

Should We Care About Central Bank Digital Currency?



Roger Wattenhofer

POLL

The image shows the word "POLL" written on a corkboard. Each letter is on a separate piece of paper, pinned to the board with a pushpin. The 'P' is on a red paper with a white pushpin. The 'O' is on a white paper with an orange pushpin. The first 'L' is on a white paper with a blue pushpin. The second 'L' is on a white paper with a green pushpin.



The image shows a detailed architectural floor plan of a house, rendered in blue ink on a white background. The plan includes several rooms: a Family Room at the top, a Kitchen, a Dining Room, a Living Room, a Bathroom, a Bedroom, and a Hallway. There are numerous annotations, dimensions, and notes throughout the drawing, such as 'EXIST. BRICK WALL TO BE DEMOLISHED', 'EXIST. JOISTS', 'EXIST. GUARD', 'EXIST. WIND MILL', and 'EXIST. WIND MILL'. Dimensions are given in feet and inches, such as '13'-4"', '7'-0"', '7'-2"', '45'-8"', '6'-0"', '3'-2x4 WALK-IN CLOSET', and '2x4 @ 16" O.C. (C.I.B)'. The word 'Payments' is written in a large, white, sans-serif font across the center of the image, partially overlapping the architectural lines.

Payments


POLL

The image shows the word "POLL" written on a corkboard. Each letter is on a separate piece of paper, pinned to the board with a pushpin. The 'P' is on a red paper with a white pushpin. The 'O' is on a white paper with an orange pushpin. The first 'L' is on a white paper with a red base and a blue pushpin. The second 'L' is on a white paper with a green pushpin.







The background is a detailed architectural blueprint of a house renovation project, overlaid with a blue tint. The drawing shows various rooms including a Family Room, a Bedroom, a Bathroom, and a Kitchen area. Annotations include dimensions like '13'-4"', '7'-0"', and '45'-8"', as well as notes such as 'EXIST. BRICK RIPUP TO BE DEMOLISHED', 'EXIST. JOISTS', and 'WALK-IN CLOSET'. The text 'Central Bank Digital Currency (CBDC)' is prominently displayed in the center in a large, white, sans-serif font.

Central Bank Digital Currency (CBDC)



POLL

The image shows the word "POLL" written on a corkboard. Each letter is on a separate piece of paper, pinned to the corkboard with a pushpin. The 'P' is on a red paper with a white pushpin. The 'O' is on a white paper with an orange pushpin. The first 'L' is on a white paper with a blue pushpin. The second 'L' is on a white paper with a green pushpin.





Central Bank Digital Currency (CBDC)

Better Than Cash

Better Than Plastic/Apps

Better Than Crypto

The background is a detailed architectural blueprint of a house, rendered in white lines on a dark blue background. The blueprint shows various rooms including a 'FAMILY ROOM', 'BEDROOM', 'BATH', and 'CLOSET'. It is filled with technical drawings, dimensions, and handwritten notes. The text 'What's Wrong with Plastic/Apps?' is superimposed in the center in a large, white, sans-serif font. The text is split across two lines: 'What's Wrong' on the top line and 'with Plastic/Apps?' on the bottom line. The blueprint includes labels like 'EXIST. BRICK RIPUP TO BE DEMOLISHED', 'EXIST. JOISTS', 'EXIST. GUARD', and 'EXIST. WIND ABOVE TO BE SUPPORTED'. Dimensions such as '13'-4"', '7'-0"', '7'-2"', '45'-8"', '9'-5"', '2'-0"', '3'-2x4', and '2'-4x4' are visible throughout the drawing. The overall aesthetic is technical and professional, typical of a construction or renovation project plan.

What's Wrong

with Plastic/Apps?



Electromagnetic
Impulse (EMP)

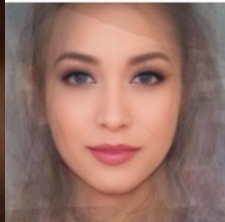
Not Offline


Hacker

Privacy

Fees

Trust/Bankruptcy



The background is a detailed architectural blueprint of a house, rendered in a dark blue color. The drawing includes various rooms such as a 'FAMILY ROOM', 'BEDROOM', 'BATH', and 'KITCHEN'. It features numerous handwritten annotations in white ink, including dimensions like '13'-4"', '7'-0"', and '45'-8"', as well as notes such as 'EXIST. BRICK RIPUP TO BE DEMOLISHED', 'EXIST. JOISTS', and 'WALK-IN CLOSET'. The overall style is that of a professional architectural plan with a focus on structural and renovation details.

