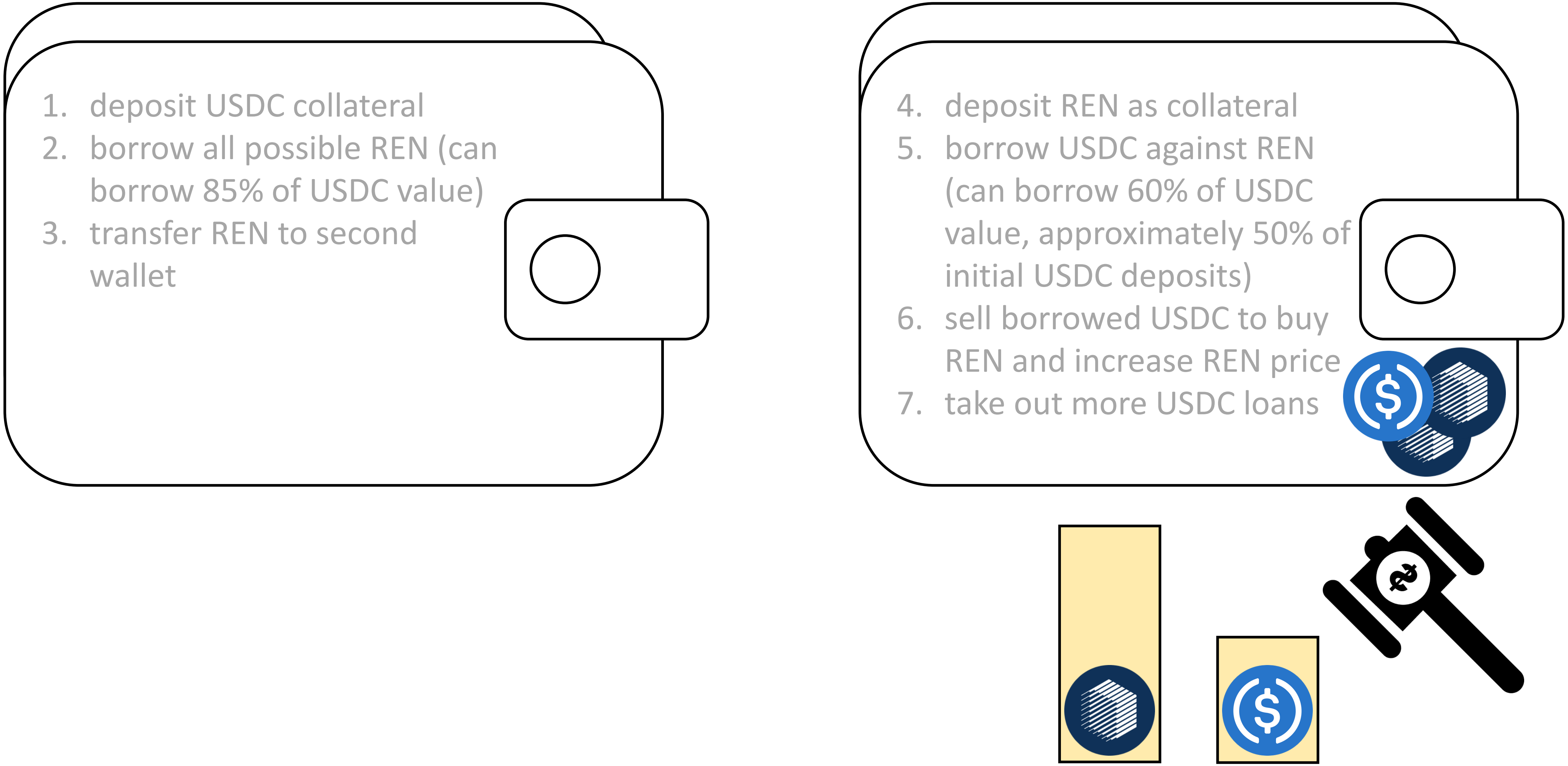


1. deposit USDC collateral
2. borrow all possible REN (can borrow 85% of USDC value)
3. transfer REN to second wallet



4. deposit REN as collateral
5. borrow USDC against REN (can borrow 60% of USDC value, approximately 50% of initial USDC deposits)
6. sell borrowed USDC to buy REN and increase REN price
7. take out more USDC loans

