BITCOIN PROTOCOL AND CONSENSUS: A HIGH LEVEL OVERVIEW

Max Fang & Viget

TERMINOLOGY
BLOCKCHAIN FUNDAMENTALS

Bitcoin is the technology that started it all

- Bitcoin is a cryptocurrency

Blockchain is the technology underlying Bitcoin

- Enables distributed consensus

Community terminology

- **"crypto"**, **"cryptocurrency"** - Bitcoin, Ethereum, more technical
- **"private blockchains"**, **"permissioned ledgers"**, or just **"blockchain"**
- **"distributed tech"** or **"decentralized tech"** - umbrella term

AUTHOR: MAX FANG

BITCOIN AND CONSENSUS

BLOCKCHAIN AT BERKELEY

Slide by Viget

Blockchain fundamentals

Bitcoin is the technology that started it all

- Bitcoin is a cryptocurrency

Blockchain is the technology underlying Bitcoin: Enables distributed consensus

Community terminology

- **"crypto"**, **"cryptocurrency"** - Bitcoin, Ethereum, more technical
- **"private blockchains"**, **"permissioned ledgers"**, or just **"blockchain"**
- **"distributed tech"** or **"decentralized tech"** - umbrella term

BLOCKCHAIN AT BERKELEY

SATOSHI NAKAMOTO'S INNOVATION

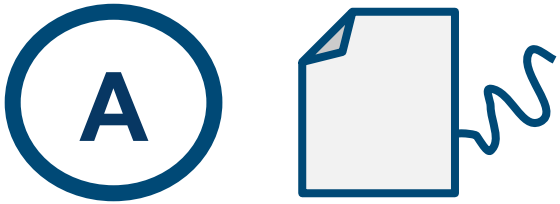
BLOCKCHAIN FUNDAMENTALS

Bitcoin was created by Satoshi Nakamoto in 2009

- Decentralized, trustless system for transactions
  - A low cost financial system that only requires an internet connection
- Nakamoto solved the Double Spending problem
  - Prevent someone from spending the same asset twice
  - Solution? The blockchain + Proof-of-Work

Slide by Viget

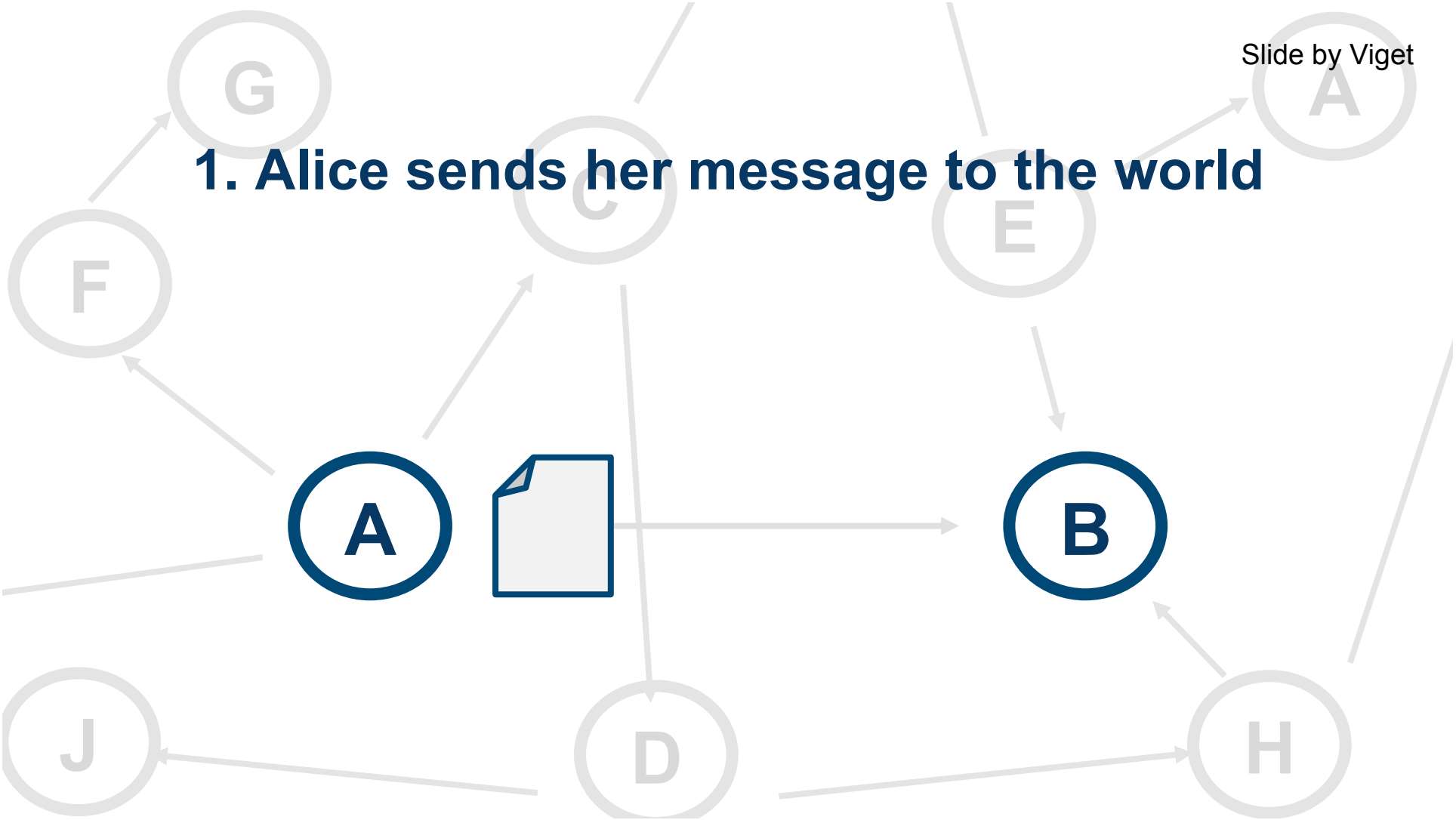
1. Alice writes and signs a message describing her transaction



“I, Alice, am giving Bob one bitcoin.”