What's Wrong with Cash?



Counterfeits

Handling Costs **Tax Evasion**

Slow Transactions

Not Automatable

Not Online **Production Costs**

Theft Crime

Covid-19

Loss



The background is a detailed architectural blueprint of a house, rendered in a dark blue color. The drawing includes various rooms such as a 'FAMILY ROOM', 'BEDROOM', 'BATH', and 'KITCHEN'. It is filled with technical lines, dimensions, and handwritten annotations in white ink. Some notes include 'EXIST. BRICK RIPUP TO BE DEMOLISHED', 'EXIST. JOISTS', 'EXIST. BLM'S', and 'EXIST. GUARD'. Dimensions like '13'-4"', '7'-0"', and '45'-8"' are scattered throughout. The overall aesthetic is that of a professional architectural plan.

What's Wrong with Bitcoin?



Handling Costs

Monetary Policy

Slow Transactions

Tax Evasion

Uncommon

Not Offline

Crime

Hacker

Energy

Key Loss

Not Simple





What About CBDC?



Uncommon

Counterfeits

Handling Costs

Tax Evasion

Slow Transactions

Monetary Policy

Not Automatable **EMP**

Not Online

Not Offline

Production Costs

Theft **Crime**

Hacker

Covid-19

Fees

Energy

Key Loss **Trust/Bankruptcy**

Not Simple **Privacy**

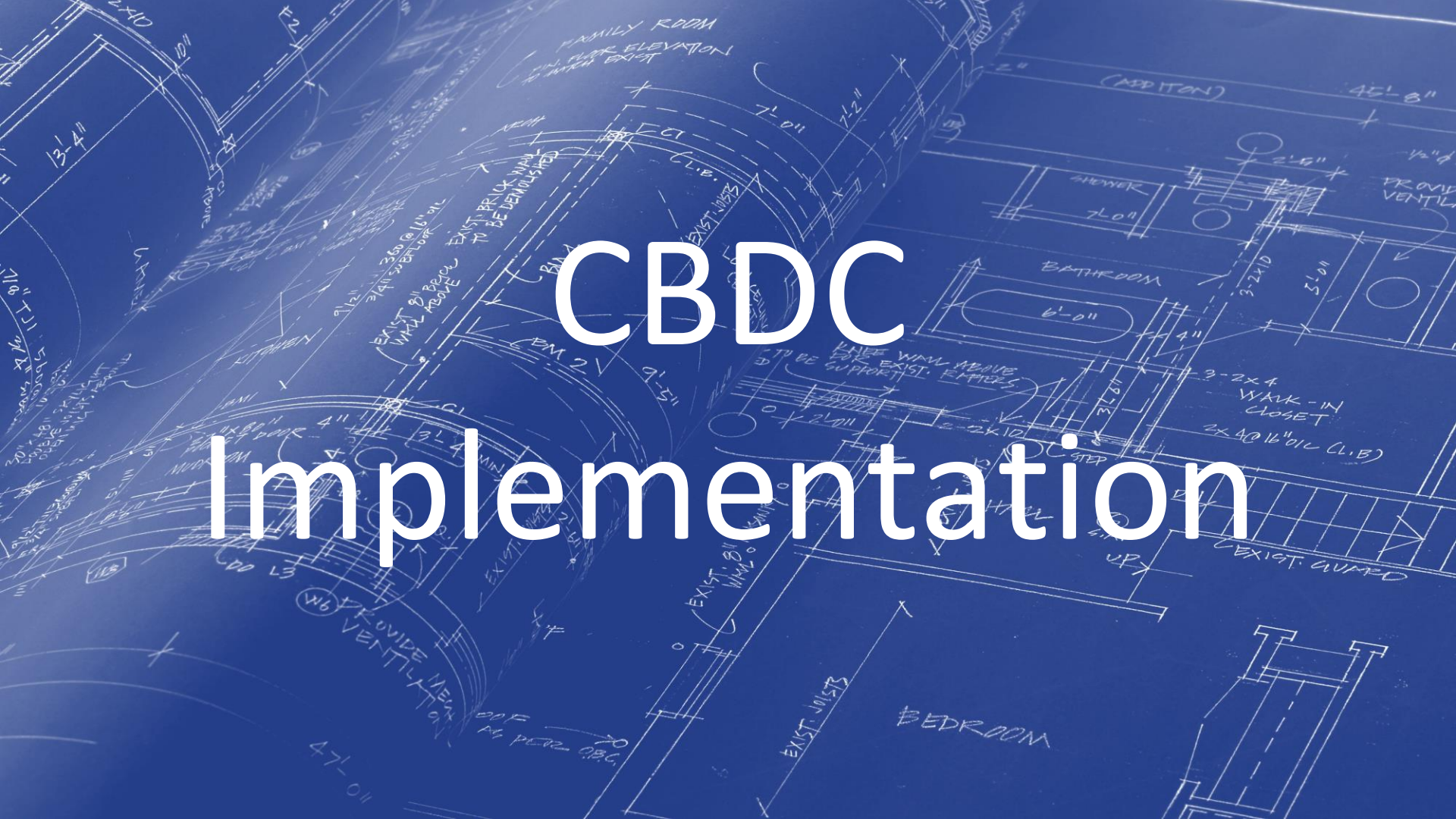


CBDC Inherits Best Features

Plastic/Apps: Simplicity, Speed, Handling Costs

Cash: Common, No Fees, No Bankruptcy Risk

