Are Blockchains Useful Beyond Digital Currencies?

Kari Kostiainen

ETH Zurich

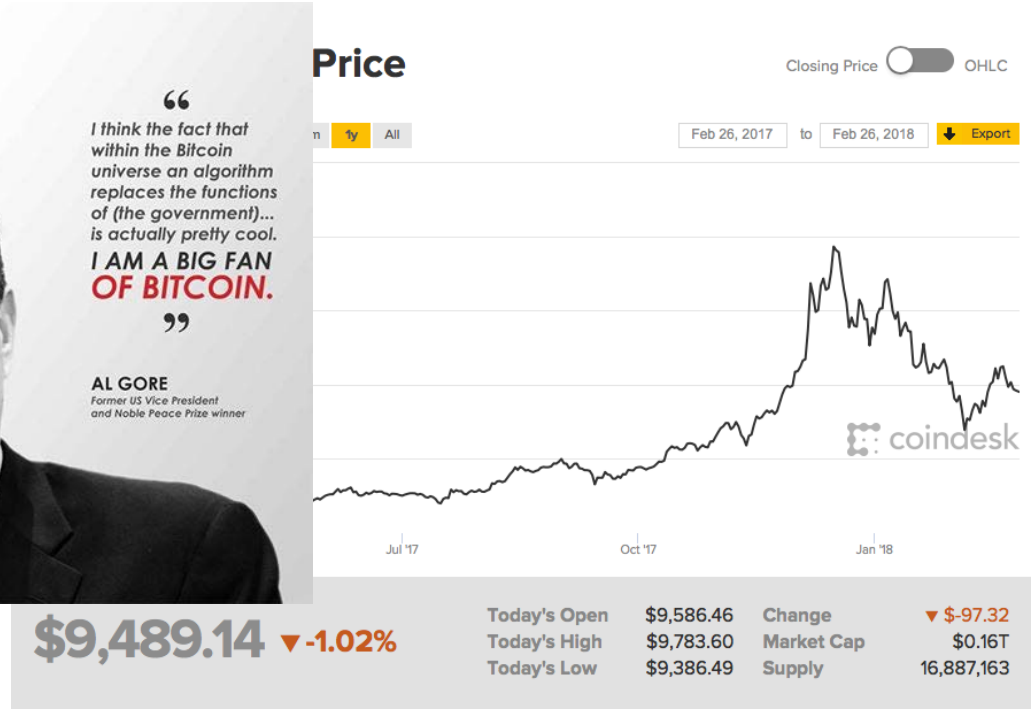
WIPO Workshop

Session: Opportunities and challenges in leveraging Blockchain

Blockchain in media

PARTNER CONTENT JOSH ZERLAN, BUTTERFLY LAB

BITCOIN AS THE ULTIMATE DEMOCRATIC TOOL



Bloomberg Markets | Markets | Tech | Pursuits | Politics | Opinion | Businessweek

Long Island Iced Tea Soars After Changing Its Name to Long Blockchain

Bitcoin biggest bubble in history, says economist who predicted 2008 crash

Nouriel Roubini calls cryptocurrency the 'mother of all bubbles' as it falls below $8,000

Future of money?

CNBC

THE FED

ECONOMY | WORLD ECONOMY | US ECONOMY | THE FED | CENTRAL BANKS

Federal Reserve starting to think about its own digital currency, Dudley says

Jeff Cox | @JeffCoxCNBCcom

Published 8:52 AM ET Wed, 29 Nov 2017 | Updated 10:21 AM ET Wed, 29 Nov 2017

CNBC

BANK OF ENGLAND | Browse | About | News & Events | Museum

The Bank of England is carrying out ongoing research into various types of digital currency, them.

ECONOMY | CENTRAL BANKS

Sweden's Central Bank Considers Digital Currency

Deputy governor says nation's sharp decline in cash usage may make it among first to adopt new system

What is digital currency?

- Common definition of **currency**
  - Unit of account
  - Store of value
  - Means of exchange
- Digital currency exists only in **electronic form**
- Isn’t money already digital?
  - We have **digital payments**
  - But people can **hold money** only in **physical form** (cash)

Current money and payments

- **Cash**
  - Good: simple and reliable, privacy
  - Bad: expensive, cannot be used online, hard to track, no transparency

- **Digital payments**
  - Good: fast, convenient, point of sale and online
  - Bad: no privacy

