Should We Care About Central Bank Digital Currency?

Roger Wattenhofer
POLL
Central Bank Digital Currency (CBDC)
Central Bank Digital Currency (CBDC)

Better Than Cash
Better Than Plastic/Apps
Better Than Crypto
What’s Wrong with Plastic/Apps?
What’s Wrong with Cash?
Production Costs

Not Automatable

Tax Evasion

Slow Transactions

Counterfeits

Handling Costs

Not Online

Government

Production Costs

Theft

Crime

Covid-19

Loss

Crime

Covid-19

Loss
What’s Wrong with Bitcoin?
What About CBDC?
Handling Costs
Slow Transactions
Not Automatable
Not Online
Not Offline
Theft
Crime
Covid-19
EMP
Fees
Key Loss
Trust/Bankruptcy
Not Simple
Privacy

Counterfeits
Tax Evasion
Monetary Policy
Production Costs
Energy
CBDC Inherits Best Features

Plastic/Apps: Simplicity, Speed, Handling Costs

Cash: Common, No Fees, No Bankruptcy Risk

Bitcoin: Privacy, Autonomy, Automatability
CBDC Implementation
Cash-Like

Simple Usage

Anonymous

Without Power/Internet
Frontend
“The problem of course is the payee can't verify that one of the owners did not double-spend the coin.”

“We need a system for participants to agree on a single history of the order in which [transactions] were received.”
no double-spending ≠ single order = consensus
Double-Spending
Blockchains Solve Double-Spending Problem
What About Network Outages?
Unchangeable
Market Cap

Anonymous?
Permissionless?
Scalable = Secure?

Asynchrony
Finality
Throughput
Energy (PoW)
Smart Contracts
Unchangeable
## Many Alternatives

<table>
<thead>
<tr>
<th>Feature</th>
<th>Bitcoin and Ethereum</th>
<th>Ouroboros</th>
<th>Algorand</th>
<th>PBFT</th>
<th>HoneyBadger BFT</th>
<th>Broadcast-based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permissionless</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proof-of-work free</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Finality</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Asynchronous</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Deterministic</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open smart contracts</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
POLL
Without Consensus

A Non-Consensus Based Decentralized Financial Transaction Processing Model with Support for Efficient Auditing

by

Saurabh Gupta

ABC: Asynchronous Blockchain without Consensus

Jakub Siriwinski and Roger Wattenhofer

ETH Zurich

{jeliwinski, wattenhofer}@ethz.ch

Abstract. There is a preconception that a blockchain needs consensus. But consensus is a powerful distributed property with a remarkably high price tag. So one may wonder whether consensus is at all needed.

We introduce a new blockchain architecture called ABC that functions without establishing consensus, and comes with an array of additional features finality and does not rely on costly proof of work calculations. ABC cannot support certain applications but it is suitable for applications where mostly read-heavy, write-light traffic is observed and the value of the data is low, and where a typical consensus-based blockchain such as Bitcoin is too slow or too expensive.

A Thesis Presented in Partial Fulfillment of the Requirements for the Degree of Master of Science
Asynchronous* Throughput Finality Energy (PoS) Permissionless Scalable
Base Layer
Base Layer
Usual Safety Condition

Less than 1/3 (1 out of 4) Maliscious
Base Layer

Needed: 3 out of 4 signatures
Double-Spending
Double-Spending
Double-Spending
Parallelization
Sharded Signing

L → Z

V → C

sign please

sign please
Sharded Signing

L \rightarrow Z

V \rightarrow C

sign please

A-F
G-K
L-P
Q-U
V-Z
Second Layer
Short History of Cryptocurrencies
Buy 2 pizzas with 10k BTC
Buy 2 pizzas with 10k BTC

Smart Contracts! ...but why?
Smart Contracts! ... but why?

Buy 2 pizzas with 10k BTC

10k BTC = 30 million pizzas!
Smart Contracts! ...but why?

Buy 2 pizzas with 10k BTC

10k BTC = 30 million pizzas!

Smart Contracts: Uniswap...
Smart Contract Problem
A Posteriori Consensus

$3f + 1 \rightarrow 5f + 1$
Permissionless?
Multiple Participants?

Participants Known?

No Blockchain (use database)

Permissioned Blockchain

Permissionless Blockchain
Decentralized Finance
Account Types
Base Layer Account

“I don’t trust anybody but myself”

Key to account only with owner Anonymous (apart from ID service)
Bank Account

“I trust my bank more than myself”

Key to account shared/split with bank
Access to account through bank
Payment Layer Account

“For my daily payments”

Key to account on phone
Credit card or debit card
Offline Payments
No Electricity, No Internet, No Computer?
Known (Returning) Customer
Registered Account
Security Token
Small Amount
Wishing you a

HAPPY BIRTHDAY

QR Code
Uncommon
Handling Costs
Slow Transactions
Not Automatable
Not Online
Not Offline
Theft
Crime
Covid-19
Hacker
Fees
Key Loss
Trust/Bankruptcy
Not Simple
Privacy
Counterfeits
Tax Evasion
Monetary Policy
Production Costs
Energy
EMP
Thank You!

Questions & Comments?

Roger Wattenhofer, ETH Zurich, www.disco.ethz.ch
Ene, mene, eins, zwei, drei, Bitcoins bringe mir herbei. Hash Hash.