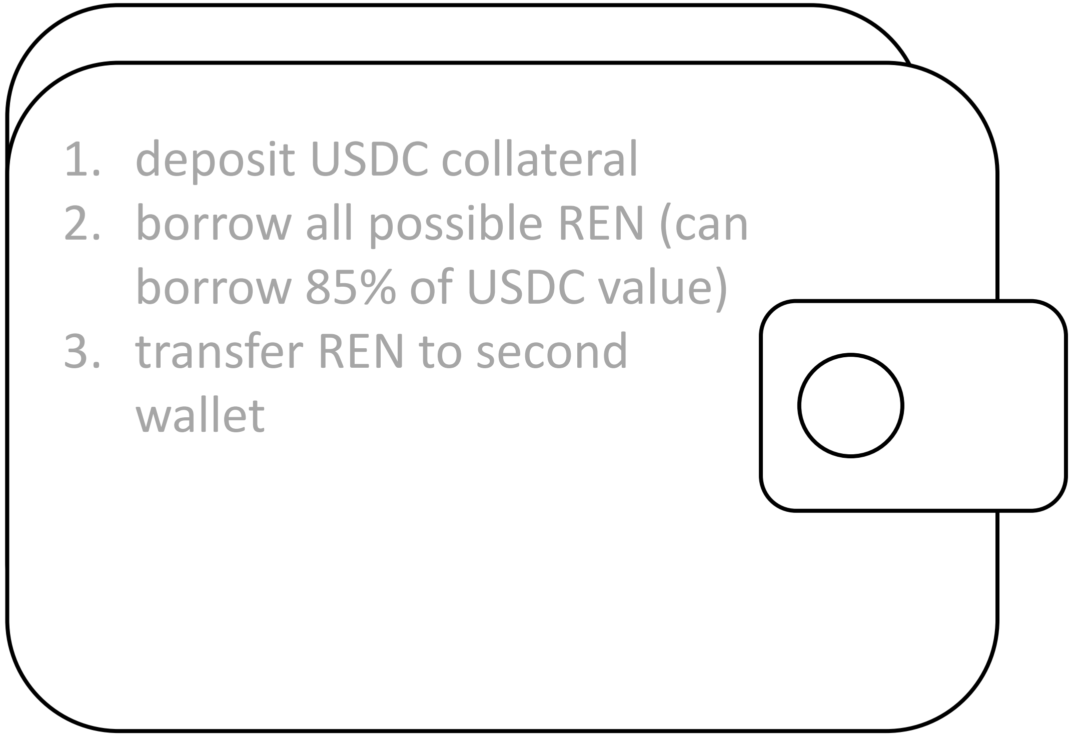
Avi Eisenberg’s proposed attack



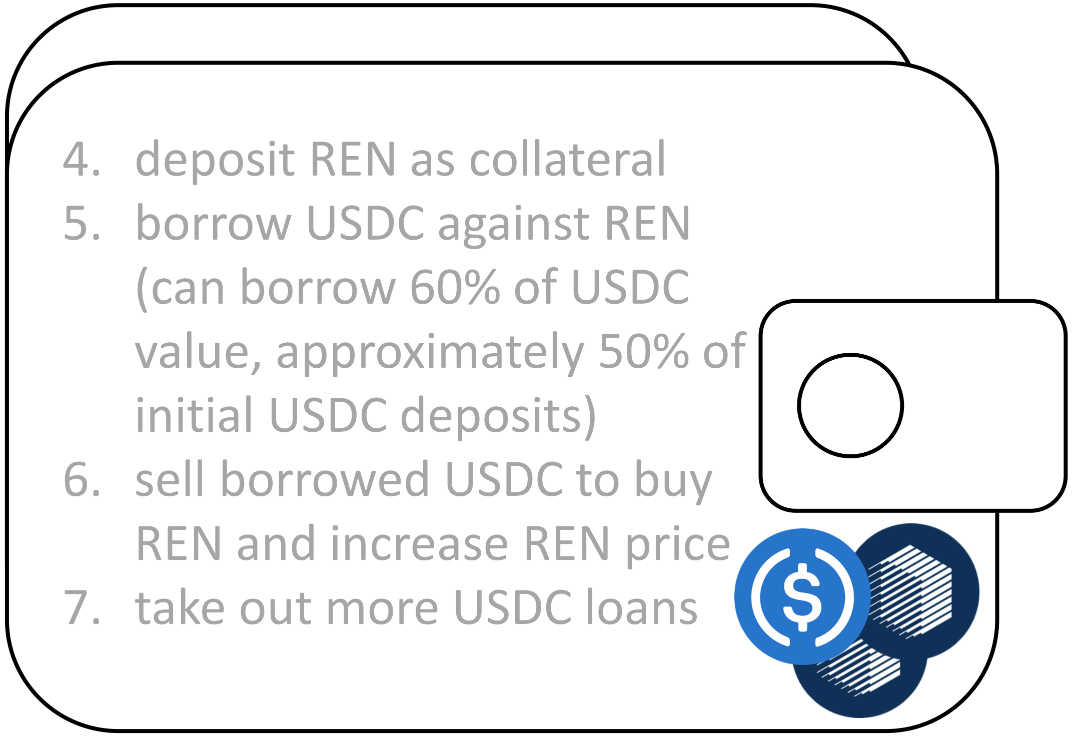
1. deposit USDC collateral
2. borrow all possible REN (can borrow 85% of USDC value)
3. transfer REN to second wallet

4. deposit REN as collateral
5. borrow USDC against REN (can borrow 60% of USDC value, approximately 50% of initial USDC deposits)
6. sell borrowed USDC to buy REN and increase REN price
7. take out more USDC loans

Avi Eisenberg’s proposed attack



1. deposit USDC collateral
2. borrow all possible REN (can borrow 85% of USDC value)
3. transfer REN to second wallet



4. deposit REN as collateral
5. borrow USDC against REN (can borrow 60% of USDC value, approximately 50% of initial USDC deposits)
6. sell borrowed USDC to buy REN and increase REN price
7. take out more USDC loans