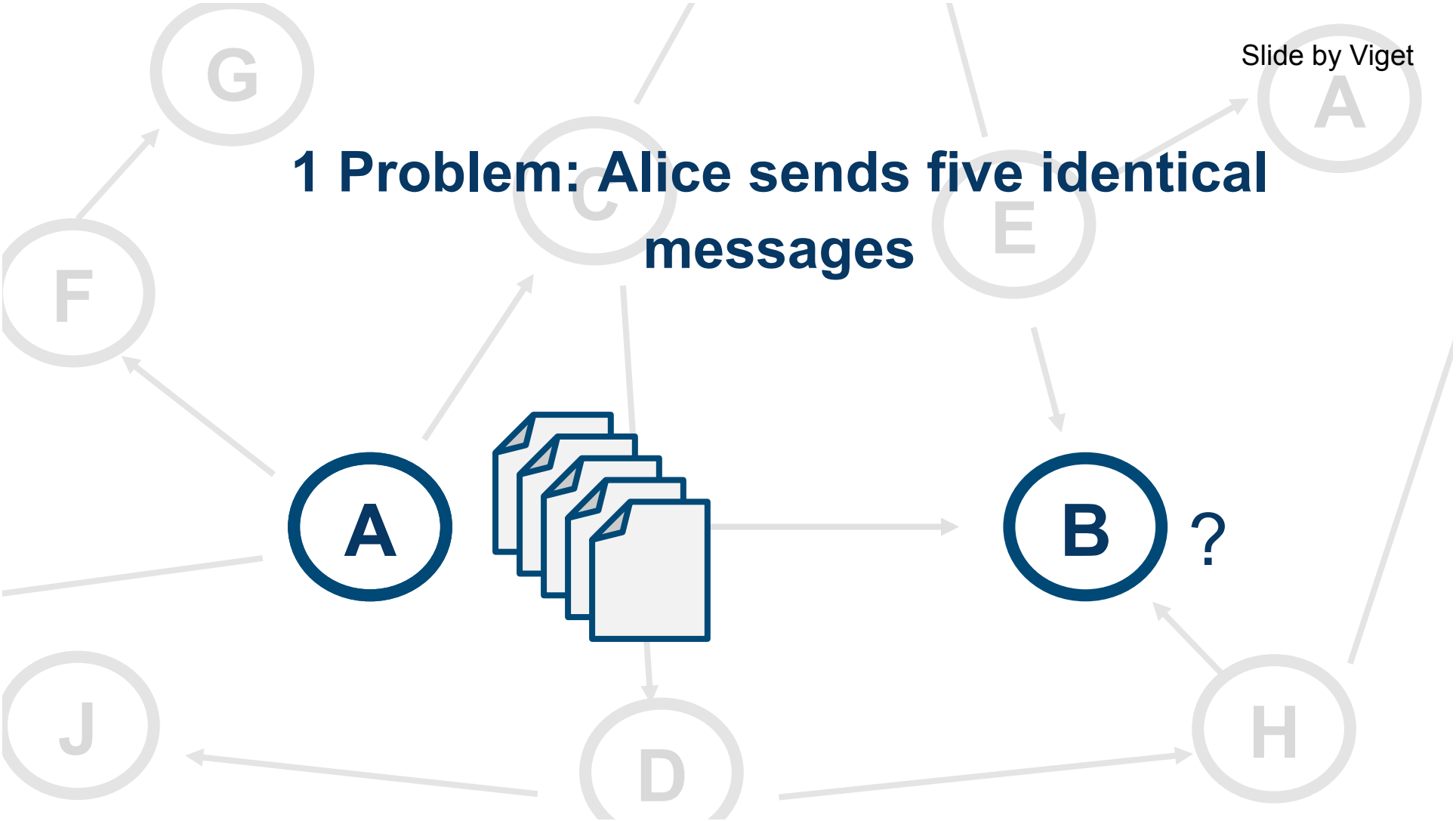
Slide by Viget

1. Alice sends her message to the world



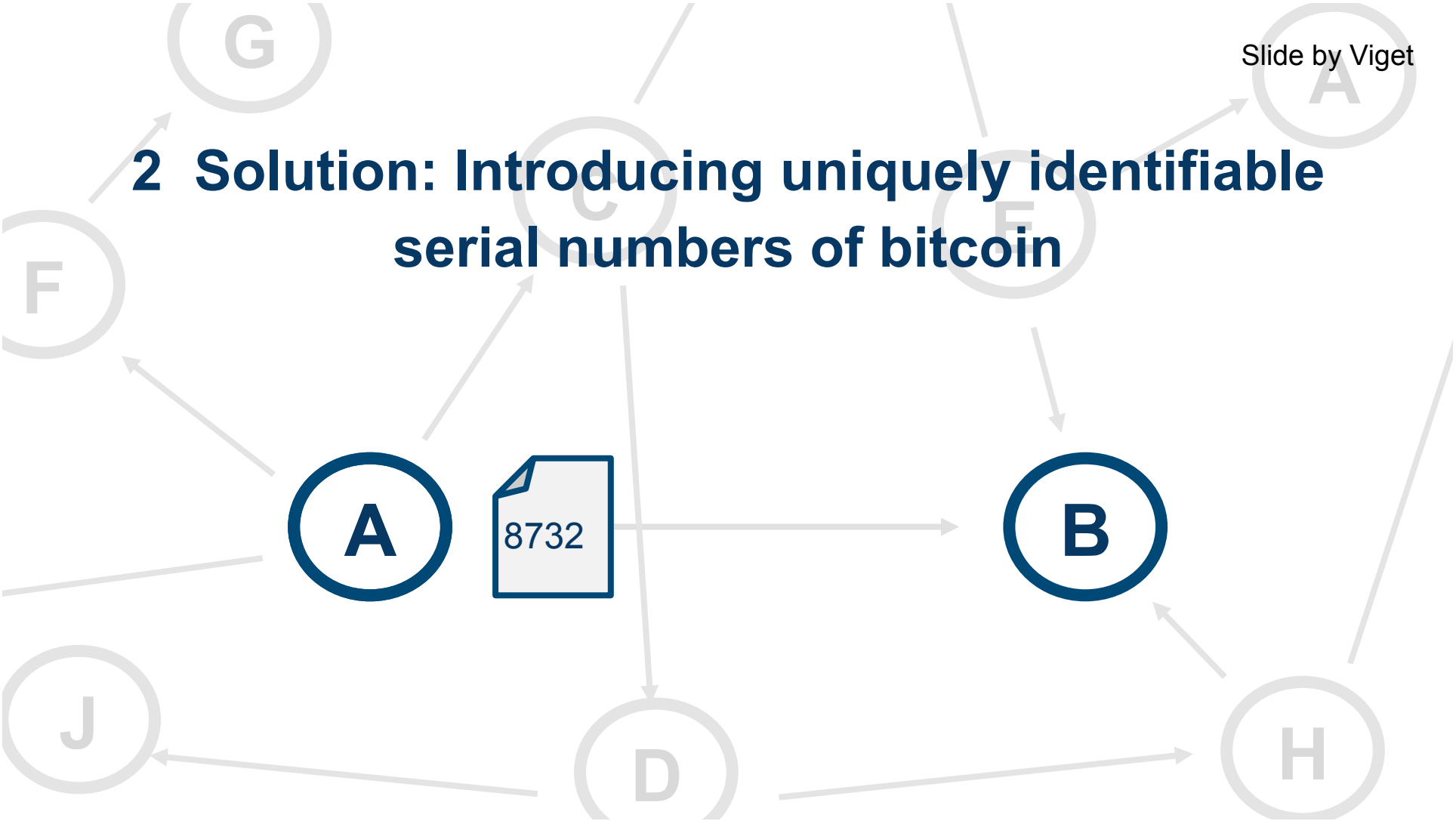
Slide by Viget

1 Problem: Alice sends five identical messages



Slide by Viget

2 Solution: Introducing uniquely identifiable serial numbers of bitcoin



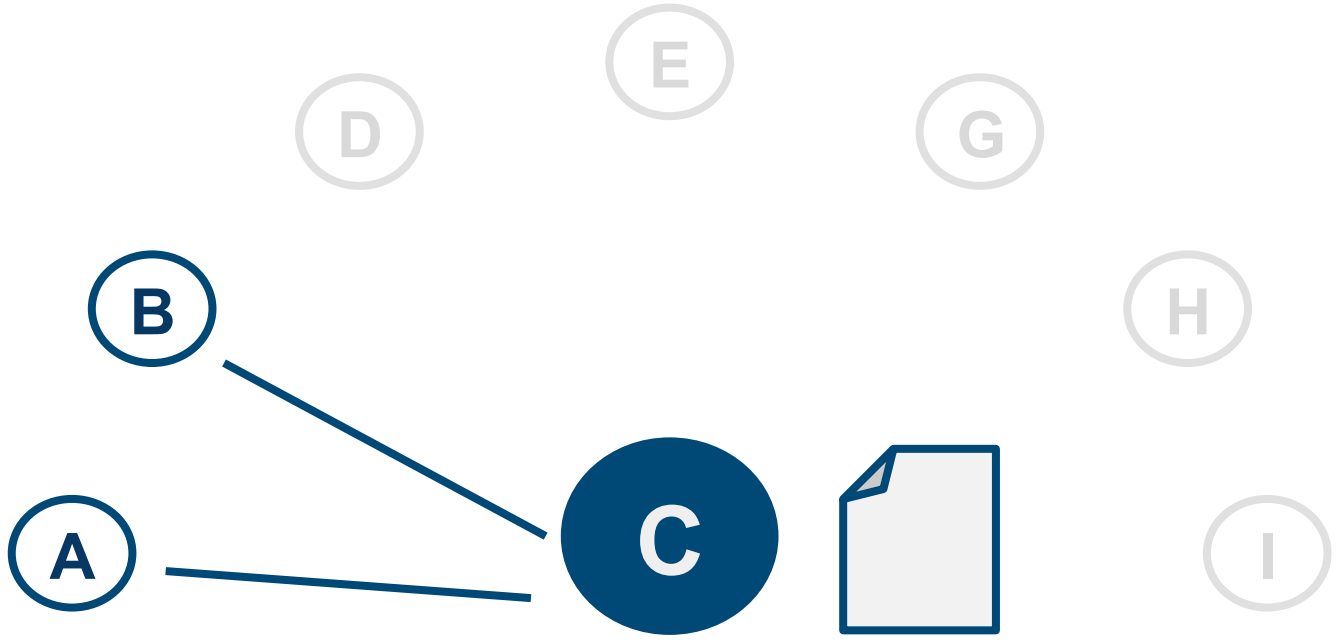
Slide by Viget

2 Where do serial numbers come from?

?

