Elmo: Recursive Virtual Channels for Bitcoin

Aggelos Kiayias
Orfeas Stefanos Thyfronitis Litos
IOHK, University of Edinburgh

11/6/2021

VISA

20,000 tx/s

bitcoin

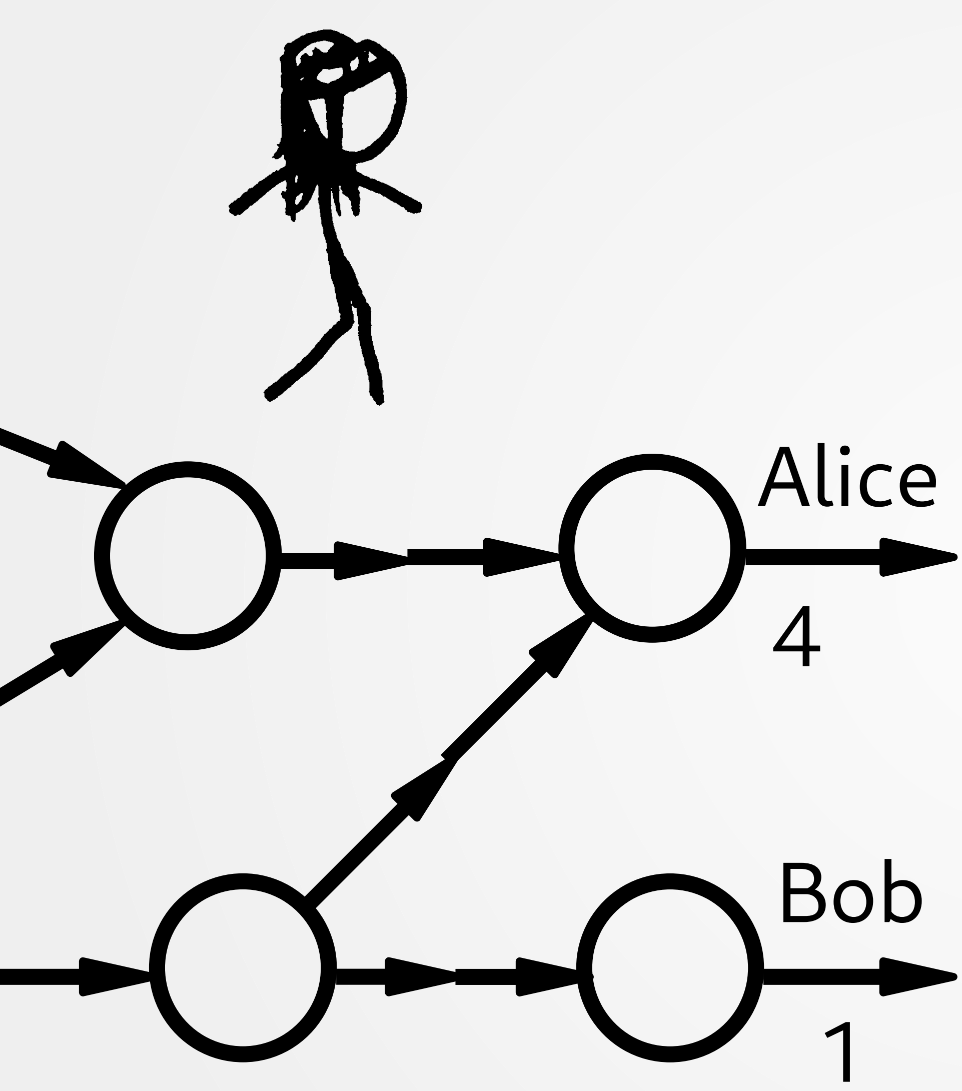
7 tx/s

Problem

All txs validated by all wallets

Solution

- Move most txs off-chain
- Resolve disputes on-chain

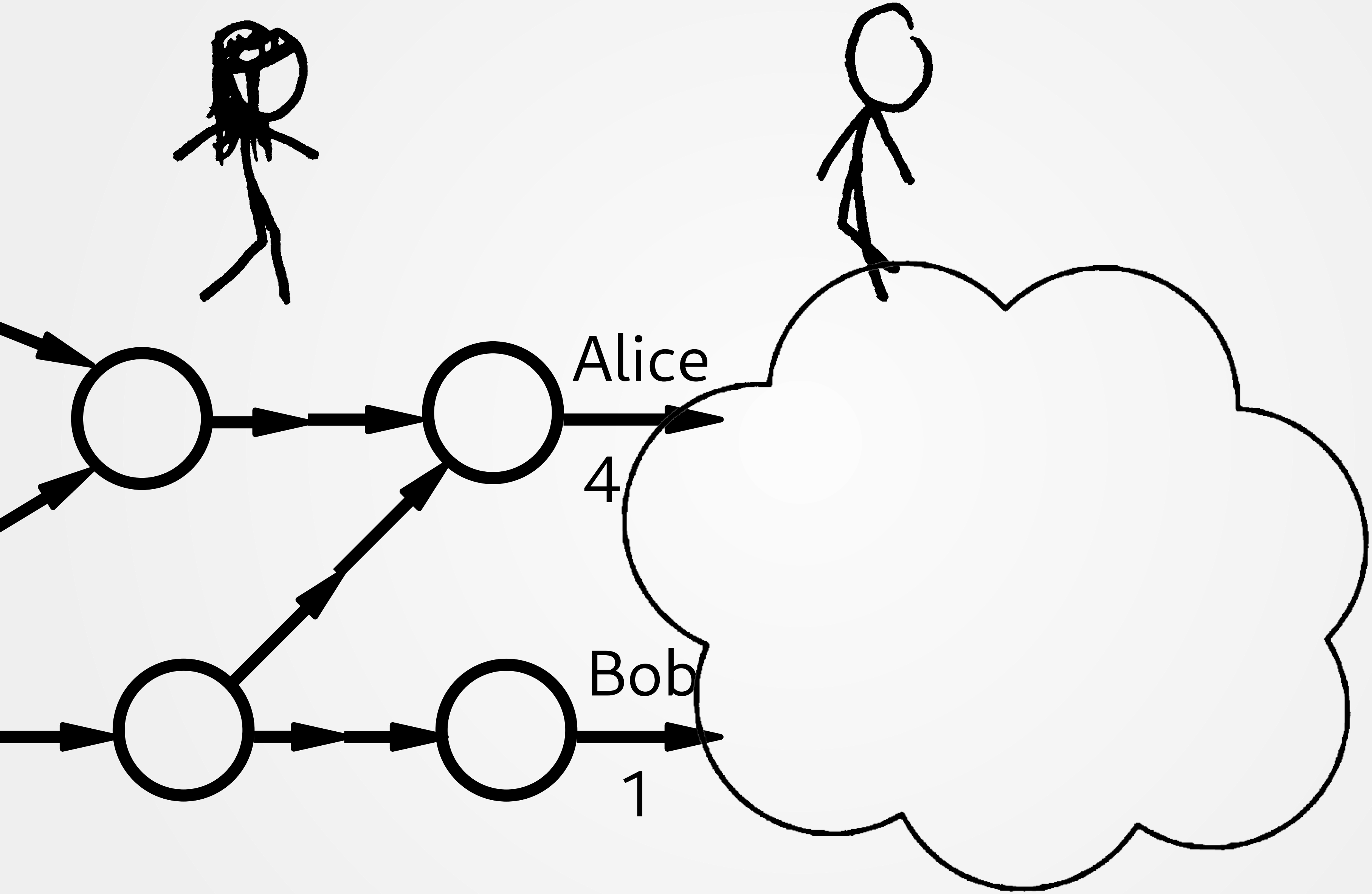


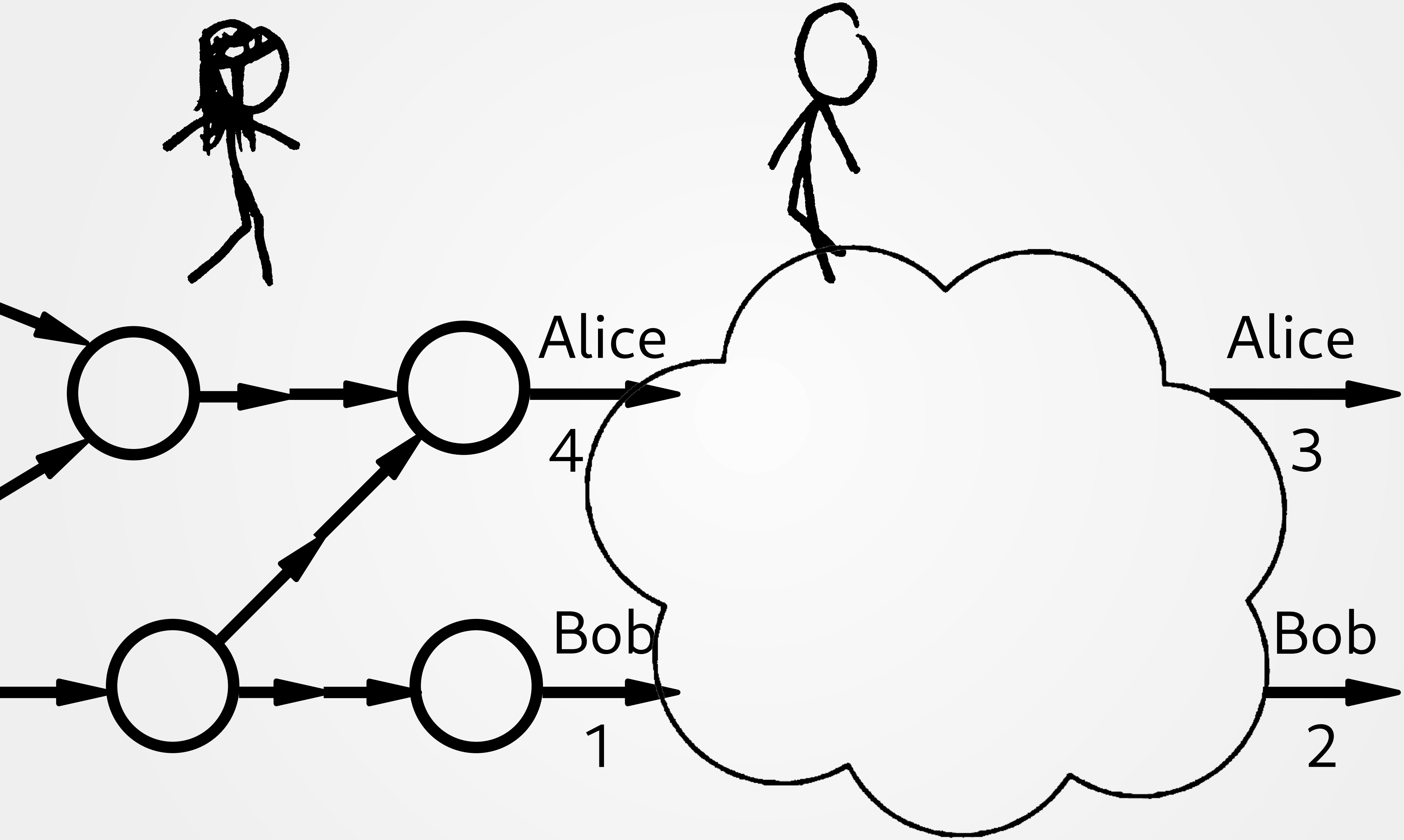
Alice

4

Bob

1


Alice
4
Bob
1


Alice
4
Alice
3
Bob
1
Bob
2

Previous solutions

i. Duplex Micropayment Channels

- 1st complete proposal
- 2-party channels
- Initially agree on a closing tx with an absolute timelock
- Update by creating a new closing tx with a shorter timelock
- ❌ Limited lifespan

Previous solutions

ii. Lightning Channels

- 1st real-life implementation
- 2-party channels
- Initially agree on (revocable) closing tx
- Update by creating a new closing tx and revoking the previous
- ✓ Unlimited lifespan
- ✓ Multi-hop payments
- ✗ Hops active for each payment

Previous solutions

iii. eltoo

- (Possibly) the future of Lightning
- 2-party channels
- Initially agree on a closing tx
- Update by creating a new closing tx which can spend any old closing tx
- ✓ Unlimited lifespan
- ✓ Conceptual simplicity
- ✗ Needs ANYPREVOUT

Previous solutions

iv. Atomic Multi-Channel Updates with Constant Collateral in Bitcoin-Compatible Payment-Channel Networks

- Enables performing multiple payments in an atomic fashion
- ✓ Enables new applications (e.g. crowdfunding)