Digital currency wish list

Features

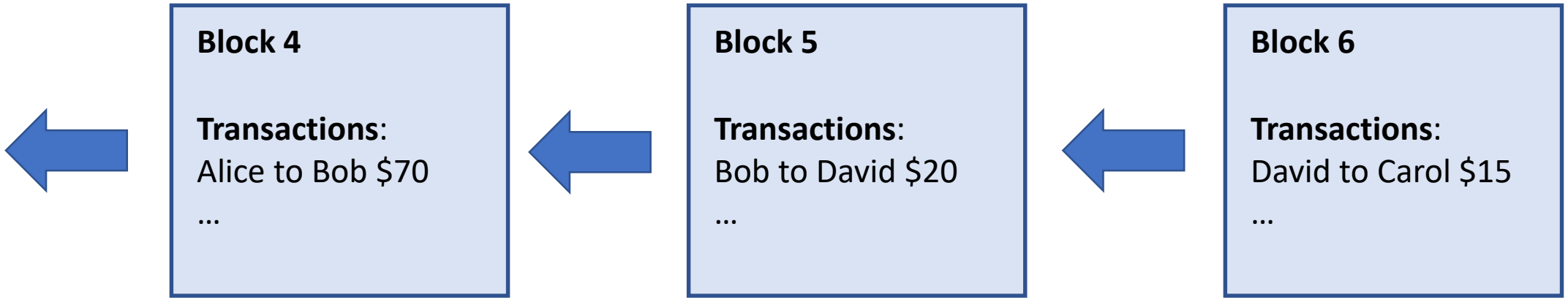
- Inexpensive
- Privacy
- Performance
- Regulation
- Supply control
- Transparency
- Decentralized

Benefits

- People
  - Convenience
  - Improved privacy (online)
- Businesses
  - Cost savings
- Authorities
  - More control
  - Cost savings
- Everyone
  - Increased trust

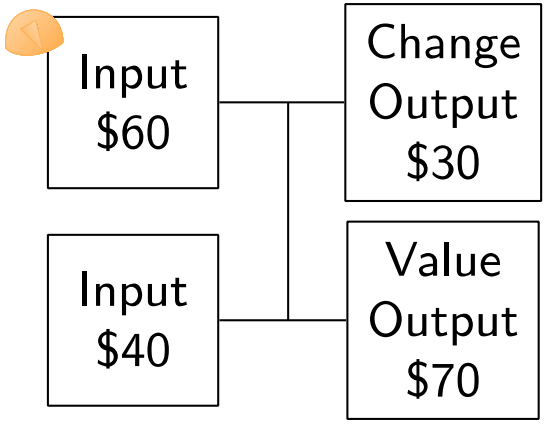
Takeaway #1:
Such digital currency would be useful!

What is a blockchain?



- **Key building blocks:** transaction, consensus, network
- Two main types: **permissioned** or **permissionless**
- **Main features:** decentralized, append-only, publicly-verifiable

Transaction correctness



Alice to Bob $70

60 + 40 = 30 + 70

Bob to David $20

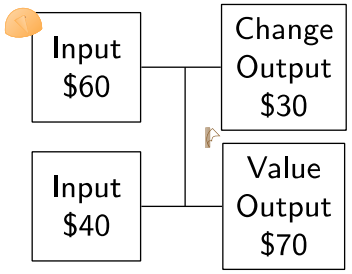
70 = 50 + 20

Existing payments and blockchain currencies

	Privacy	Performance	Supply control	Transparency	Regulation	Decentralized	Inexpensive
Cash	✓	✓	✓	✗	✗	✓	✗
Credit cards	✗	✓	✓	✗	✓	✓	★
Bitcoin	✗	✗	✗	✓	✗	★	★
Hyperledger	✗	✓	✓	✓	✗	✓	✓
Zcash	✓	✗	✗	✓	✗	✓	★

Research example: PRCash

- **Permissioned blockchain** with central issuer
  - Main challenge: **privacy and regulation**



- Transactions use **commitments**

$$g^{r_1} h^{v_1} \cdot g^{r_2} h^{v_2} = g^{r_1+r_2} h^{v_1+v_2}$$

- Regulation using **range proofs**

	Privacy	Performance	Supply control	Transparency	Regulation	Decentralized	Inexpensive
PRCash	✓	✓	✓	✓	✓	✓	✓

From currencies to applications

Smart contract = code that is ”executed on blockchain”

- **Transactions** = contract call that updates blockchain state

1. Participants send money to contract-controlled account
2. Contract code defines when that money is sent out

- Better than traditional contracts or business applicagions?
- Potential benefits: **transparent, “non-stoppable”, anonymous**

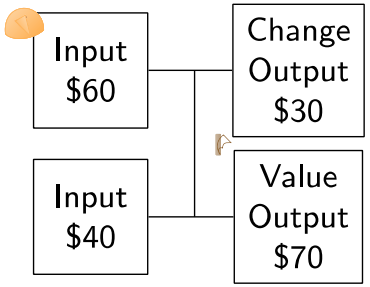
Many use cases suggested…

- **Blockchain claimed to "revolutionize" many industries**
  - Supply chain management
  - Insurance
  - Government
  - Healthcare
  - Music…

- But do these use cases make sense?

