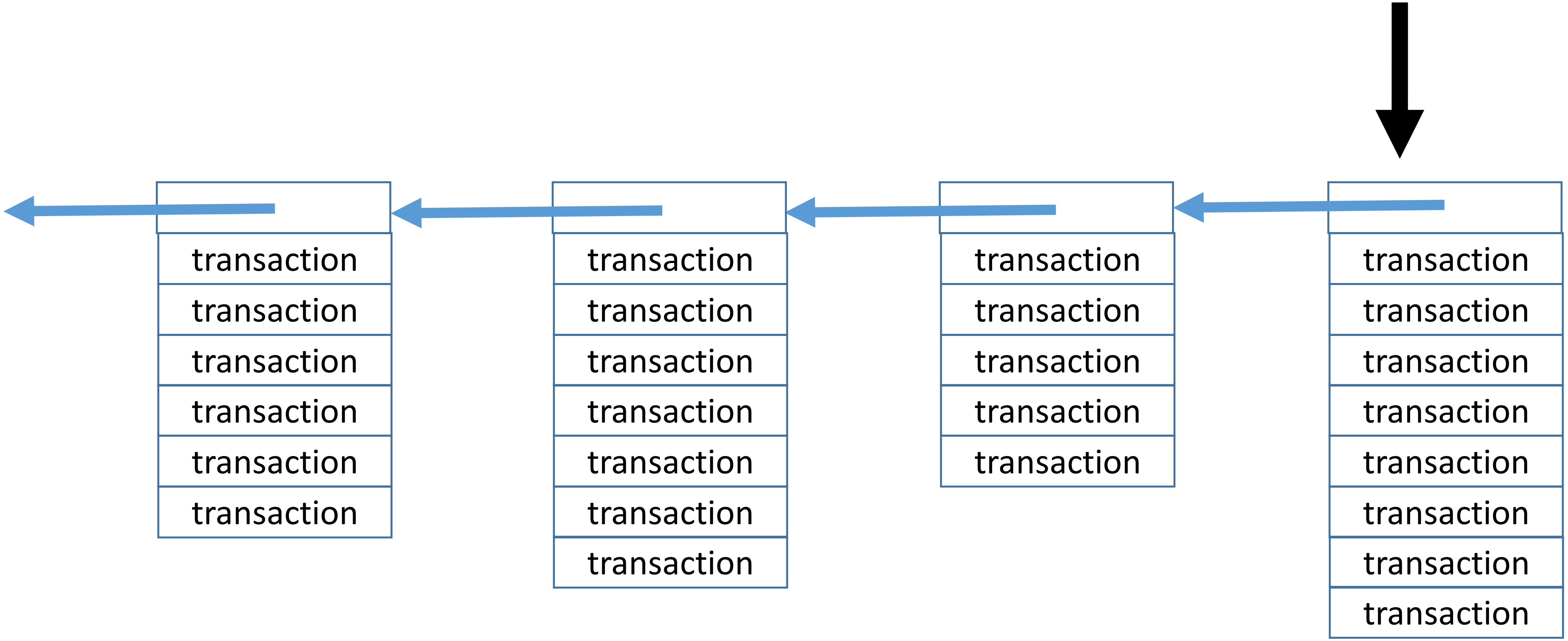
Blockchain and Cryptocurrencies: Technical Background

Ed Felten

Deputy U.S. Chief Technology Officer

OSTP

What is a blockchain?



Newest block is at the end

transaction
transaction
transaction
transaction
transaction
transaction

transaction
transaction
transaction
transaction
transaction
transaction
transaction

transaction
transaction
transaction
transaction
transaction

transaction
transaction
transaction
transaction
transaction
transaction
transaction
transaction

Why a blockchain?

- Gives you a public ledger that is tamper-*evident*
  - Any attempt to rewrite history will be detected
- If we assume previously published blocks remain available forever, then ledger is tamper-*proof*

- Doesn’t solve all problems, just those where a public ledger helps

- Not most efficient approach, if you just want to publish information

Who publishes the blocks?