Bitcoin: Privacy, Autonomy, Automatability

The background is a detailed architectural blueprint of a house, rendered in white lines on a dark blue background. The blueprint shows various rooms including a Family Room, Kitchen, Bathroom, and Bedroom. It includes dimensions, annotations like 'EXIST. BRICK RIPUP TO BE DEMOLISHED', and structural notes such as 'EXIST. JOISTS'. The text 'CBDC Implementation' is overlaid in large, white, sans-serif font in the center of the image.

CBDC Implementation



FRONTEND



BACKEND

PHILOSOPHY



The image shows a detailed architectural floor plan drawn on blue paper. The plan includes several rooms: a Family Room at the top, a Kitchen on the left, a Bathroom in the center, a Bedroom at the bottom, and a Walk-in Closet. The drawing is filled with technical annotations, including dimensions (e.g., 13'-4", 7'-0", 45'-8", 6'-0", 3'-2x4), material notes (e.g., 'EXIST. BRICK RIPUP TO BE DEMOLISHED'), and structural references (e.g., 'EXIST. JOISTS', 'EXIST. SILL MEMBERS'). There are also notes about existing conditions and proposed changes, such as 'EXIST. BRICK RIPUP TO BE DEMOLISHED' and 'EXIST. BRICK RIPUP TO BE DEMOLISHED'. The word 'Philosophy' is written in a large, white, sans-serif font across the center of the plan. The overall style is that of a professional architectural drawing.