- ✗ Has a huge title

Previous solutions

vi. Perun/General State Channel Networks

- Enable pairwise virtual channels & full smart contract capabilities off-chain
- ❌ No recursive virtual channels
- ❌ Needs Turing-complete language

Previous solutions

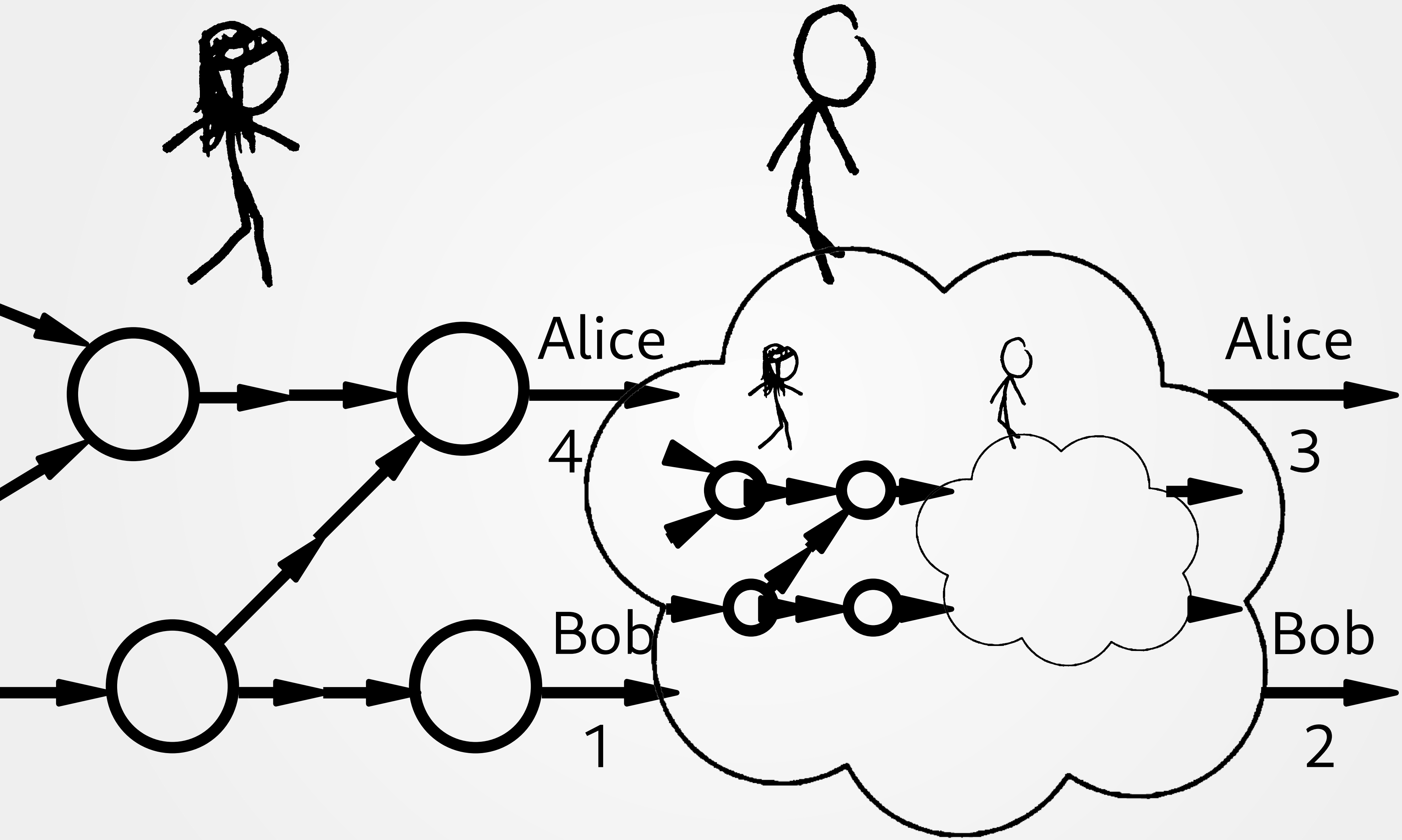
vii. Scalable funding of Bitcoin micropayment channel networks

- Adds multi-party coin pools
- Channels funded off-chain by pools
- ✓ Increases off-chain scalability
- ✗ No payments in multi-party pools
- ✗ No virtual channels

Previous solutions

viii. Generalized Bitcoin Compatible Channels

- Enables arbitrary bitcoin script off-chain
- 2-party channels
- ✓ Generalizes Lightning
- ✗ Multi-hop payments not analyzed
- ✗ Recursion not analyzed


Alice
4
Bob
1
Alice
3
Bob
2

Previous solutions

ix. Lightweight Virtual Payment Channels

- Enables Virtual Channels for Bitcoin
- 2-party channels
- ✓ Open channels entirely off-chain
- ✗ Limited channel lifetime
- ✗ Only one intermediary possible
- ✗ Recursion not analyzed

Previous solutions

x. Bitcoin Compatible Virtual Channels

- Enables Virtual Channels for Bitcoin
- 2-party channels
- ✓ Open channels entirely off-chain
- ✓ Unlimited channel lifetime
- ✗ Only one intermediary possible
- ✗ Recursion not possible

Elmo features

Enables opening long-lived “virtual” channels without any on-chain TXs

Elmo features

Variadic

Elmo channels built on top of a path of preexisting “base” channels of any length

