



The power of Bitcoin multisignature transactions

Oleg Andreev

October 7, 2014

Part 1

Keys and Signatures

Part 2

Multisig Basics

Part 3

Multisig Use Cases

Part 4

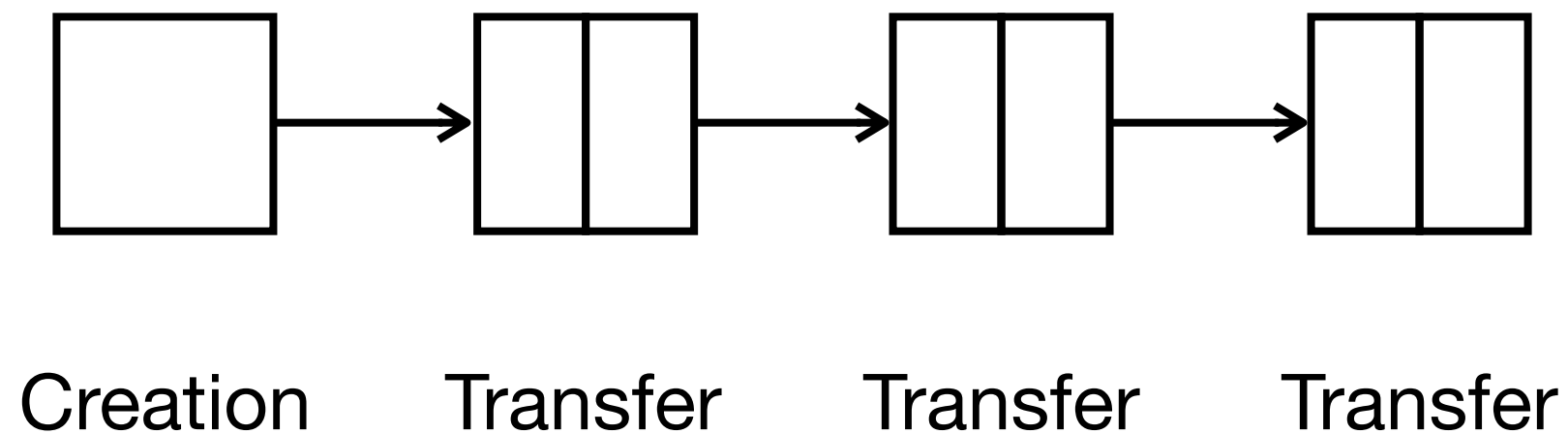
Ultimate Vault

Part 1

Keys and Signatures

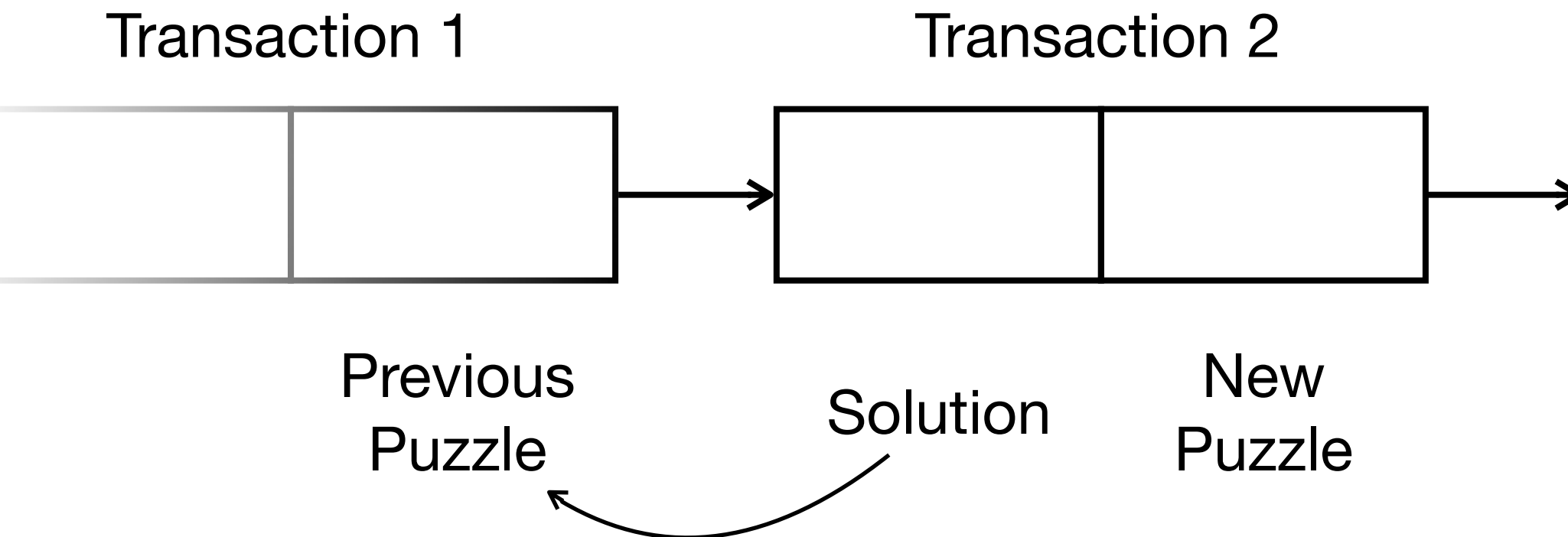
Coin is a chain of proofs

checked and recorded by everyone