Cash-Like

Simple Usage

Anonymous

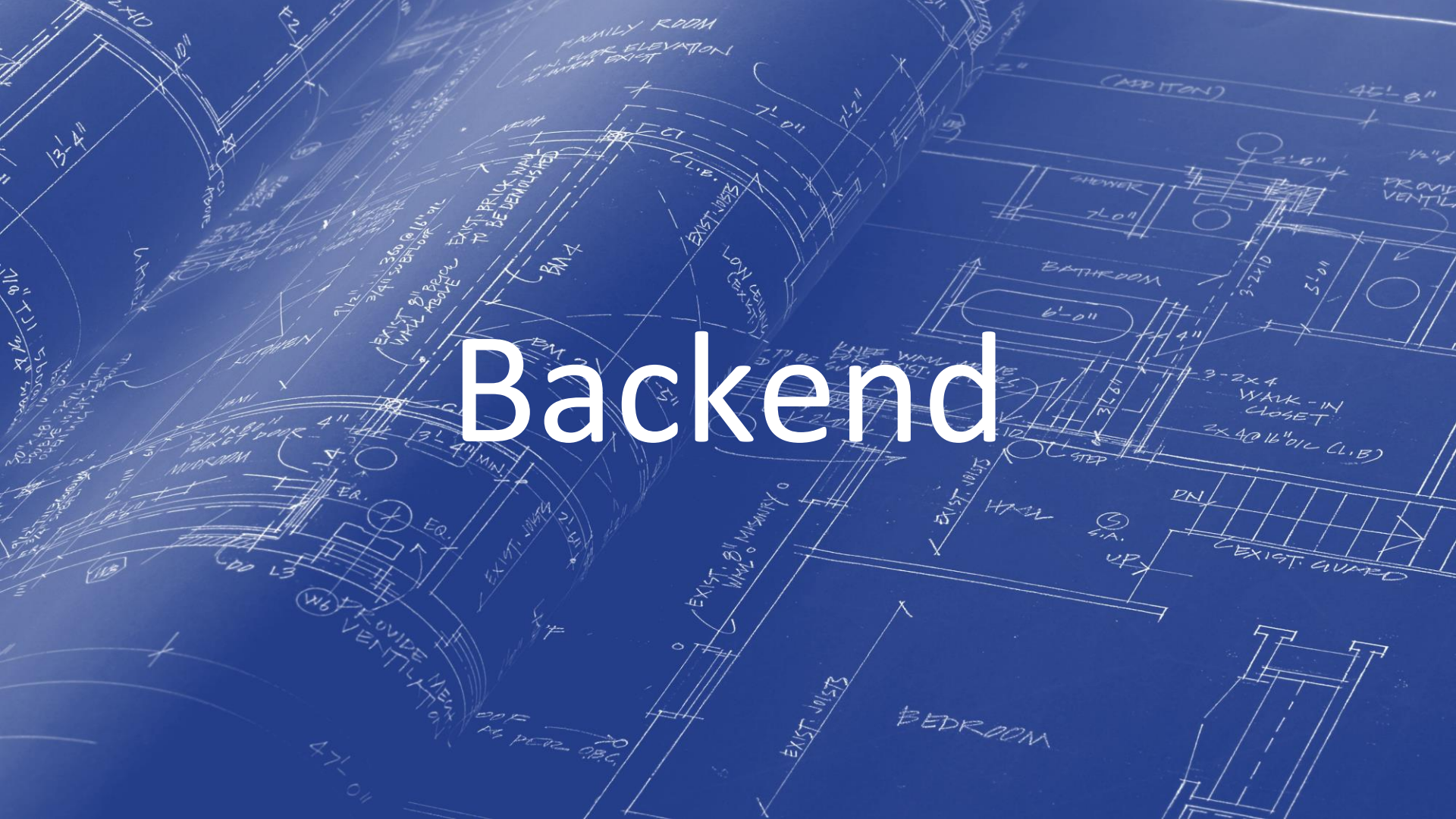
Without Power/Internet

Frontend





Backend



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

“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

JOHN DOE OR JANE DOE
123 MAIN STREET
ANYTOWN, TN 01234
PHONE 555-1212

2670
87-823/641

19

Pay to the Order of _____ \$ _____

Bank of Yourtown
YOURTOWN, TN

6-73 Dollars  Security details on back

For _____ MP

⑆012345678⑆ ⑆98765432⑆


JOHN DOE OR JANE DOE
123 MAIN STREET
ANYTOWN, TN 01234
PHONE 555-1212

2670
87-823/641