Elmo features

Recursive

Base channels may be virtual

Elmo features

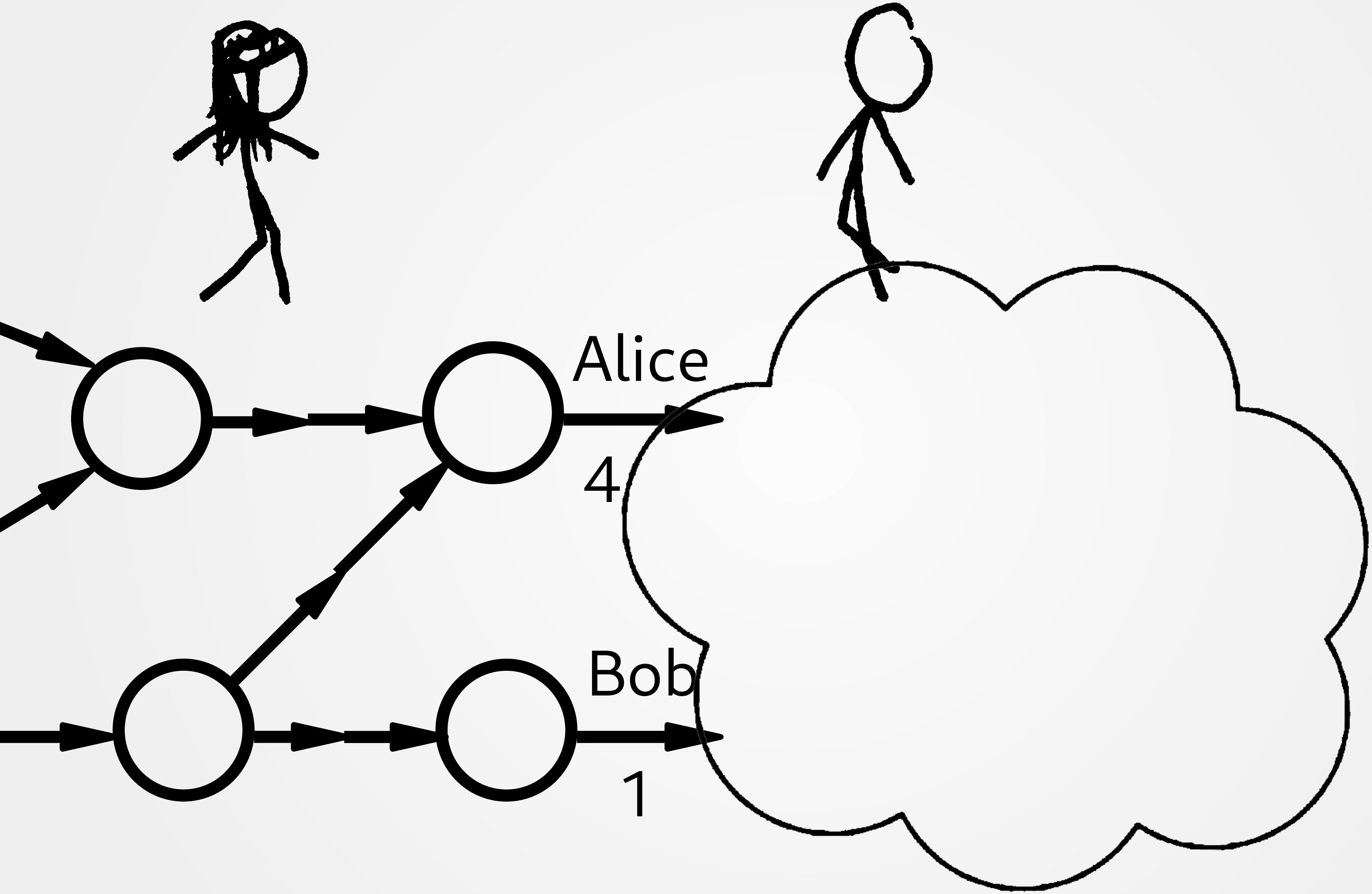
Symmetric

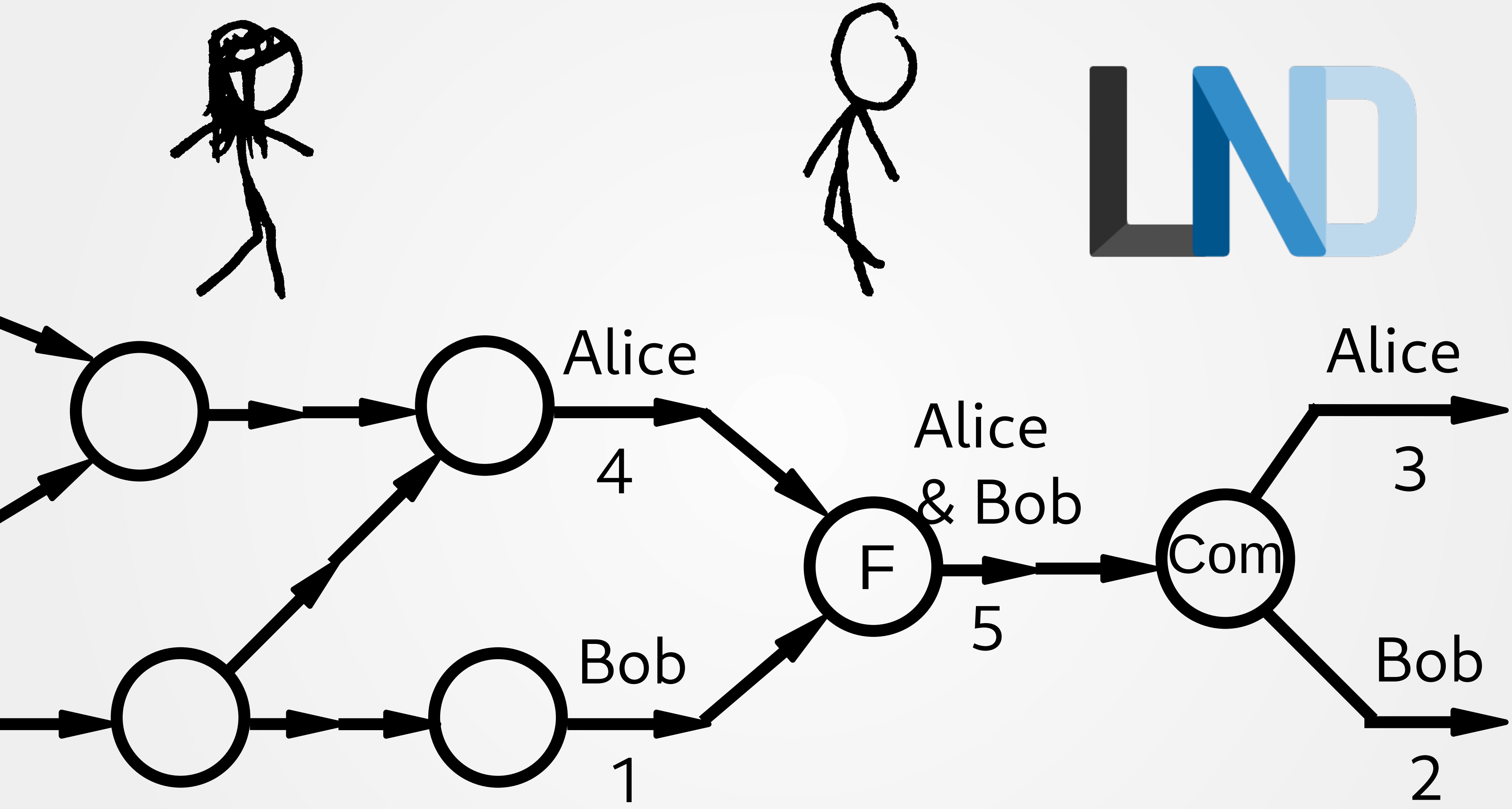
Cost of closing is the same for endpoints

Similarly for intermediaries

Design decisions

- UC secure
- Functionality for a single channel
- State machine
- Uses $\mathcal{G}_{\text{ledger}}$ [BMTZ'17, BGKRZ'18]


Alice
4
Bob
1



Alice

4

Alice
& Bob

F

5

Com

Alice

3

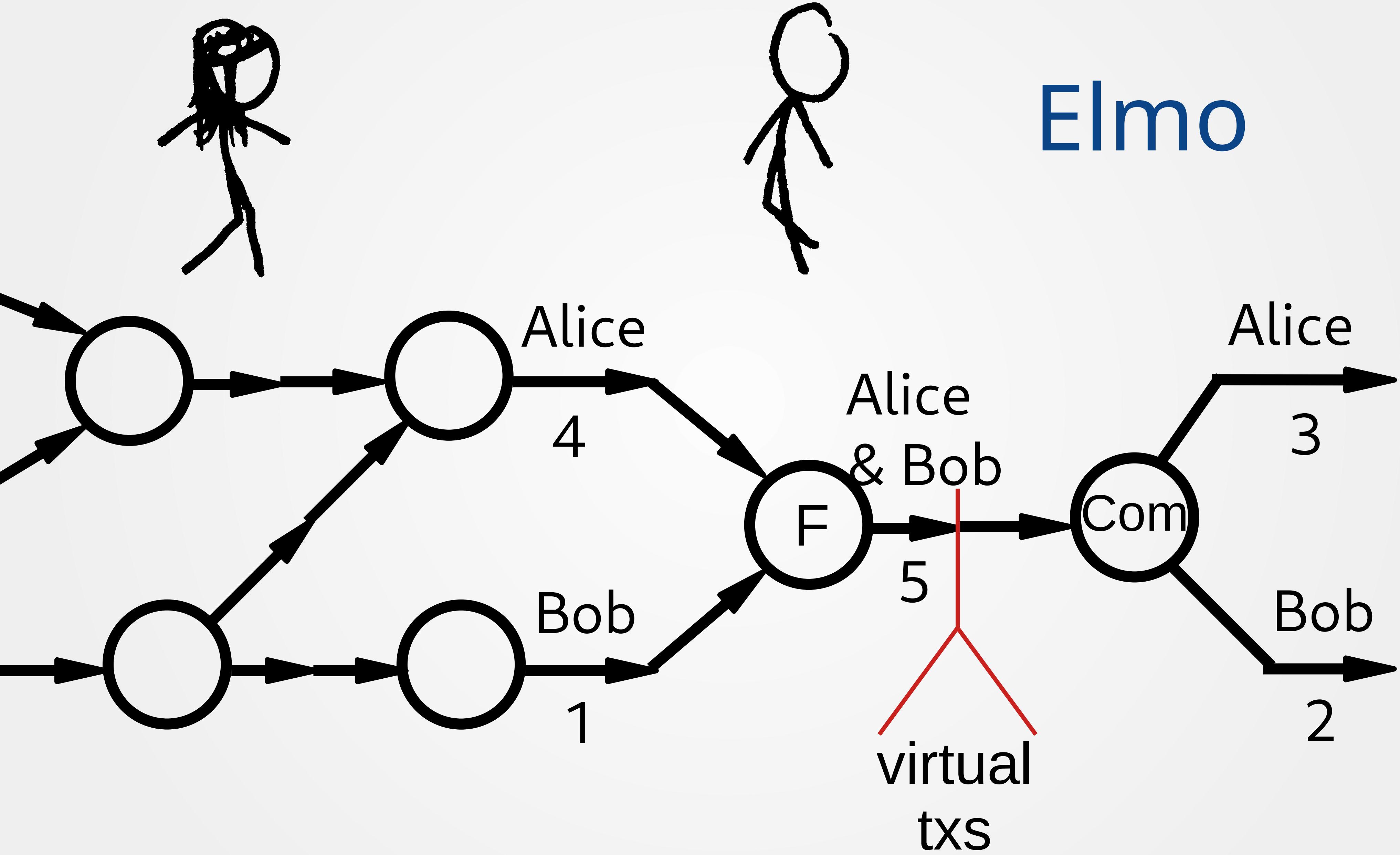
Bob

1

Bob

2

Elmo



Construction

Intermediary *i* has 3 classes of virtual TXs:

- “Initiator” TX
  - Spends left & right funding outputs
  - Has virtual output with interval [*i*]

Construction

Intermediary *i* has 3 classes of virtual TXs:

