TECHNISCHE UNIVERSITÄT WIEN
Vienna | Austria

FAKULTÄT FÜR INFORMATIK
Faculty of Informatics

S&P SECURITY & PRIVACY GROUP

Breaking and Fixing Virtual Channels: Domino Attack and Donner

Lukas Aumayr[1], Pedro Moreno-Sanchez[2], Aniket Kate[3], Matteo Maffei[1,4]

[1]TU Wien, [2]IMDEA Software Institute, [3]Purdue University, [4]Christian Doppler Laboratory Blockchain Technologies for the Internet of Things

What’s in store?

1. Existing Virtual Channel solutions & Domino attack:

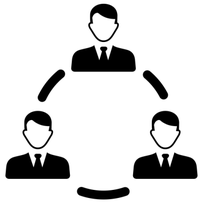
New attack on
Virtual Channels

What's in store?

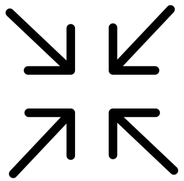
1. Existing Virtual Channel solutions & Domino attack:

New attack on
Virtual Channels

2. Donner virtual channels:



Generic solution for apps over
multiple hops



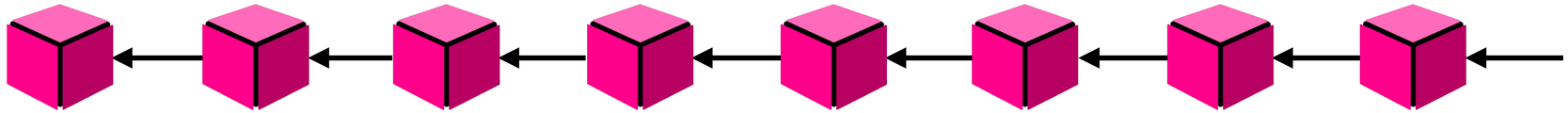
Constant overhead

Fair, unlimited lifetime
and fee model

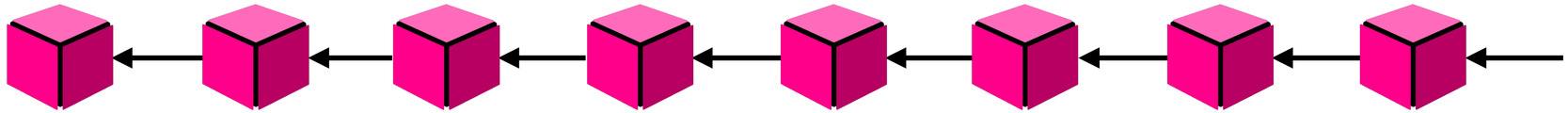
Better security,
privacy & latency

Background

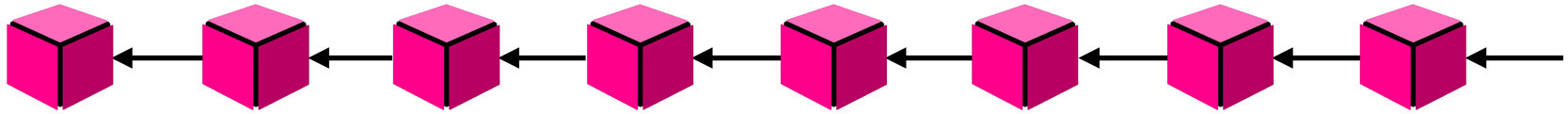
Scalability



Scalability

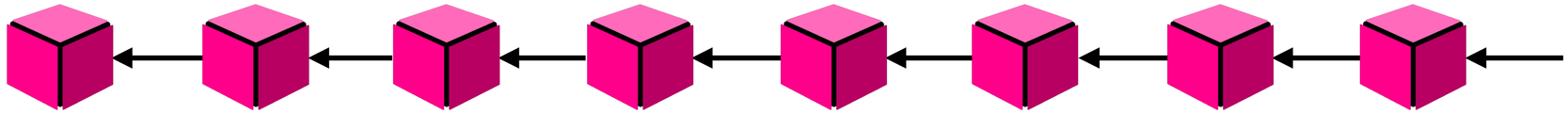


Scalability



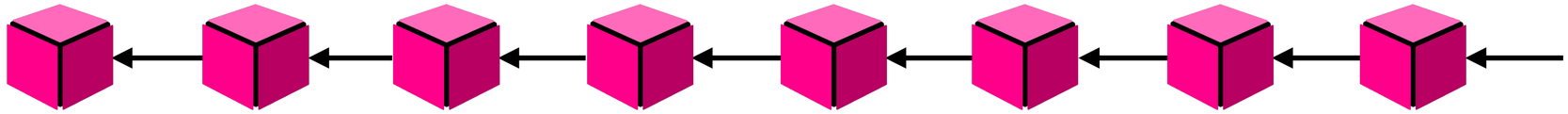
- Blockchain: records every transaction

Scalability



- Blockchain: records every transaction
- Global consensus: everyone checks the whole blockchain

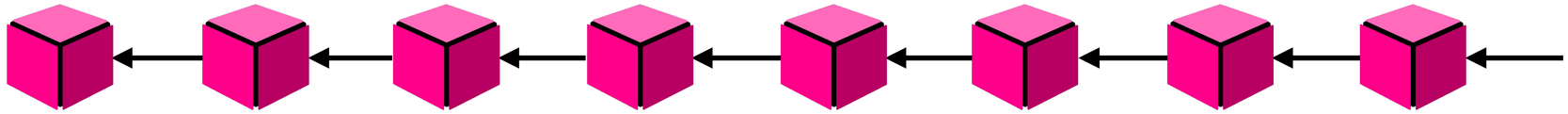
Scalability



- Blockchain: records every transaction
- Global consensus: everyone checks the whole blockchain

Bitcoin's **transaction rate:** ~10 tx/sec
Visa's transaction rate: ~10K tx/sec

Scalability



- Blockchain: records every transaction
- Global consensus: everyone checks the whole blockchain

Bitcoin's **transaction rate:** ~10 tx/sec
Visa's transaction rate: ~10K tx/sec

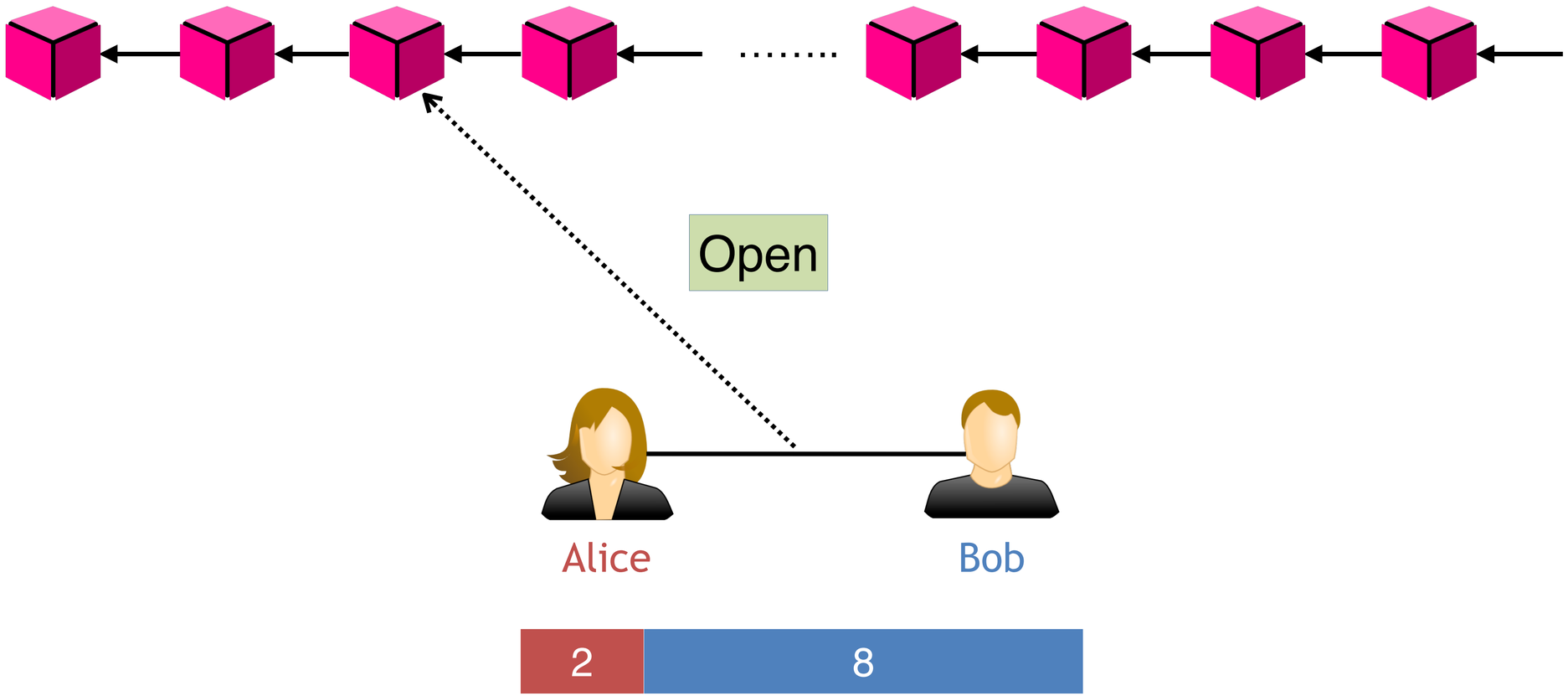
Exchange transactions locally off-chain, Blockchain for disputes

Payment channels

Alice

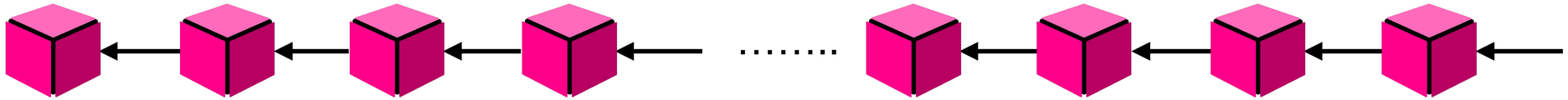
Bob

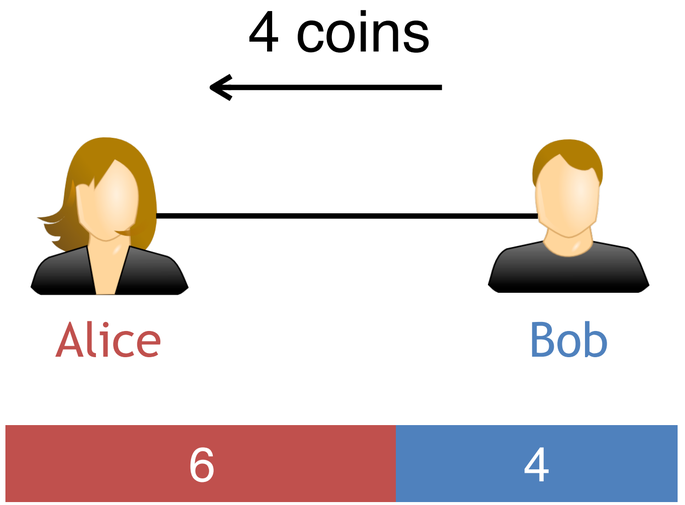
Payment channels



Funded on-chain

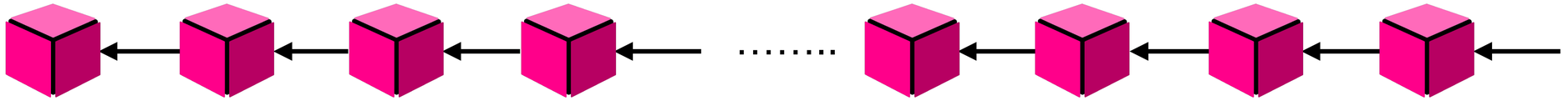
Payment channels

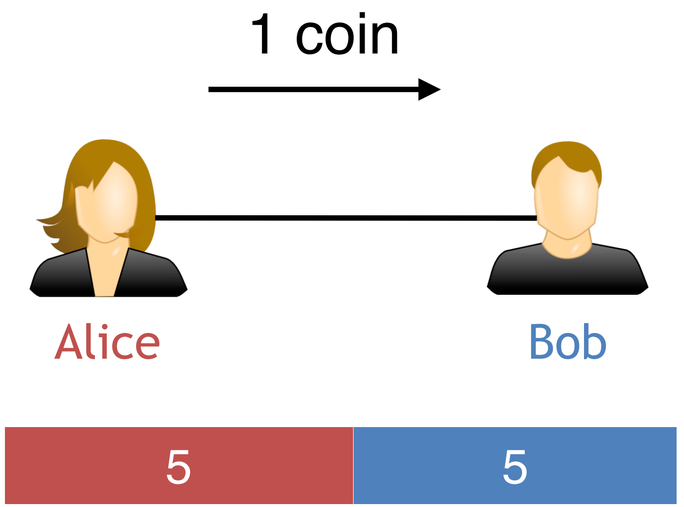




Arbitrarily many payments off-chain

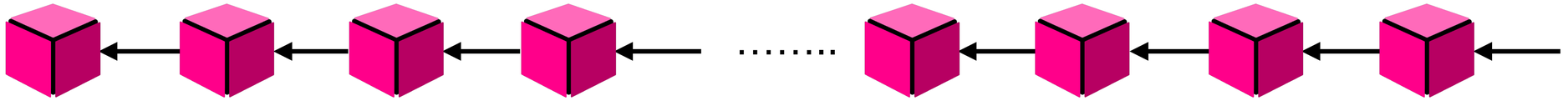
Payment channels

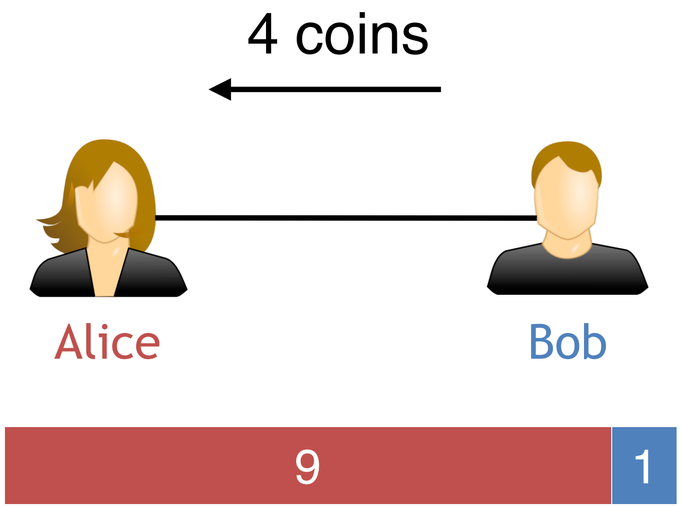




Arbitrarily many payments off-chain

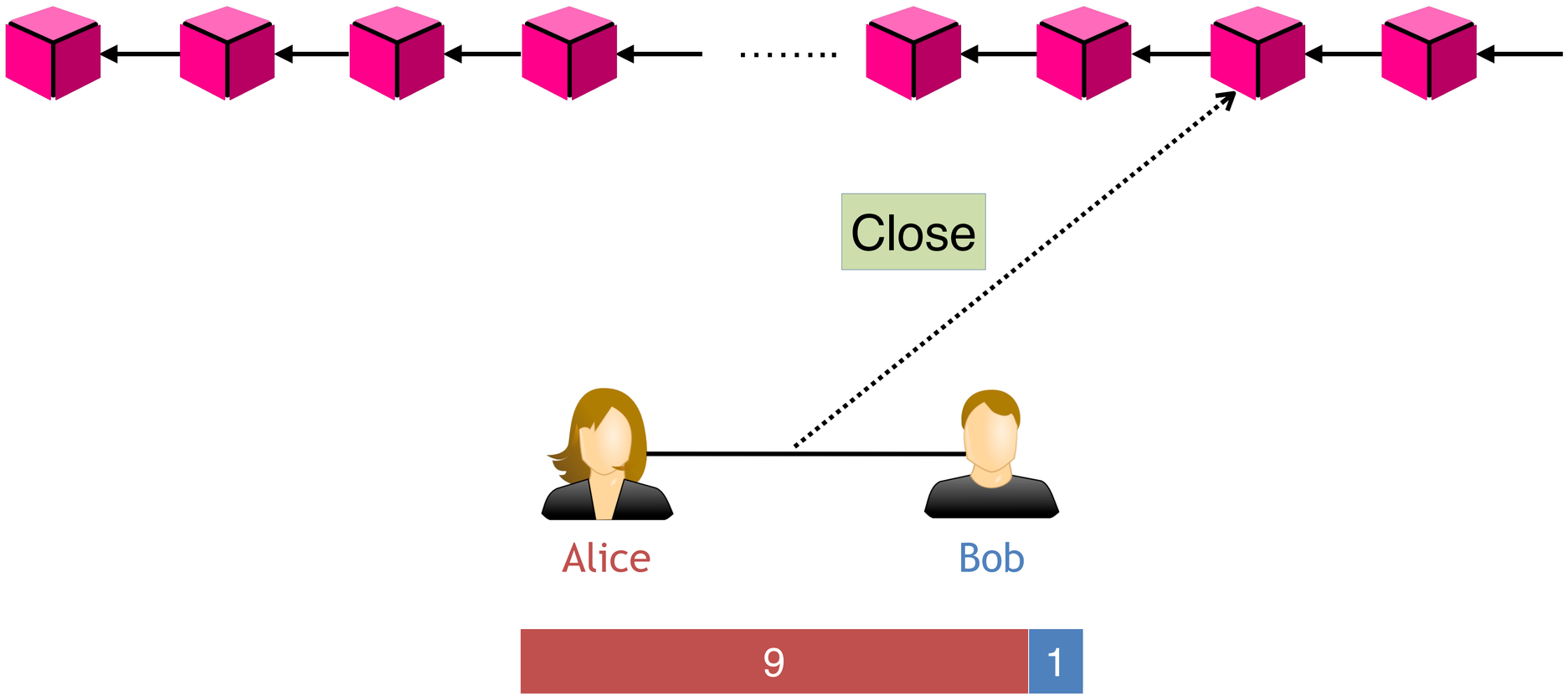
Payment channels





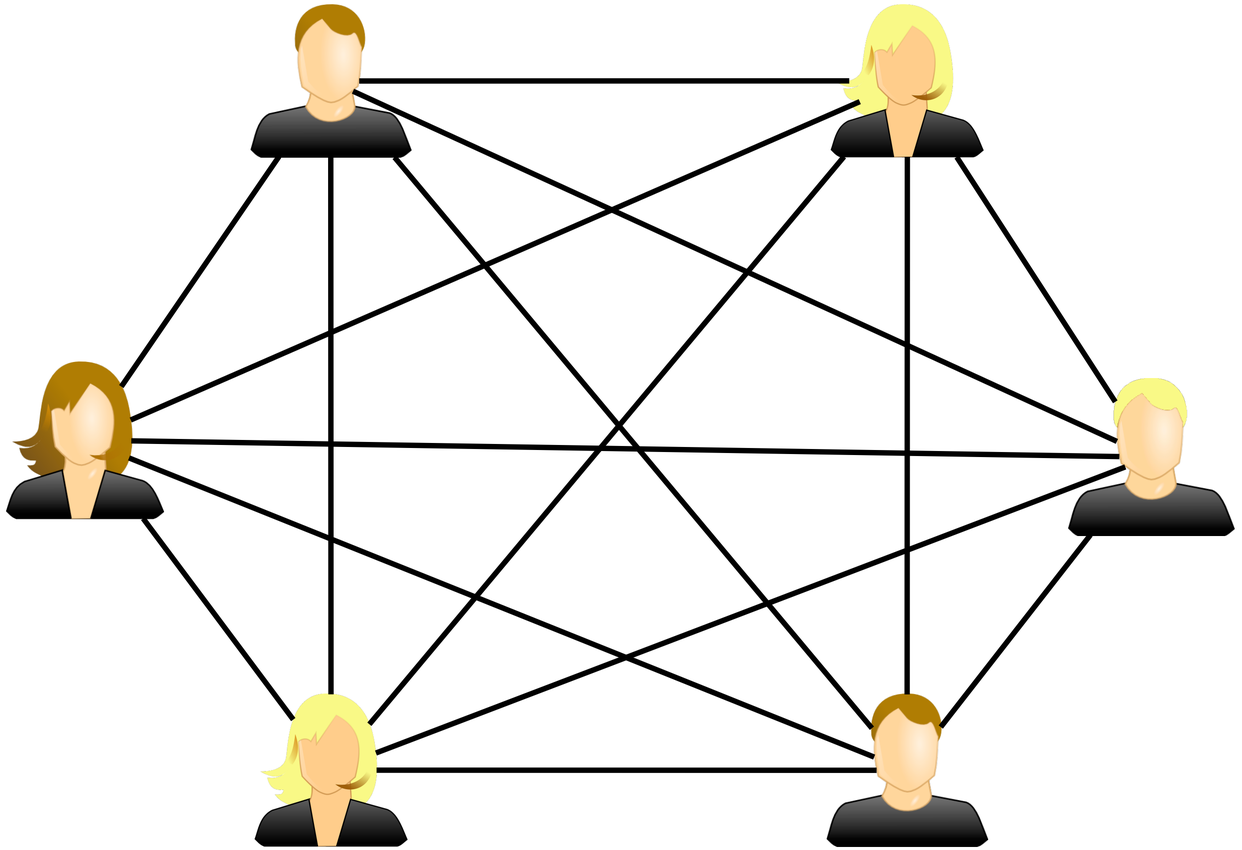
Arbitrarily many payments off-chain

Payment channels



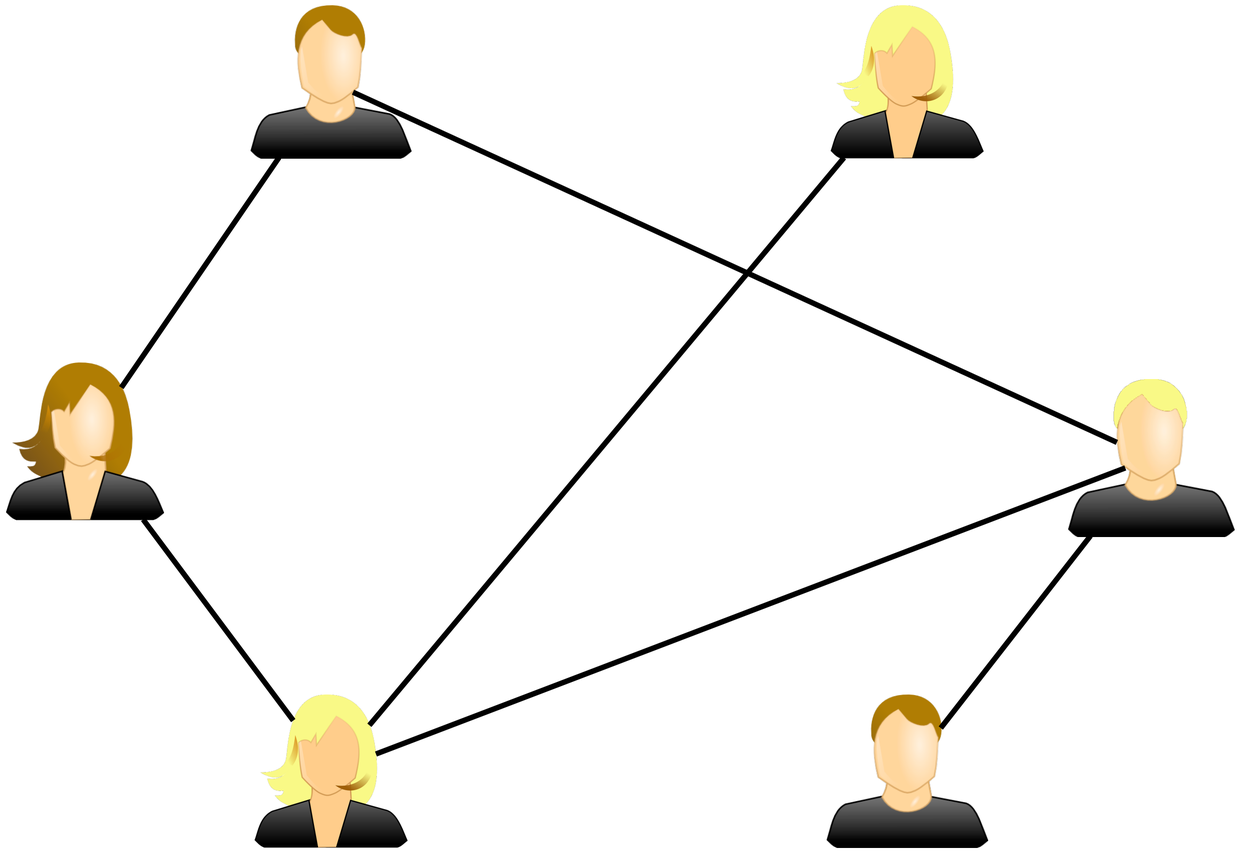
Only 2 transactions on-chain

Paying to anybody?