Central authority model:

authority makes blocks, digitally signs them and publishes

Quorum model:

well-known list of authorities

authorities agree “behind the scenes” on contents of next block

authorities sign the agreed-upon block, and publish it

users trust any block signed by a quorum of authorities

Fully decentralized model:

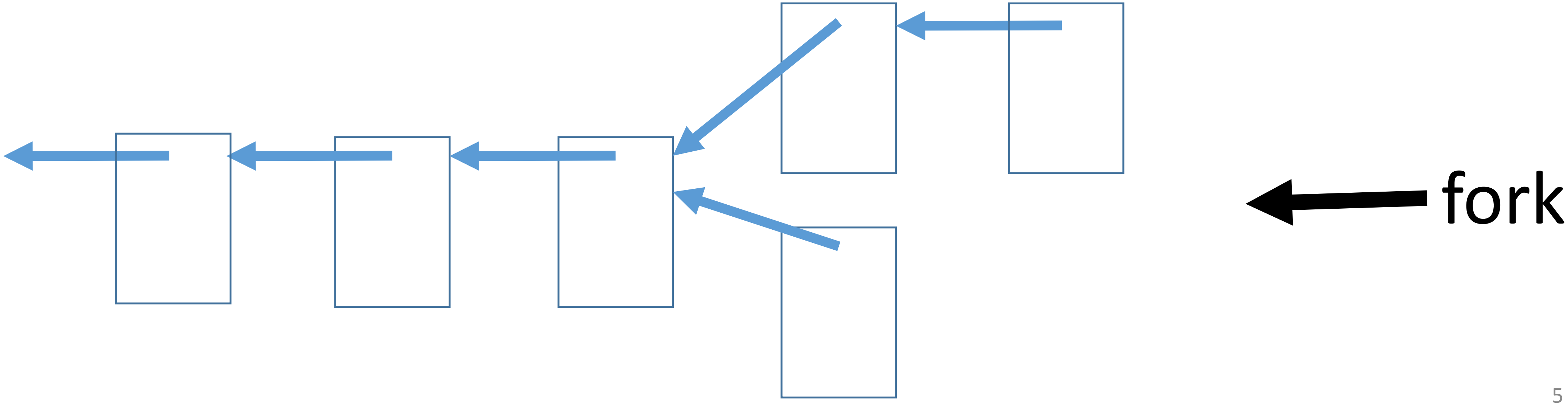
“everyone cooperates” to agree on the next block

Required properties

Liveness: At least one new block is published in every time step.

Consensus: No block has more than one successor.

or: "No forks."



Preventing forks

With a central authority: If we see a fork, punish the authority.

With a quorum system:

If we see a fork, some authority must have misbehaved.

Punish that authority.

Fully decentralized approach: It’s very complicated!

Fully decentralized consensus: why it’s hard

Need all participants to agree on the next block, but:

- Very large number of participants
- Don’t know who they are
- Some might be sock puppets for others
- Participants have incentive to manipulate the outcome
- Participating honestly might be costly (computing, bandwidth, etc.)
- Can’t assume a single legal system that reaches all participants

Seems impossible?

Decentralized consensus: using incentives

Solution concept: design an incentive mechanism so that

- if everyone* rationally maximizes their revenue,
- and assumes that everyone* else rationally maximizes their revenue
- then consensus will result.

Note that the mechanism must be self-enforcing, in the sense that it relies only on cryptographic math and the laws of the universe, not on legal enforcement.

“everyone*” means: almost everyone, a large majority

Nakamoto’s Solution (in Bitcoin)

- Create a blockchain and a digital currency together, each depending on the other (“symbiotic”)

- Use the blockchain to record transfers of the currency
- Use the currency to pay people to make new blocks for the blockchain
  - Key idea: payment contingent on the new block being accepted as valid

- Why it seems* to lead to consensus:
  - If you make a block that forks the chain, it might not be accepted by others
  - If you make a block that doesn’t create a fork, it is more likely to be accepted
  - So your incentive is to avoid making a fork