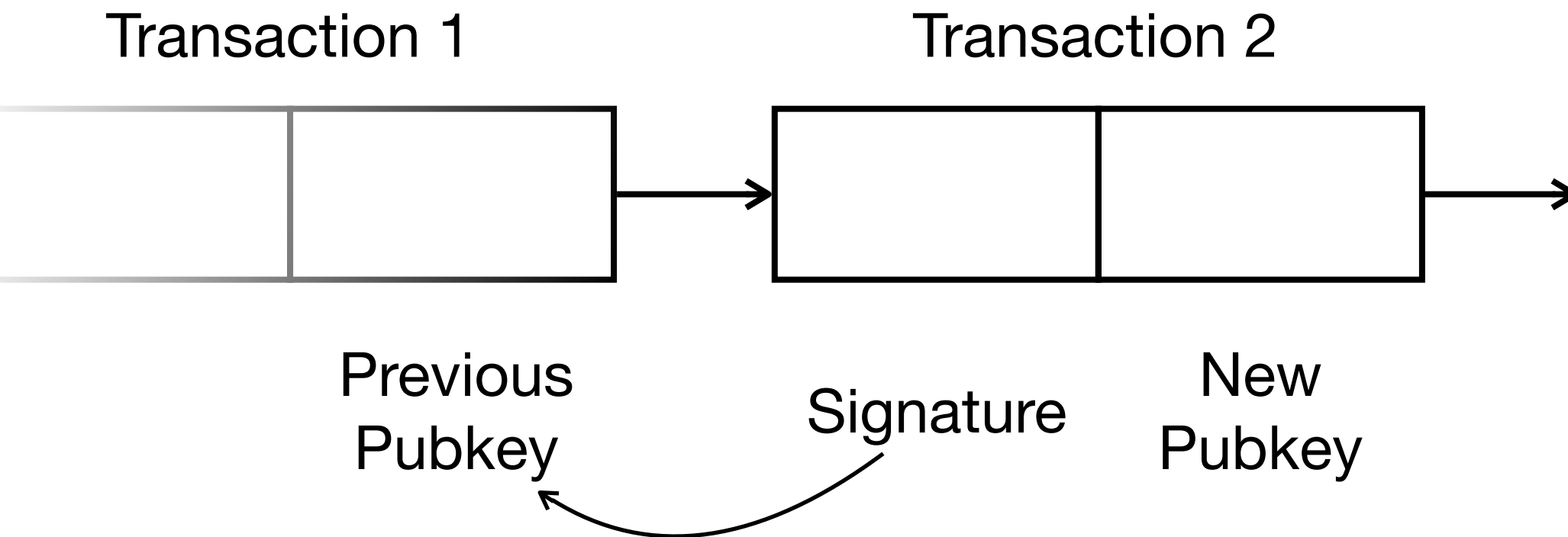
Transfer = puzzle + solution

solution links back to a previous puzzle



Puzzle is a public key

solution is a signature



Cryptographic signature

Created with a private (secret) key

Verified with a public key

Ownership is

the knowledge of the private key

Part 2

Multisig Basics