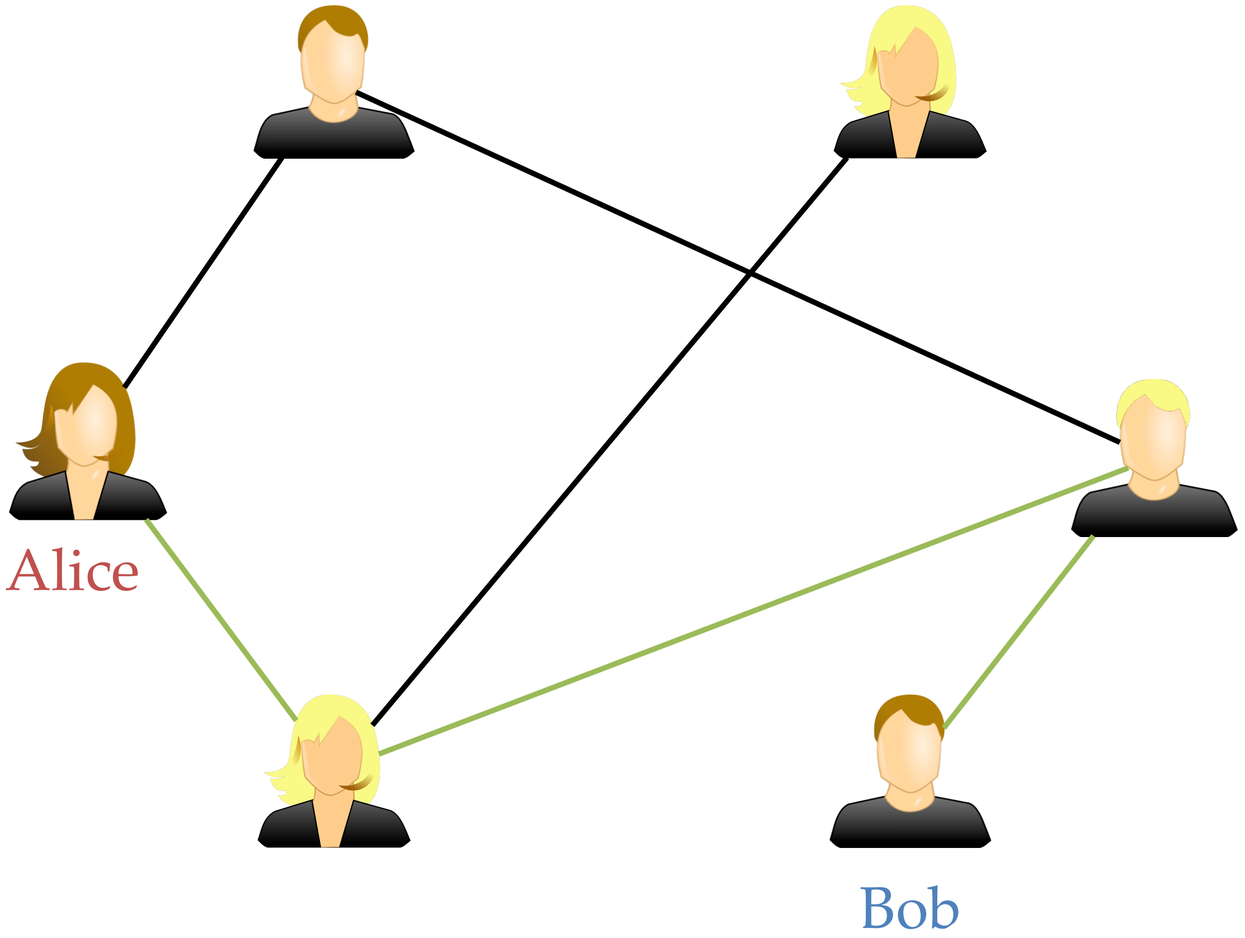


Infeasible to open a channel with everybody

Instead form Network!

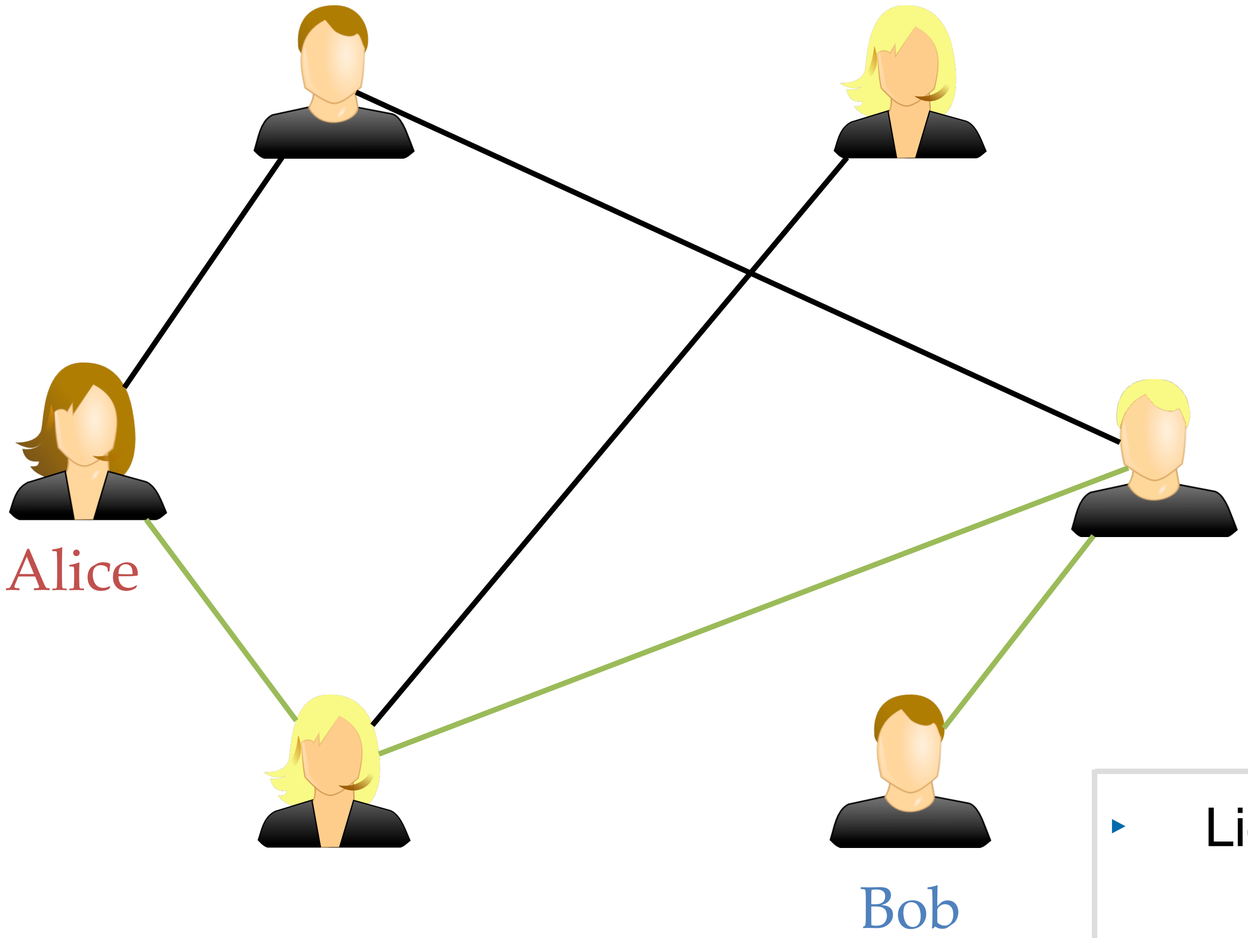


Instead form Network!



- Multi-hop payments (MHPs)

Instead form Network!



- Lightning Network (LN) [1]
  - 134M $ locked
  - 16k nodes
  - 76k channels
- VISA research [2], CBDC [3]

[1] J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," *2016*
[2] M. Christodorescu et al., "Universal Payment Channels: An Interoperability Platform for Digital Currencies," 2021
[3] M. Zamini et al., "Cross-Border Payments for Central Bank Digital Currencies via Universal Payment Channels," 2021

Nice solution, but …

Limitations of MHPs

What we would like

Only for payments

Nice solution, but …

Limitations of MHPs

Only for payments

Each payment routed via intermediaries

What we would like

Nice solution, but …

Limitations of MHPs

Only for payments

Each payment routed via intermediaries

more fees

less privacy

less reliable

What we would like

Nice solution, but …

Limitations of MHPs

Only for payments

Each payment routed via intermediaries

- more fees
- less privacy
- less reliable

What we would like

DLCs [4], games, betting, etc.

[4] T. Dryja,"Discreet Log Contracts," https://adiabat.github.io/dlc.pdf

Nice solution, but …

Limitations of MHPs		What we would like
Only for payments		DLCs [4], games, betting, etc.
Each payment routed via intermediaries		Involve intermediaries only for setup/closure

- more fees
- less privacy
- less reliable

[4] T. Dryja,"Discreet Log Contracts," https://adiabat.github.io/dlc.pdf

Nice solution, but …

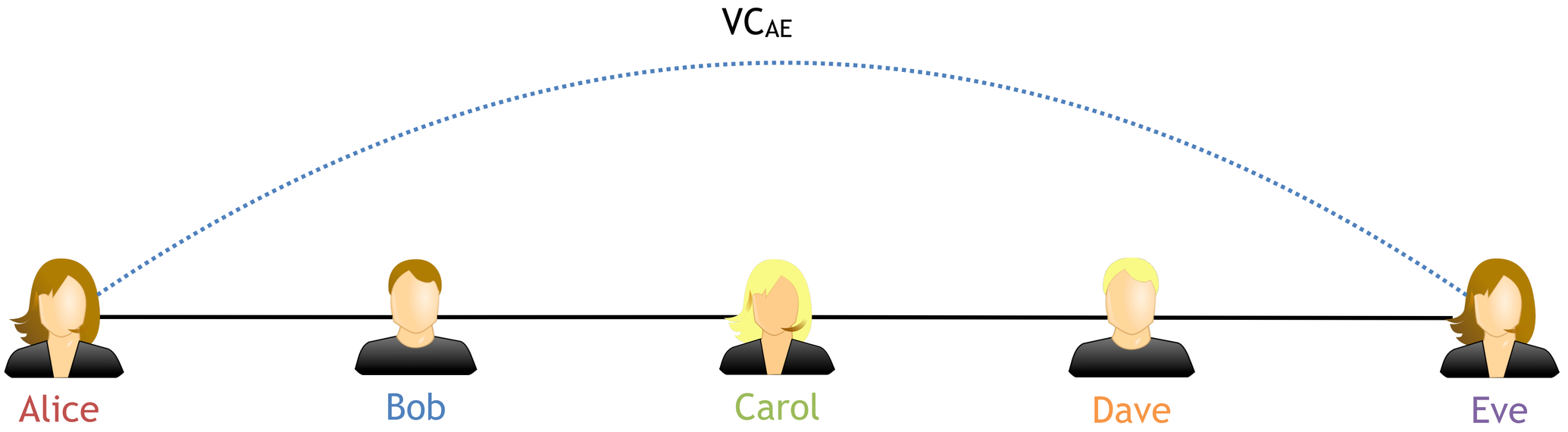
Limitations of MHPs		What we would like
Only for payments		DLCs [4], games, betting, etc.
Each payment routed via intermediaries		Involve intermediaries only for setup/closure
more fees		fewer fees
less privacy		more privacy
less reliable		more reliable

[4] T. Dryja,"Discreet Log Contracts," https://adiabat.github.io/dlc.pdf

Virtual Channels & the Domino Attack

Virtual channels idea

- Bypass intermediaries
- Fund off-chain - on top of existing channels



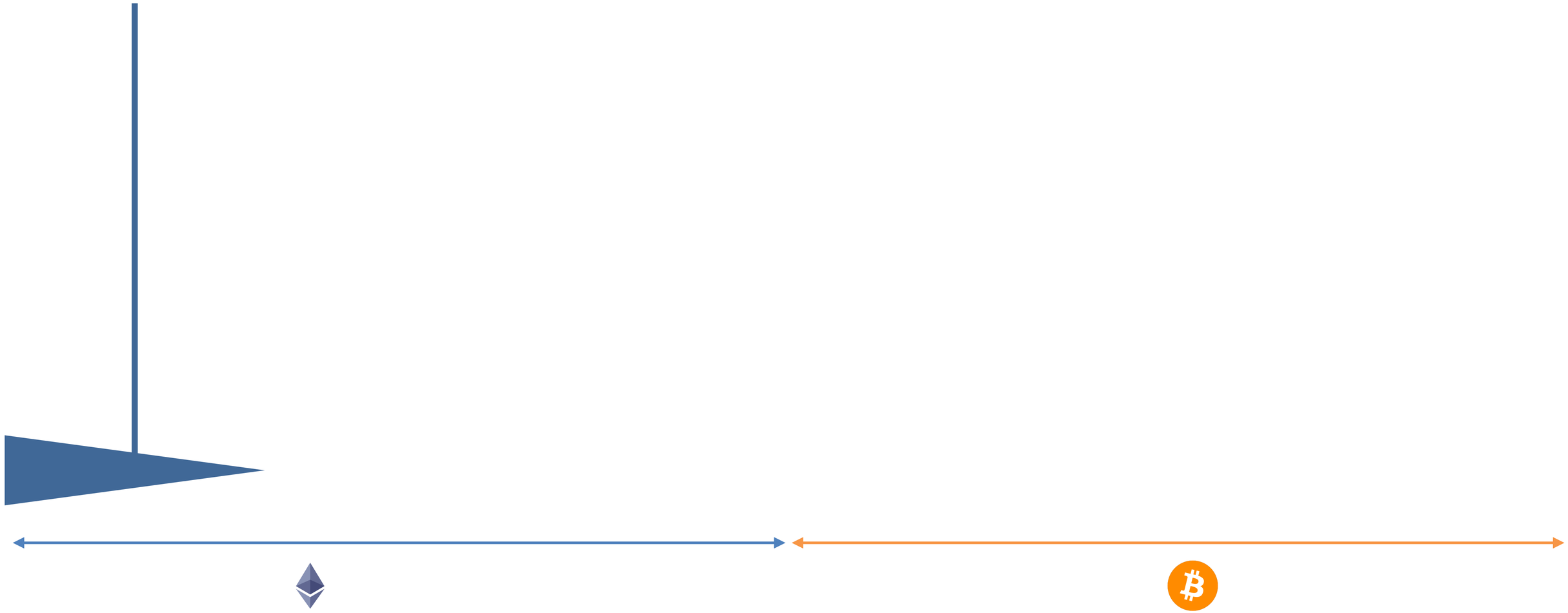
Virtual channels timeline

2017:

Dziembowski, Eckey, Faust, and Malinowski (IEEE S&P'19)

Perun: Virtual Payment Hubs over Cryptocurrencies

- only 1 intermediary
- Turing-complete scripting



Virtual channels timeline

2017:

Dziembowski, Eckey, Faust, and Malinowski (IEEE S&P'19)

Perun: Virtual Payment Hubs over Cryptocurrencies

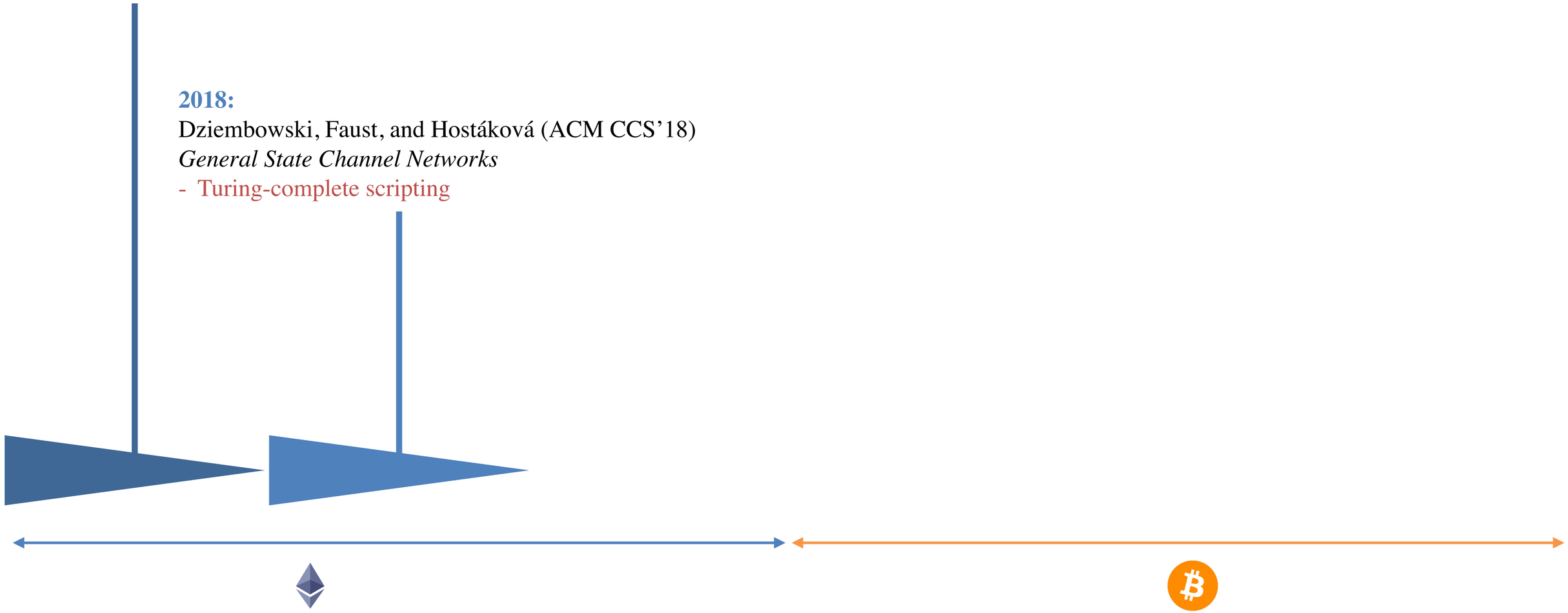
- only 1 intermediary
- Turing-complete scripting

2018:

Dziembowski, Faust, and Hostáková (ACM CCS'18)

General State Channel Networks

- Turing-complete scripting

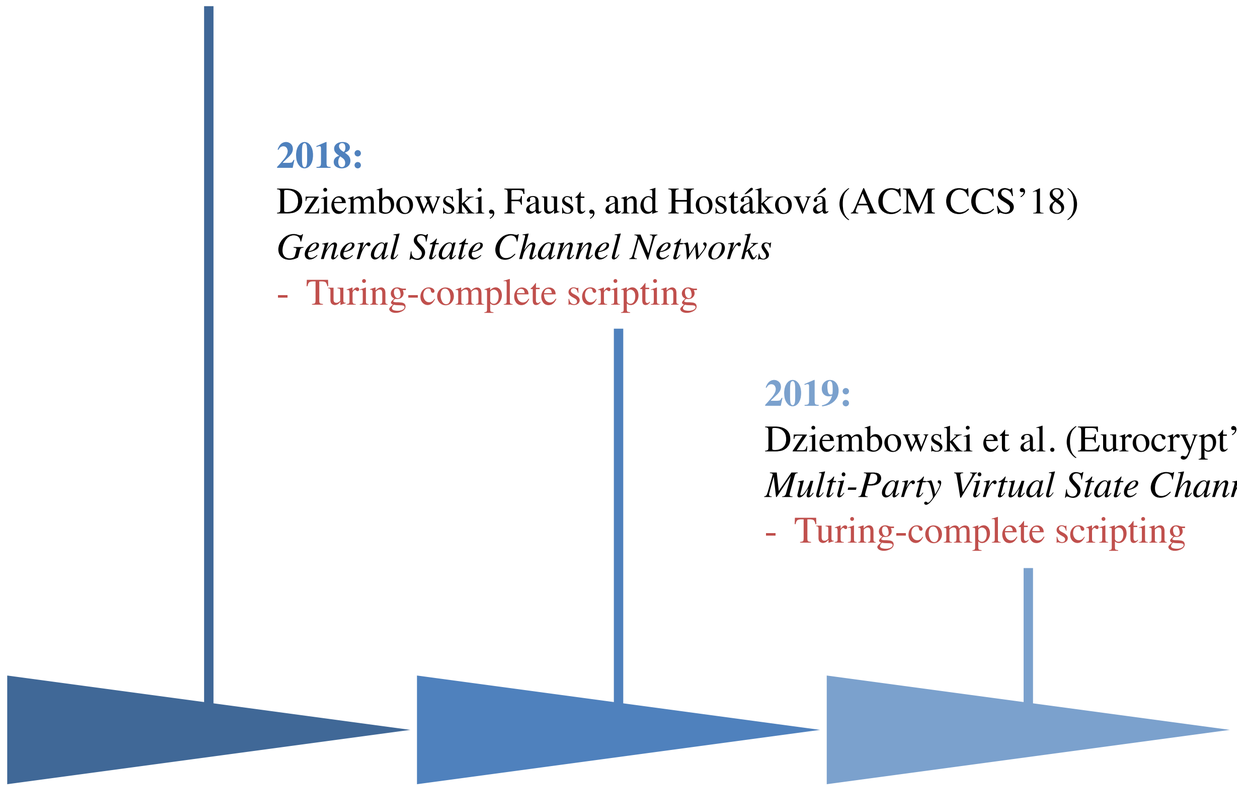


Virtual channels timeline

2017:
Dziembowski, Eckey, Faust, and Malinowski (IEEE S&P'19)
Perun: Virtual Payment Hubs over Cryptocurrencies
- only 1 intermediary
- Turing-complete scripting