Example 1: supply chain management

- Common idea: use blockchain to track items
- Problem: **no simple correctness criteria**
- Example transaction: “Mona Lisa is in Kari’s garage”
- **Trusted data sources needed!**



60 + 40 = 30 + 70

Image source: oxfordcollegeofprocurementandsupply.com

Example 2: government

- Common idea: implement land or property registry as blockchain
- Same problem: “Kari owns White House”
- **Traditional database probably better solution**

Image source: esri.com

Example 3: insurance

- Common example: **flight delay insurance**
  1. Customer loads money to smart contract
  2. Insurer loads money to smart contract
  3. Flight delayed, contract pays the customer

$$g^{r_1} h^{v_1}$$

Commitment

- **Might work!**
- Problems for insurance in general: **user privacy, business confidentiality**

- Possible solutions
  - Fully-homomorphic encryption, zero-knowledge proofs, trusted hardware…

Image source: myjoyonline.com

Example 4: healthcare

- Storing **patient data** on blockchain = **bad idea!**

- Combines the previous problems
  - Correctness
  - Privacy

Image source: fortinet.com

Example 5: music industry

- Example idea: **smart contract distributes royalties**
  1. Customer purchases a song
  2. Smart contract makes sure that artist, label, store all get their fare share

- **Sort of works…** when all entities follow the rules

- **But malicious entities may bypass the contract!**
  - Above example: store sells the song without triggering the contract

- **More general point:** contracts cannot control assets beyond money!

Image source: time.com

Recap of common challenges

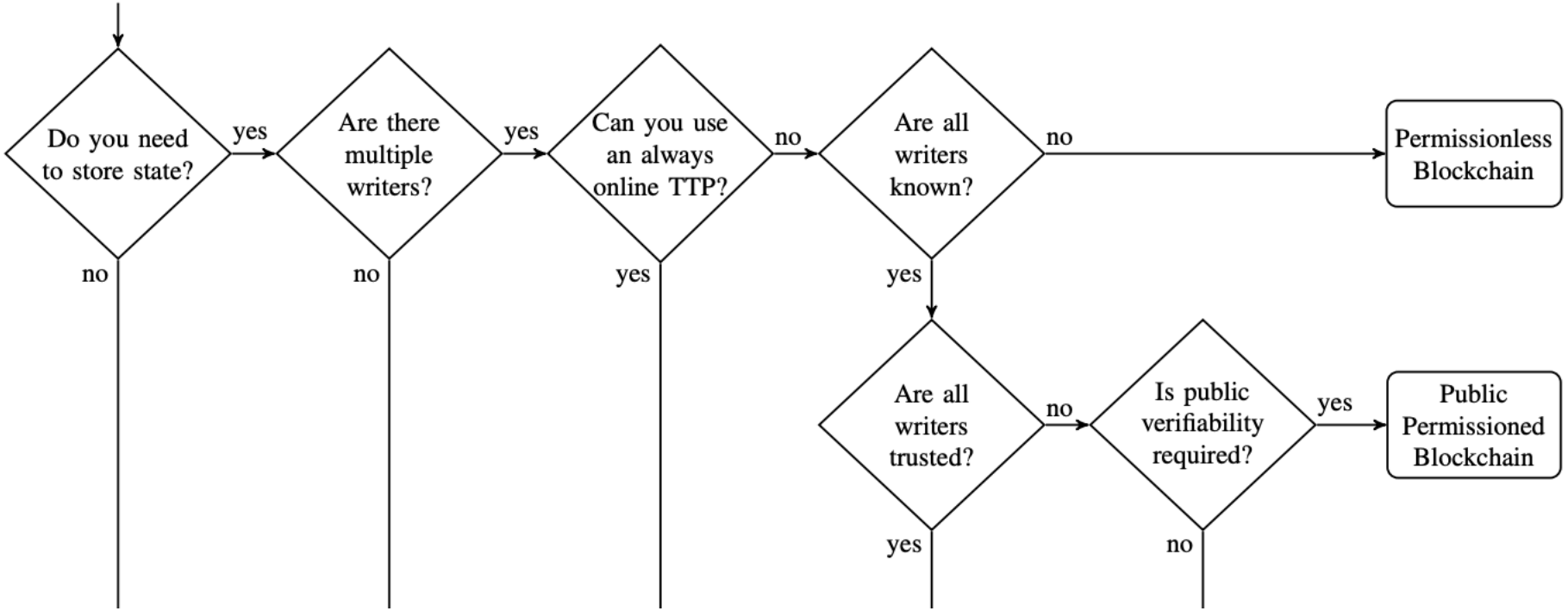
1. No correctness criteria → trusted data sources needed
2. Conflict between transparency and privacy
3. Smart contracts cannot control other assets beyond money

What are good use cases for blockchains?

- Applications where **transparency is desirable**
- Applications where **public-verifiability is feasible**
- Applications where **the controlled asset is monetary**
- Applications where **a (distributed) database is insufficient**

Takeaway #2:
Probably we don’t know the right applications yet

Reading material: Do you need a blockchain?



Thank you!

kari.kostiainen@inf.ethz.ch