- "Initiator" TX
  - Spends left & right funding outputs
  - Has virtual output with interval [*i*]
- "Extend-interval" TXs
  - Spends 1 funding output and 1 virtual output with interval [*j*, …, *i*-1] or [*i*+1, …, *j*]
  - Has virtual output w/ interval [*j*, …, *i*] or [*i*, …, *j*]

Construction

Intermediary i has 3 classes of virtual TXs:

- "Initiator" TX
  - Spends left & right funding outputs
  - Has virtual output with interval $[i]$
- "Extend-interval" TXs
  - Spends 1 funding output and 1 virtual output with interval $[j, \ldots, i-1]$ or $[i+1, \ldots, j]$
  - Has virtual output w/ interval $[j, \ldots, i]$ or $[i, \ldots, j]$
- "Merge-intervals" TXs
  - Spends 2 virtual outputs with intervals $[j, \ldots, i-1]$ and $[i+1, \ldots, \mathrm{k}]$
  - Has virtual output with interval $[j, \ldots, k]$

Example 1
Fundee wants to close

t=0

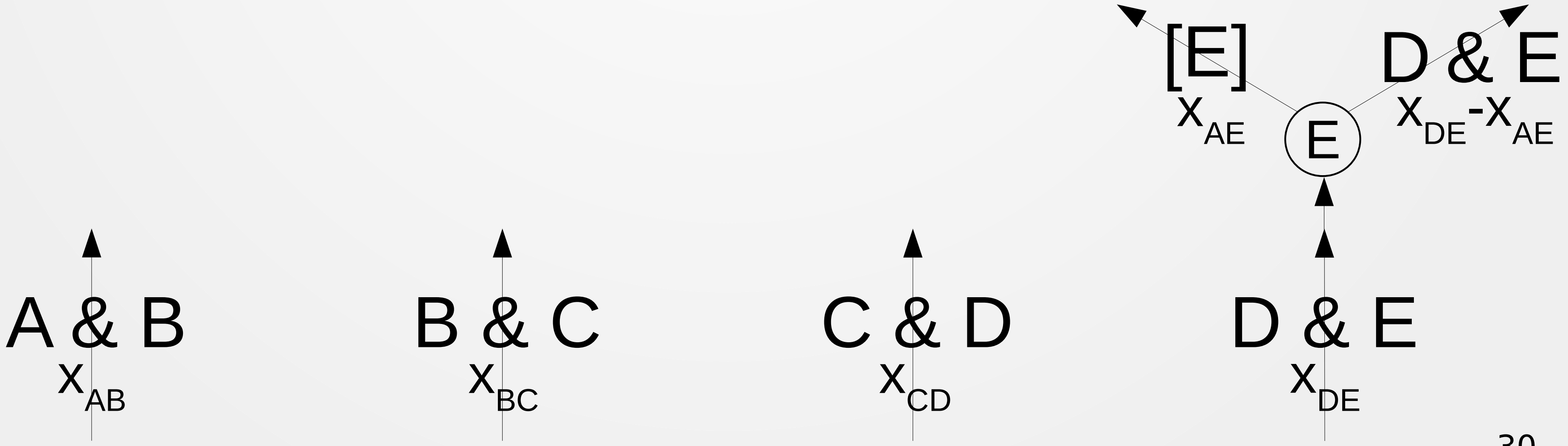
A & B x_{AB}

B & C x_{BC}

C & D x_{CD}

D & E x_{DE}

t=1



[E]

x_{AE}

D & E

x_{DE}-x_{AE}

E

A & B

x_{AB}

B & C

x_{BC}

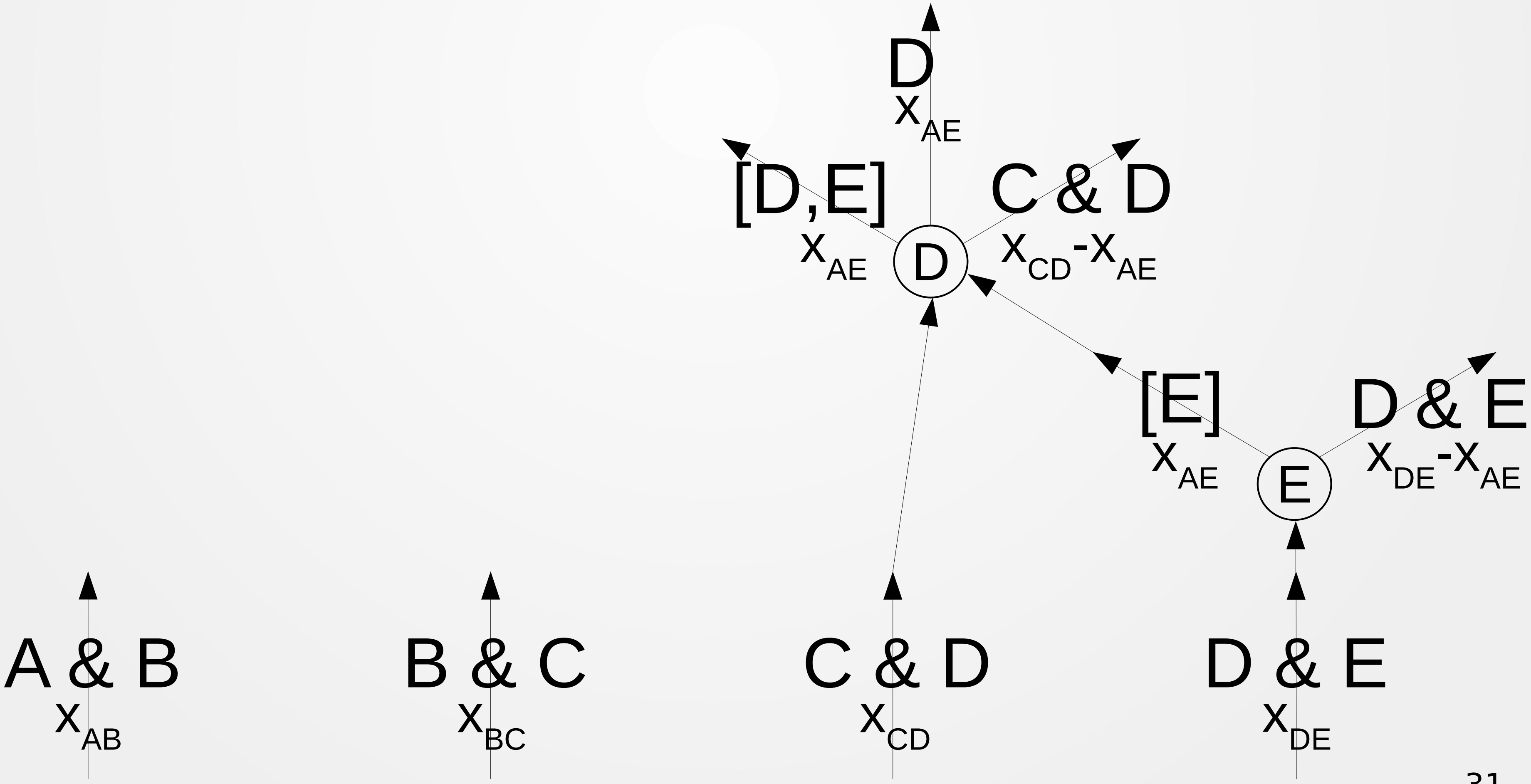
C & D

x_{CD}

D & E

x_{DE}

t=2



D

x_{AE}

[D,E]

x_{AE}

C & D

x_{CD}-x_{AE}

D

[E]