2018:
Dziembowski, Faust, and Hostáková (ACM CCS'18)
General State Channel Networks
- Turing-complete scripting

2019:
Dziembowski et al. (Eurocrypt'19)
Multi-Party Virtual State Channels
- Turing-complete scripting



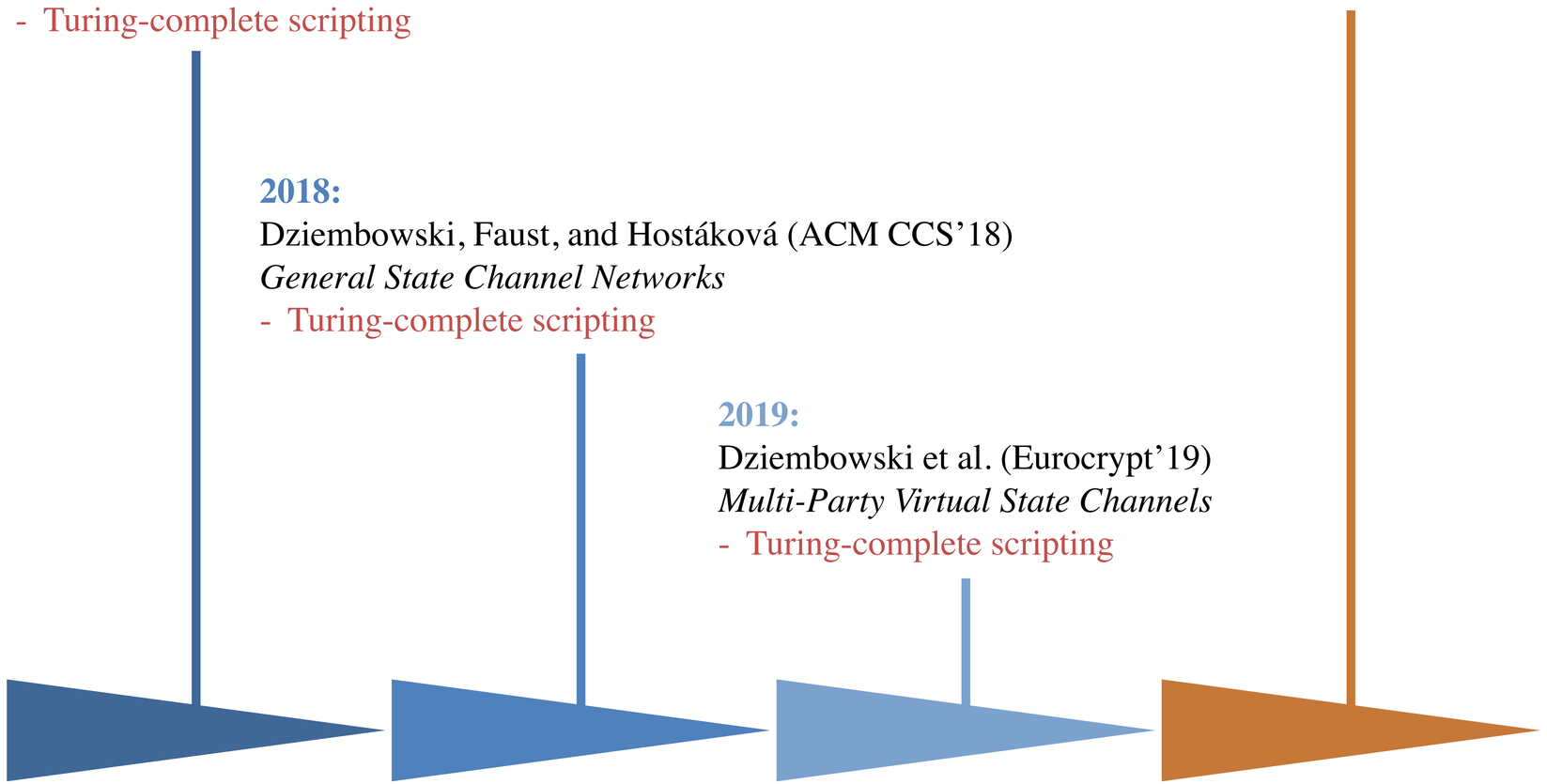
Virtual channels timeline

2017:
Dziembowski, Eckey, Faust, and Malinowski (IEEE S&P'19)
Perun: Virtual Payment Hubs over Cryptocurrencies
- only 1 intermediary
- Turing-complete scripting

2018:
Dziembowski, Faust, and Hostáková (ACM CCS'18)
General State Channel Networks
- Turing-complete scripting

2019:
Dziembowski et al. (Eurocrypt'19)
Multi-Party Virtual State Channels
- Turing-complete scripting

2020:
Aumayr et al. (IEEE S&P'21)
Bitcoin-Compatible Virtual Channels
- only 1 intermediary



Virtual channels timeline

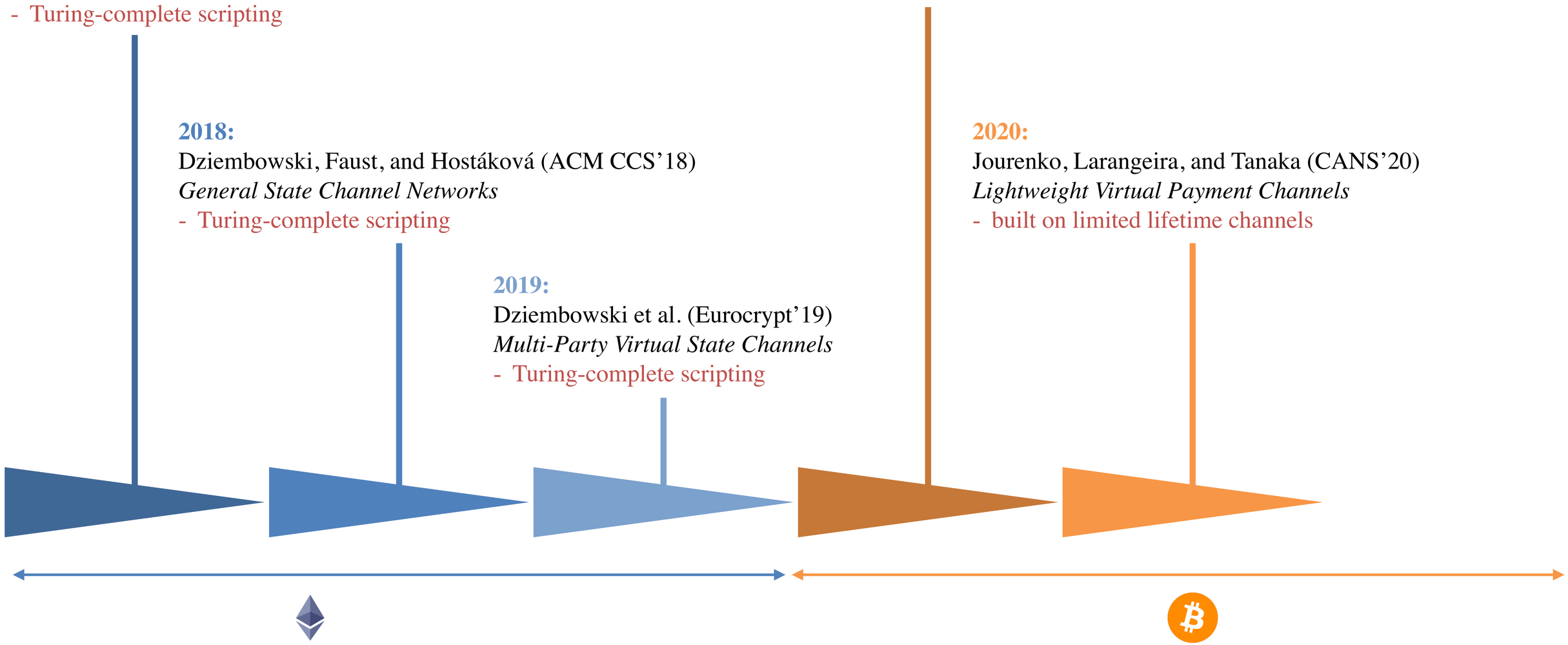
2017:
Dziembowski, Eckey, Faust, and Malinowski (IEEE S&P'19)
Perun: Virtual Payment Hubs over Cryptocurrencies
- only 1 intermediary
- Turing-complete scripting

2018:
Dziembowski, Faust, and Hostáková (ACM CCS'18)
General State Channel Networks
- Turing-complete scripting

2019:
Dziembowski et al. (Eurocrypt'19)
Multi-Party Virtual State Channels
- Turing-complete scripting

2020:
Aumayr et al. (IEEE S&P'21)
Bitcoin-Compatible Virtual Channels
- only 1 intermediary

2020:
Jourenko, Larangeira, and Tanaka (CANS'20)
Lightweight Virtual Payment Channels
- built on limited lifetime channels



Virtual channels timeline

2017:
Dziembowski, Eckey, Faust, and Malinowski (IEEE S&P'19)
Perun: Virtual Payment Hubs over Cryptocurrencies
- only 1 intermediary
- Turing-complete scripting

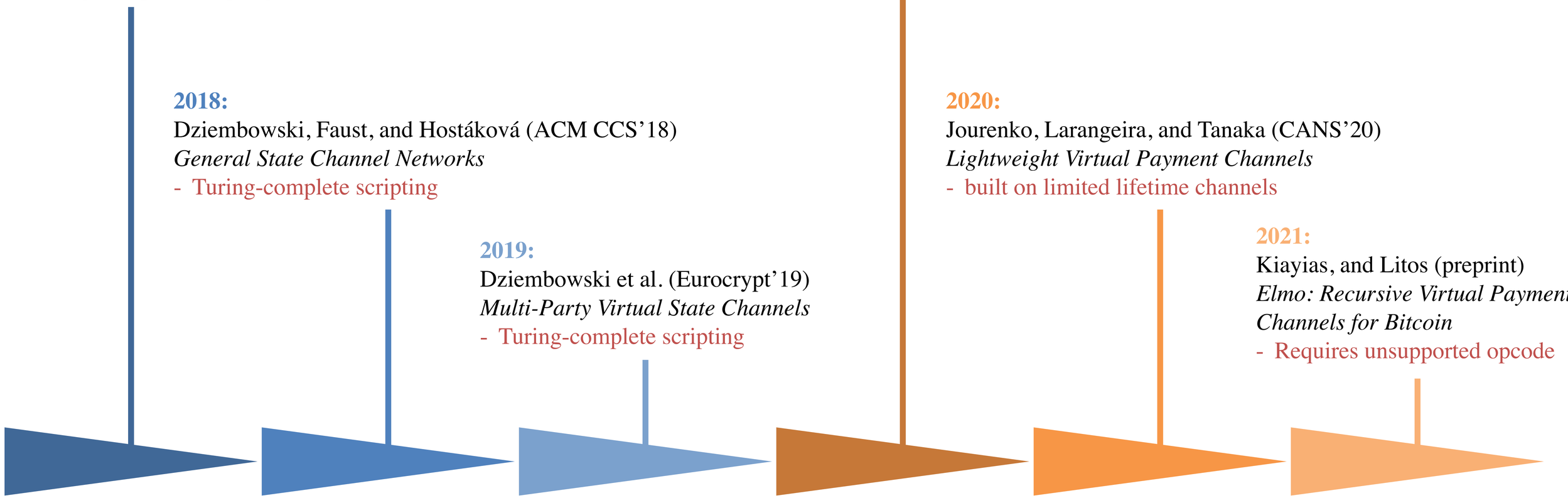
2018:
Dziembowski, Faust, and Hostáková (ACM CCS'18)
General State Channel Networks
- Turing-complete scripting

2019:
Dziembowski et al. (Eurocrypt'19)
Multi-Party Virtual State Channels
- Turing-complete scripting

2020:
Aumayr et al. (IEEE S&P'21)
Bitcoin-Compatible Virtual Channels
- only 1 intermediary

2020:
Jourenko, Larangeira, and Tanaka (CANS'20)
Lightweight Virtual Payment Channels
- built on limited lifetime channels

2021:
Kiayias, and Litos (preprint)
Elmo: Recursive Virtual Payment Channels for Bitcoin
- Requires unsupported opcode



Virtual channels timeline

2017:
Dziembowski, Eckey, Faust, and Malinowski (IEEE S&P'19)
Perun: Virtual Payment Hubs over Cryptocurrencies
- only 1 intermediary
- Turing-complete scripting

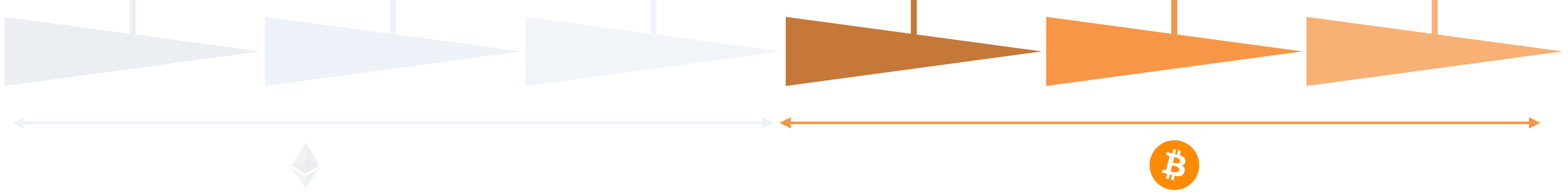
2018:
Dziembowski, Faust, and Hostáková (ACM CCS'18)
General State Channel Networks
- Turing-complete scripting

2019:
Dziembowski et al. (Eurocrypt'19)
Multi-Party Virtual State Channels
- Turing-complete scripting

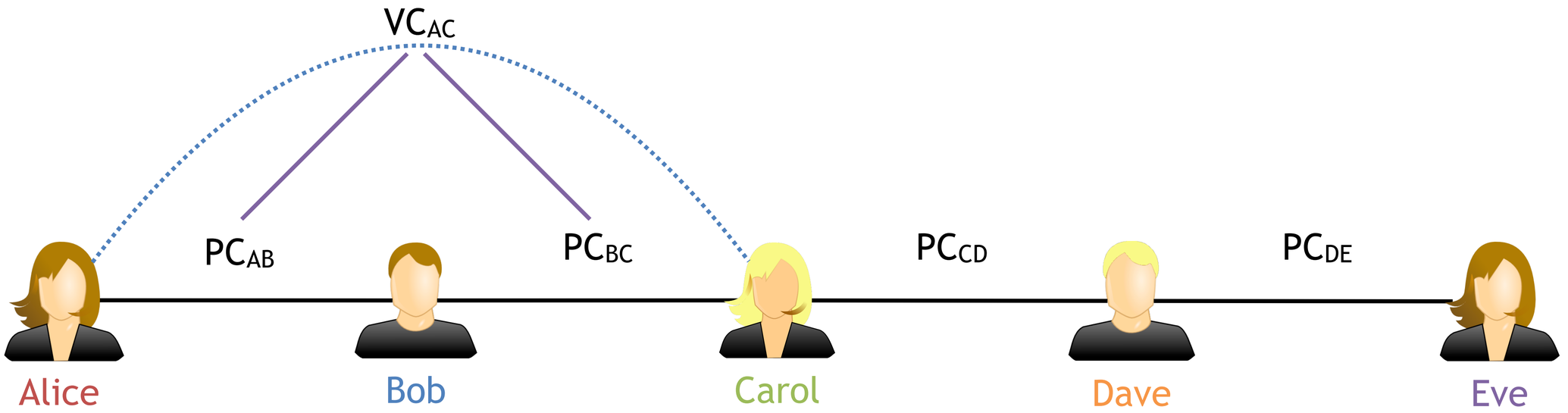
2020:
Aumayr et al. (IEEE S&P'21)
Bitcoin-Compatible Virtual Channels
- only 1 intermediary

2020:
Jourenko, Larangeira, and Tanaka (CANS'20)
Lightweight Virtual Payment Channels
- built on limited lifetime channels

2021:
Kiayias, and Litos (preprint)
Elmo: Recursive Virtual Payment Channels for Bitcoin
- Requires unsupported opcode

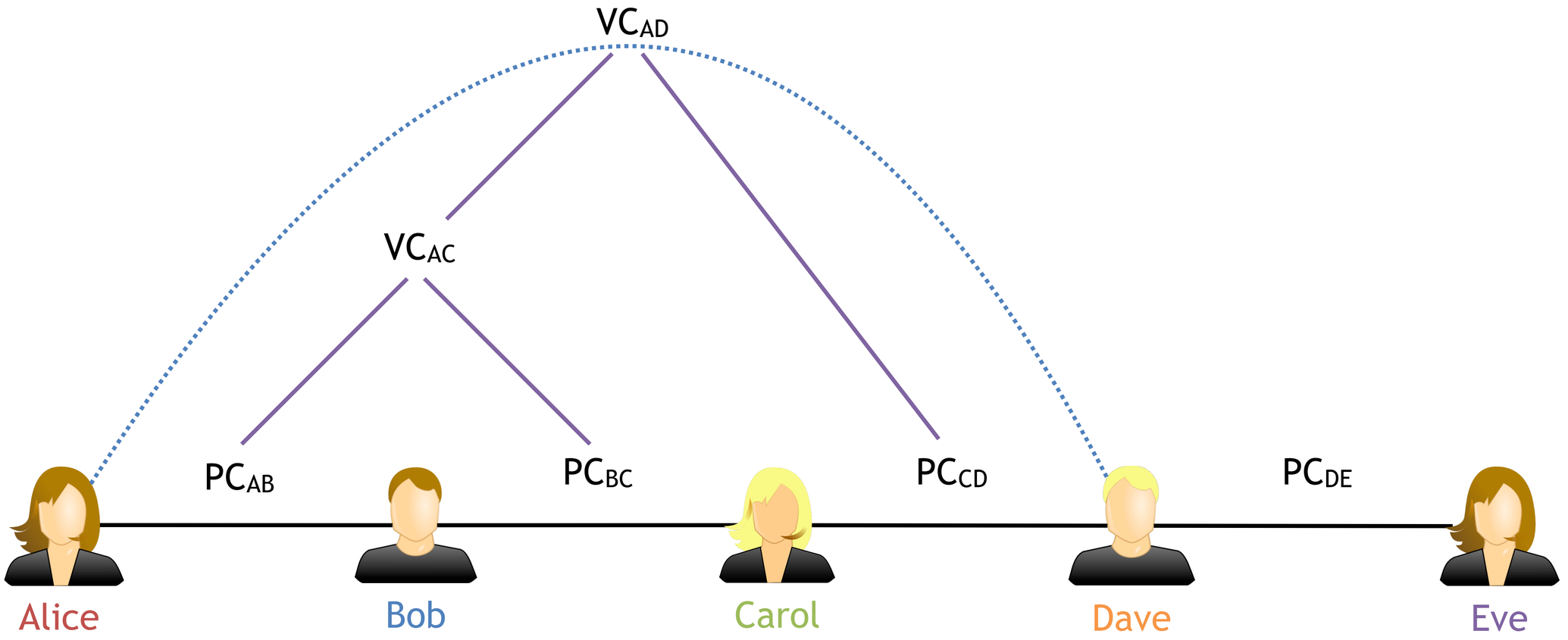


Rooted design



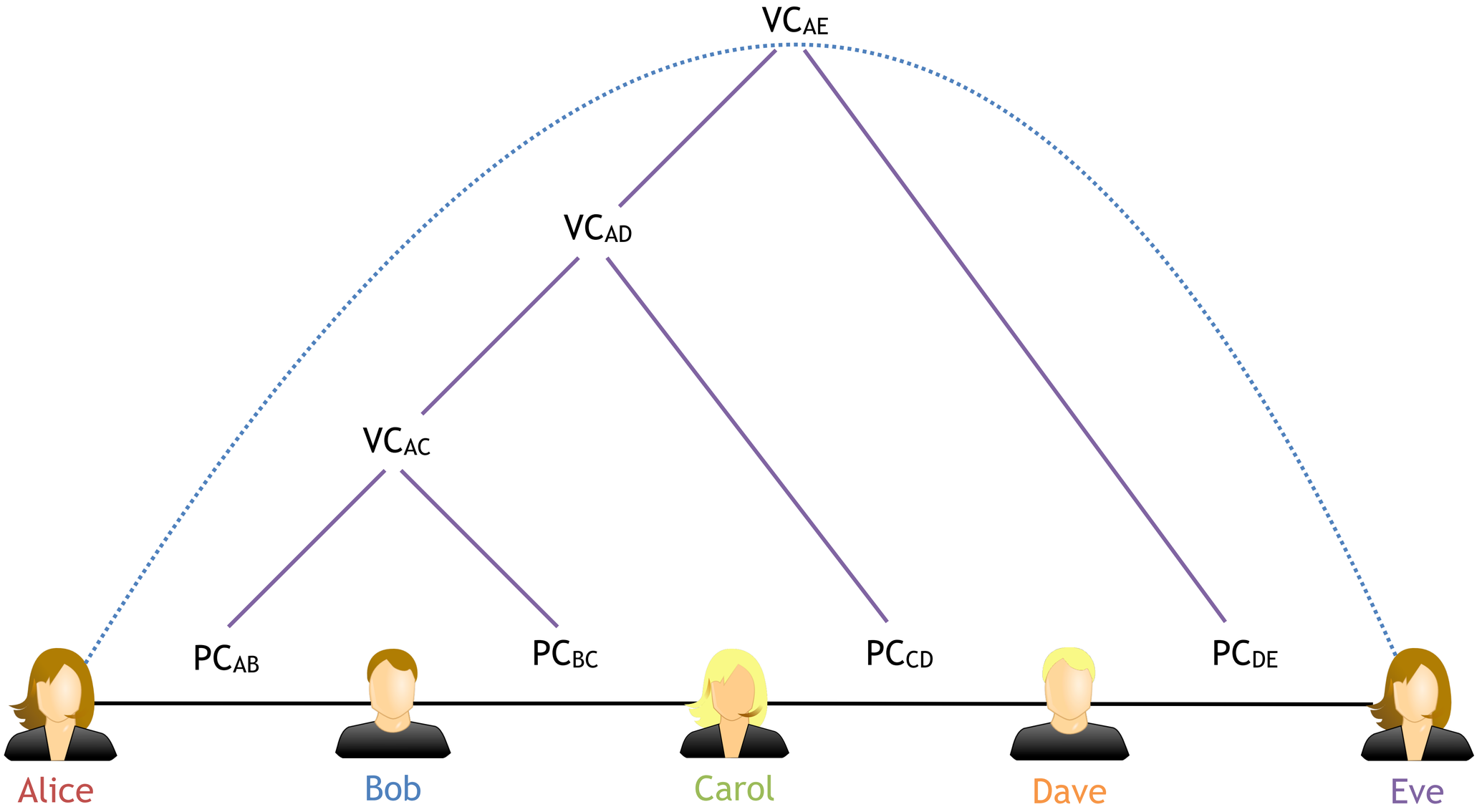
Example: Jourenko, Larangeira, and Tanaka, “Lightweight Virtual Payment Channels,” 2021