19

Pay to the Order of _____ \$ _____

Bank of Yourtown
YOURTOWN, TN

6-73 Dollars  Security details on back

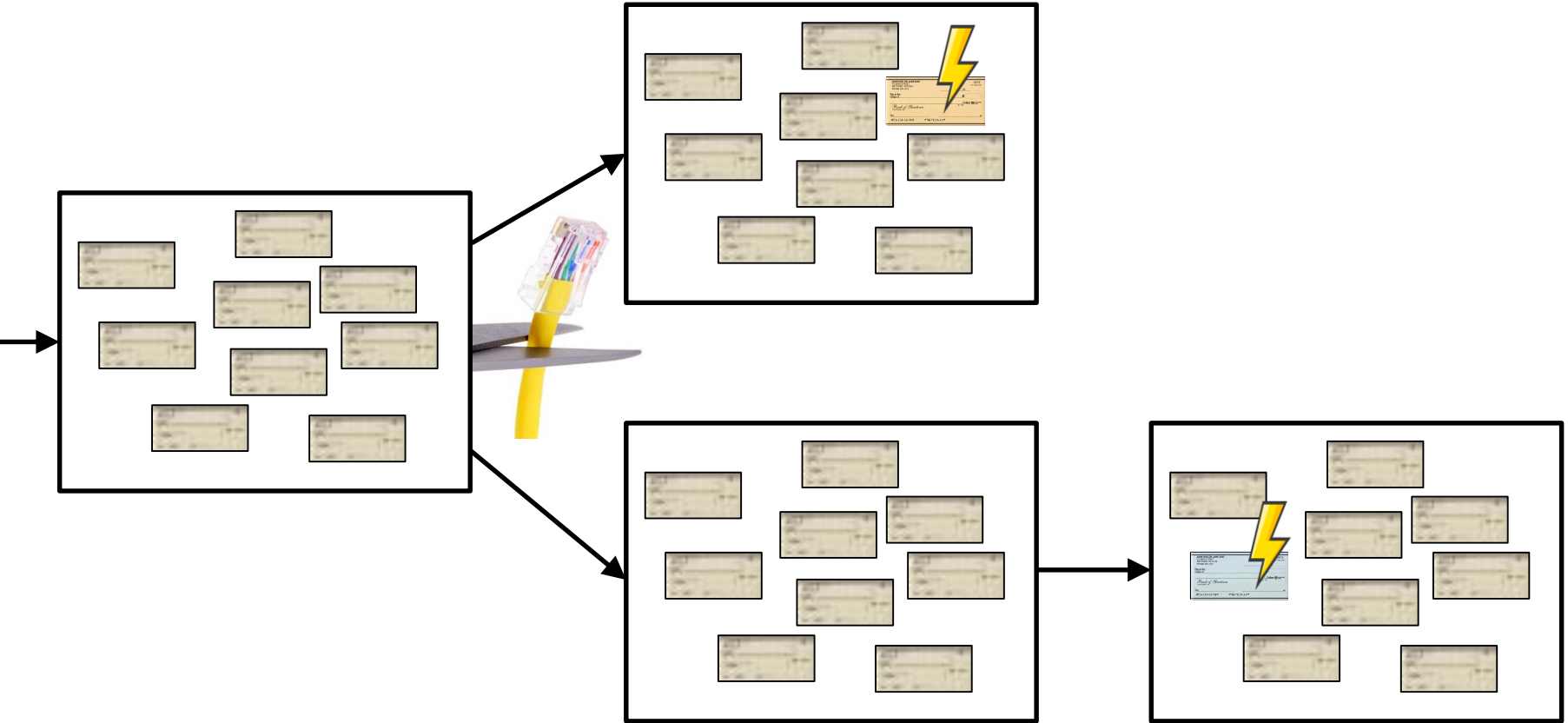
For _____ MP

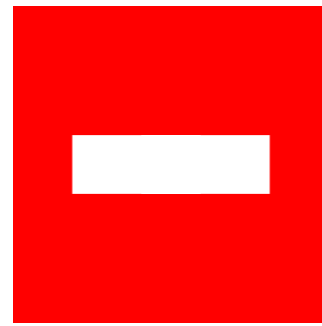
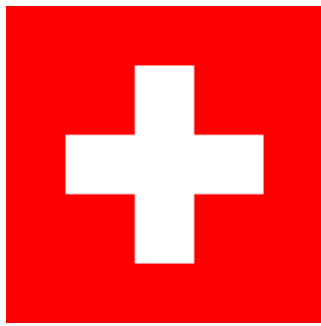
⑆012345678⑆ ⑆98765432⑆

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

	Bitcoin and Ethereum	Ouroboros	Algorand	PBFT	HoneyBadger BFT	Broadcast- based
Permissionless	✓	✓	✓			
Proof-of-work free		✓	✓	✓	✓	✓
Finality			✓	✓	✓	✓
Asynchronous					✓	✓
Deterministic				✓		✓
Open smart contracts	✓	✓	✓	✓	✓	