x_{AE}

D & E

x_{DE}-x_{AE}

E

A & B

x_{AB}

B & C

x_{BC}

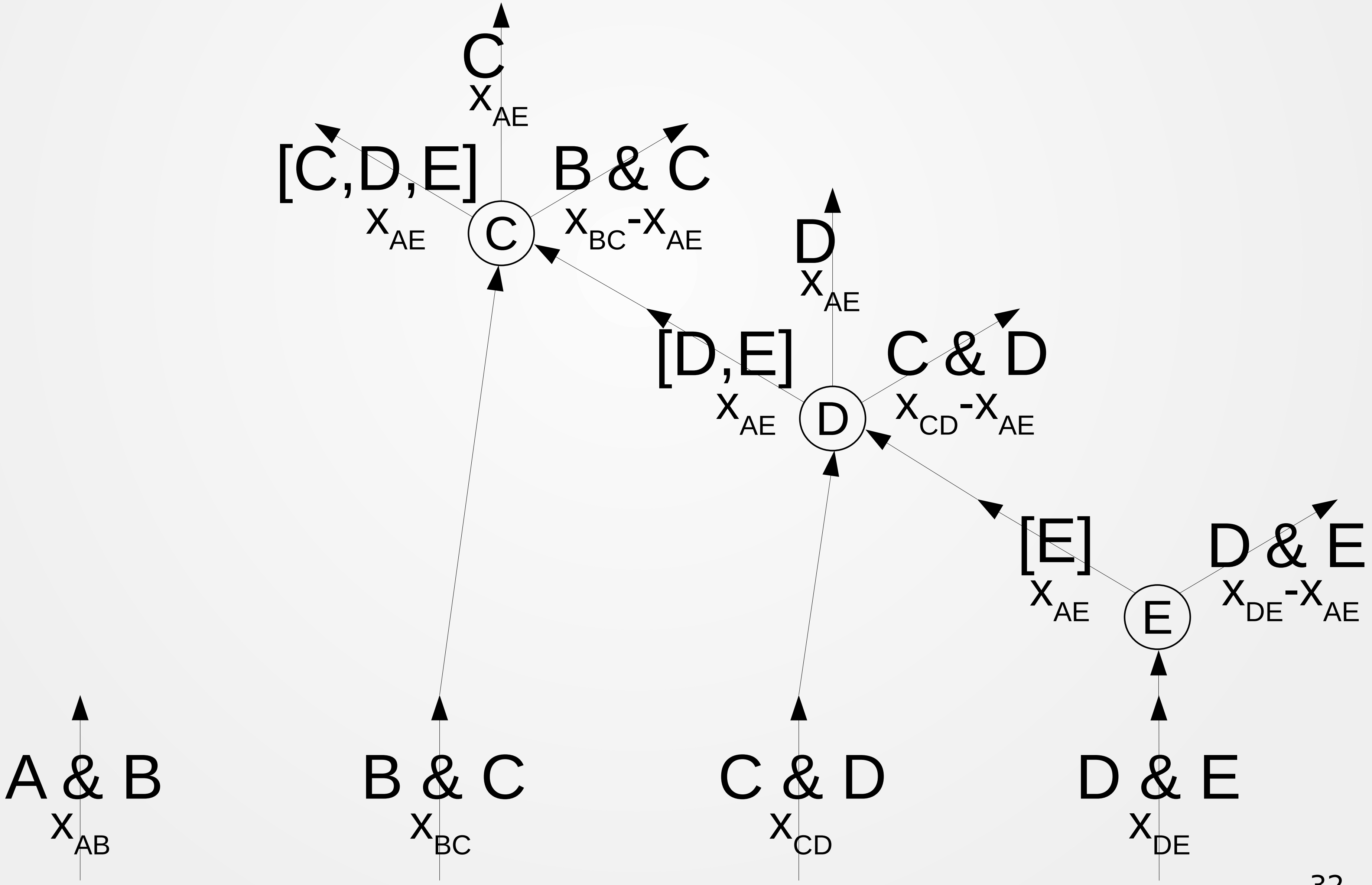
C & D

x_{CD}

D & E

x_{DE}

t=3



C
x_{AE}

[C,D,E]
x_{AE}

C

B & C
x_{BC}-x_{AE}

D
x_{AE}

[D,E]
x_{AE}

D

C & D
x_{CD}-x_{AE}

[E]
x_{AE}

E

D & E
x_{DE}-x_{AE}

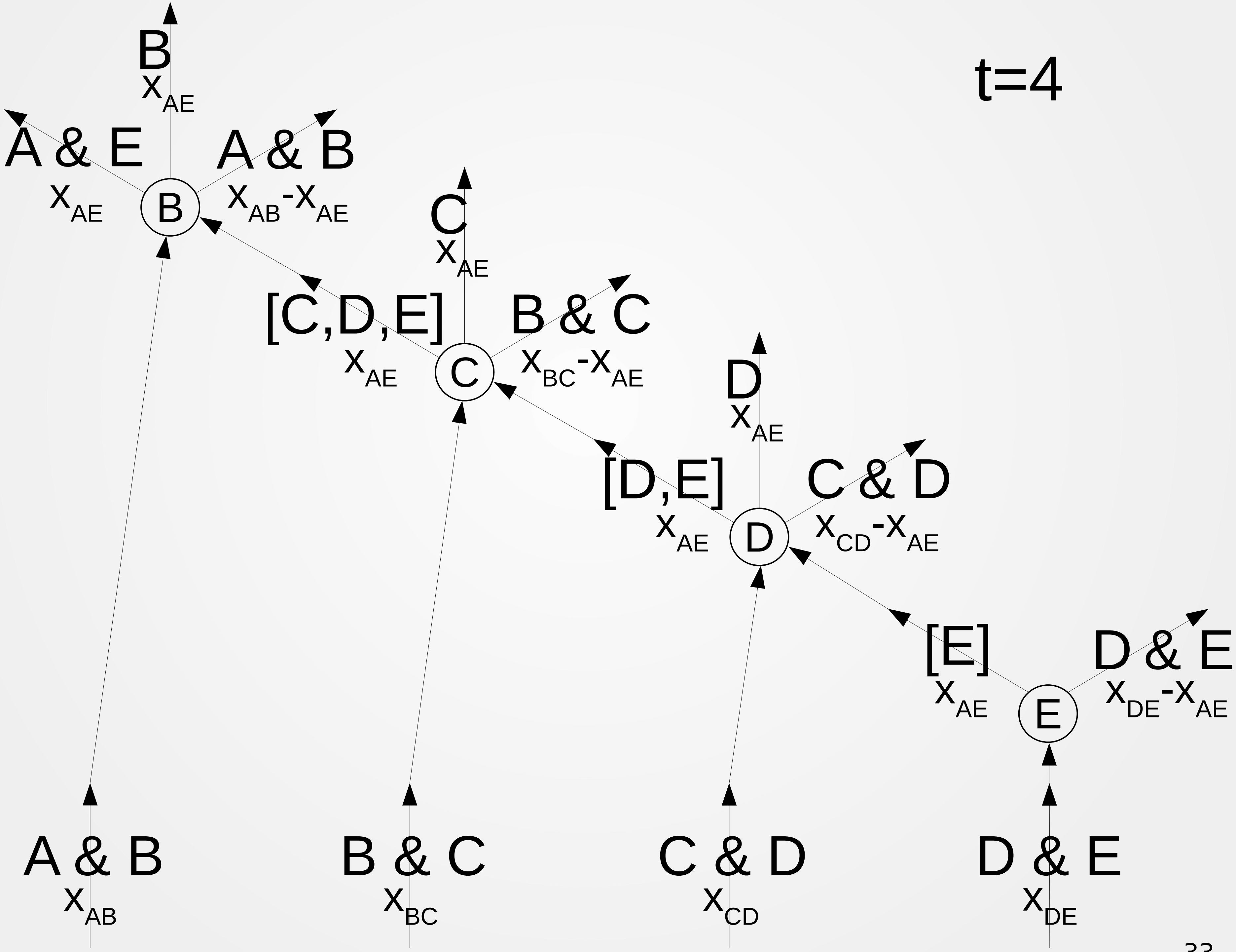
A & B
x_{AB}

B & C
x_{BC}

C & D
x_{CD}

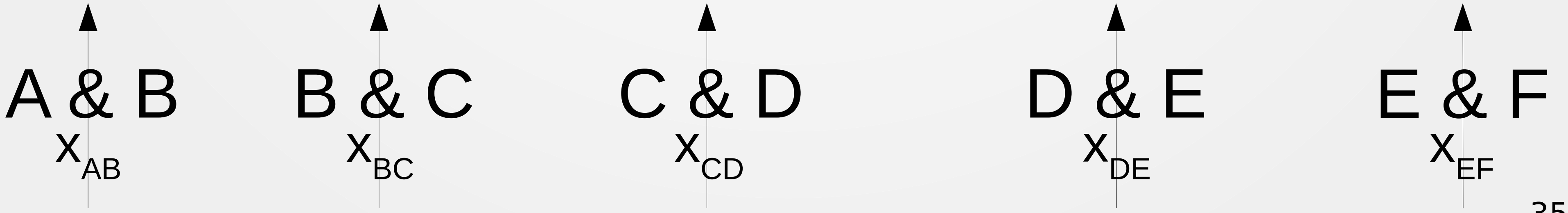
D & E
x_{DE}

t=4


B
x_{AE}
A & E
x_{AE}
B
A & B
x_{AB}-x_{AE}
C
x_{AE}
[C,D,E]
x_{AE}
C
B & C
x_{BC}-x_{AE}
D
x_{AE}
[D,E]
x_{AE}
D
C & D
x_{CD}-x_{AE}
[E]
x_{AE}
E
D & E
x_{DE}-x_{AE}
A & B
x_{AB}
B & C
x_{BC}
C & D
x_{CD}
D & E
x_{DE}

Example 2
Simultaneous initiators

t=0



A & B x_{AB}

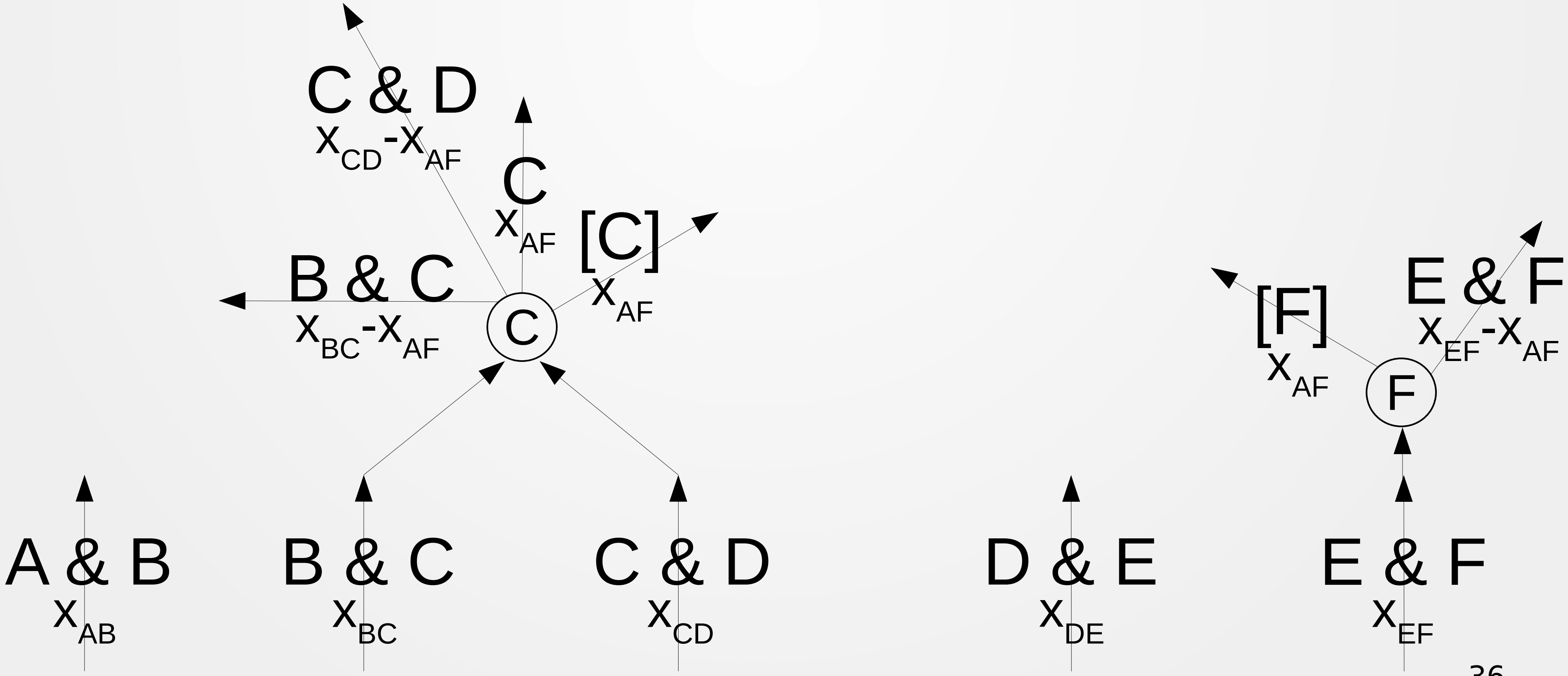
B & C x_{BC}

C & D x_{CD}

D & E x_{DE}

E & F x_{EF}

t=1



C & D

x_{CD}-x_{AF}

C

x_{AF}

[C]