Rooted design



Example: Jourenko, Larangeira, and Tanaka, “Lightweight Virtual Payment Channels,” 2021

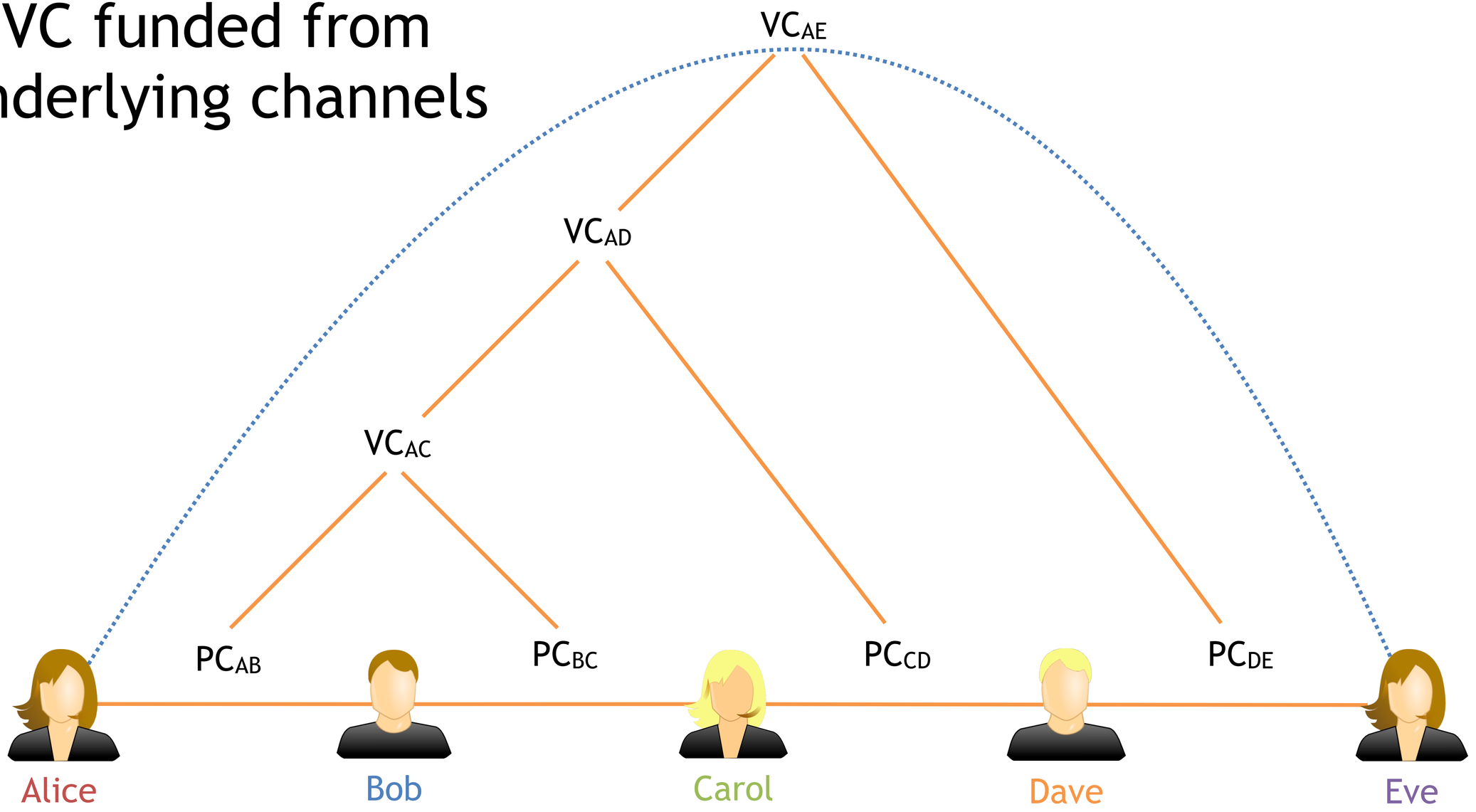
Rooted design



Example: Jourenko, Larangeira, and Tanaka, “Lightweight Virtual Payment Channels,” 2021

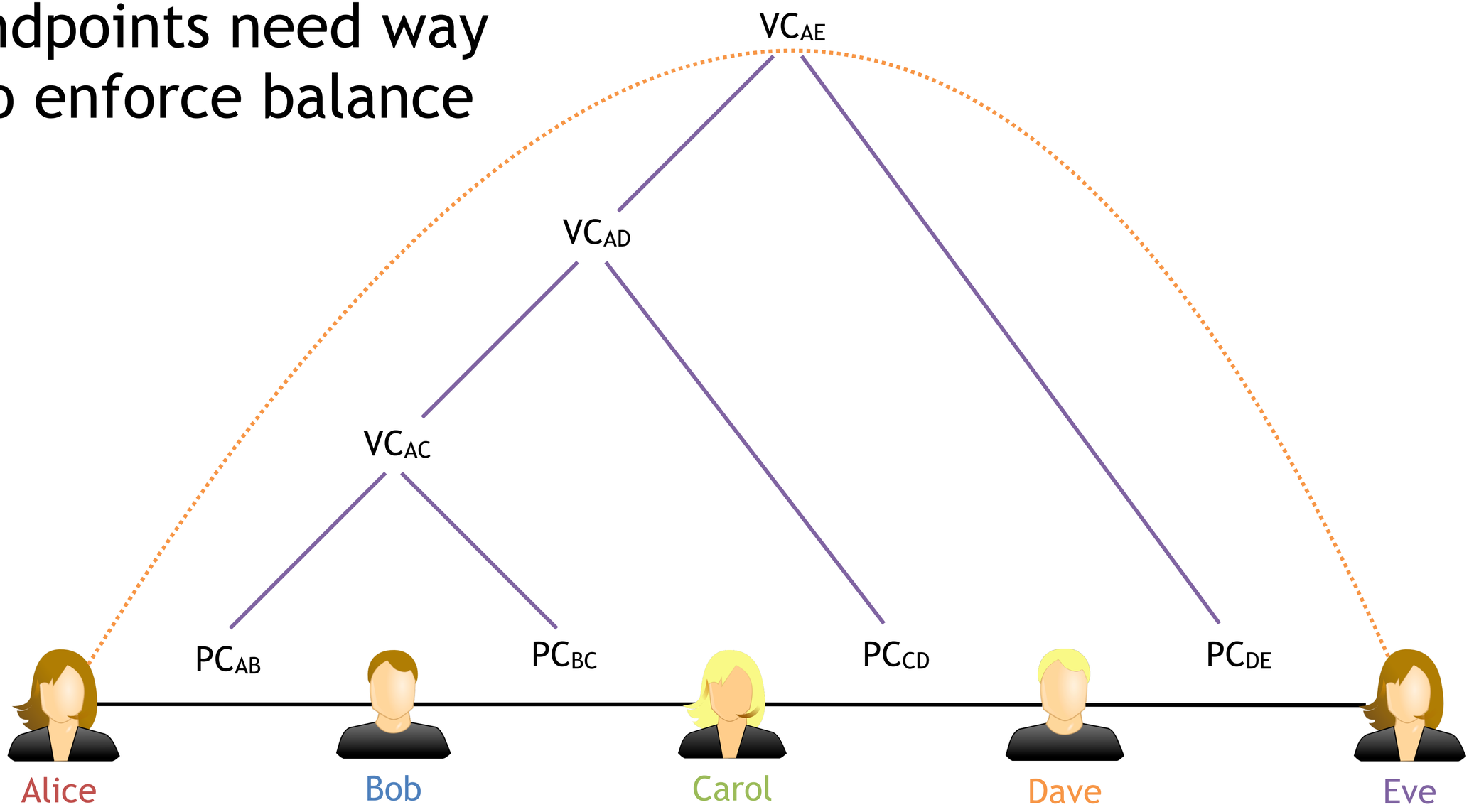
Two observations

(1) VC funded from underlying channels

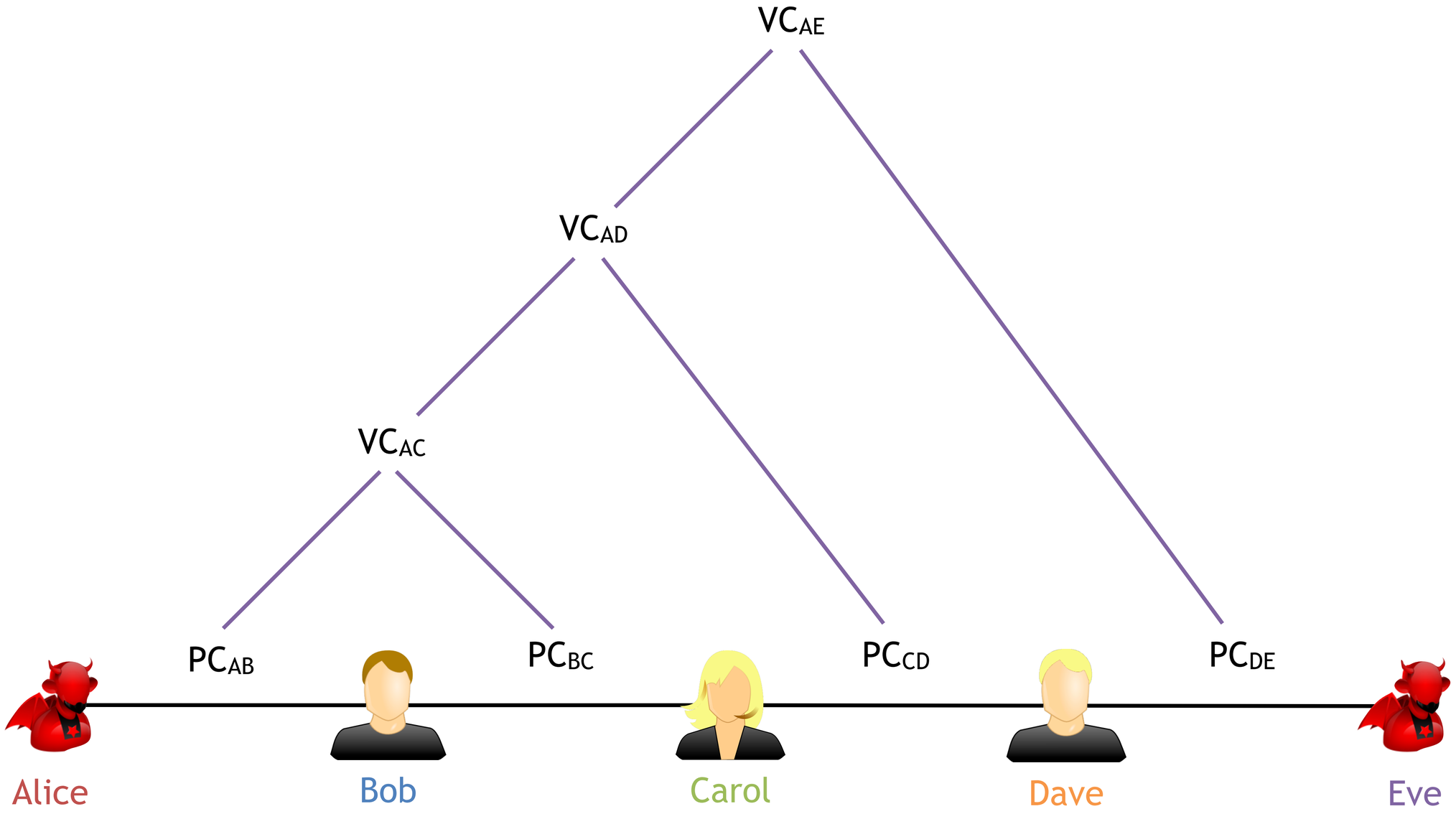


Two observations

(2) Endpoints need way to enforce balance

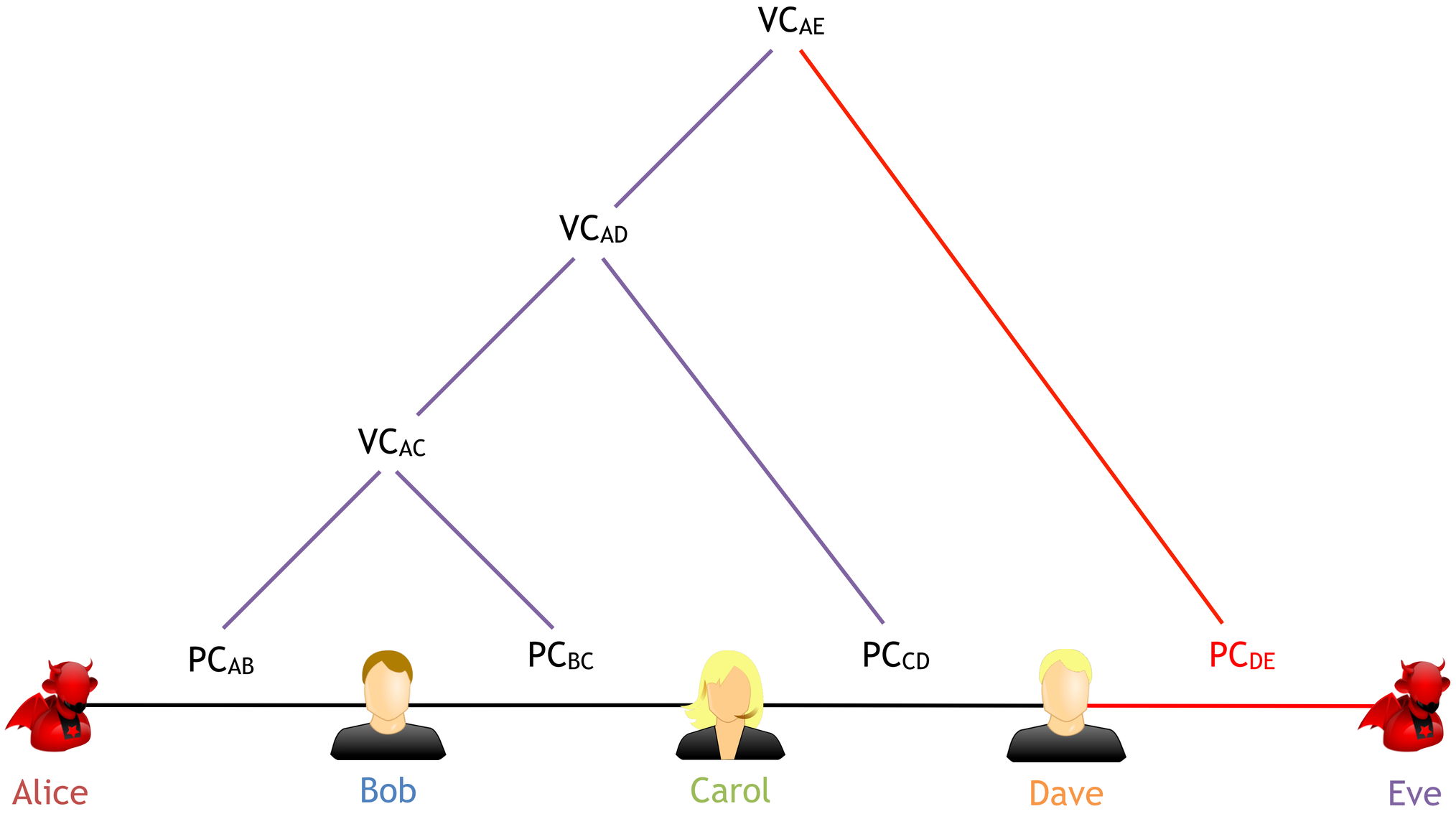


Domino attack



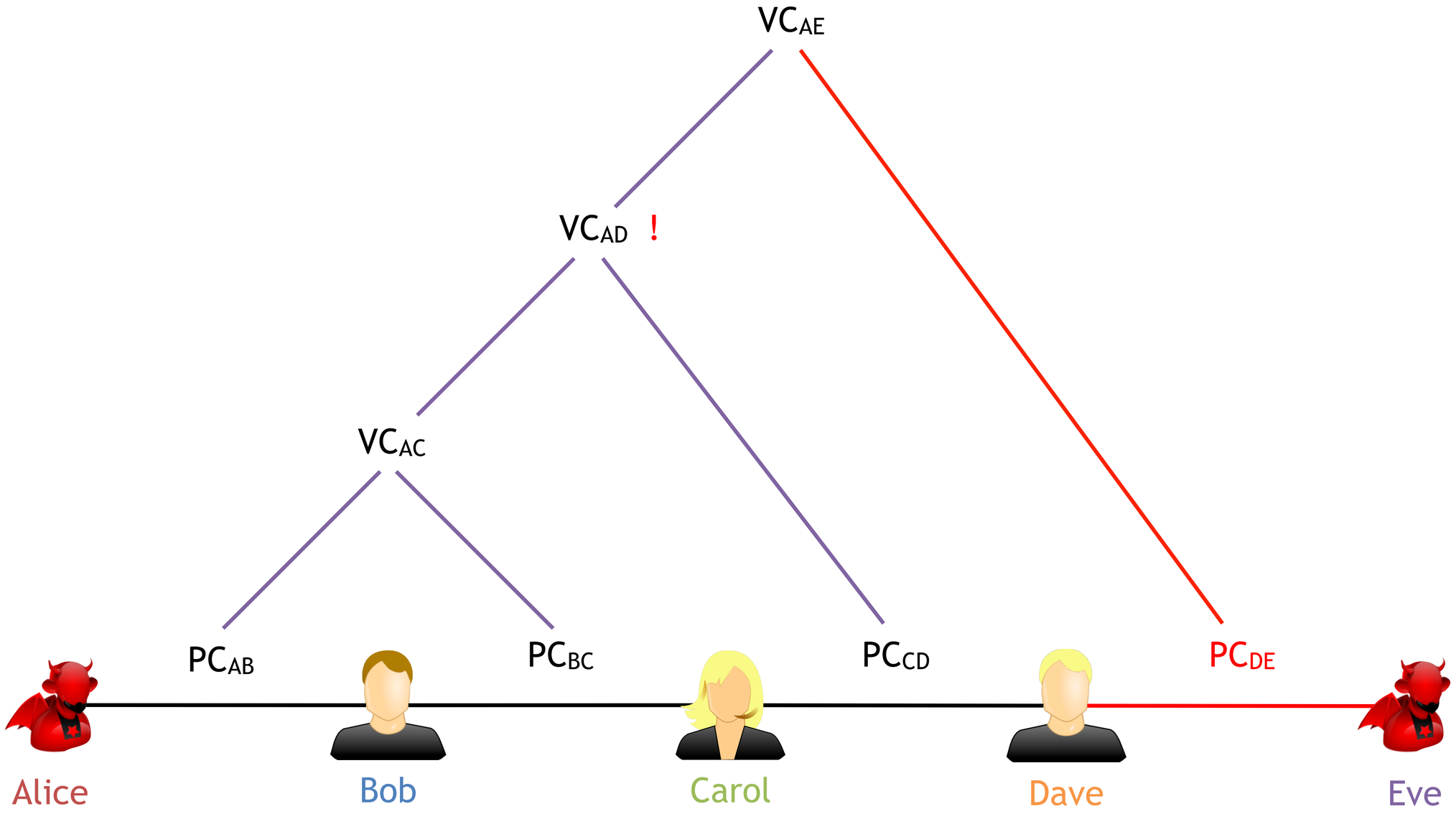
Alice (or Eve) has to have a way to forcefully ensure her balance on-chain.

Domino attack



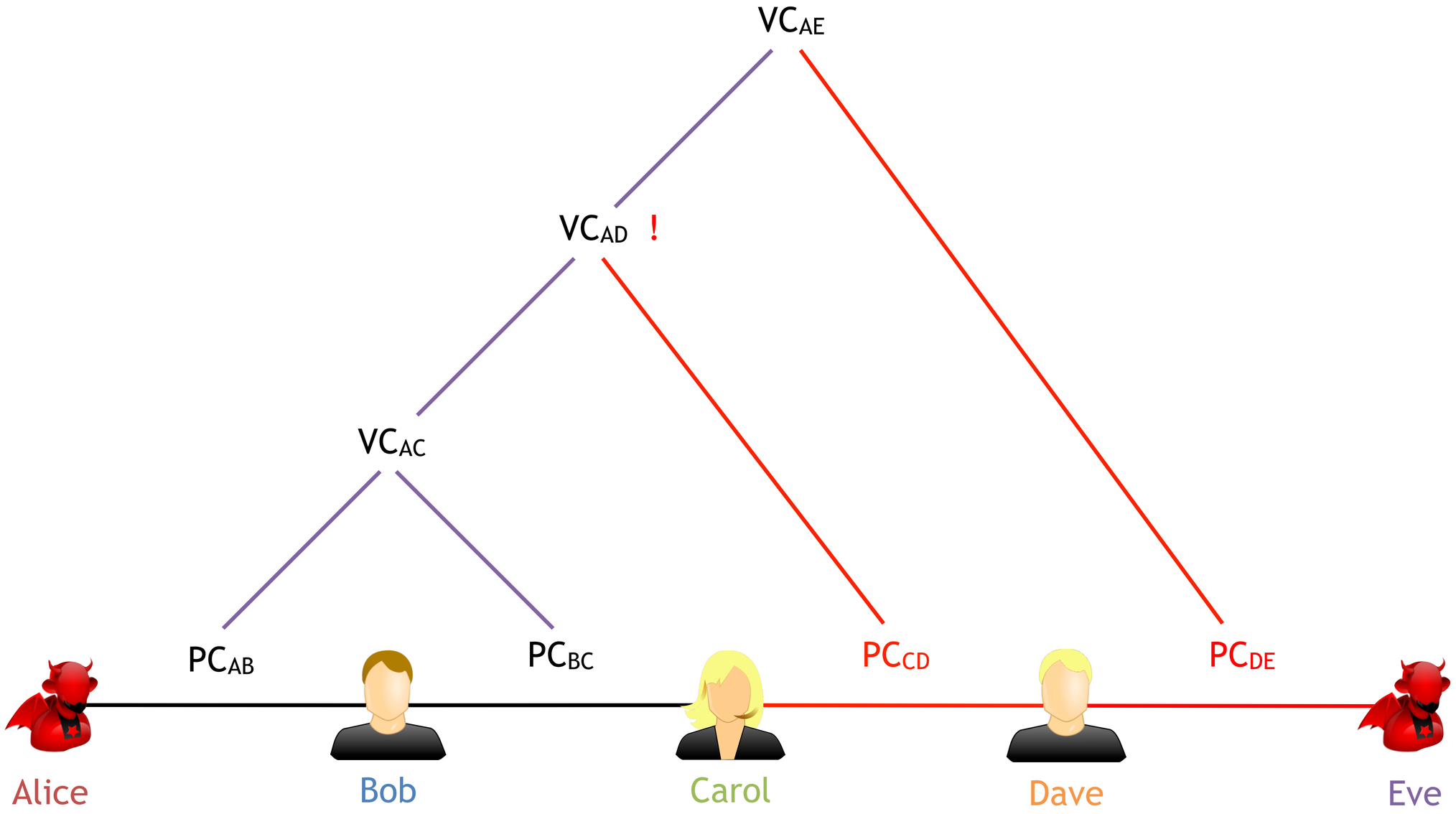
Eve initiates sequence to put VC_{AE} balance on-chain.