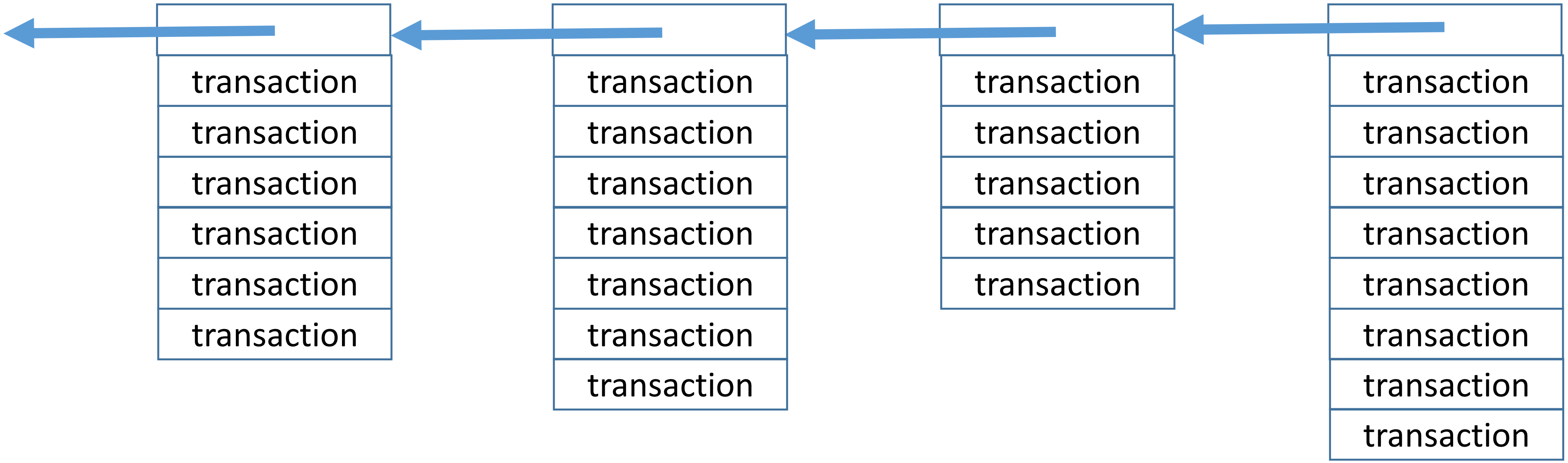
Implications …

Any blockchain must either:

- use a centralized or quorum approach, or
- be symbiotic with a digital currency.

A “bare” blockchain that is fully decentralized is not something we know how to build.

But: what is a valid transaction?



Valid transactions (in Bitcoin)

Payment of Coin C from Person A to Person B: valid if

- Person A owns Coin C, and
- Person A has digitally signed the transaction.

Creation of new coins: valid if

- No more than 25 new coins are created, and
- This is the only coin creation transaction in the current block.

[other transaction types omitted]

What if a transaction is invalid?

If a block contains an invalid transaction, ignore that whole block.

Result: incentive to avoid creating blocks with invalid transactions.

Therefore: A transaction will be accepted as valid if everyone* believes it will be accepted as valid.

Therefore: A transaction validity rule will be enforced if everyone* believes it will be enforced.

Therefore: The rules will change whenever everyone* believes they have changed.

Privacy / Anonymity

- Bitcoin currency and blockchain use “pure pseudonyms.”
  - Pseudonym is just a randomly generated crypto key.
  - Anyone can make a new pseudonym at any time.
  - Anyone can make as many as they like, whenever needed.

- Easy for anyone to “follow the money” because all transactions are published on the blockchain.
- But don’t see identity of actors, only pseudonyms.
  - Crucial question: Can you link pseudonym to identity?
  - Answer: Sometimes; it’s complicated.

Coming soon: Fully anonymous cryptocurrency

- Researchers have discovered fancy crypto tricks that allow fully anonymous cryptocurrency.
  - Blockchain consists entirely of cryptoblobs that nobody can read.
  - But you can:
    - Prove to a third party that you own a coin, and
    - Transfer coins to another party

- Blockchain conveys absolutely nothing of use to an analyst.

- A startup company is building this now.   (Zerocash / Zcash)

Blockchain and Cryptocurrencies: Technical Background

Ed Felten

Deputy U.S. Chief Technology Officer

OSTP