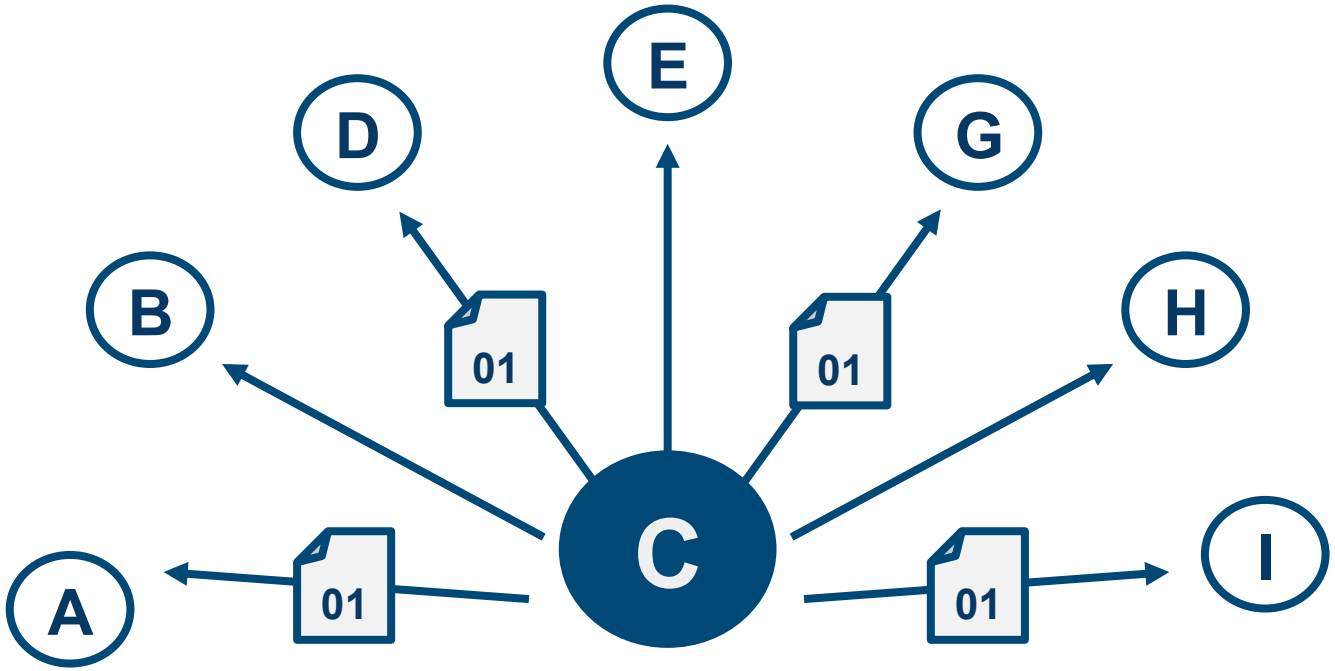
Slide by Viget

2 Usual solution (centralized): A central bank manages transactions and balances each banknote has a serial number



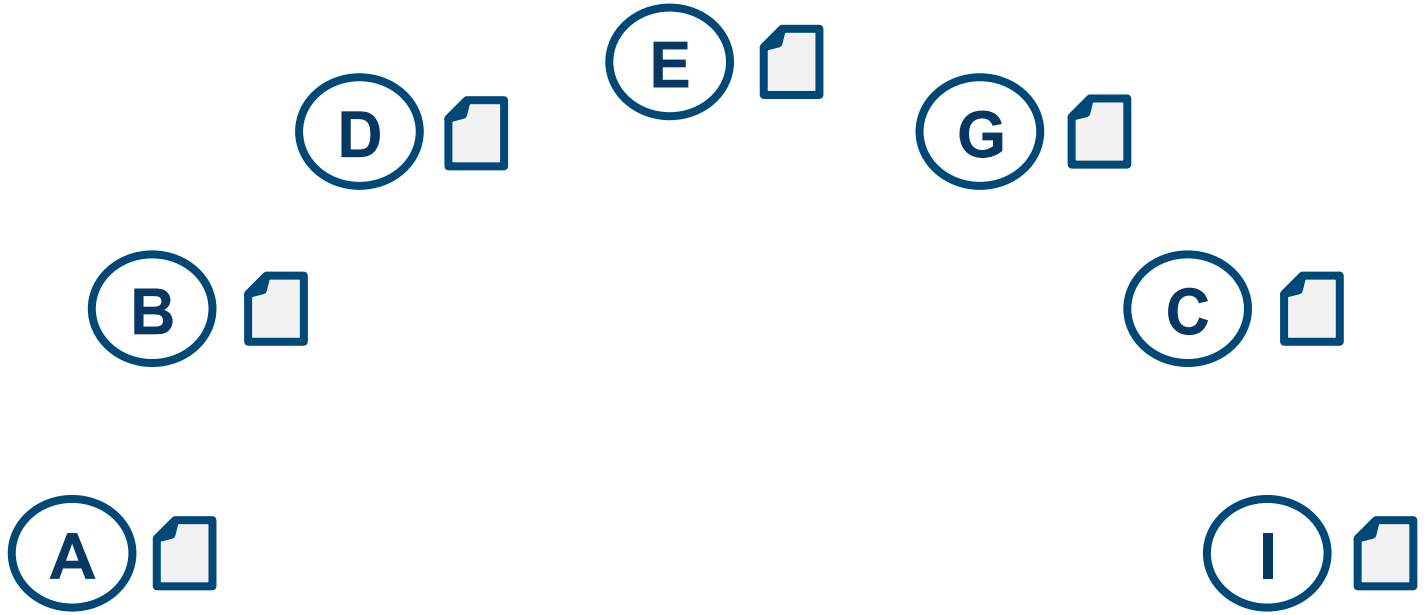
Slide by Viget

2 Central bank: Centralization



Slide by Viget

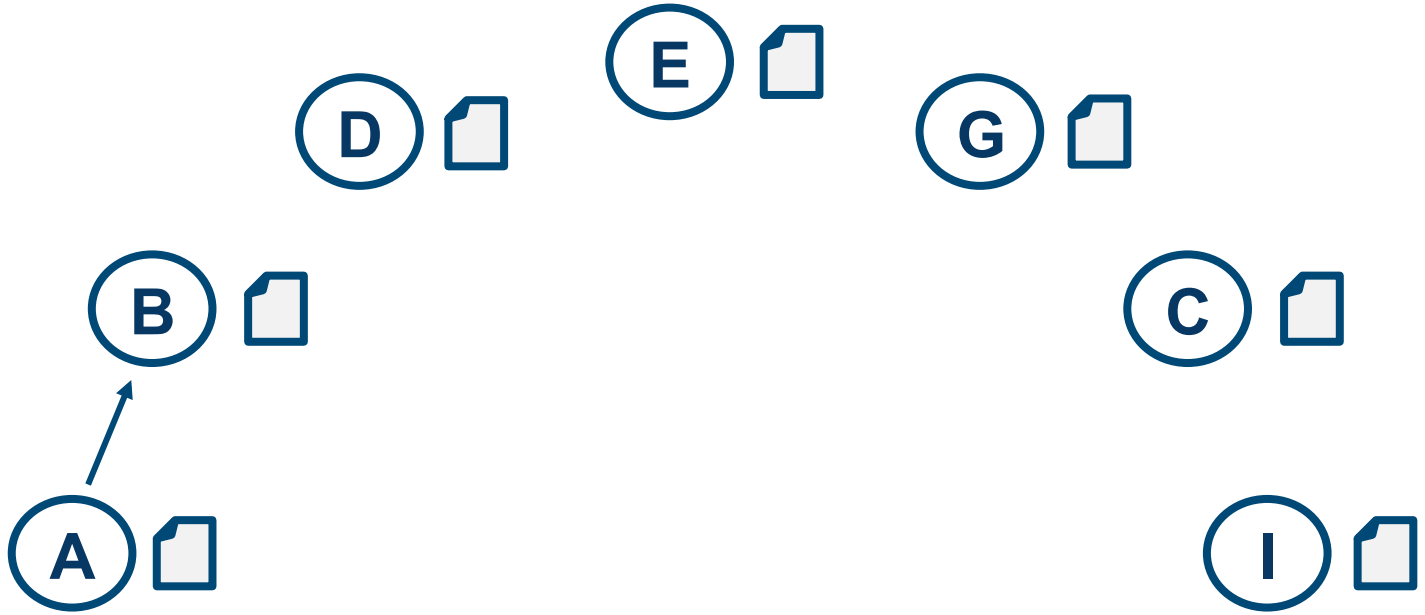
3 Distributed: Making everyone the bank
Everyone has a complete record of transactions