Domino attack



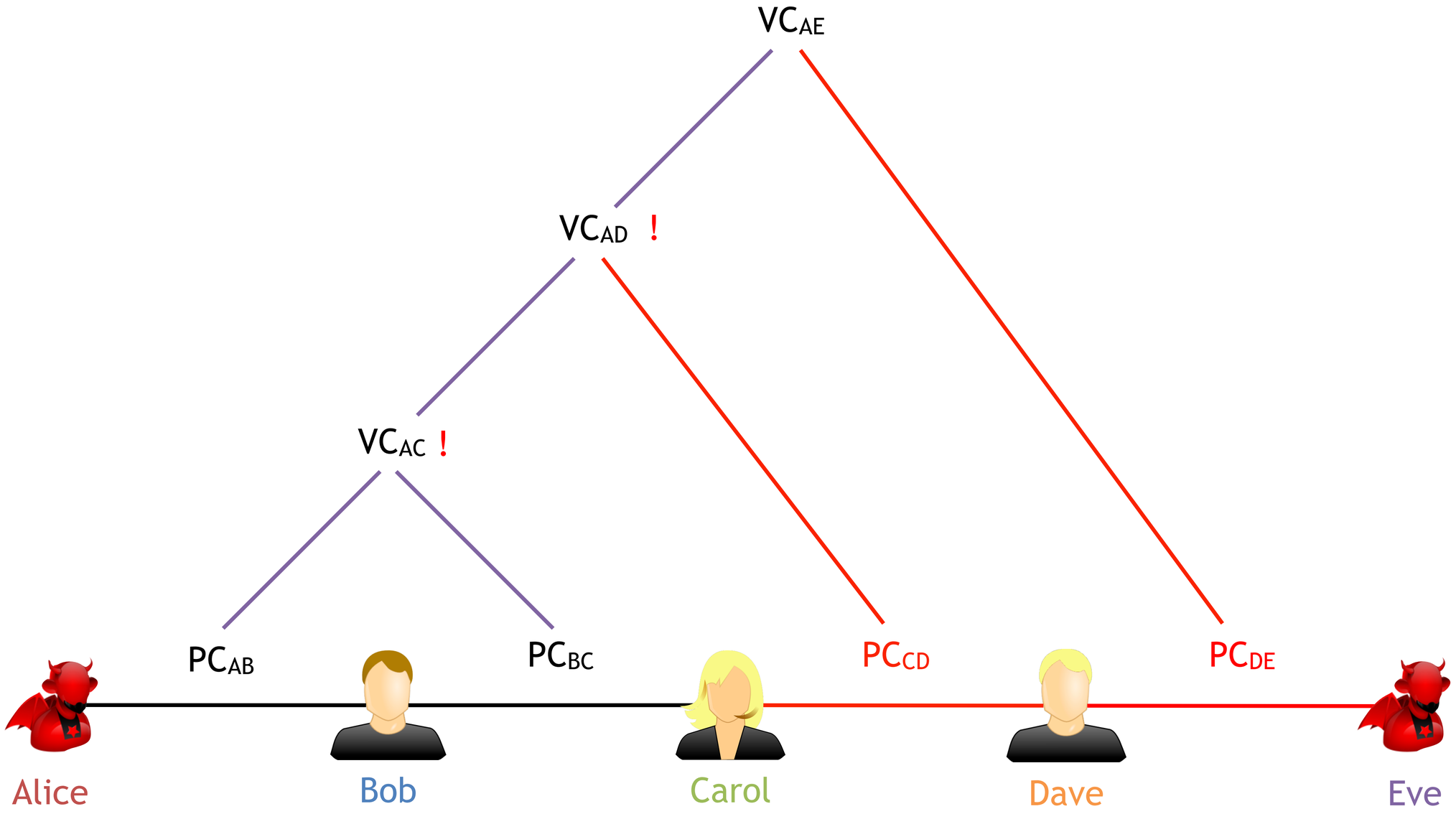
Dave has to react or will lose money otherwise.

Domino attack



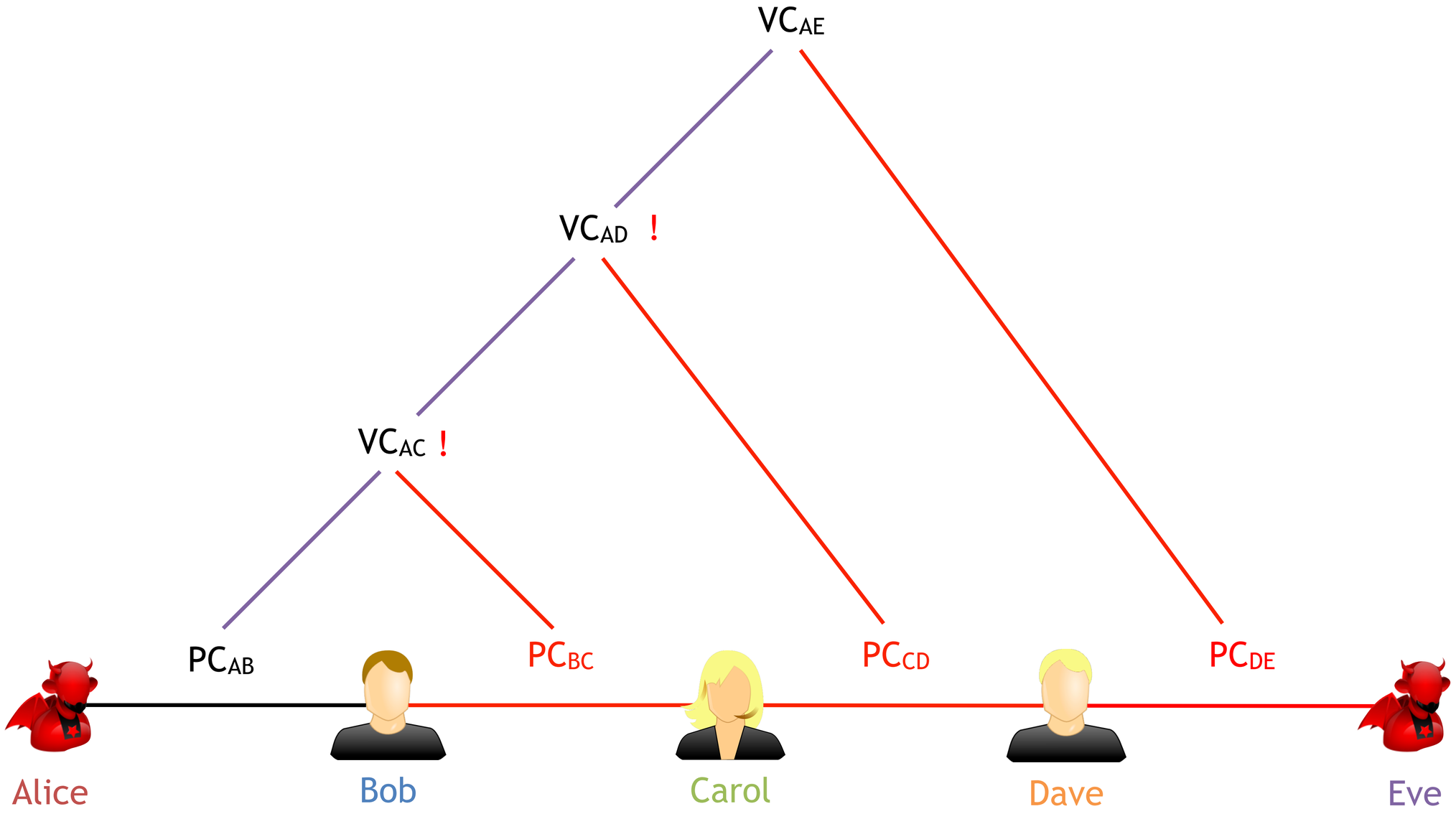
Dave initiates sequence to put VC_{AD} balance on-chain.

Domino attack



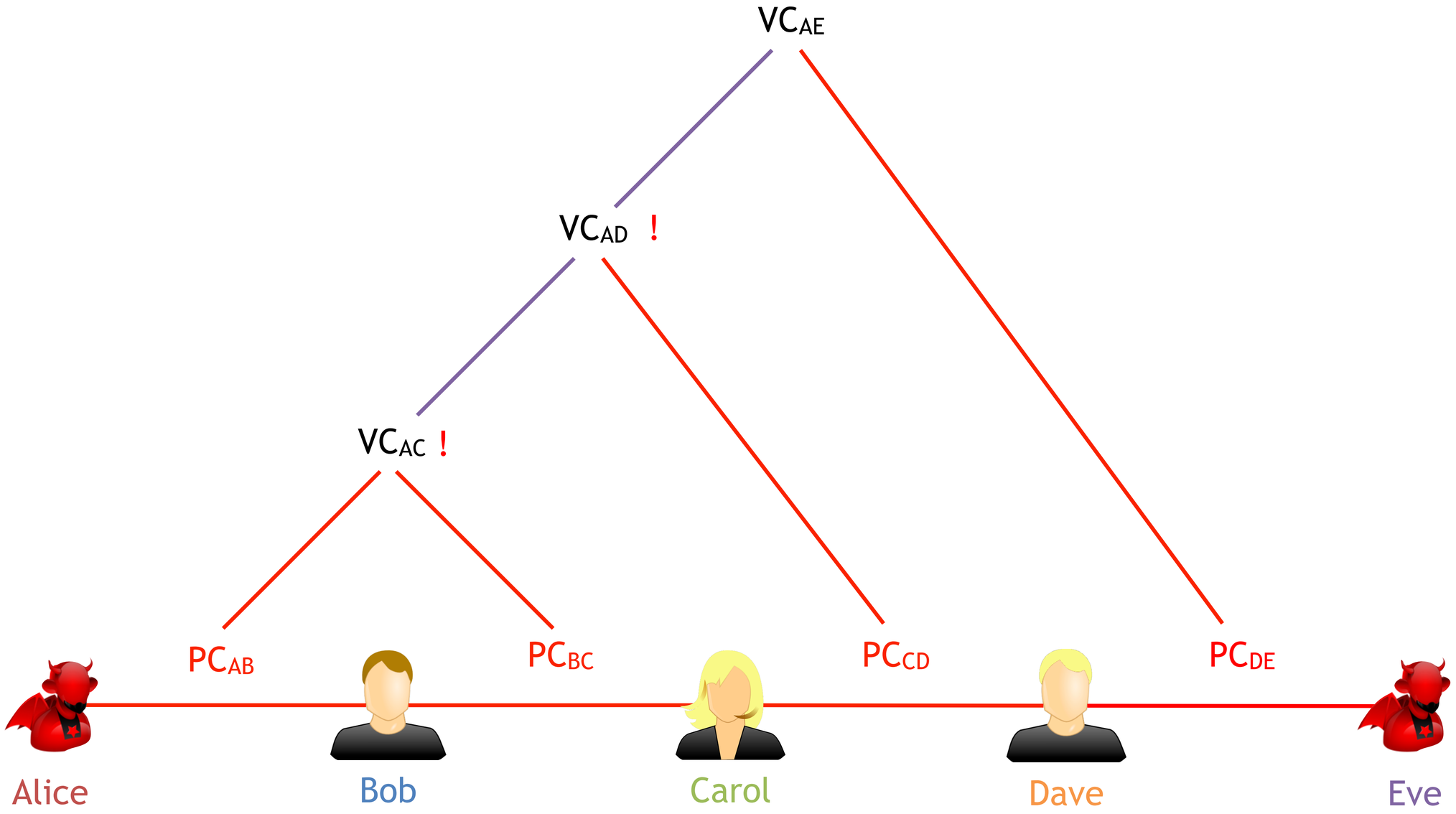
Carol has to react or will lose money otherwise.

Domino attack



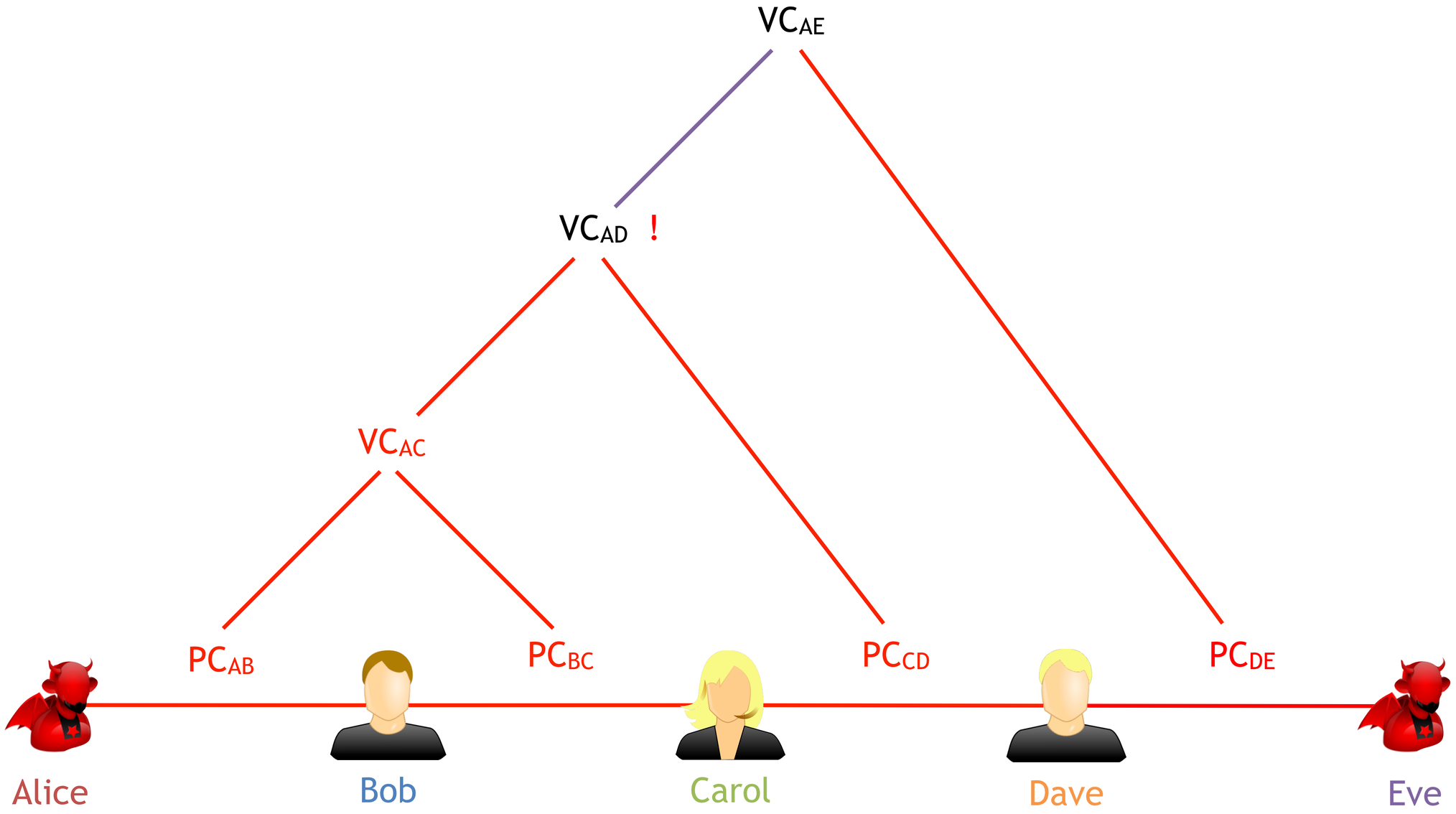
Carol initiates sequence to put VC_{AC} balance on-chain.

Domino attack



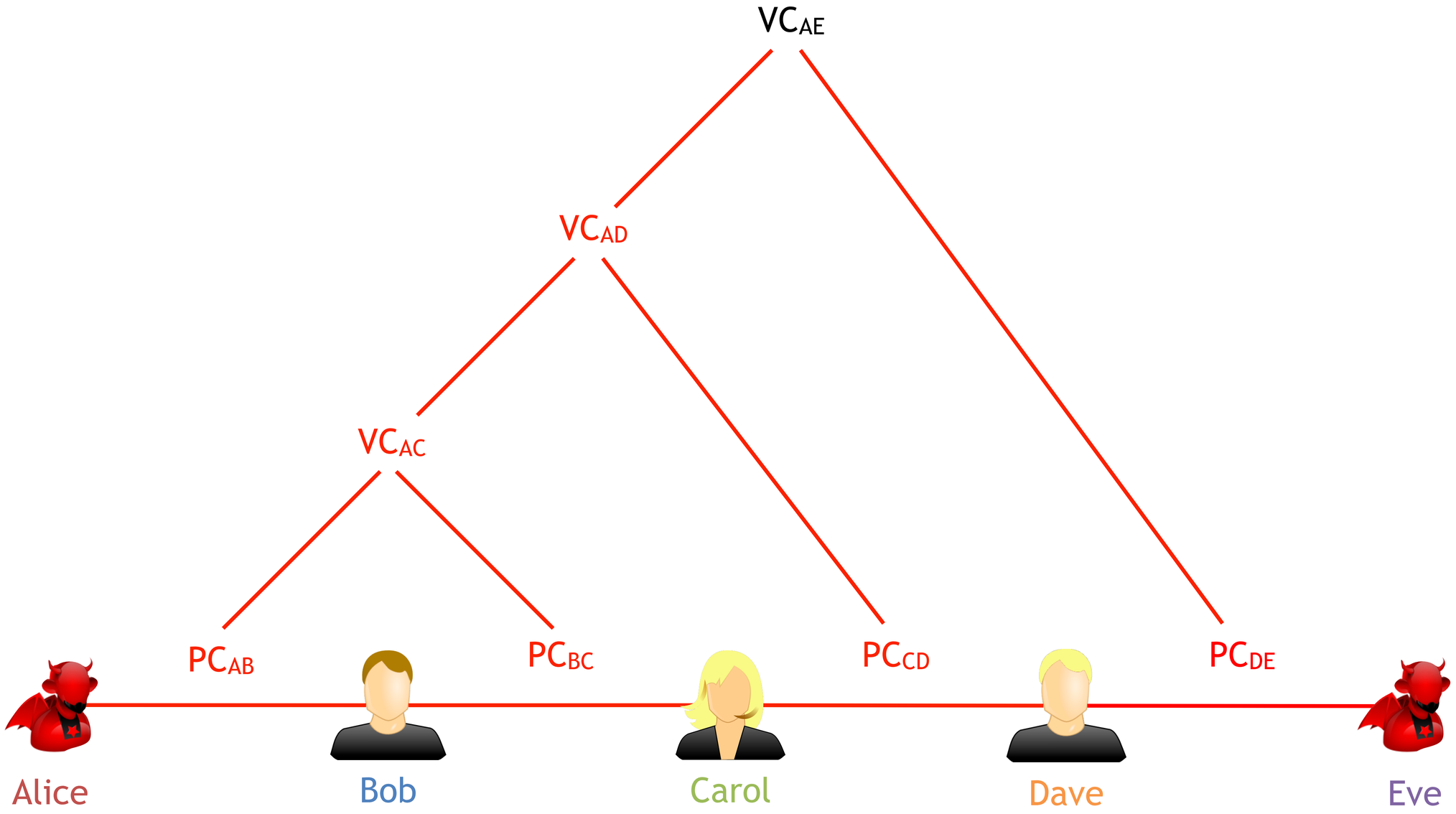
Bob has to react and puts PC_{AB} on-chain