Normal transaction

Condition = 1 public key

Solution = 1 signature

Ownership = 1 private key

Opcode: OP_CHECKSIG

Multisig transaction

Condition = 2+ public keys

Solution = 1+ signatures

Ownership = 2+ parties

Opcode: OP_CHECKMULTISIG

M-of-N policy model

N parties can vote

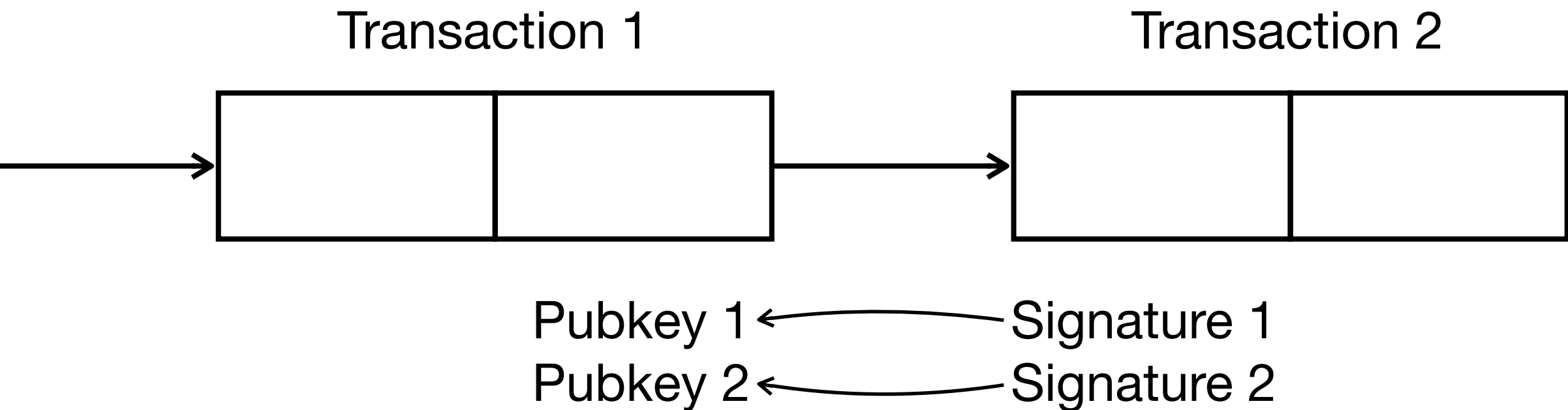
M votes unlock funds