Slide by Viget

3. Making everyone the bank

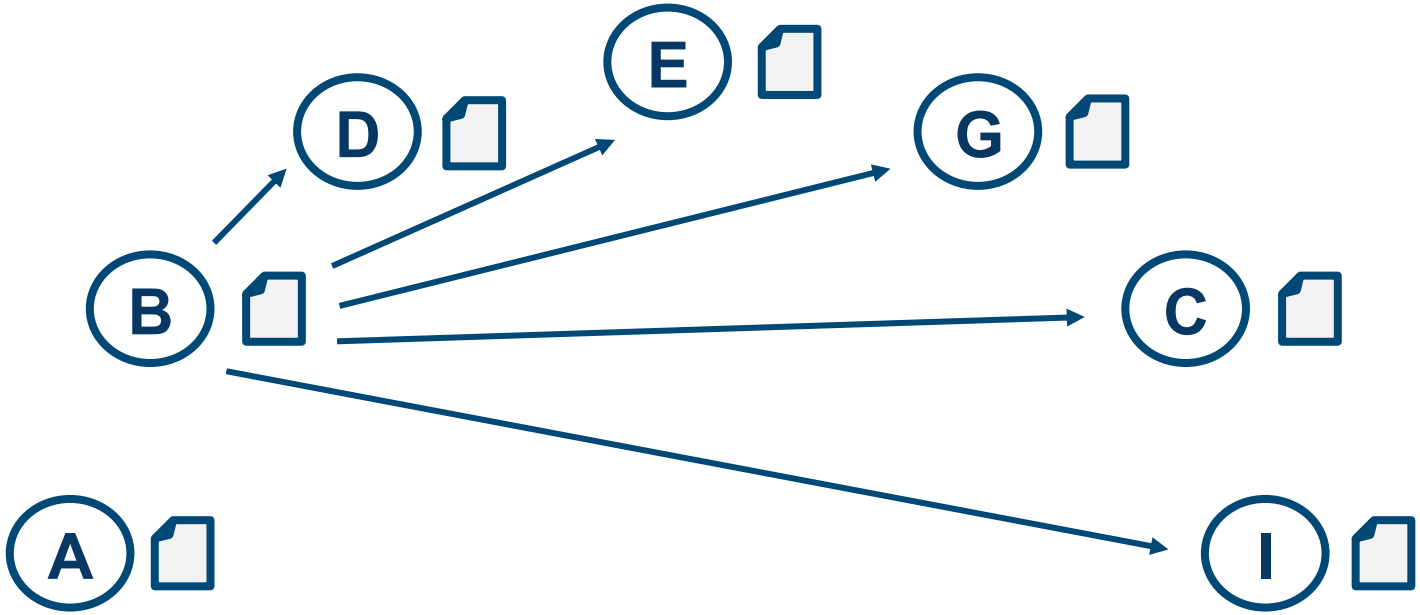
3.1 Alice sends her transaction to Bob



Slide by Viget

3. Making everyone the bank

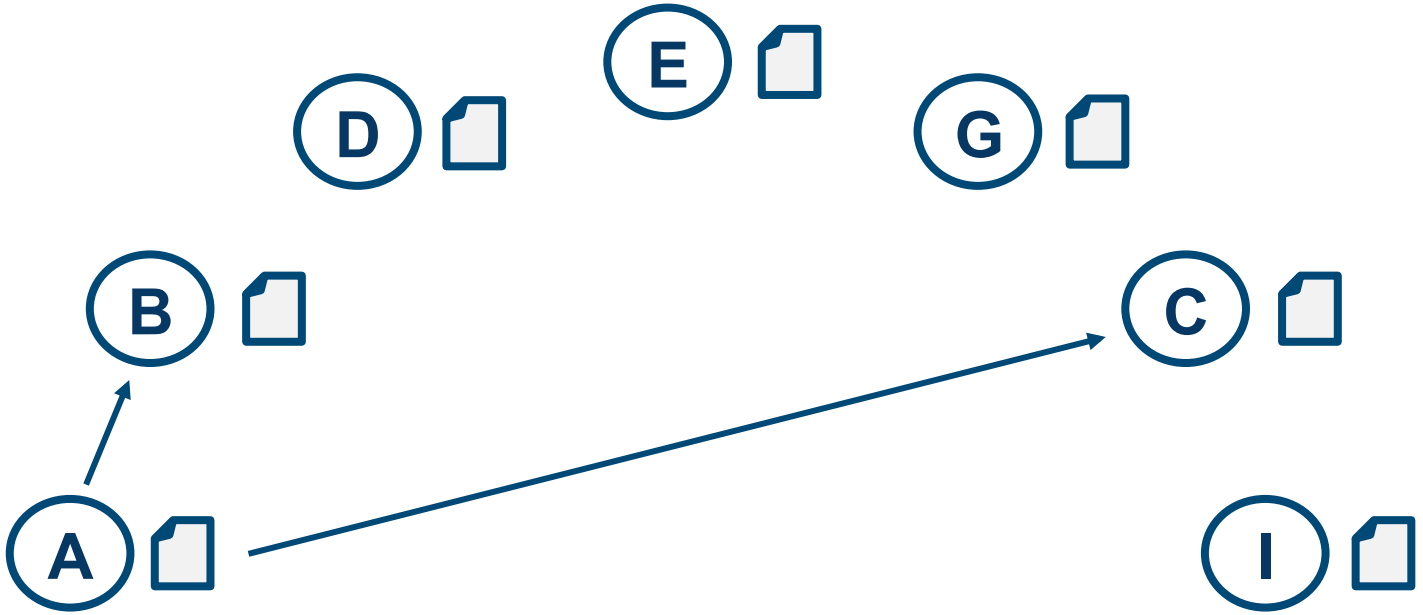
3.2 Bob announces the transaction to the world



Slide by Viget