Domino attack



All payment channels are on-chain, VCs can be closed

Domino attack



All payment channels are on-chain, VCs can be closed

Domino attack

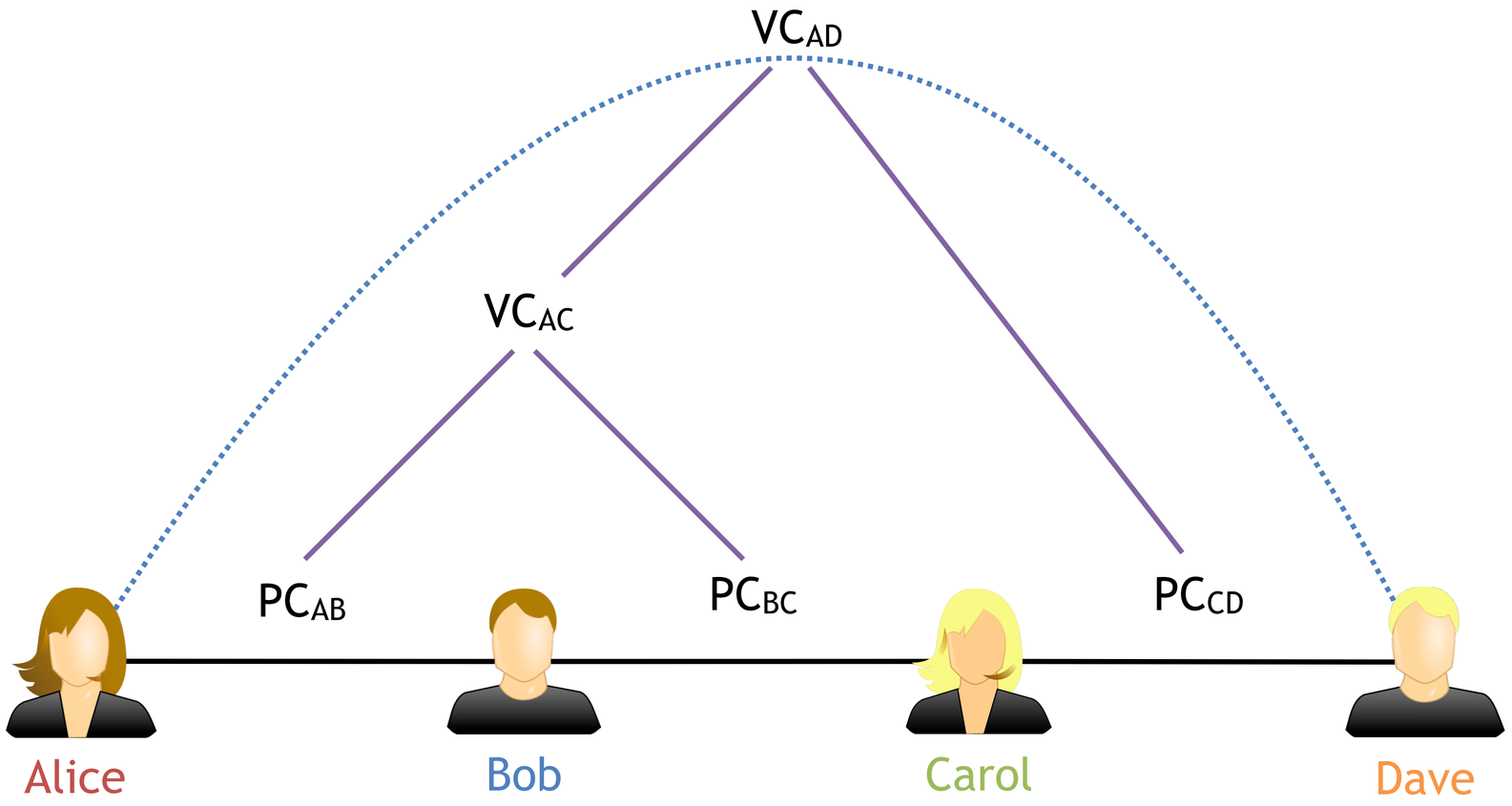
- An attacker can destruct the underlying PCN!
  - Simulation on Lightning Network (LN) snapshot
  - Spend 1 BTC to shut down whole LN
- Existing constructions should not be used

Donner

Recall reasons for Domino attack

(1) VC funded from underlying channels

(2) Endpoints need way to enforce balance

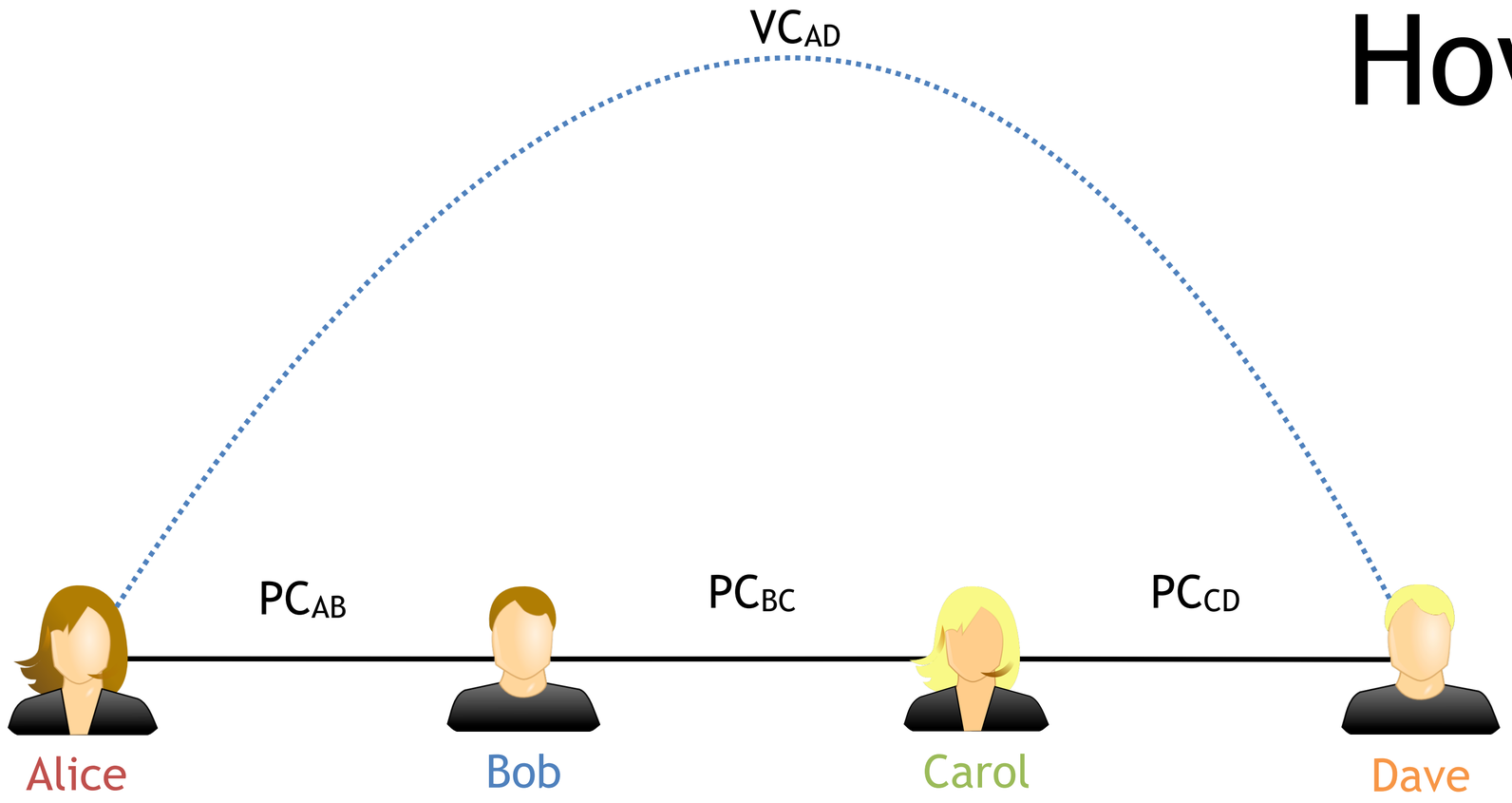


Donner idea

(1) ~~VC funded from underlying channels~~

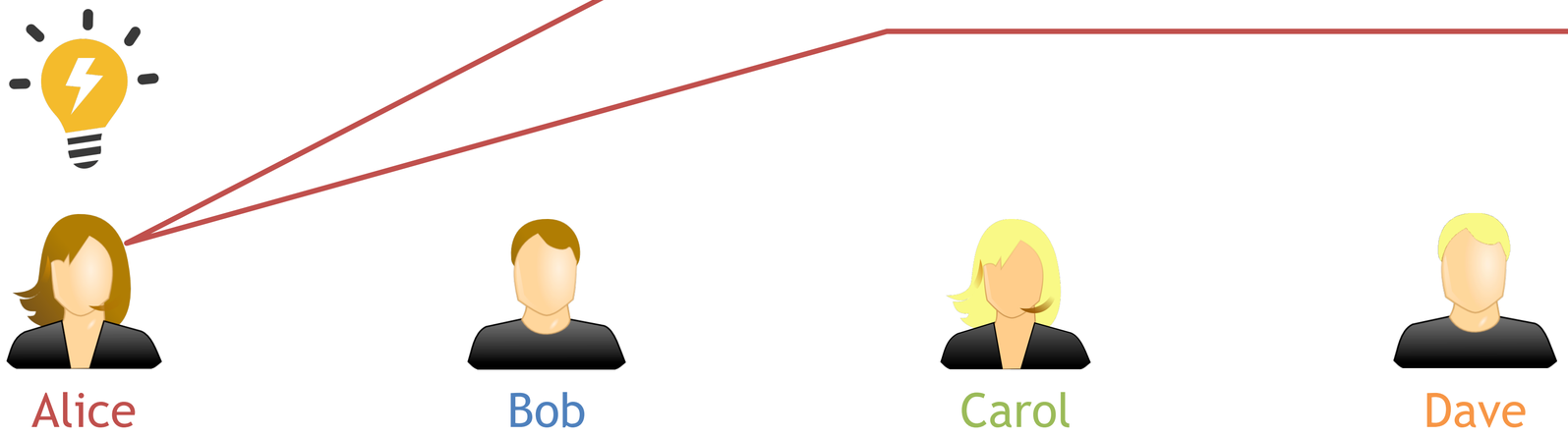
(2) Endpoints need ~~way to enforce balance~~ to be sure not to lose money

How?

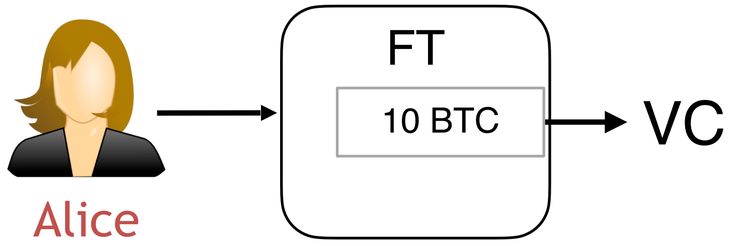


Virtual Channel

- Let me fund the VC from a tx FT that does not exist

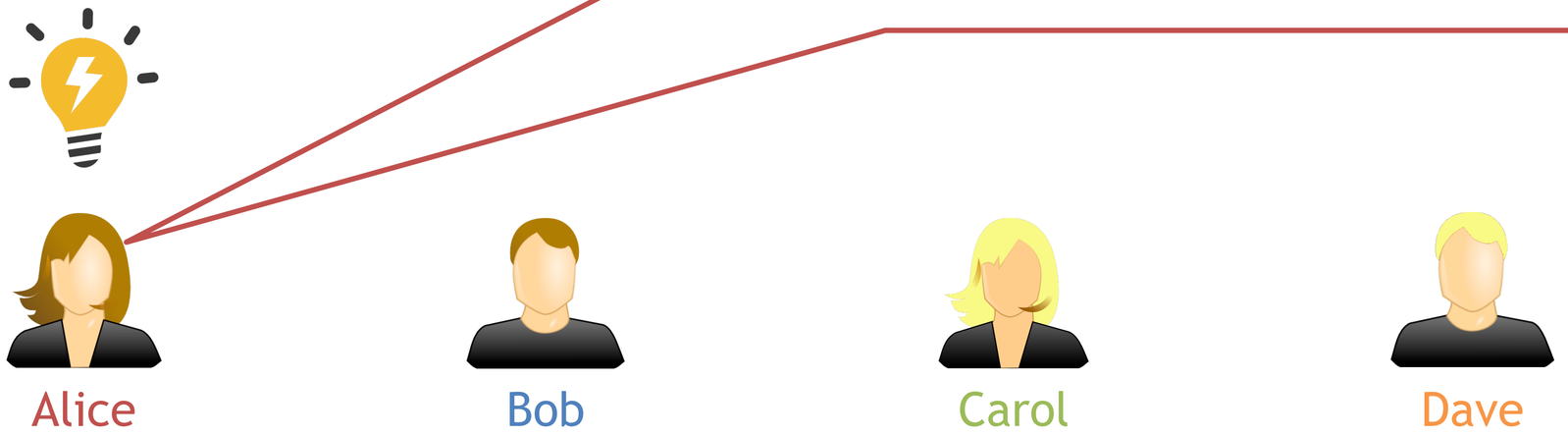


Virtual Channel

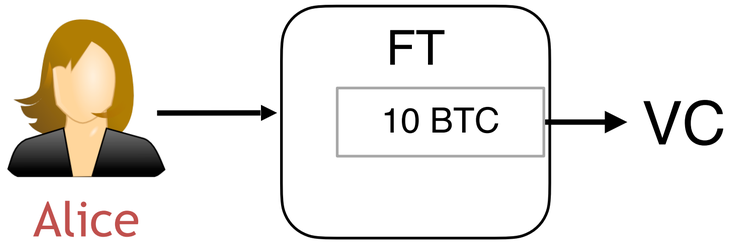


Funding transaction
of the virtual channel

- Let me fund the VC from a tx FT that does not exist

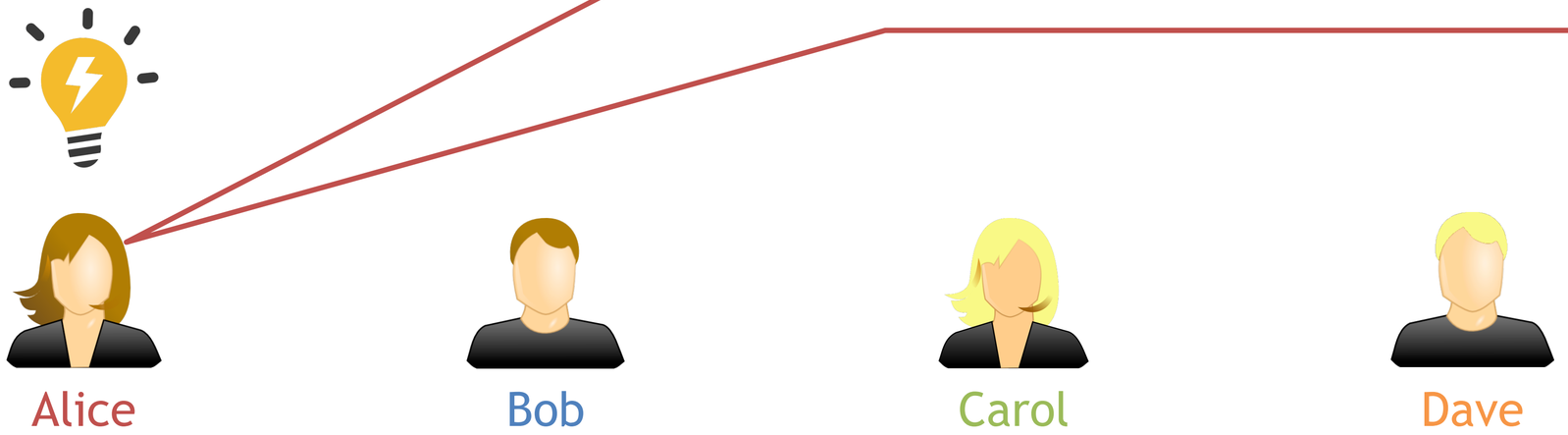


Virtual Channel

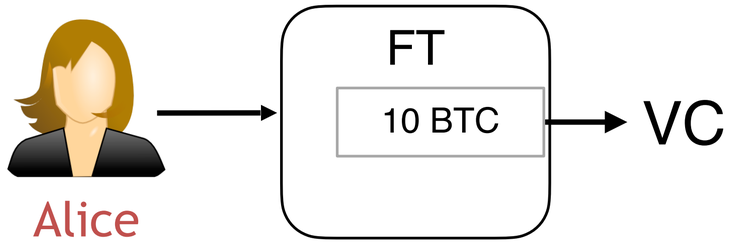


Funding transaction
of the virtual channel

- Let me fund the VC from a tx FT that does not exist
- Let's pretend it exists and use the VC

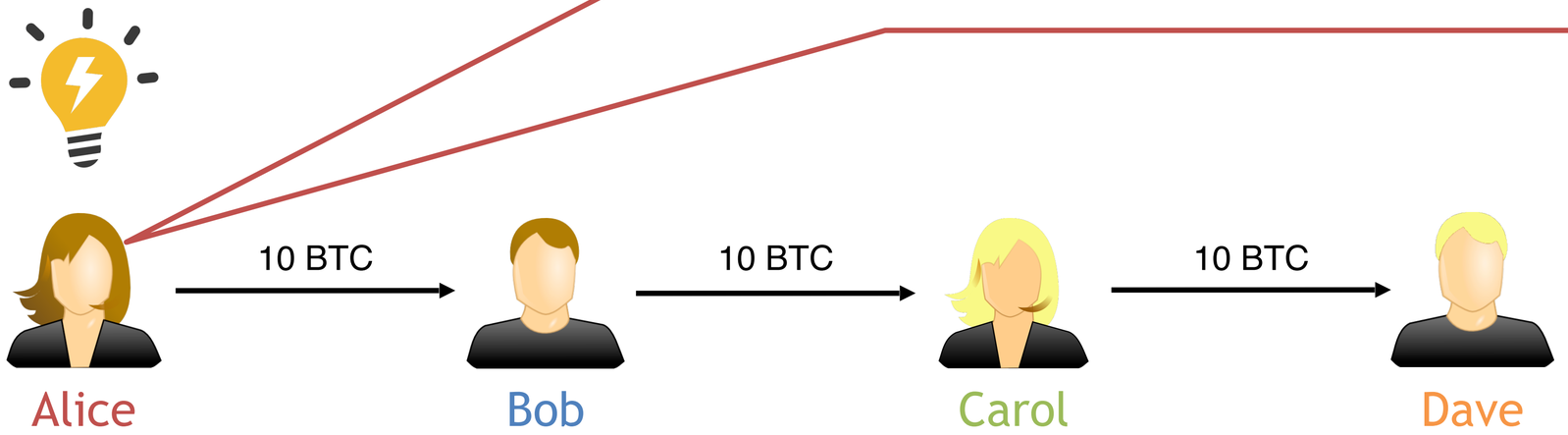


Virtual Channel

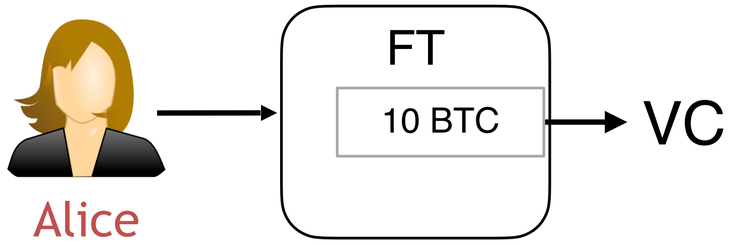


Funding transaction
of the virtual channel

- Let me fund the VC from a tx FT that does not exist
- Let's pretend it exists and use the VC
- I set up a collateral payment to you:

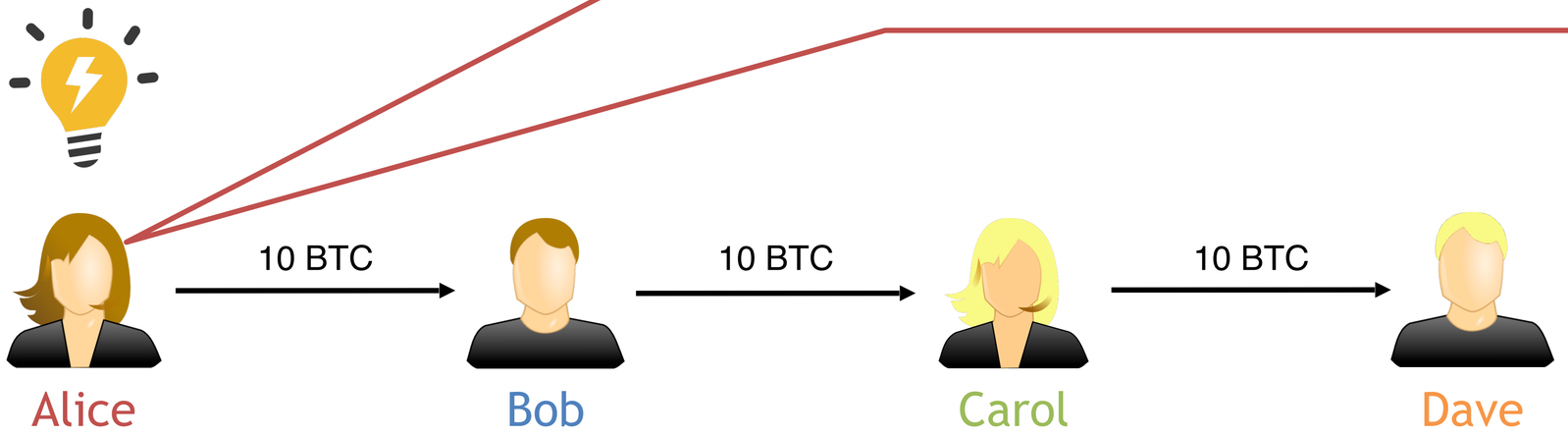


Virtual Channel

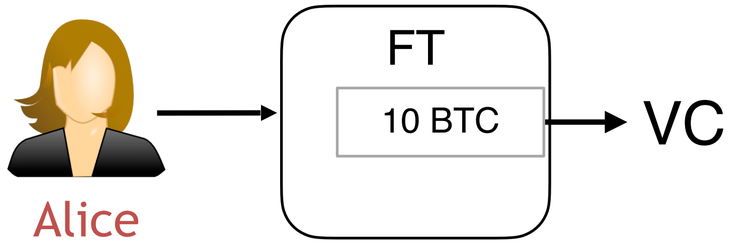


Funding transaction
of the virtual channel

- Let me fund the VC from a tx FT that does not exist
- Let's pretend it exists and use the VC
- I set up a collateral payment to you:
  - FT on-chain: I (Alice) get money back

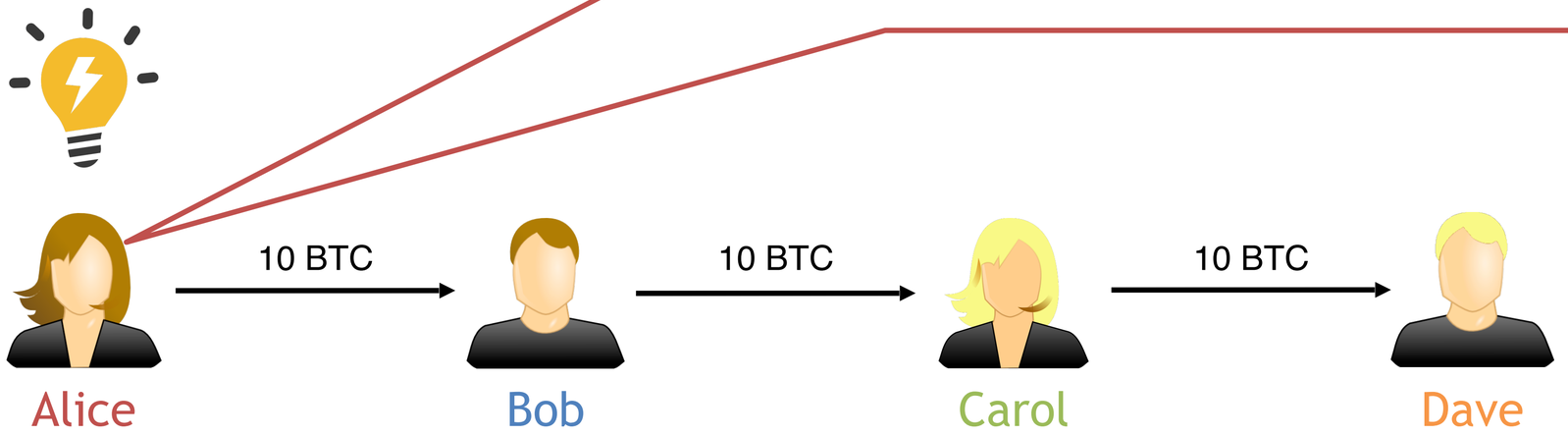


Virtual Channel



Funding transaction
of the virtual channel

- Let me fund the VC from a tx FT that does not exist
- Let's pretend it exists and use the VC
- I set up a collateral payment to you:
  - FT on-chain: I (Alice) get money back
  - Else: You (Dave) get money after timeout