$$M \leq N$$

$N \leq 15$ in practice

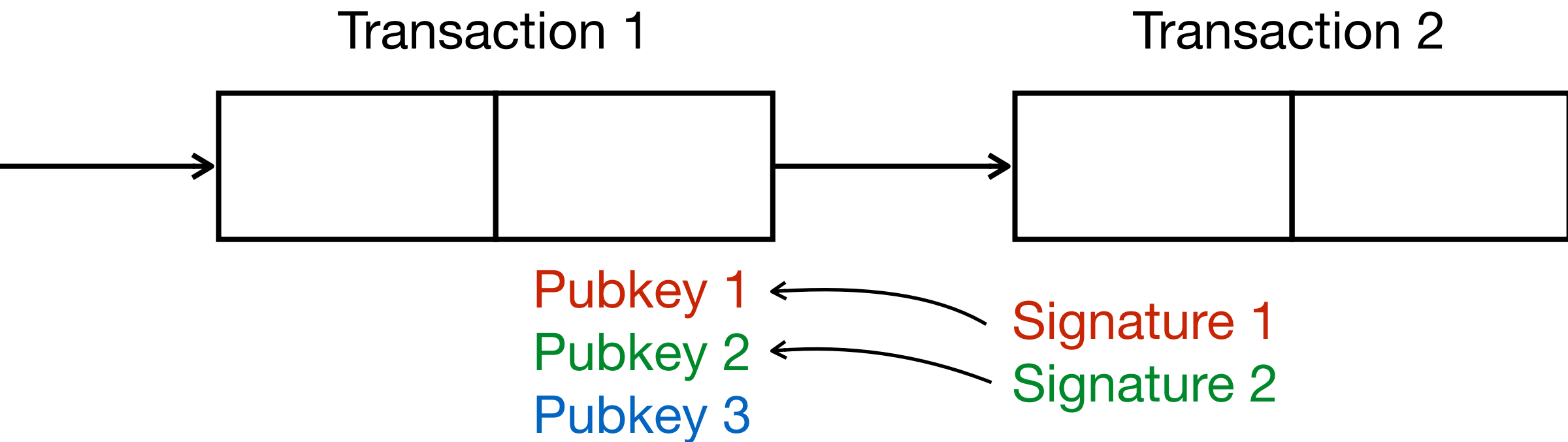
2-of-2 multisig

joint ownership



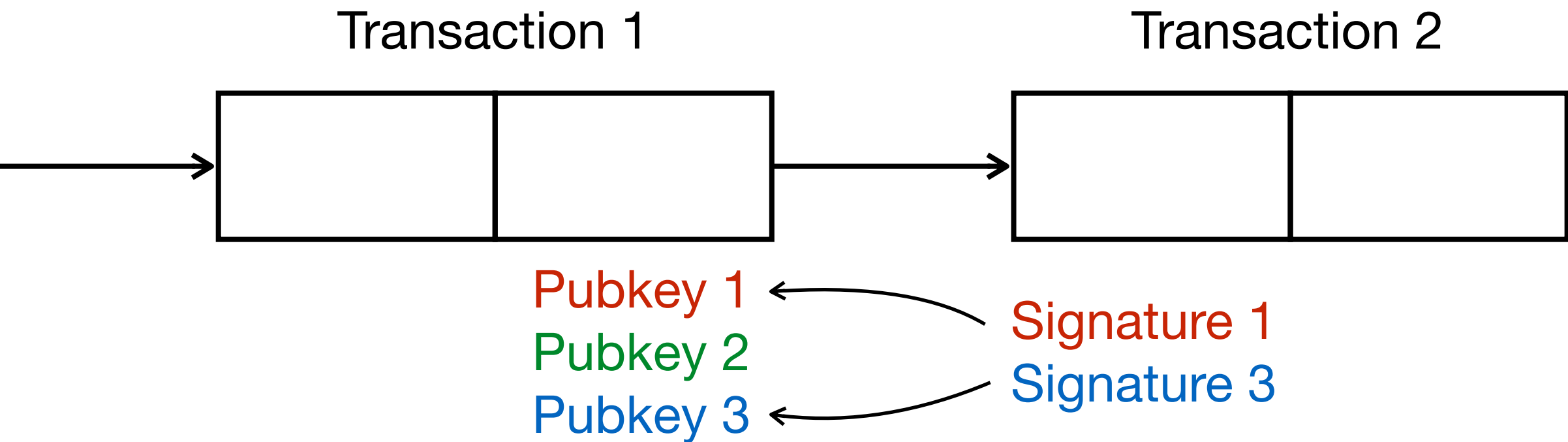
2-of-3 multisig

majority vote



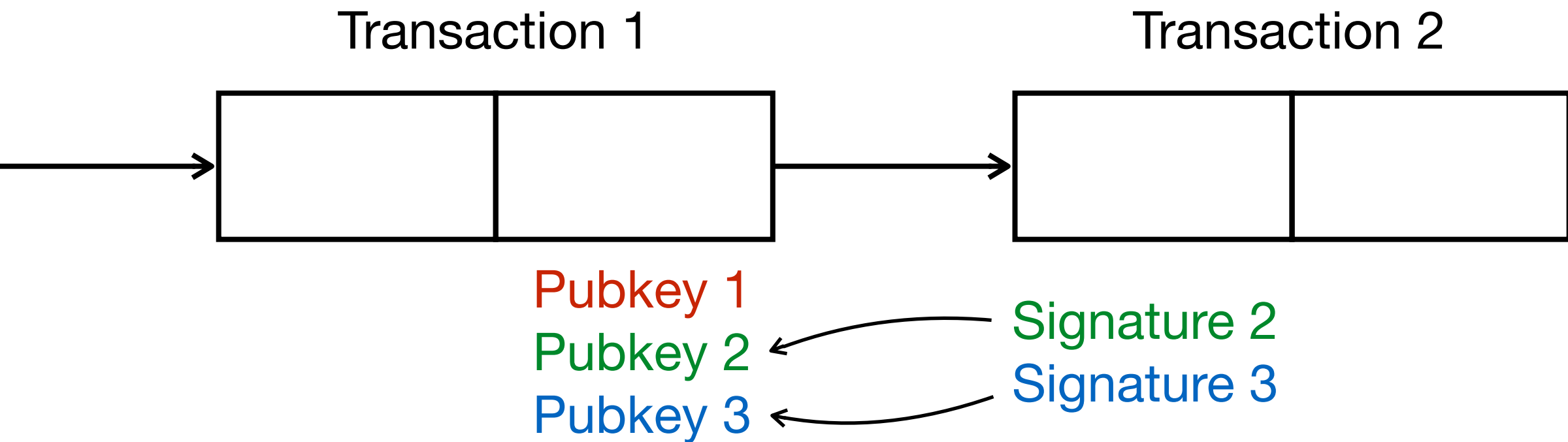
2-of-3 multisig

majority vote



2-of-3 multisig

majority vote



Key features

Data loss protection (redundant keys)