3. Making everyone the bank : Problem

3.3 Alice double spends on Bob and Charlie

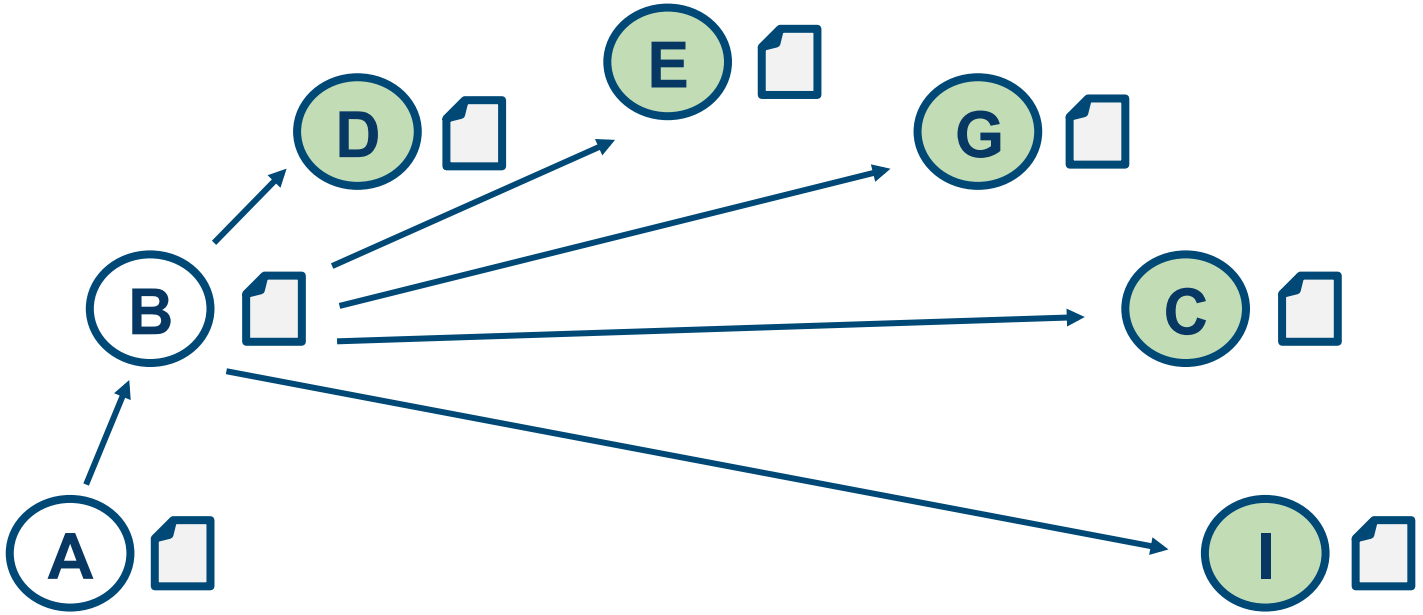


Slide by Viget

3. Making everyone the bank

3.4 Everyone verifies transactions

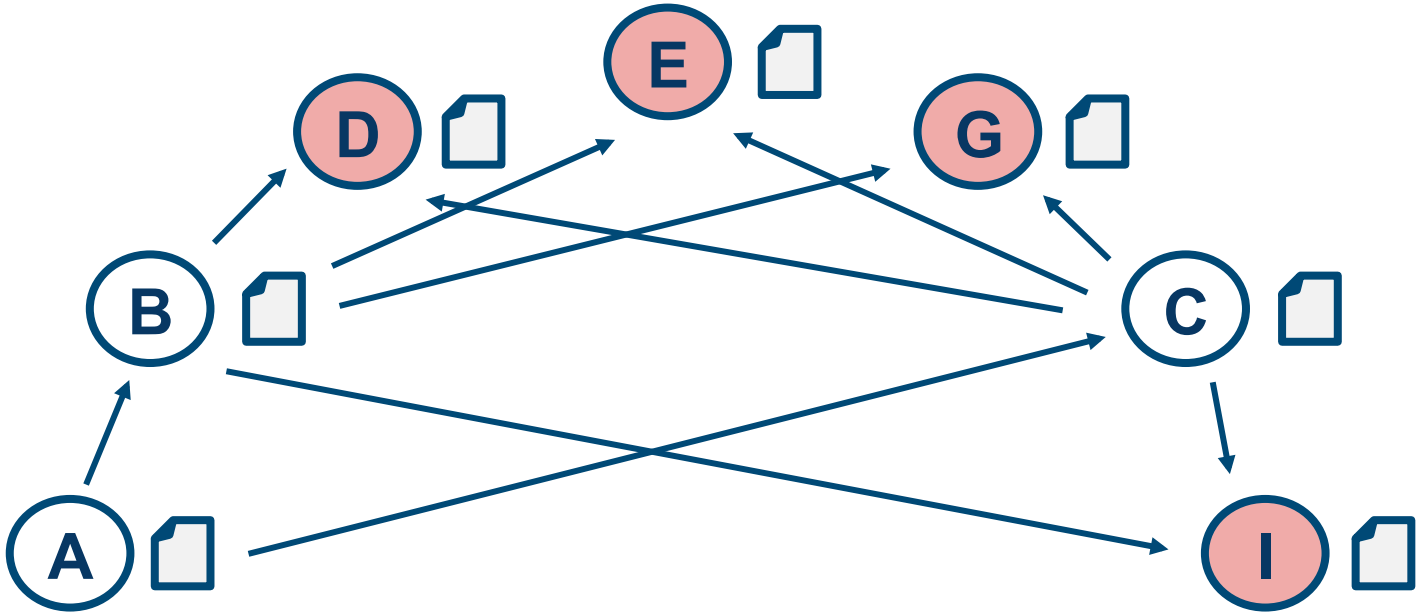
A transaction is accepted if everybody accepts