x_{AF}

B & C

x_{BC}-x_{AF}

C

[F]

x_{AF}

E & F

x_{EF}-x_{AF}

F

A & B

x_{AB}

B & C

x_{BC}

C & D

x_{CD}

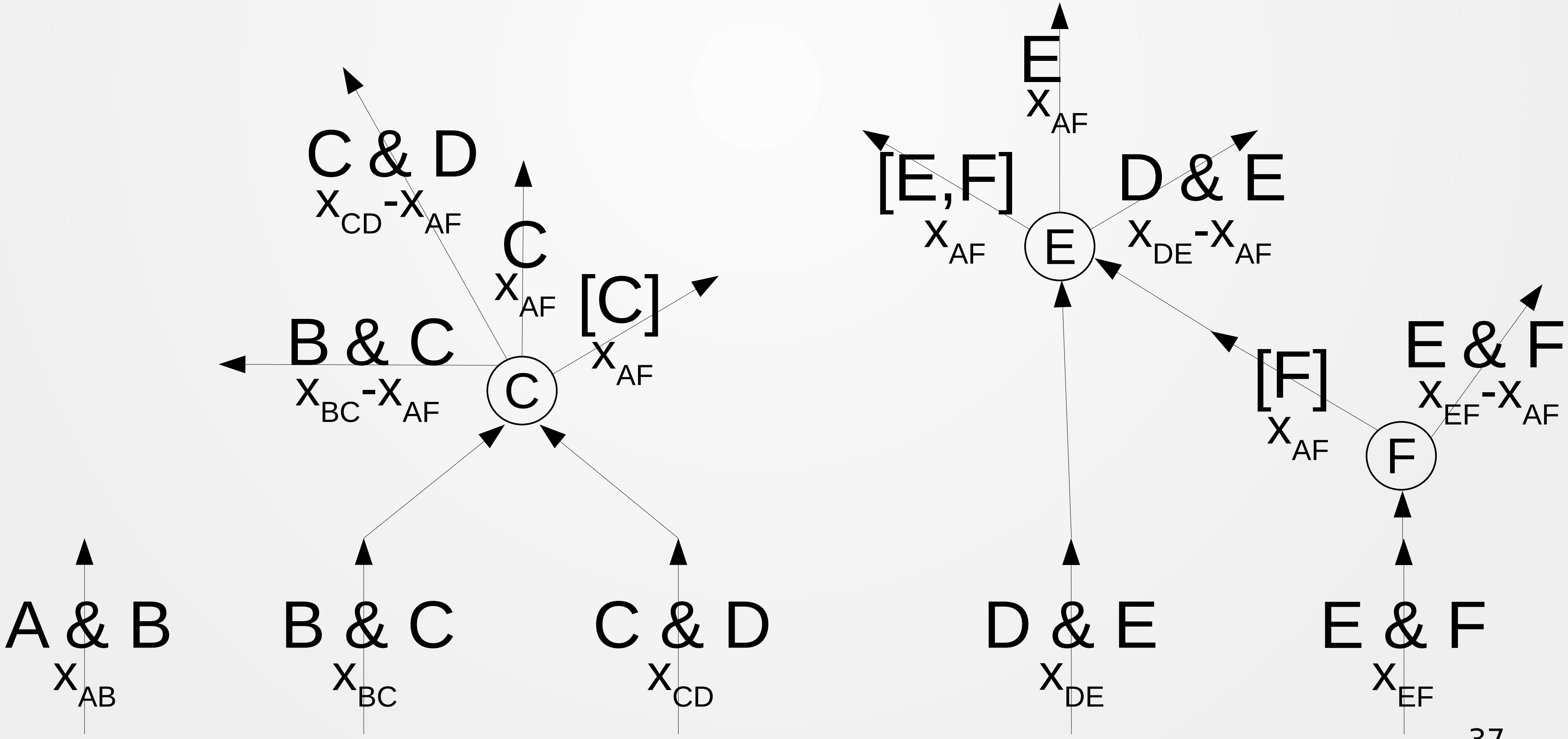
D & E

x_{DE}

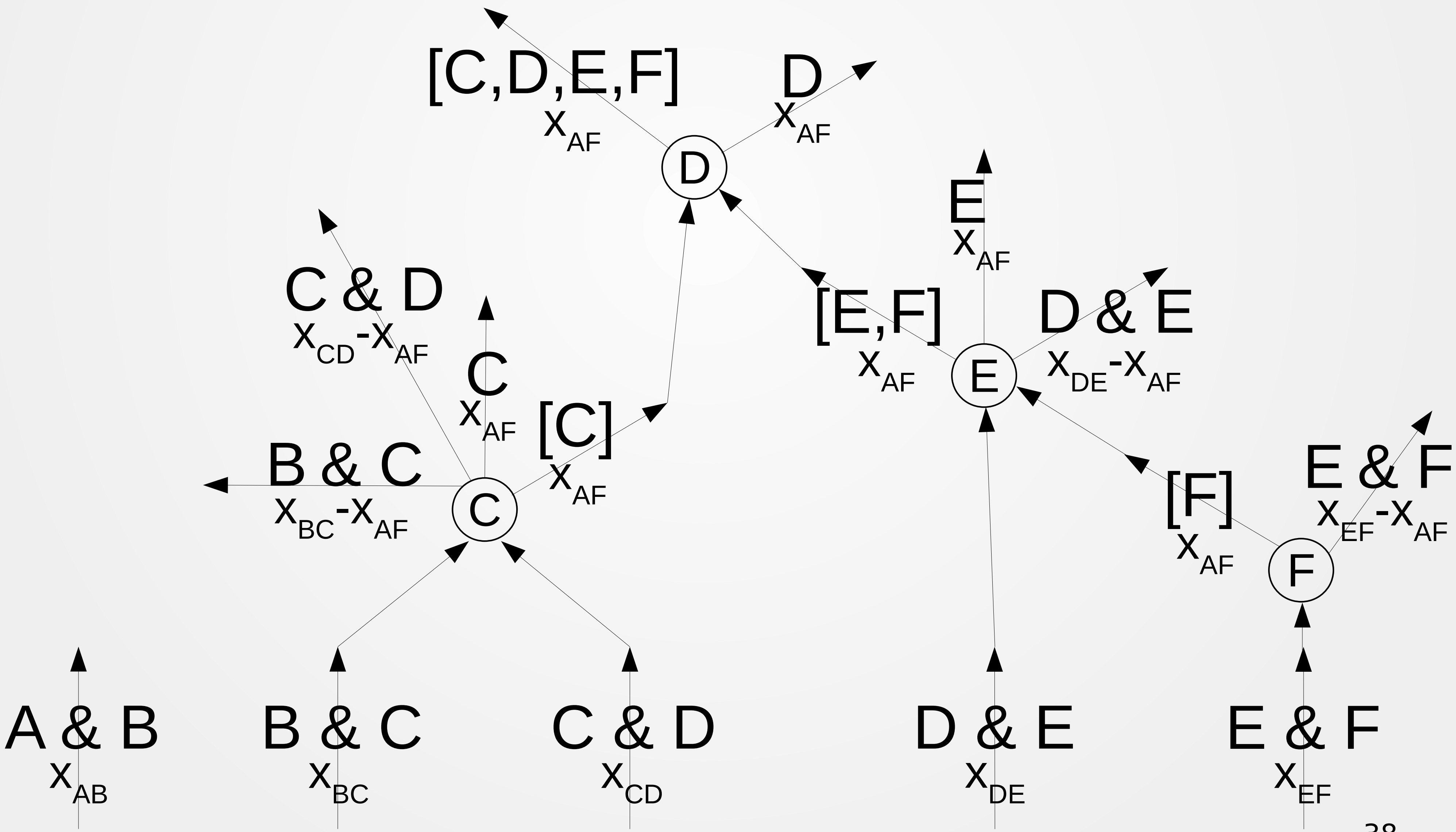
E & F

x_{EF}

t=2


E
x_{AF}
C & D
x_{CD}-x_{AF}
[E,F]
x_{AF}
D & E
x_{DE}-x_{AF}
C
x_{AF}
E
[C]
x_{AF}
B & C
x_{BC}-x_{AF}
E & F
x_{EF}-x_{AF}
C
[F]
x_{AF}
F
A & B
x_{AB}
B & C
x_{BC}
C & D
x_{CD}
D & E
x_{DE}
E & F
x_{EF}