Data theft protection (separate parties)

Backdoor protection (no secret sharing)

Part 3

Multisig Use Cases

Public Keys

1

2

3

4

5

6

7

8

Signatures
1

2

3

4

5

6

Public Keys



Public Keys

1

2

3

4

5

6

7

8

1

Normal
Tx

No Extra Security

2

Joint Escrow

Sweet Spot

Too Redundant

3

Not
Redundant

4

Not
Redundant

Majority Vote

5

Not
Redundant

6

Not
Redundant

Signatures

1. Two-factor Wallet

2-of-3 multisig

Every device is a party

Phone, Laptop, Paper backup

Send from phone, co-sign on laptop

Protection against partial data loss,
backdoors, theft.

2. Escrow Service

2-of-3 multisig

One key per party, one key for escrow agent.

When both parties agree, agent can't censor or take funds.

When parties disagree, agent can side with one of them, but can't take funds to themselves.

3. Company Funds

2-of-3 multisig

Three founders

One key per founder

Protection against loss or theft

Majority vote

4. Weighted Voting

5-of-9 multisig

CEO has 3 keys.

Managers have 2 keys.

CEO and 1 manager can unlock.

3 managers can unlock without the CEO.

5. Joint EscrowTM

2-of-2 multisig

Mutually distrusting parties

Atomic lock up of the insurance deposit

Atomic unlock

Nash equilibrium

For black markets and ad hoc interactions where reputation or insurance are too expensive/impossible.

Part 4

Ultimate Vault

Threats

Device manufacturers (*bugs, leaks, backdoors*)

Wallet app developers (*bugs, leaks, backdoors*)

Physical thieves (*stealing funds, privacy invasion*)

Remote thieves (*malleability, tx history exploits*)

Yourself (*forgetting password, UI misuse*)

Ultimate Vault

Multi-party bank

4-of-7 custodians

Blind signatures for privacy

“When Bitcoin and Digicash had a baby:
Blind signatures for Bitcoin by @oleganza”