Slide by Viget

3. Making everyone the bank

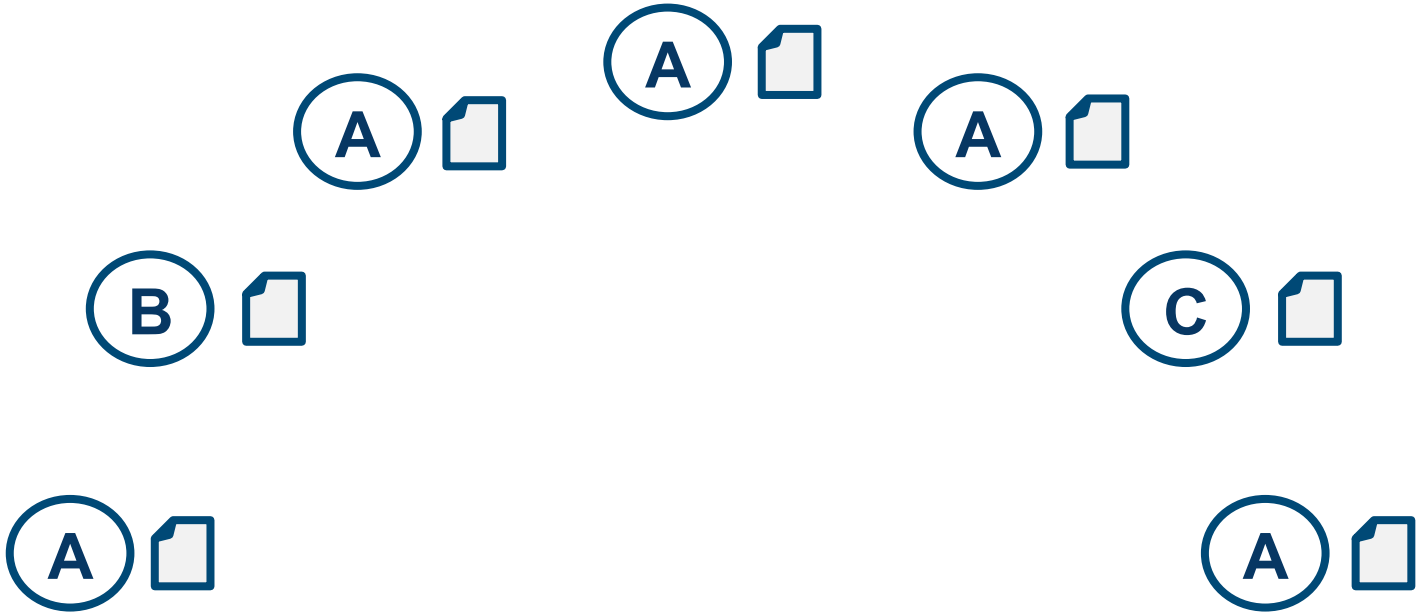
3.4 Everyone verifies transactions therefore Alice is prevented from double spending