t=3



[C,D,E,F]
x_{AF}

D
x_{AF}

D

E
x_{AF}

C & D
x_{CD}-x_{AF}

C
x_{AF}

[E,F]
x_{AF}

D & E
x_{DE}-x_{AF}

E

[C]
x_{AF}

B & C
x_{BC}-x_{AF}

C

E & F
x_{EF}-x_{AF}

[F]
x_{AF}

F

A & B
x_{AB}

B & C
x_{BC}

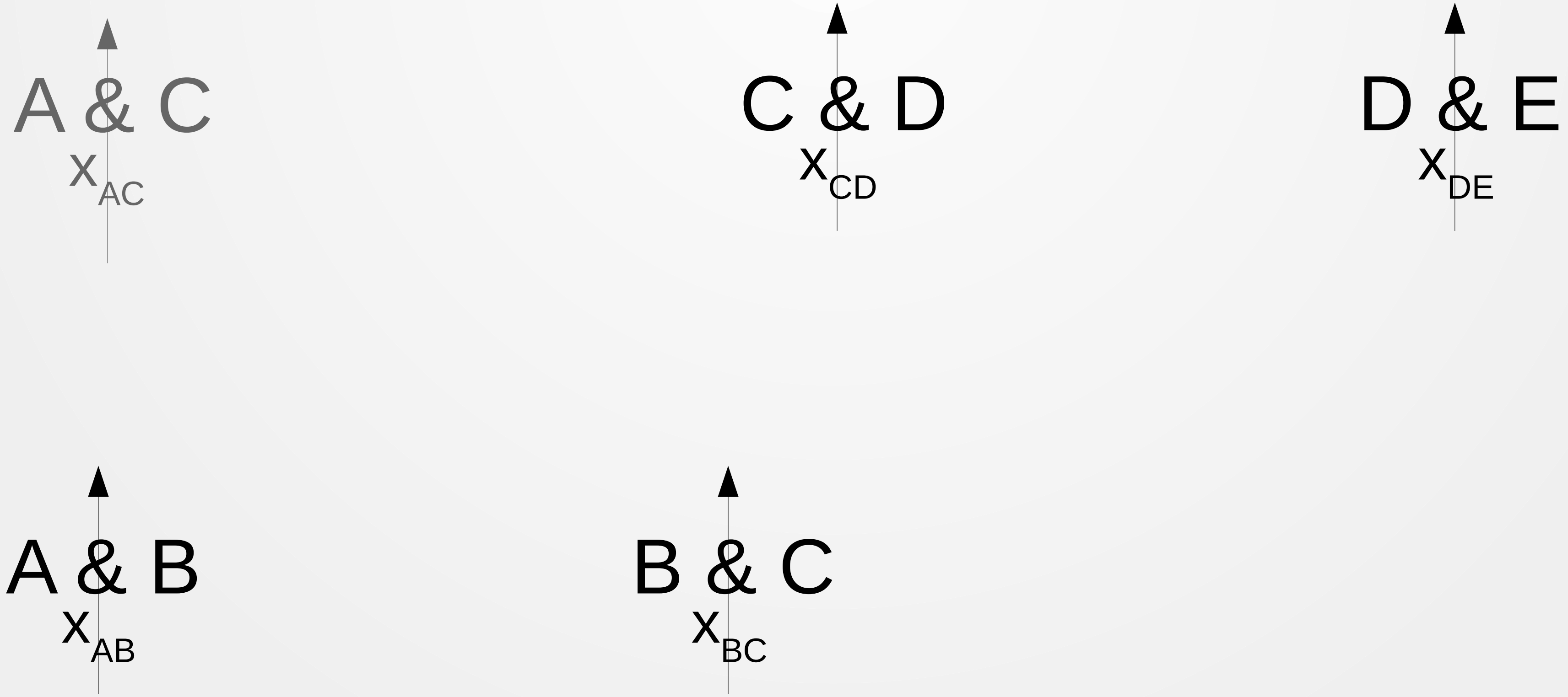
C & D
x_{CD}

D & E
x_{DE}

E & F
x_{EF}

Example 3
Virtual base channel

t=0



A & C

x_{AC}

C & D

x_{CD}

D & E

x_{DE}

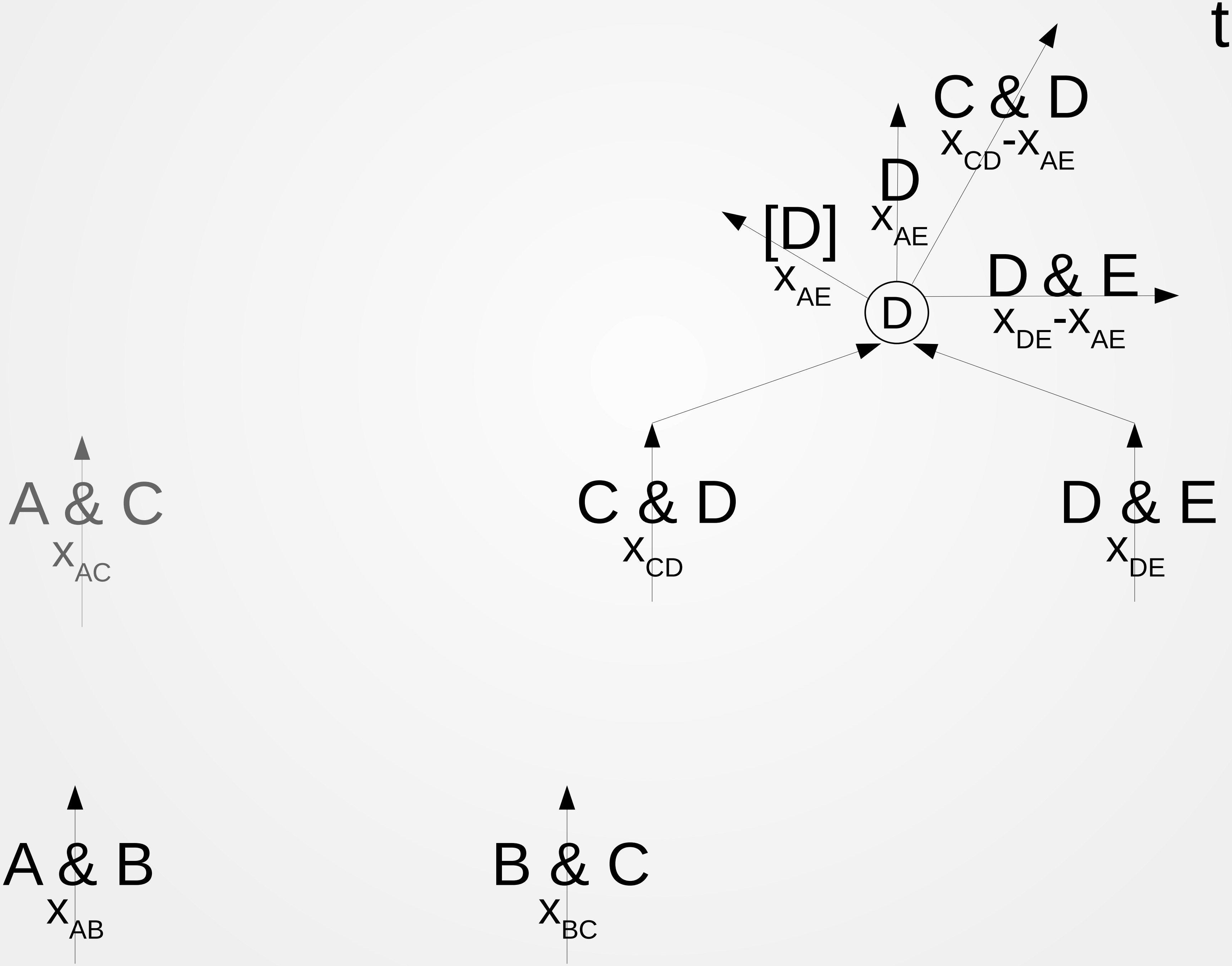
A & B

x_{AB}

B & C

x_{BC}

t=1



C & D

$x_{CD}-x_{AE}$

D

x_{AE}

[D]