— *Pelle Braendgaard*

<https://twitter.com/PelleB/status/518142249277063168>



Alex



Gino



Britney

Friends as custodians



Florence



Cecile



Eve



Dave



a, A



g, G



b, B

private &
public keys



f, F



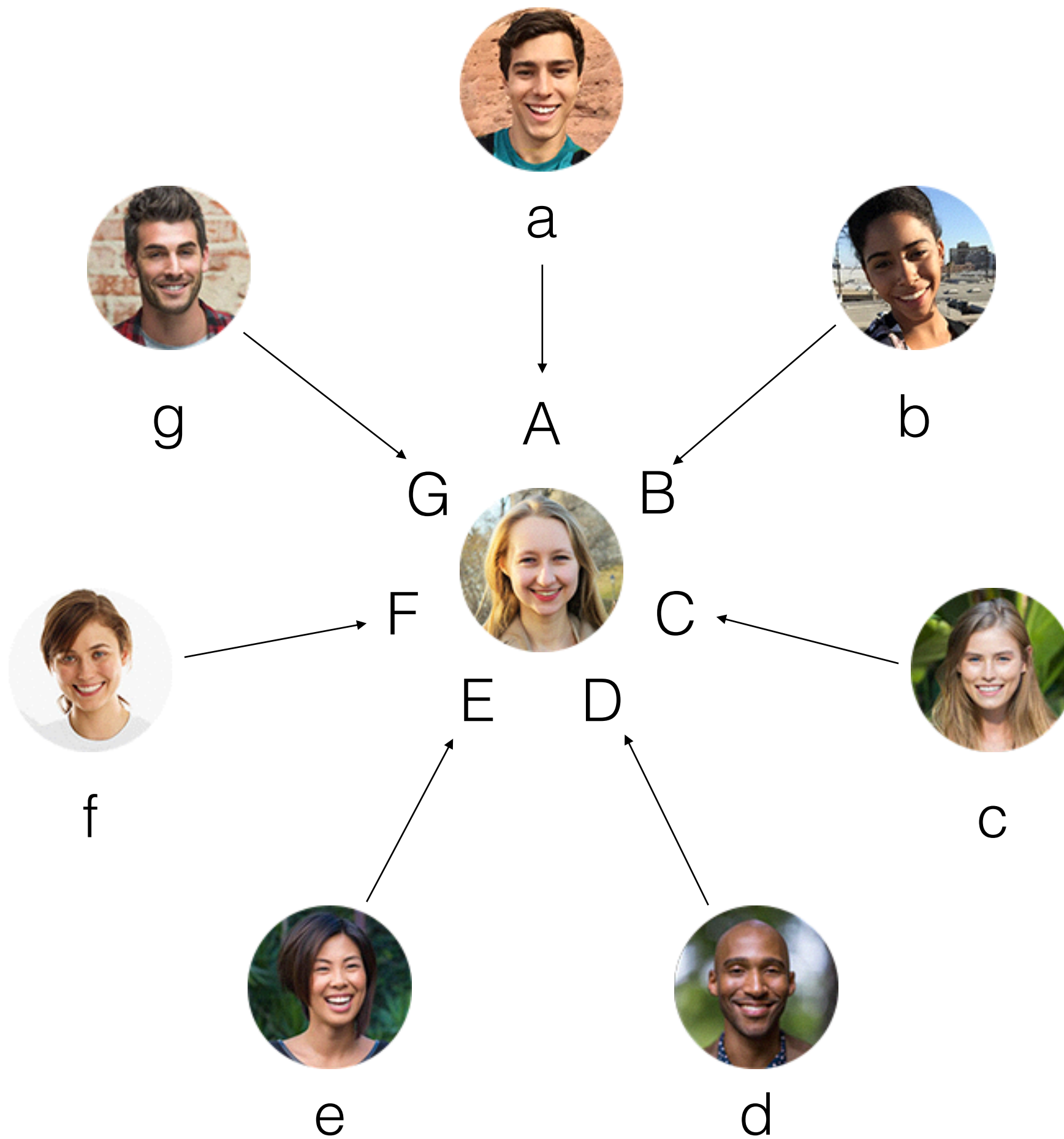
c, C



e, E



d, D



Transform public keys

A B C D E F G \longrightarrow Û Я Ñ Ì Ж Д Ø

Send funds to a multisig address



4-of-7 multisig

(Ü я Ñ Ì Ж Д Ø)