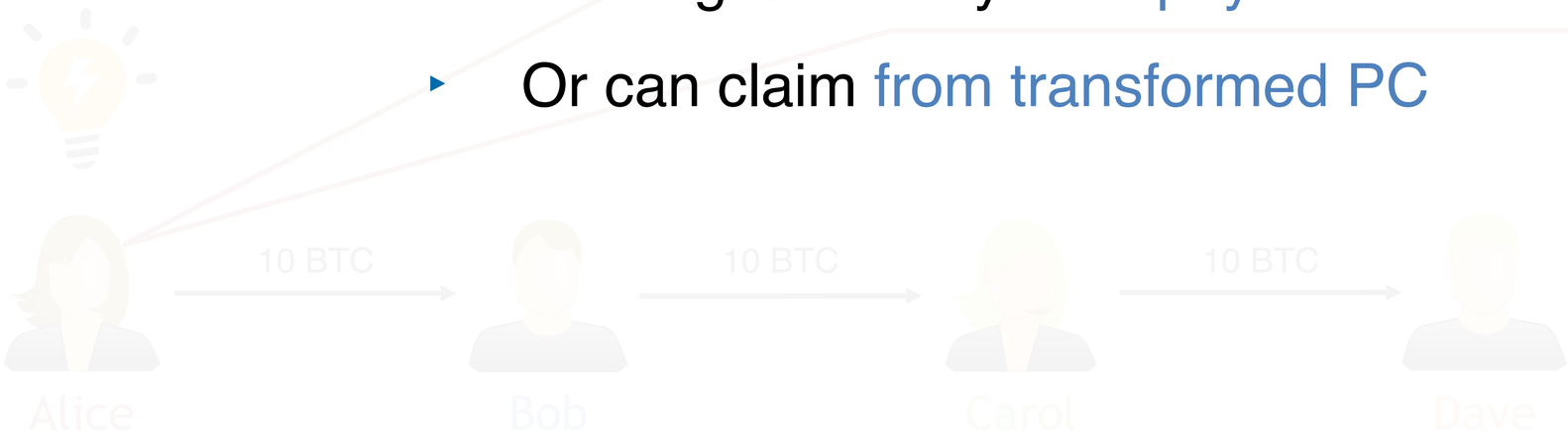
Virtual Channel

Funding transaction
of the virtual channel

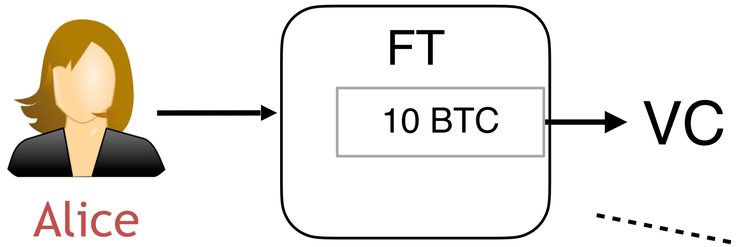
Rationale

- Posting FT, means that the VC is now funded on-chain -> PC
- Dave is safe
  - Either gets money from payment
  - Or can claim from transformed PC

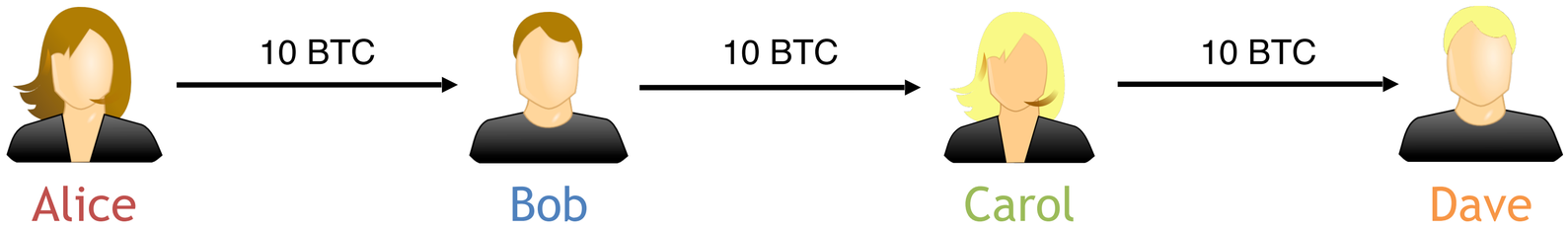
- Let me fund the VC from a tx FT that does not exist
- Let's pretend it exists and use the VC to pay collateral payment to you:
  - FT on-chain: I get money back
  - Else: You get money after timeout



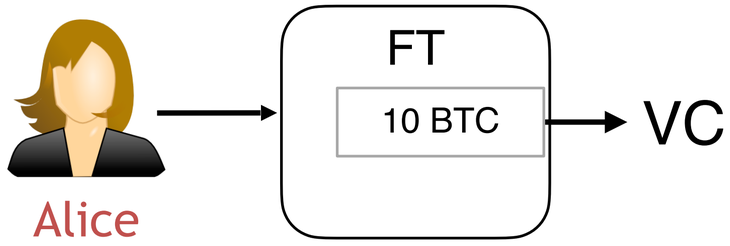
Virtual Channel

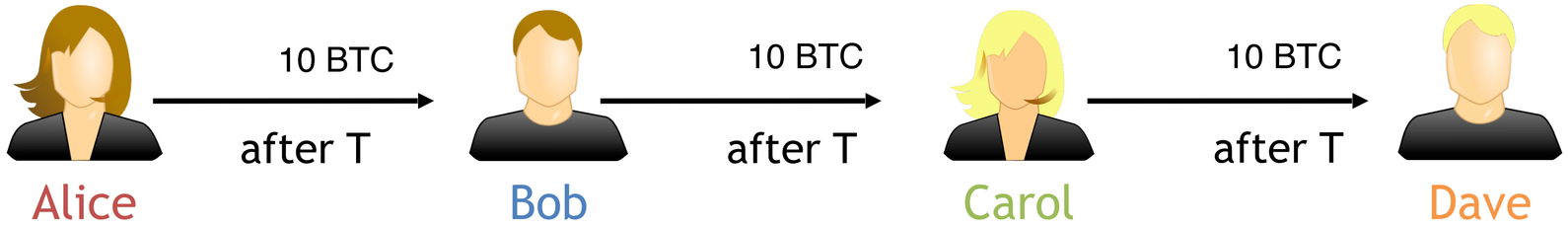


- Challenge: FT and payment must be mutually exclusive!



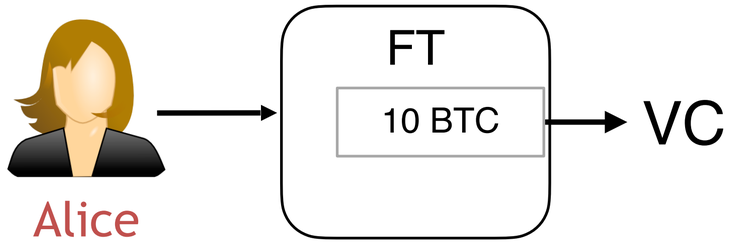
Donner (simplified)

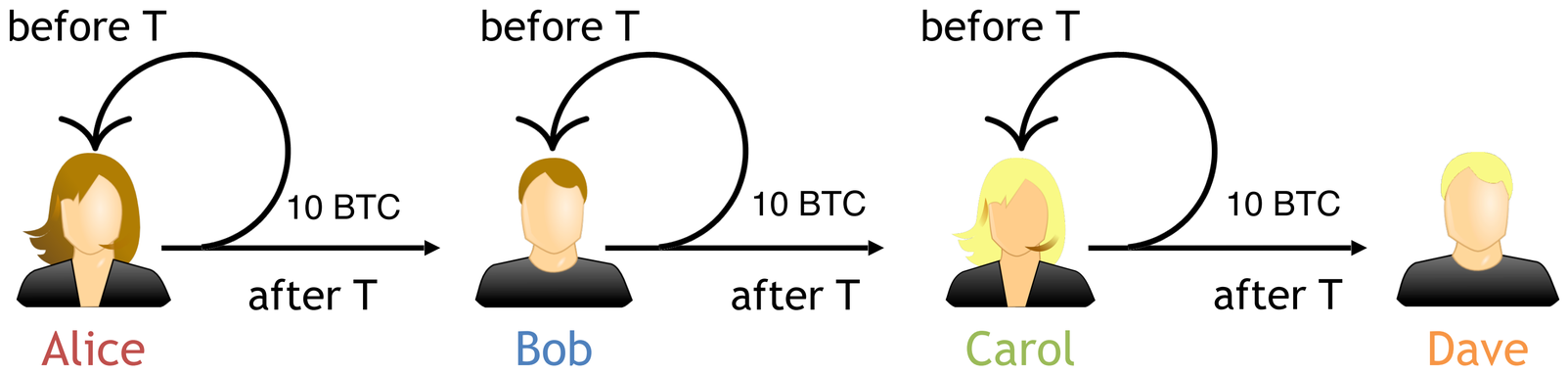




Payment is successful after timeout T

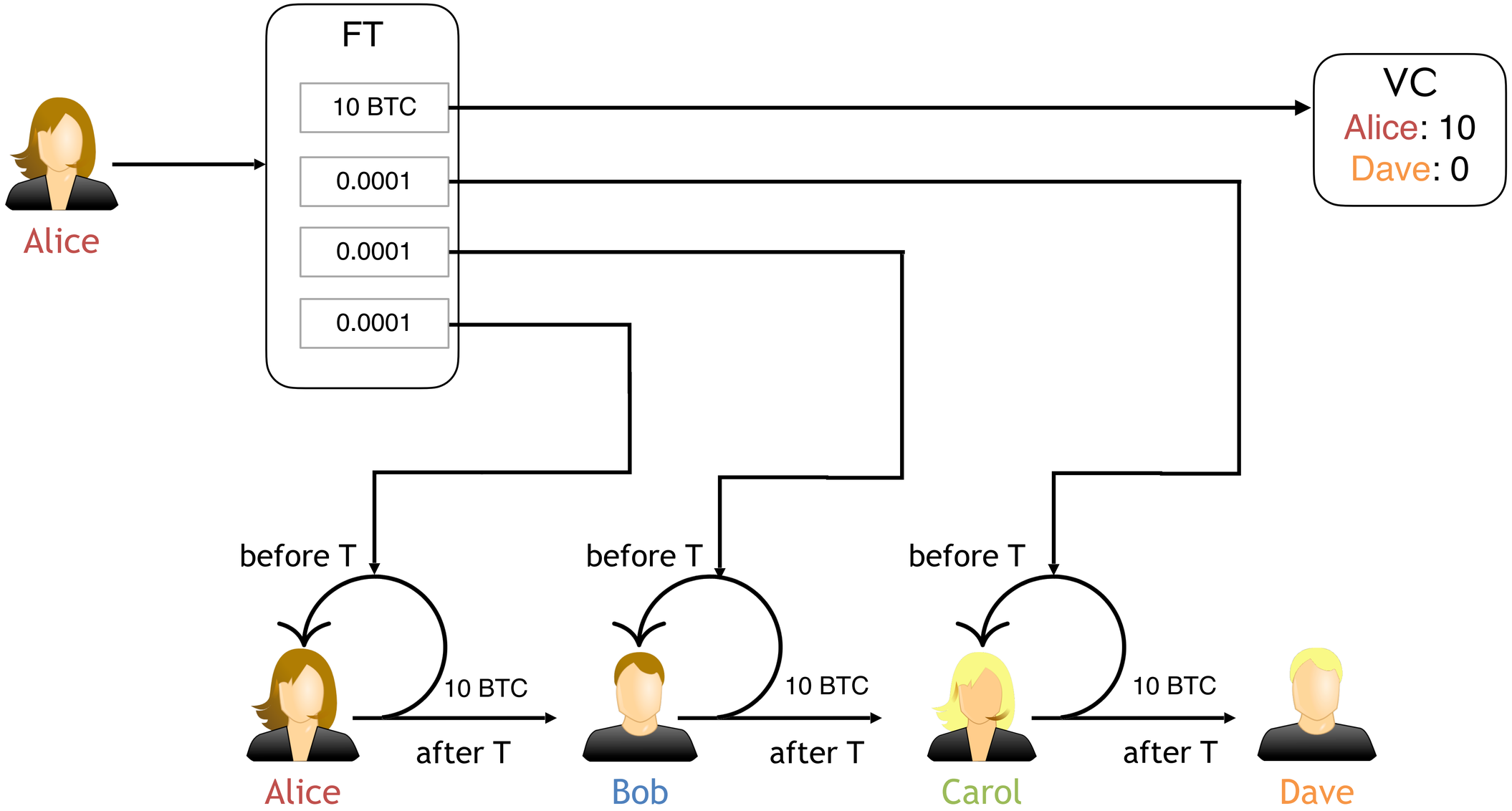
Donner (simplified)





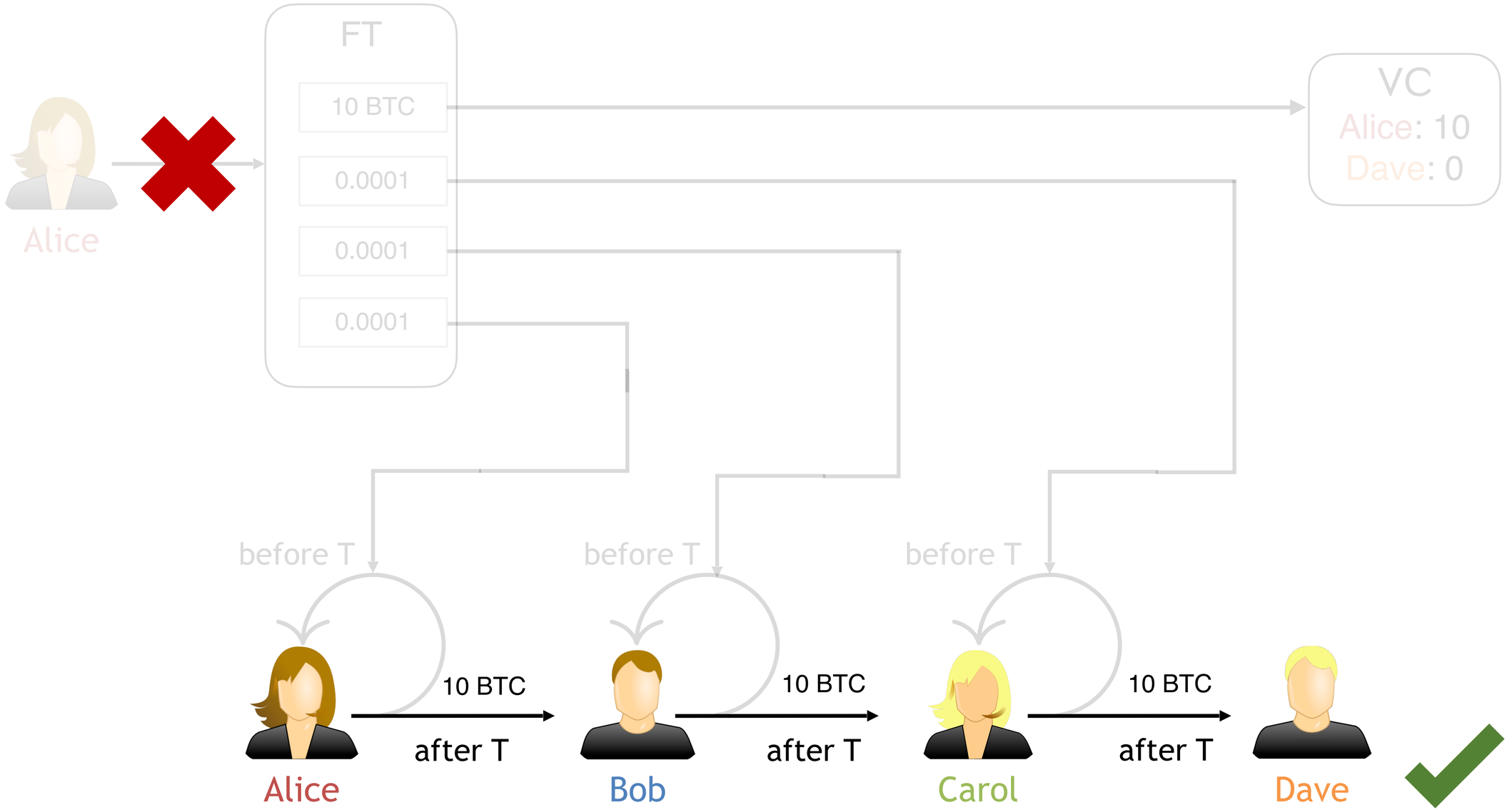
Before T, Alice can refund payment

Donner (simplified)



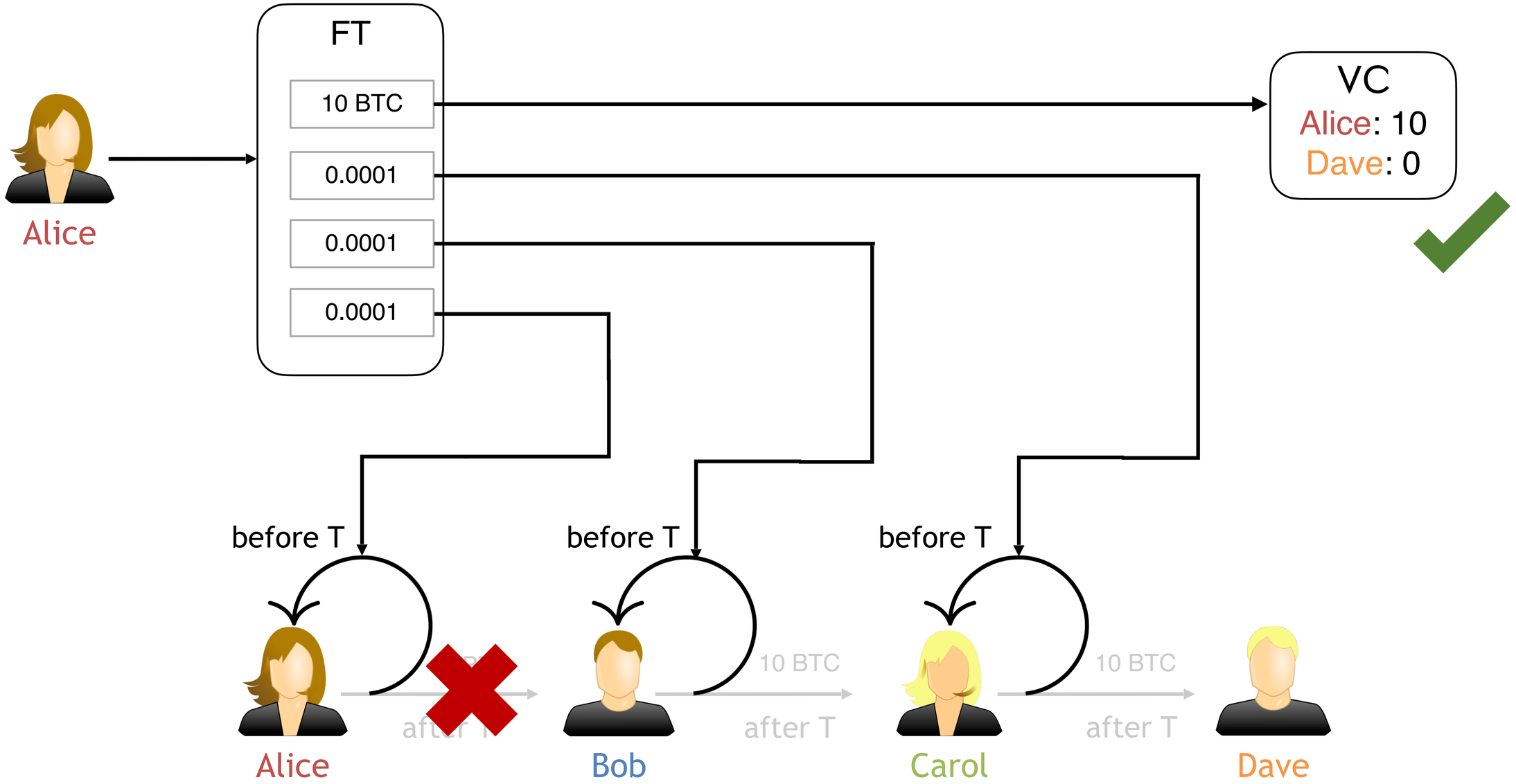
Before T, Alice can refund payment iff she posts FT

Donner (simplified)