x_{AE}

D & E

$x_{DE}-x_{AE}$

D

A & C

x_{AC}

C & D

x_{CD}

D & E

x_{DE}

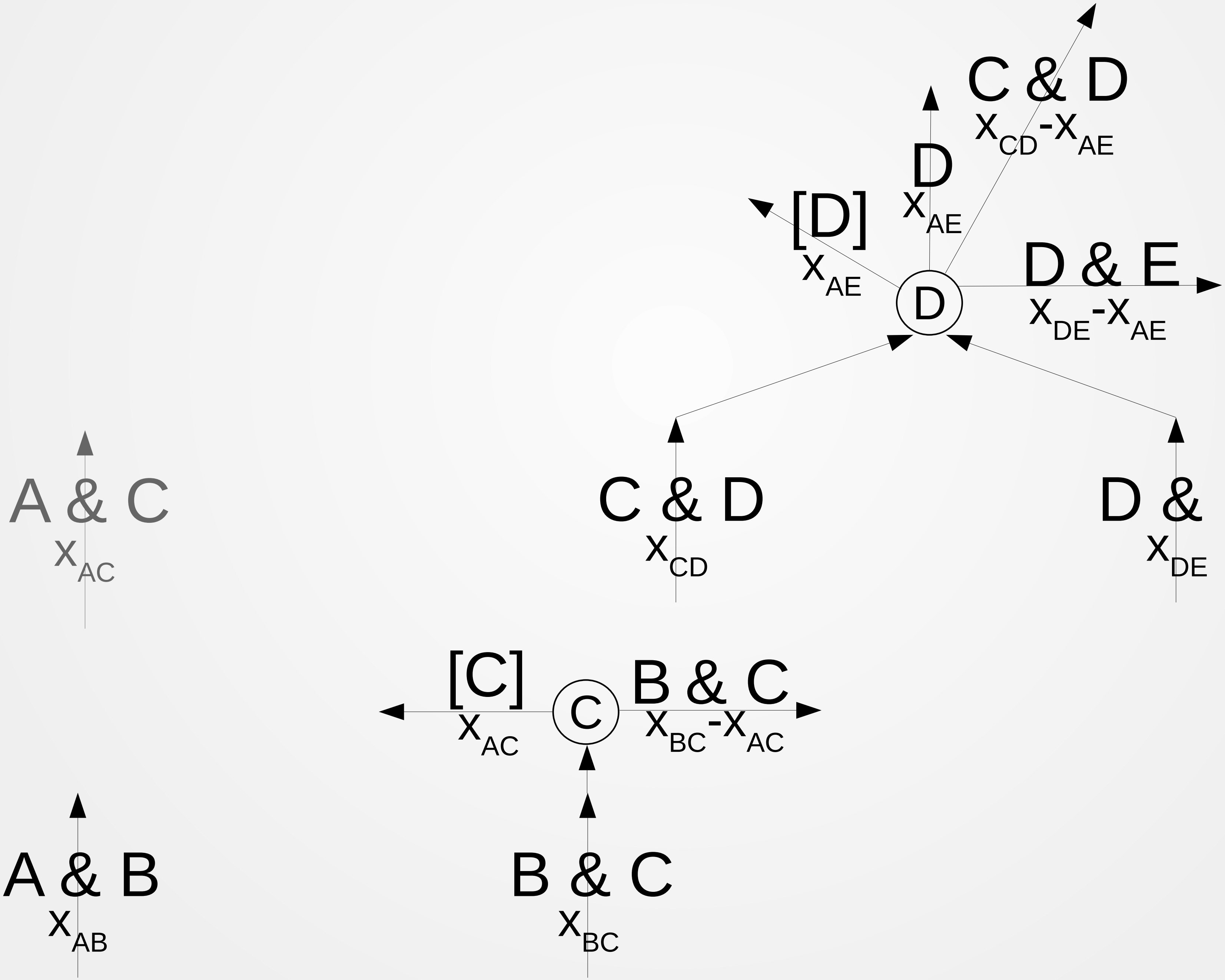
A & B

x_{AB}

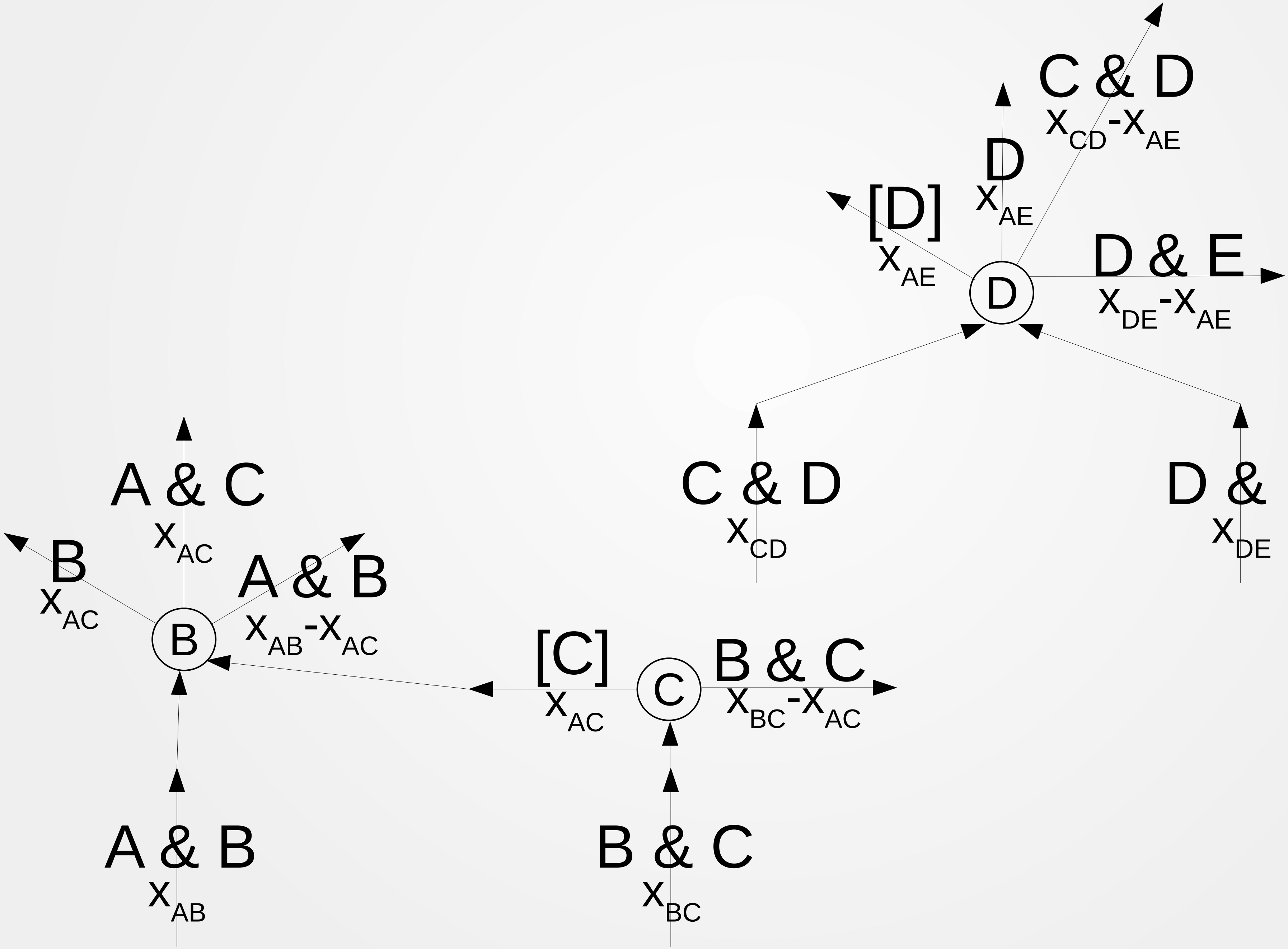
B & C

x_{BC}

t=2


C & D
x_{CD}-x_{AE}
D
x_{AE}
[D]
x_{AE}
D
D & E
x_{DE}-x_{AE}
A & C
x_{AC}
C & D
x_{CD}
D & E
x_{DE}
[C]
x_{AC}
C
B & C
x_{BC}-x_{AC}
A & B
x_{AB}
B & C
x_{BC}

t=3



C & D $x_{CD}-x_{AE}$

D x_{AE}

[D] x_{AE}

D

D & E $x_{DE}-x_{AE}$

C & D x_{CD}

D & E x_{DE}

A & C x_{AC}

B x_{AC}

A & B $x_{AB}-x_{AC}$

B

[C] x_{AC}

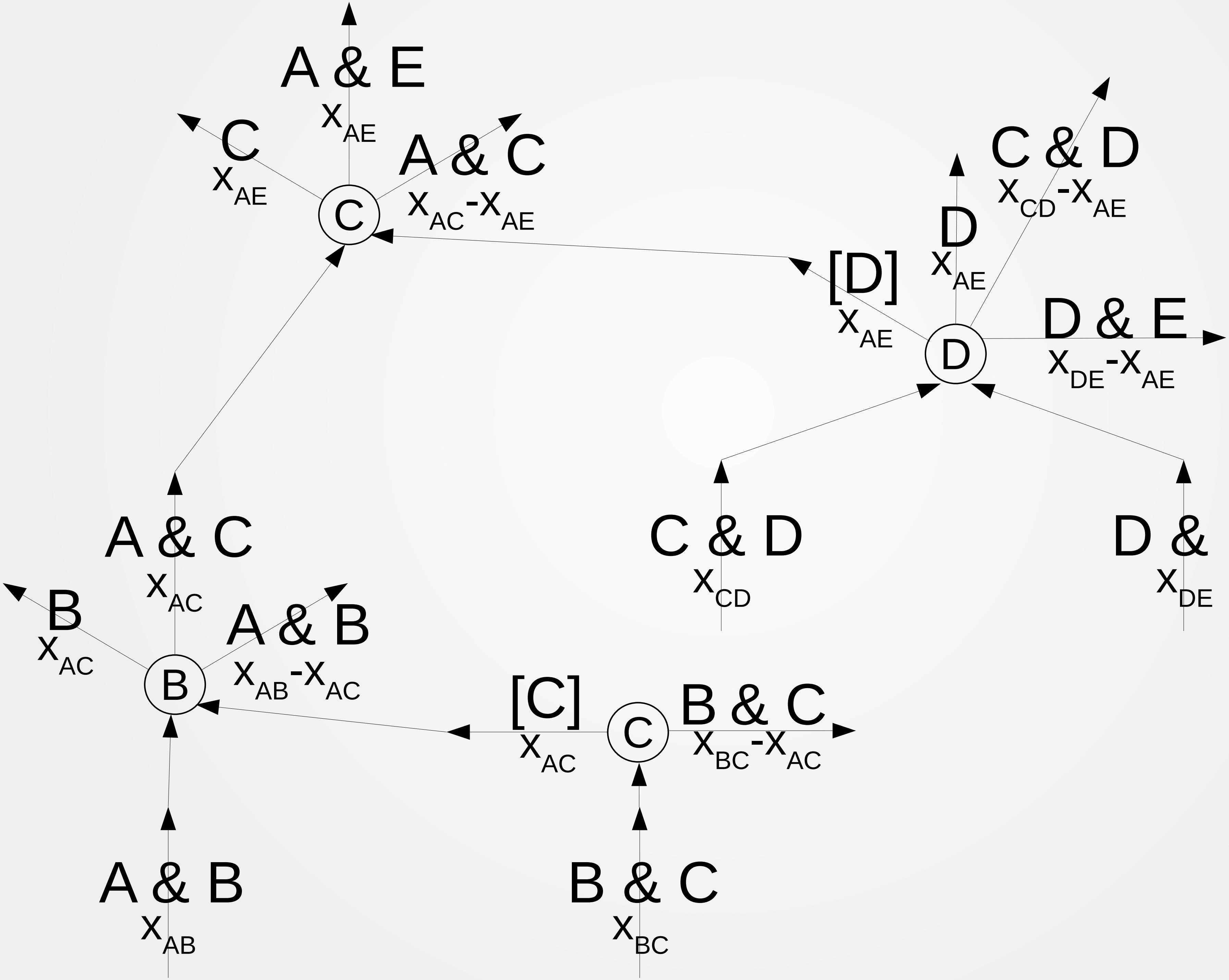
C

B & C $x_{BC}-x_{AC}$

A & B x_{AB}

B & C x_{BC}

t=4



A & E
x_{AE}

C
x_{AE}

C

A & C
x_{AC}-x_{AE}

C & D
x_{CD}-x_{AE}

D
x_{AE}

[D]
x_{AE}

D

D & E
x_{DE}-x_{AE}

A & C
x_{AC}

C & D
x_{CD}

D & E
x_{DE}

B
x_{AC}

B

A & B
x_{AB}-x_{AC}

[C]
x_{AC}

C

B & C
x_{BC}-x_{AC}

A & B
x_{AB}

B & C
x_{BC}

Summary

Construction and composable analysis of Variadic Recursive Virtual Channels for Bitcoin

Thank you!