2x

P

O

L

L

Without Consensus

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

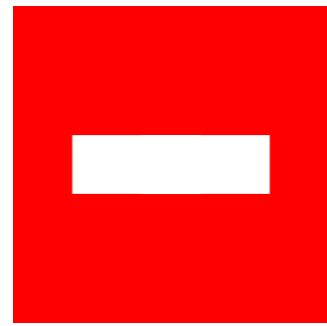
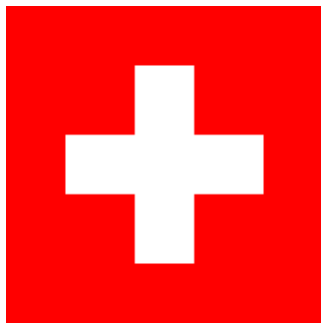
by
Saurabh Gupta

A Thesis Presented in Partial Fulfillment
of the Requirements for the Degree
Master of Science

ABC: Asynchronous Blockchain without Consensus

Jakub Sliwinski and Roger Wattenhofer
ETH Zurich
{jsliwinski,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 advantages. ABC is permissionless, deterministic, and resilient to corruption. ABC features finality and does not rely on costly proof-of-work. Thus, ABC cannot support certain



Asynchronous*
 Throughput
 Finality
 Energy (PoS)
 Permissionless
 Scalable

BRICK: Asynchronous Payment Channels

Georgia Avarikioti
 zetavar@ethz.ch
 ETH Zürich

Eleftherios Kokoris Kogias
 eleftherios.kokoriskogias@epfl.ch
 EPFL

Roger Wattenhofer
 wattenhofer@ethz.ch
 ETH Zürich

FastPay: High-Performance Byzantine Fault Tolerant Settlement

Mathieu Baudet*
 Facebook Calibra

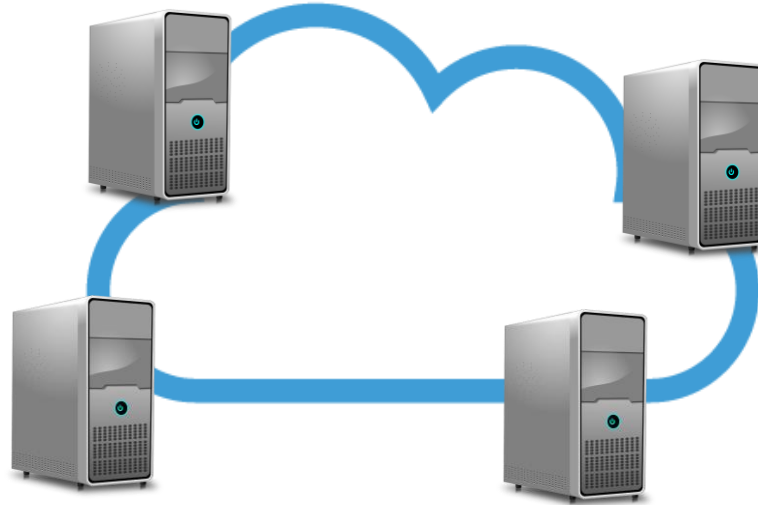
George Danezis