To unlock compose a transaction



Choose any 4 friends



f



c



e

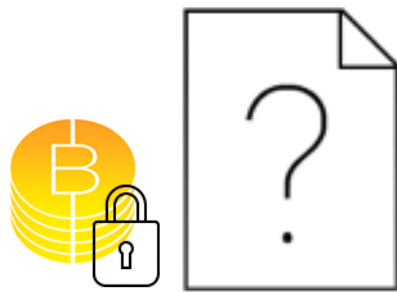


d

Blind transaction



f



c

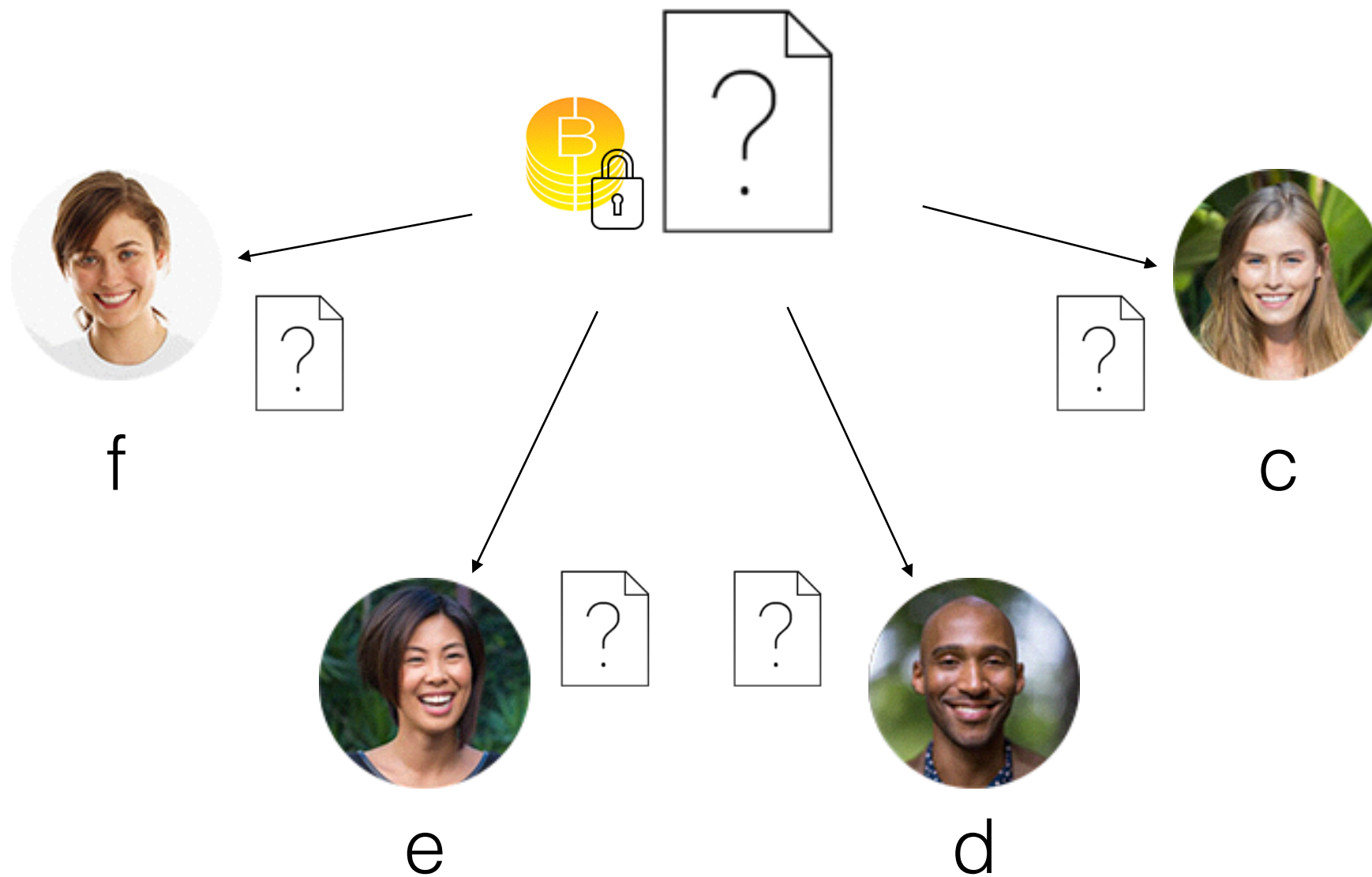


e

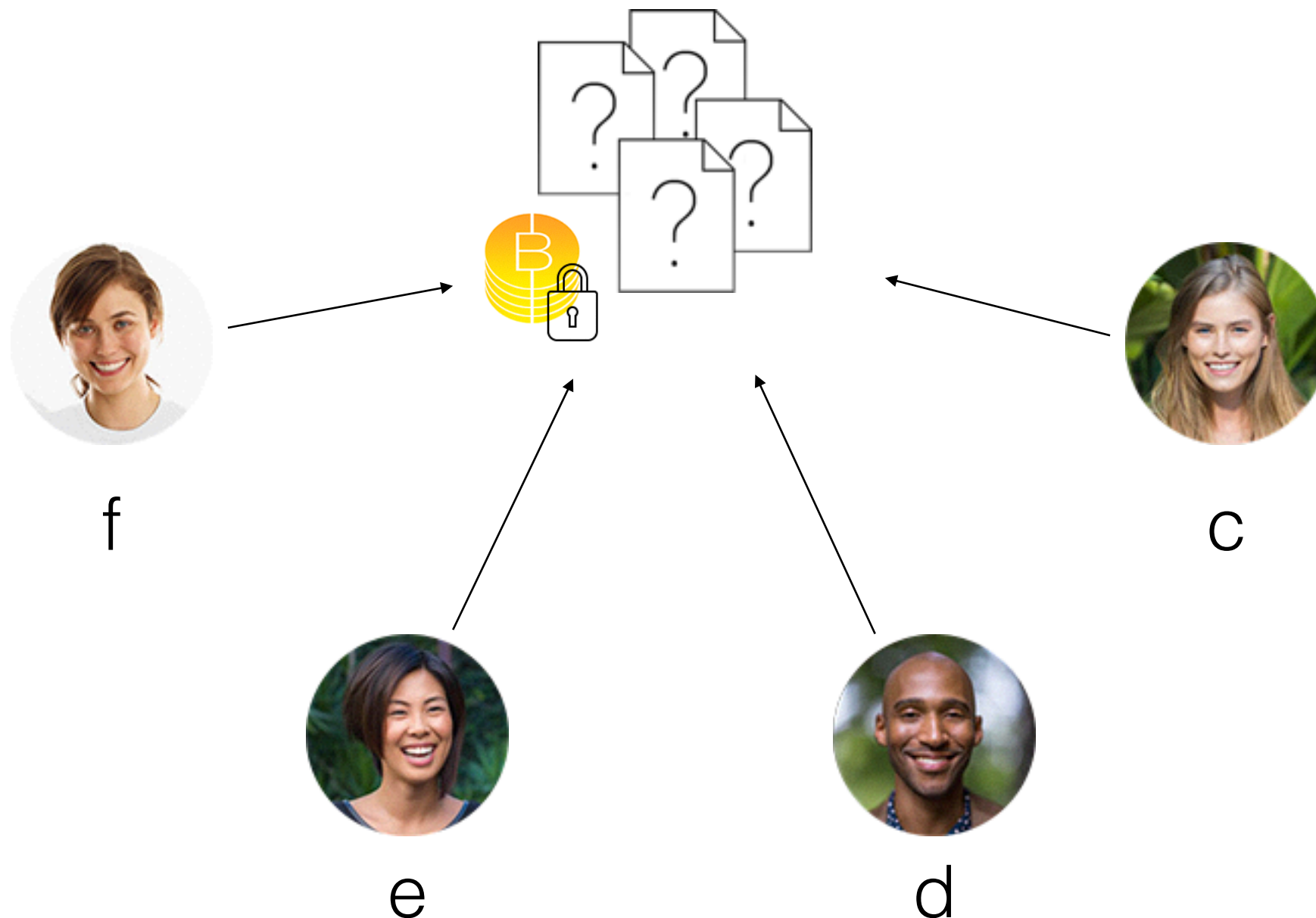


d

Ask to sign



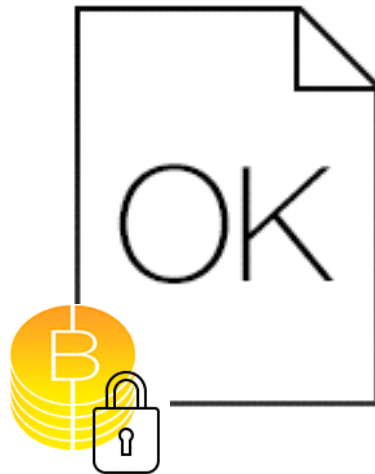
Collect signed transactions



Combine & unblind



f



c

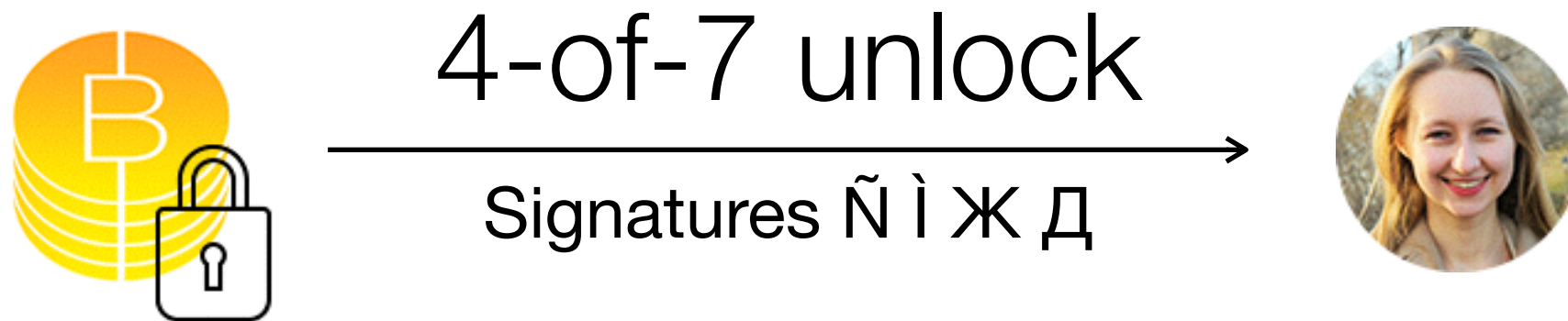


e



d

Broadcast transaction



Profit!



Ultimate vault

Friends authorize your actions like a bank.

Absolute privacy via

blind public keys,
blind signatures and
blind transactions.

Redundancy; no single point of failure.

Mutual custody — incentives to play nice.

References

1. Blind Signatures:

<http://blog.oleganza.com/post/77474860538/blind-signatures>

2. Ultimate Wallet:

<http://blog.oleganza.com/post/97712649288/the-ultimate-wallet>

3. Demo App:

<https://github.com/oleganza/blindsignaturedemo>

Oleg Andreev

blog.oleganza.com

@oleganza



<http://oleganza.com/MultisigOctober2014.pdf>