Slide by Viget

3. Making everyone the bank

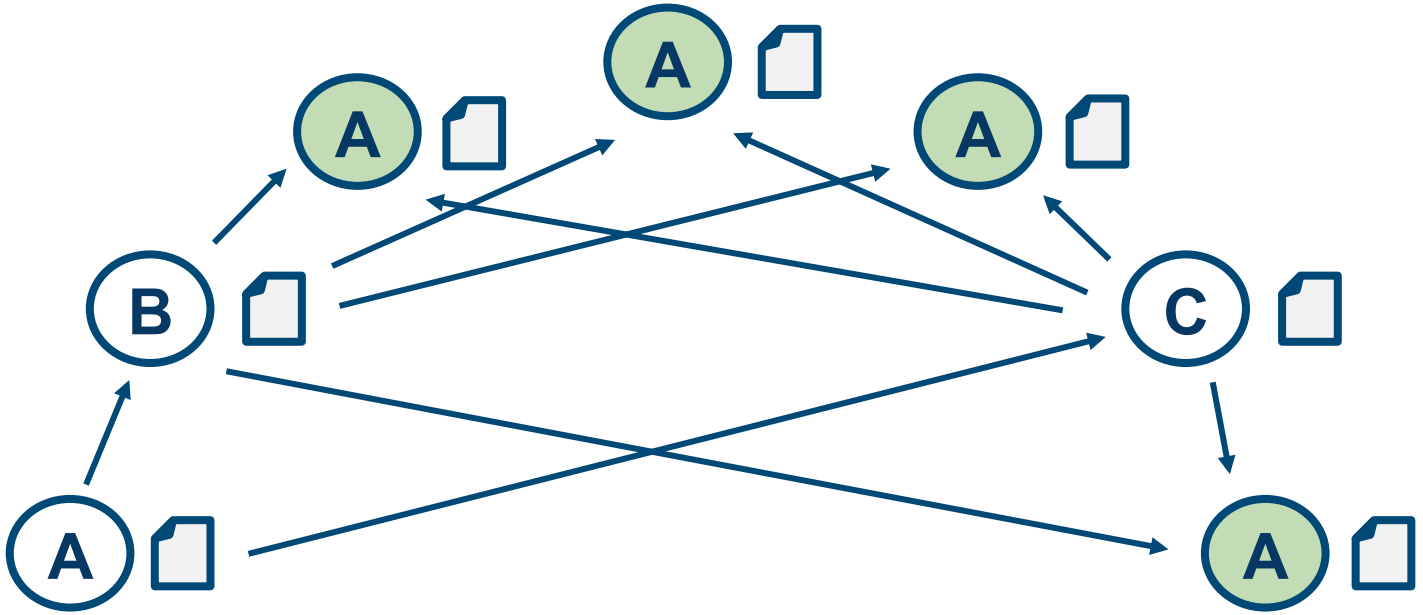
3.5 Alice sets up multiple identities



Slide by Viget

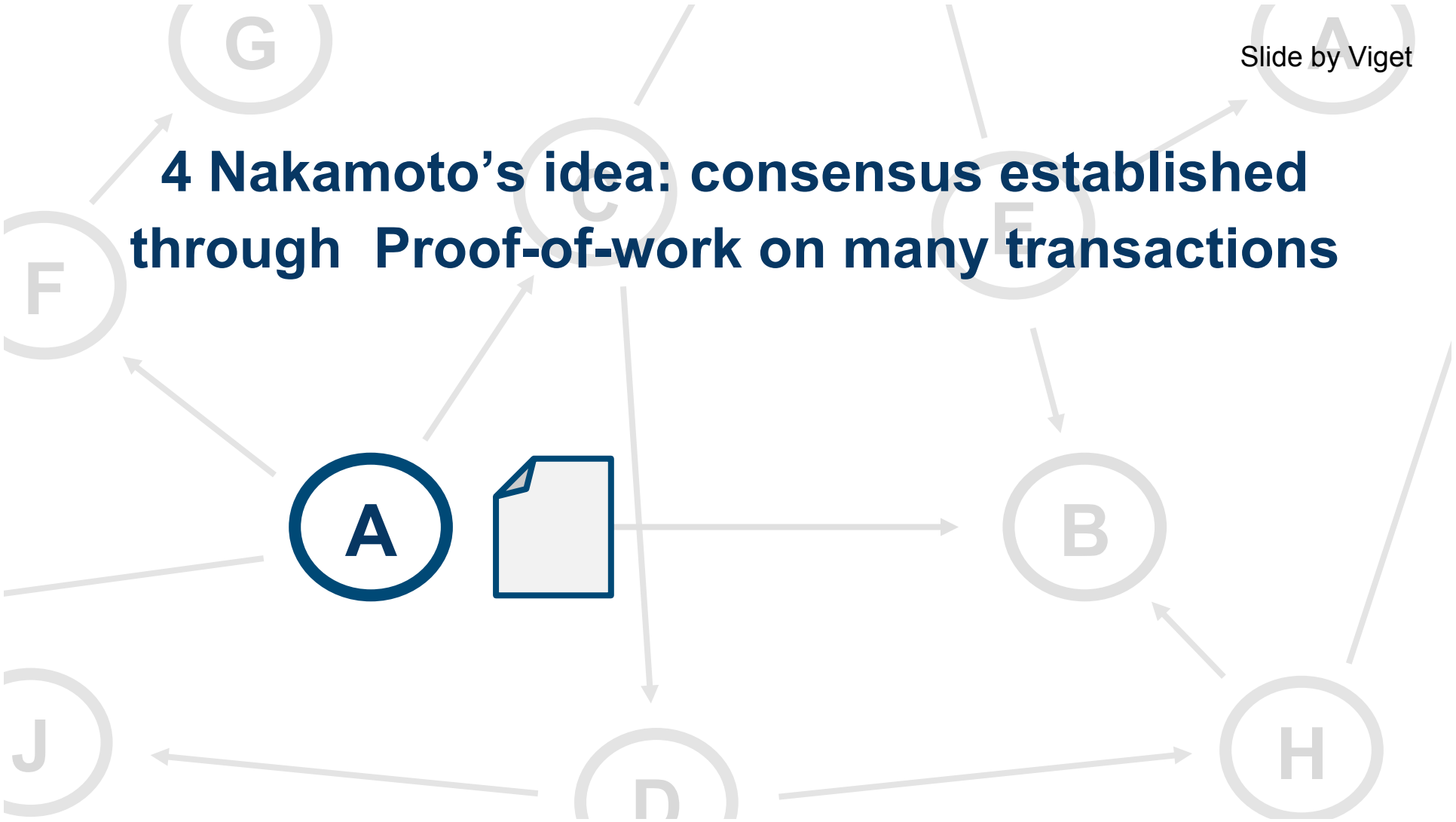
3.5 Alice double spends using multiple identities

Sybil Attack: Creating many fake identities to subvert a system



Slide by Viget

4 Nakamoto’s idea: consensus established through Proof-of-work on many transactions



Slide by Viget

4.1 Block: verify a block of transitions

Many users add to list of pending transactions

Block: a set of transactions

1. I, Tom, am giving Sue one bitcoin, with serial number 3920.
2. I, Sydney, am giving Cynthia one bitcoin, with serial number 1325.
3. I, Alice, am giving Bob one bitcoin, with serial number 1234

All transactions since Bitcoin started are stroed using as data structures a list (chain) of blocks

Slide by Viget

4.1 Verifying transactions

0 Form block

1 Check block is correct

2 Solve puzzle

3 Announce block to all users

4 users verify correctness

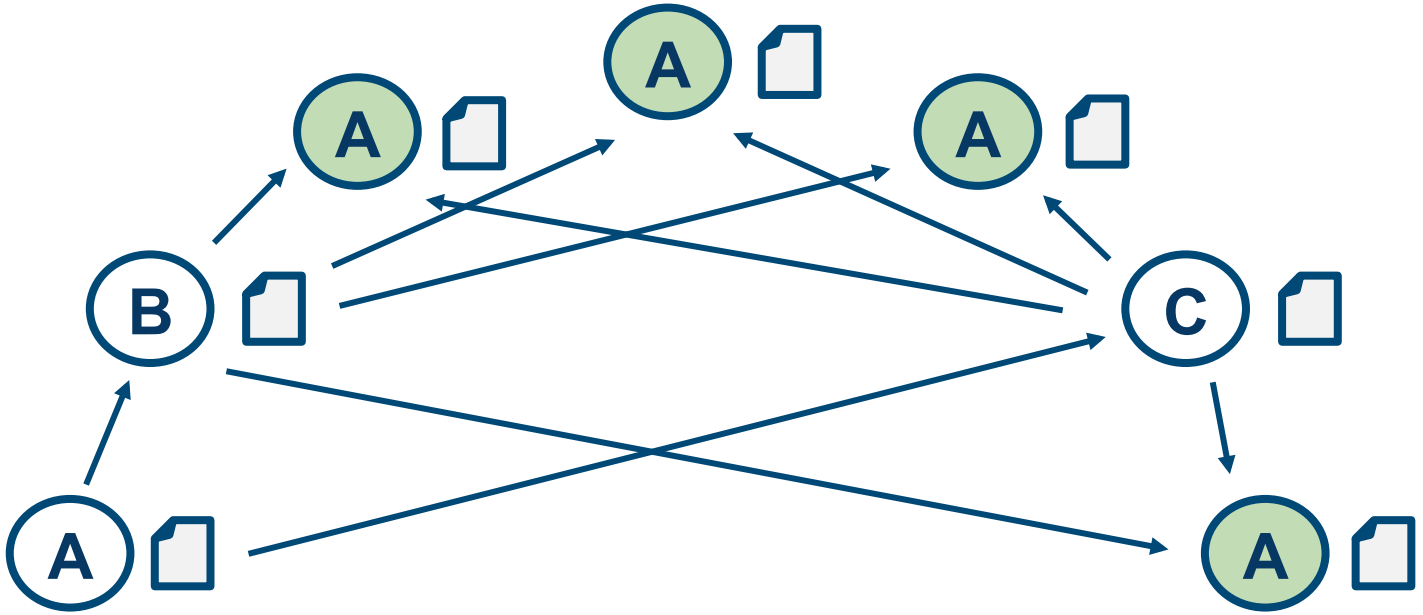
Slide by Viget

5 Nakamoto’s idea:
Solve the puzzle using Mathematics
Why the math?

Slide by Viget

5.1 Why the math?

We want to make it costly for Alice to double spends with her multiple identities