 Facebook Calibra

Alberto Sonnino
 Facebook Calibra

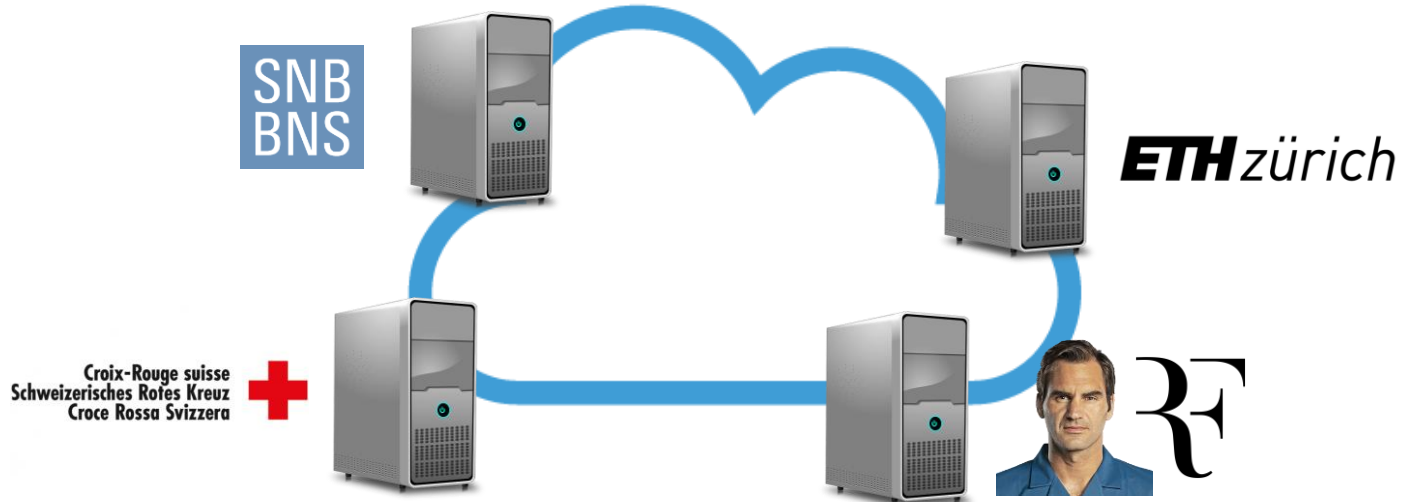
a promising solution to the scal-
 blockchain systems. Current
 assumptions to preserve
 the exact amount
 of attack. In
 tion that

demanding a synchronous network and a perfect
 exists. This means that a malicious party able to c
 from an honest party or a watchtower during
 can break the security of a channel by attac
 the underlying blockchain. Unlike blockch
 tacking liveness can slow down the system
 loss of funds, the following attack can oc
 a malicious party publishes an outdated
 that awards the party more funds tha
 ther, suppose the malicious party suc
 actions from the counterparty
 period. Then, the malicious
 funds from the c
 Blockchain
 sible [32
 d in prac
 e issues v
 channel
 ion for th
 active secu
 on-chain. A
 ren und

Base Layer



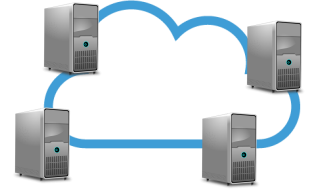
Base Layer



Usual Safety Condition

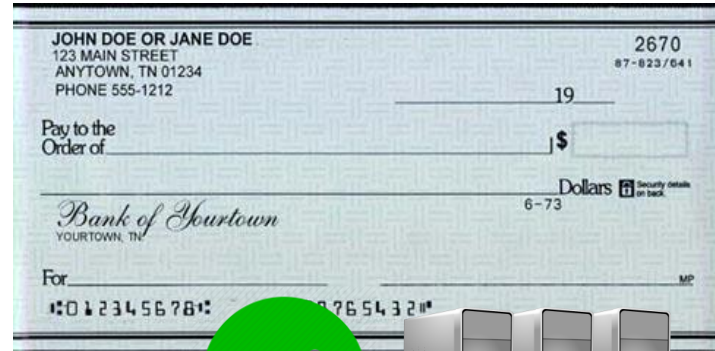
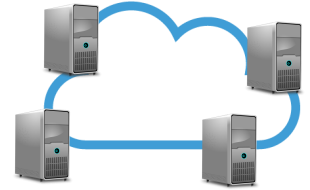
Less than $1/3$ (1 out of 4) Malicious