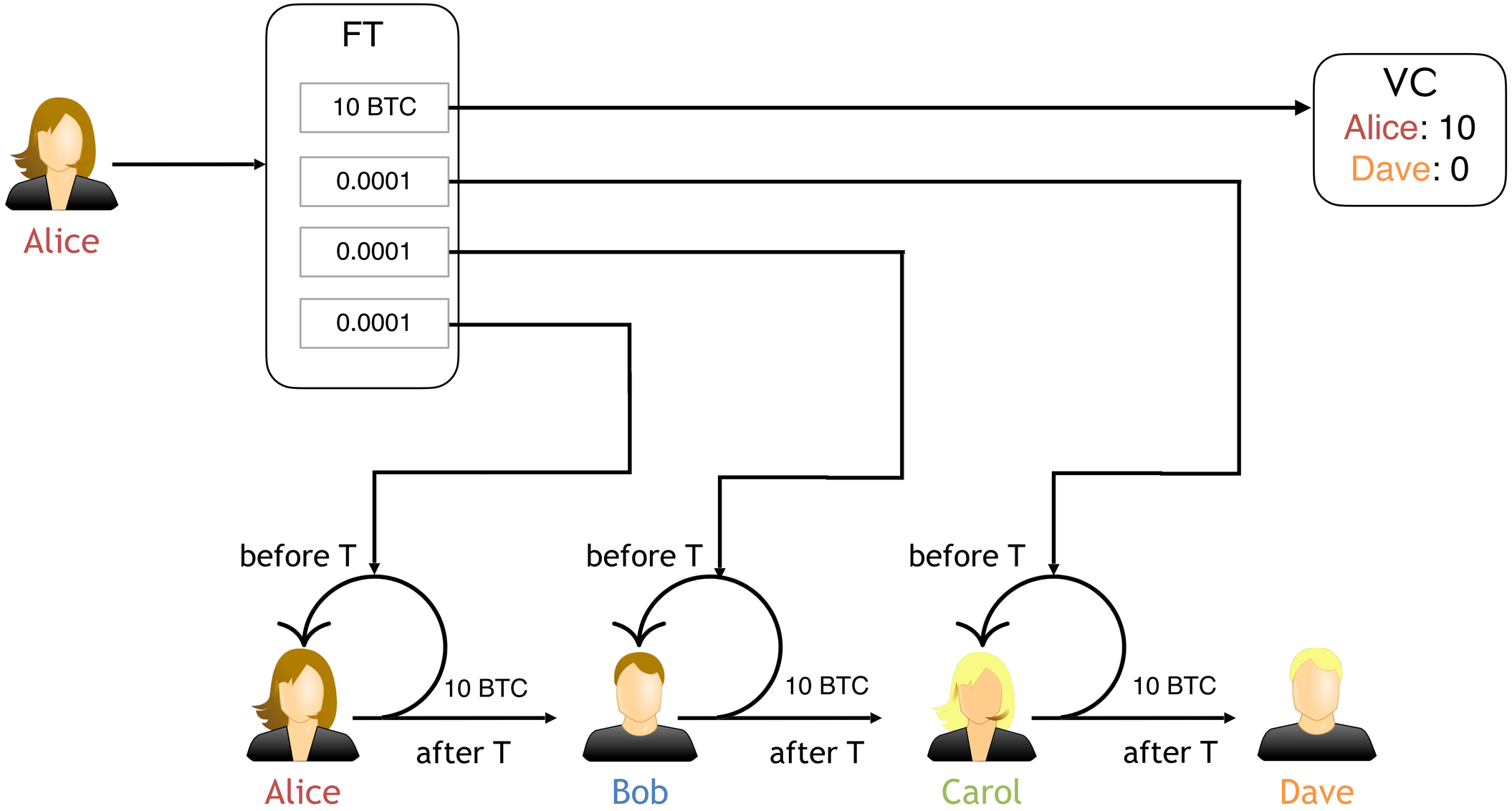
[5] L. Aumayr, P. Moreno-Sanchez, A. Kate and M. Maffei, "Blitz: Secure Multi-Hop Payments Without Two-Phase Commits," USENIX Security, *2021*

Donner (simplified)

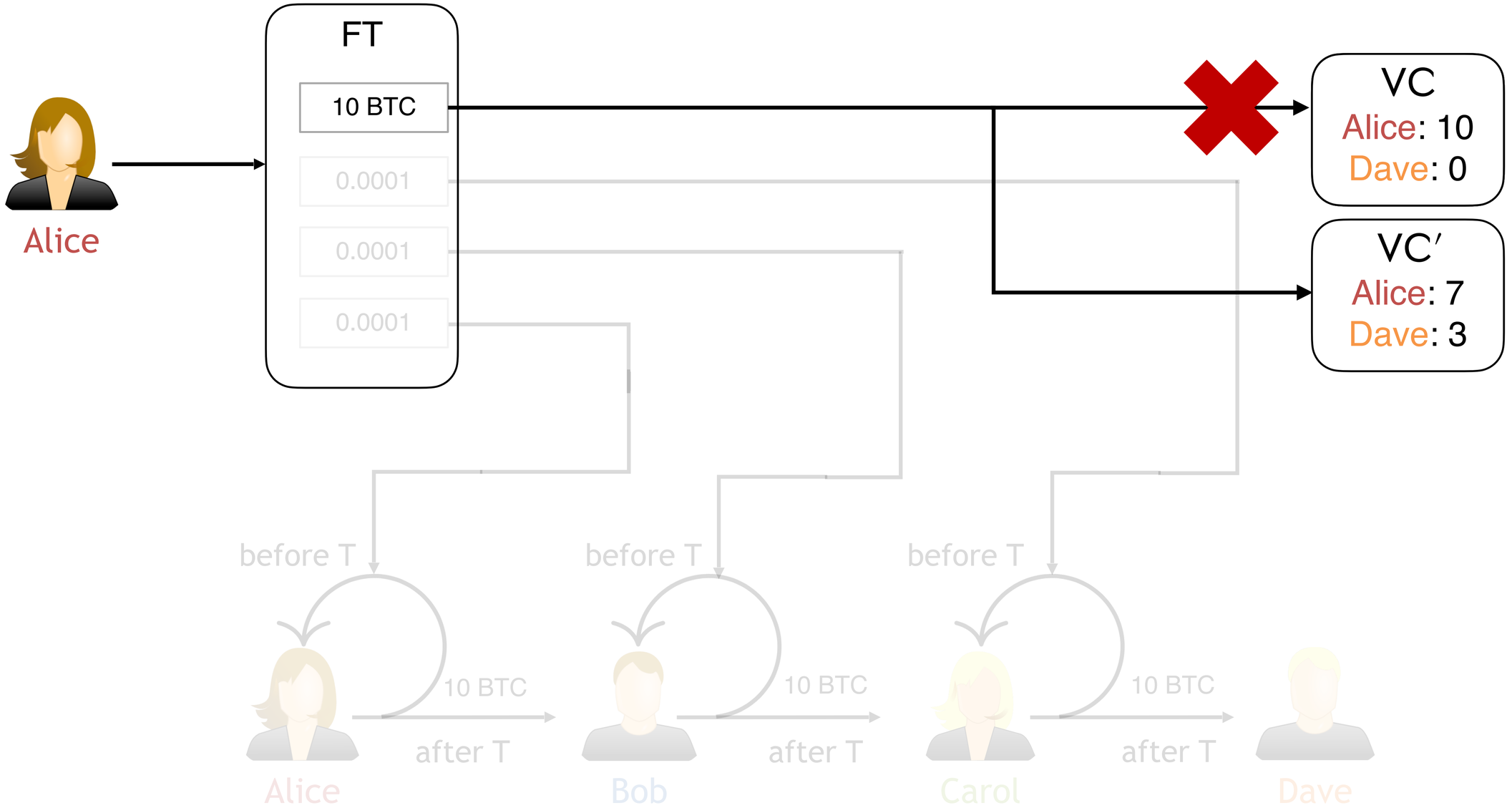


[5] L. Aumayr, P. Moreno-Sanchez, A. Kate and M. Maffei, "Blitz: Secure Multi-Hop Payments Without Two-Phase Commits," USENIX Security, *2021*

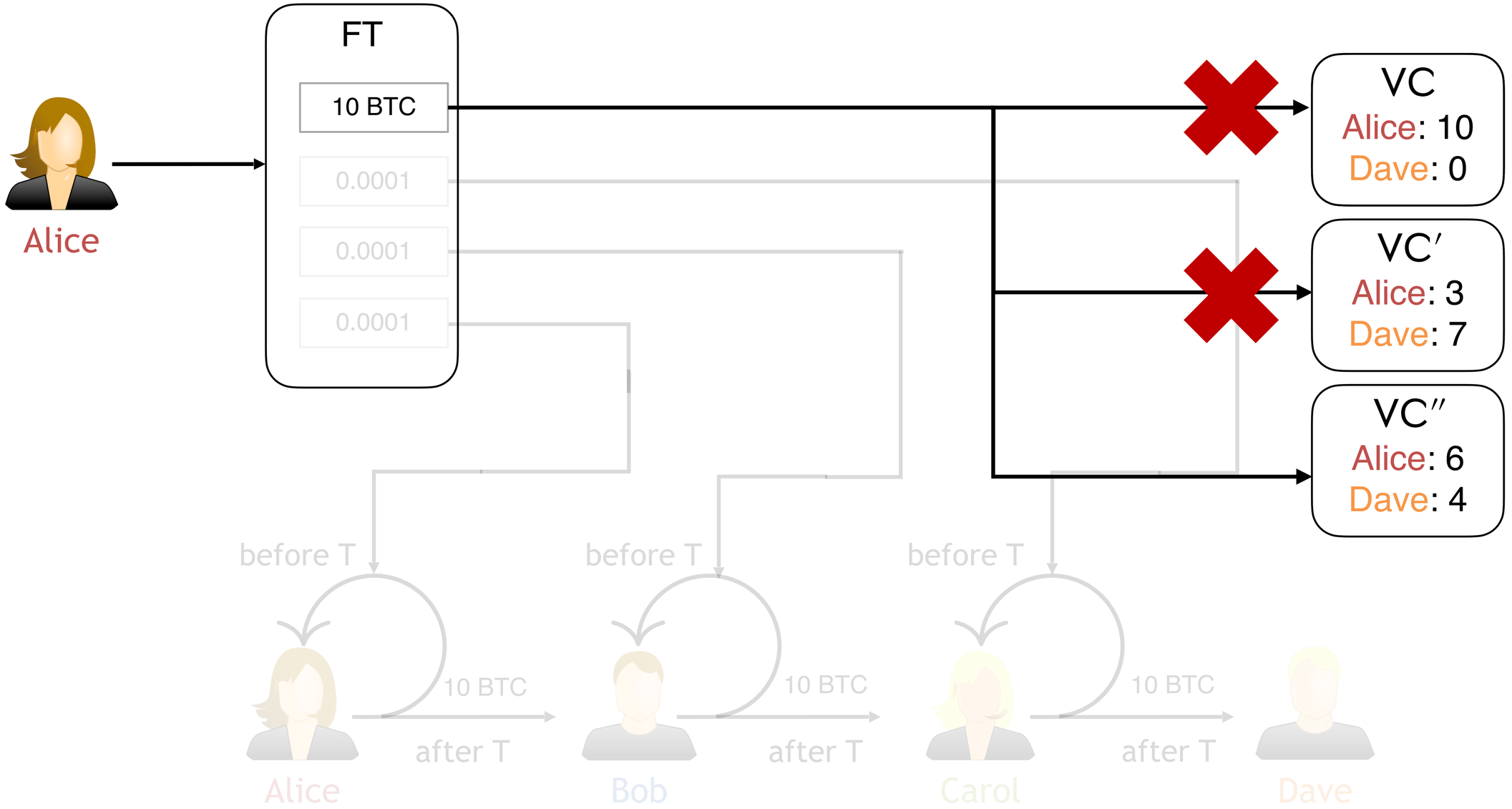
Donner (simplified)



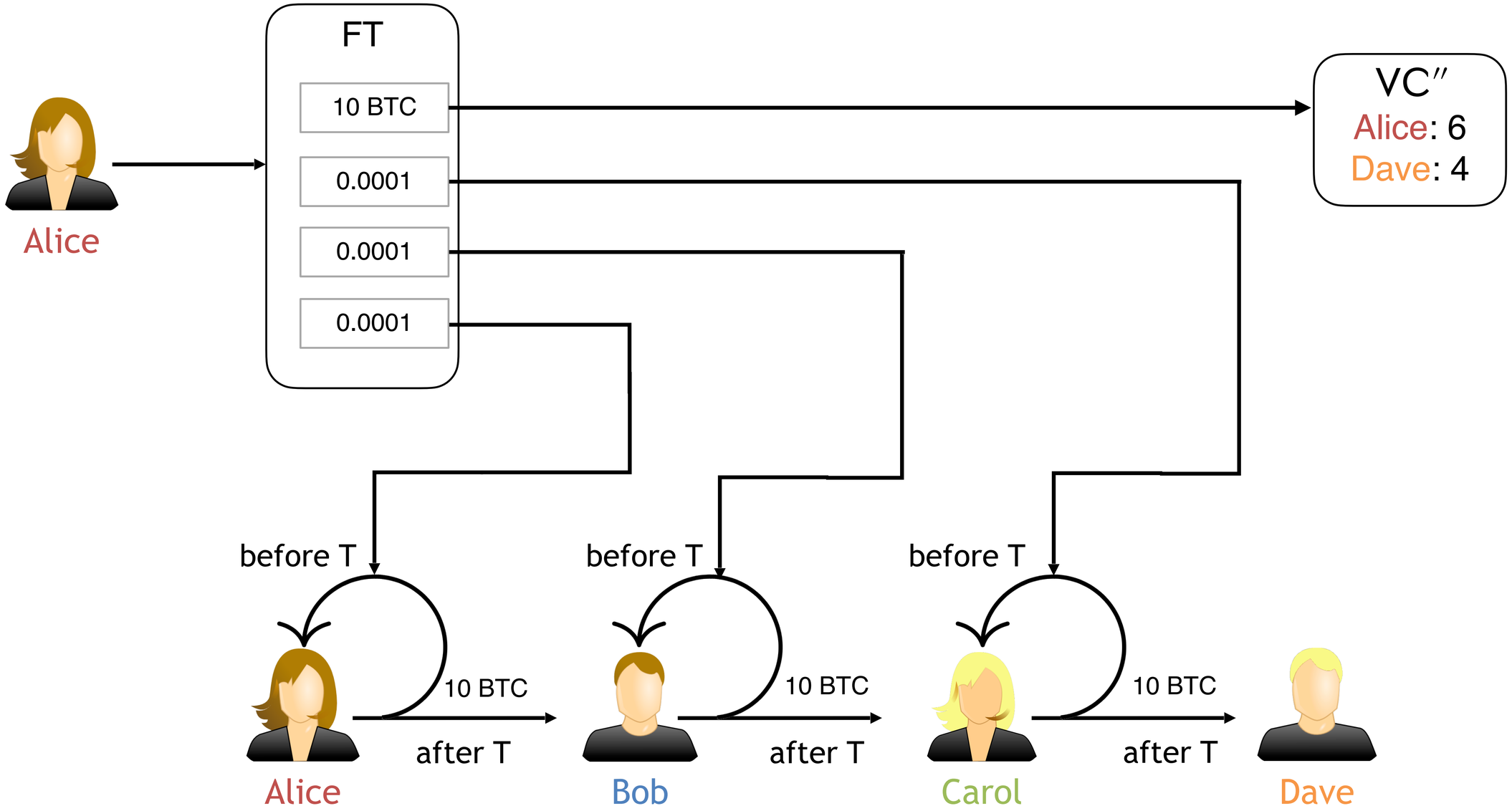
Donner (simplified)



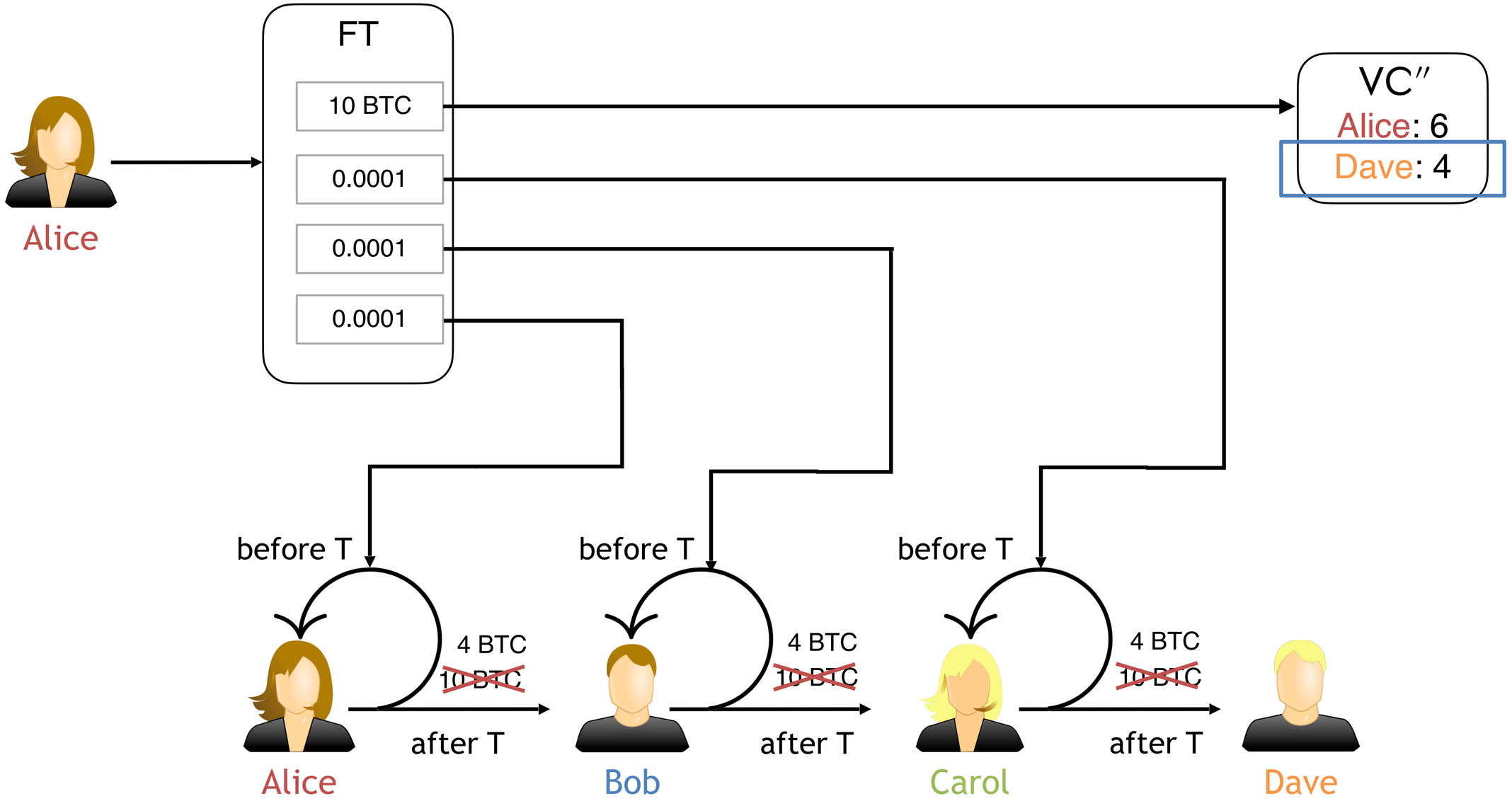
Donner (simplified)



Close VC

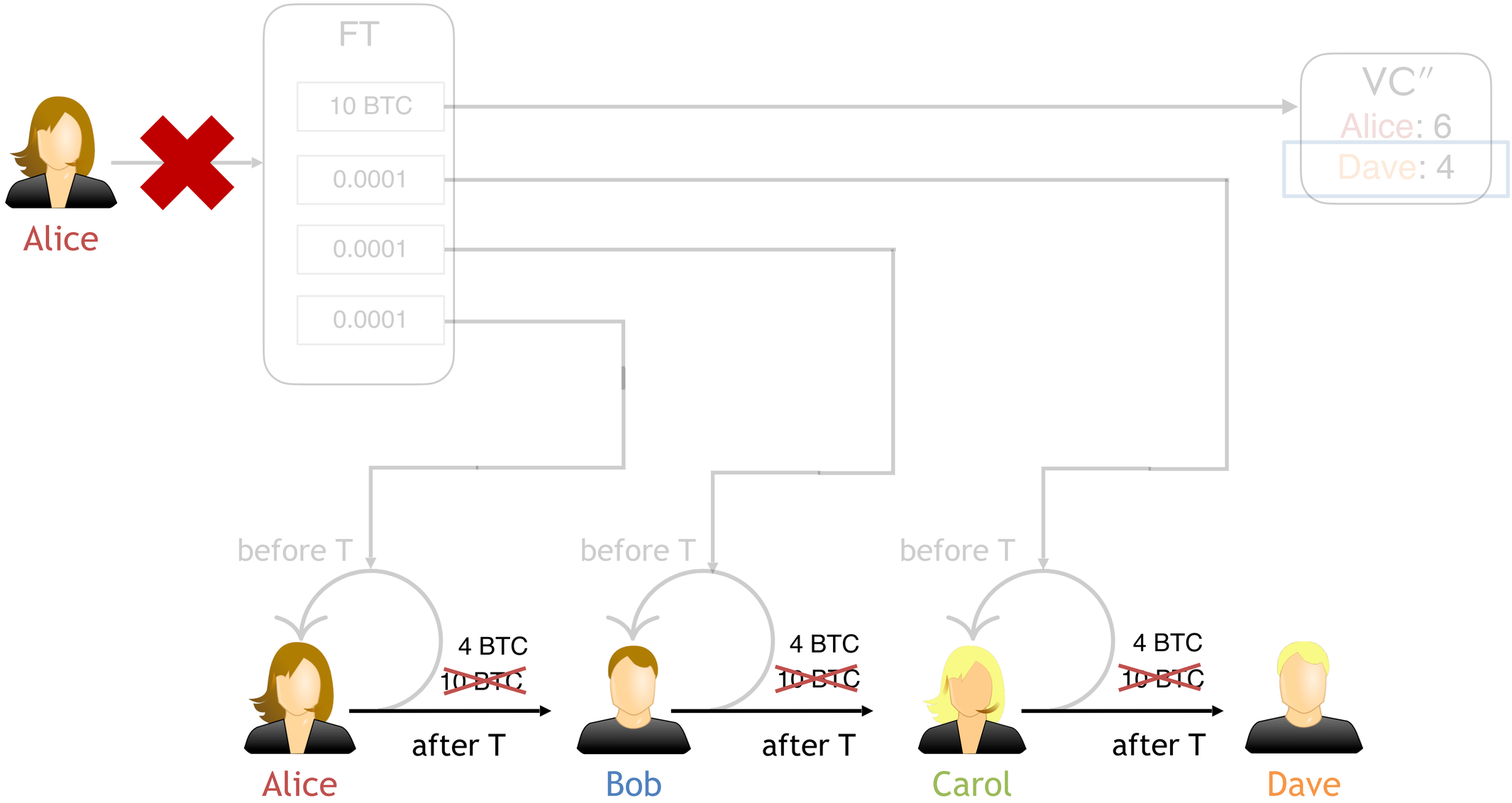

FT
10 BTC
0.0001
0.0001
0.0001
VC″
Alice: 6
Dave: 4
Alice
before T
10 BTC
after T
Alice
before T
10 BTC
after T
Bob
before T
10 BTC
after T
Carol
Dave

Close VC



Atomically update the payment to reflect final VC balance!

Close VC



Atomically update the payment to reflect final VC balance!

More details in paper!

More details in paper!

- Extending lifetime (indefinitely) 

More details in paper!

- Extending lifetime (indefinitely)

- Fair fee model

More details in paper!

- Extending lifetime (indefinitely)

- Fair fee model

- Performance evaluation (constant overhead)

More details in paper!

- Extending lifetime (indefinitely)

- Fair fee model

- Performance evaluation (constant overhead)

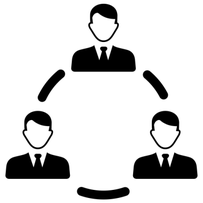
- Formalized security & privacy in UC Framework

Take home

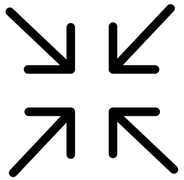
Domino attack

Devastating attack on existing VC schemes

Donner virtual channels



Generic solution for apps over multiple hops



Constant overhead

Fair, unlimited lifetime and fee model

Better security, privacy & latency

Thanks!

eprint.iacr.org/2021/855

lukas.aumayr@tuwien.ac.at

@lukas_aumayr