Slide by Viget

5.2 How is the math?
Proof-of-work as a competition
who wins the competition is paid with Bitcoins

5.2 Proof-of-work as a competition

Slide by Viget

- the winner is the first that solves a puzzle on the new block to be added to the blockchain
- the winner is paid with Bitcoins
- the rule of the game favour honest behaviour: there is an incentive to recognize the winner also for those that are not winner

Slide by Viget

Summary

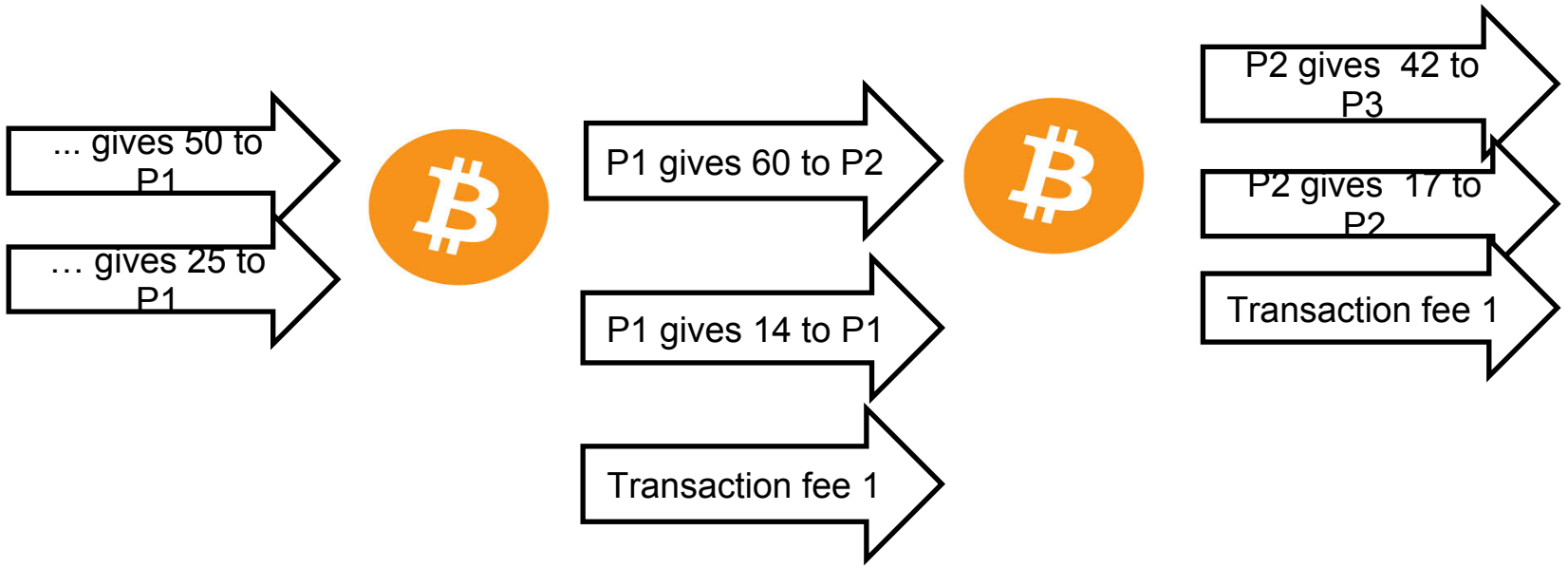
	Major feature	**Value added**
1	Signed messages announced to the network	Basis of entire system
2	Serial numbers	Uniquely identifiable transactions
3	The block chain	Shared record of transactions
4	Everyone verifies transactions	Increased security
5	Proof-of-work	Prevents double spending

How is money created in Bitcoin?

- New block **every ~10 mins**
  - **d** adjusted every ~2000 blocks
- H = **2-SHA2**
- d number of leading zeros of hash (difficulty)
- R random number, L new block
- Initial reward: **50 BTC**
  - Halved every ~4 years (now **6.25 BTC**)

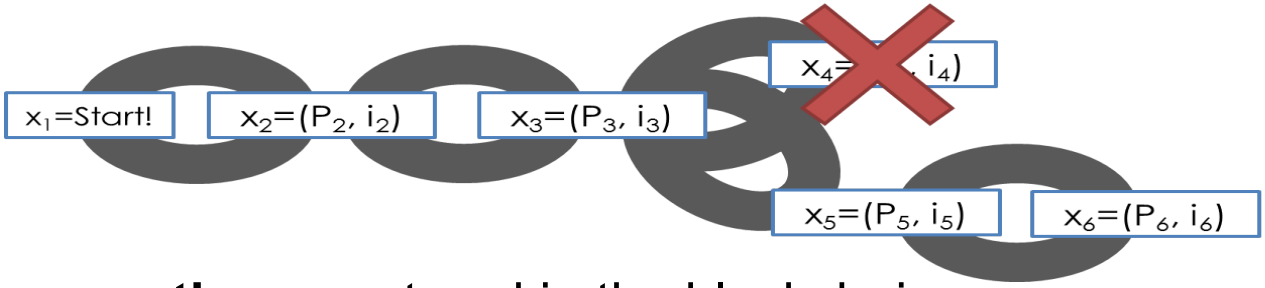
How is money transferred in Bitcoin?

Example: P1 wants to give 60 to P2



How is money stored in Bitcoin?

- Transaction in **orphaned blocks** are invalid
  - **Wait 6 blocks** (~1 hour) before accepting transaction.
  - **Checkpoints** to prevent complete history rollback



- **All transaction** are stored in the blockchain
  - (Currently ~170 GB)

Questions

1. how the protocol does not allow i) Stealing Bitcoins, ii) Denial of service attack, and iii) Double spending Bitcoins.

2. Why do miners run “full nodes” that keep track of the entire block chain whereas Bob the merchant can get away with a “light node” that implements “simplified payment verification,” needing to examine only the last few blocks?

3. If a malicious ISP completely controls a user’s connections, can it launch a double−spend attack against the user? How much computational effort would this take?

Questions

4. Even when all nodes are honest, blocks will occasionally get orphaned: if two miners Minnie and Mynie discover blocks nearly simultaneously, neither will have time to hear about the other's block before broadcasting hers.

- 4a. What determines whose block will end up on the consensus branch?
- 4b. What factors affect the rate of orphan blocks?
- 4c. If Mynie hears about Minnie's block just before she's about to discover hers, does that mean she wasted her effort?
- 4d. Do all miners have their blocks orphaned at the same rate, or are some miners affected disproportionately?

Questions

5. If a miner misbehaves, can other miners “boycott” her by refusing to build on her blocks on an ongoing basis?
6. Discuss potential problems that might arise in the future and that might dramatically liit the use of Bitcoin.