Base Layer

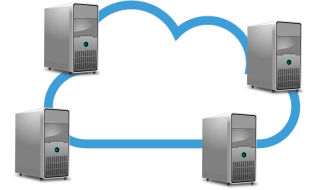


Needed: 3 out of 4 signatures

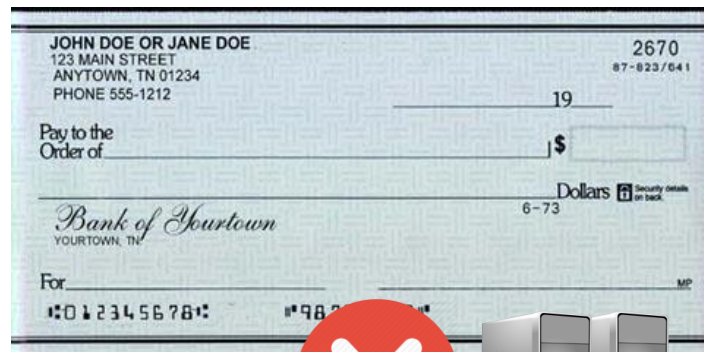
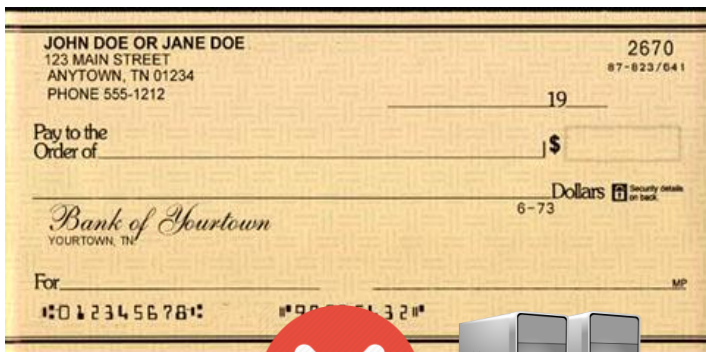
Double-Spending



Double-Spending



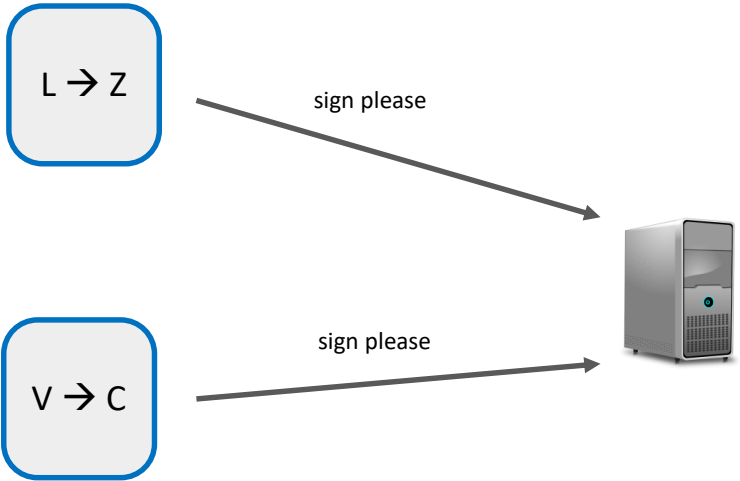
Double-Spending



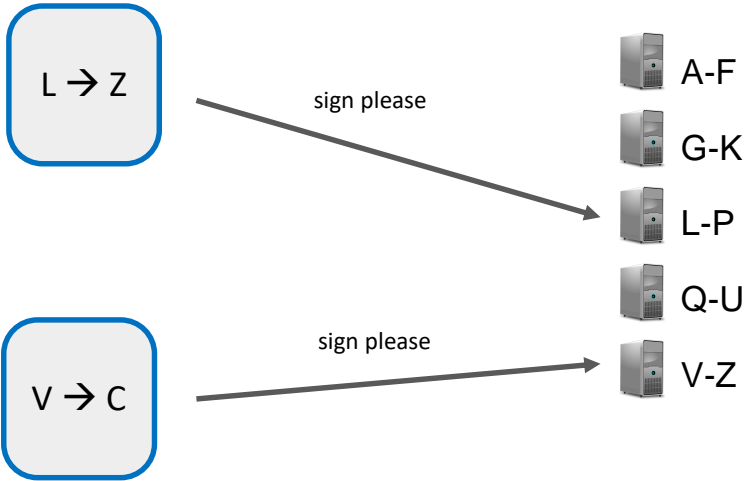
Parallelization

The image features a detailed architectural floor plan rendered in white lines on a blue background. The plan includes several rooms: a Family Room at the top, a Bathroom and Bedroom on the right, and another Bedroom at the bottom. A curved wall is shown on the left side. The drawing is annotated with numerous dimensions (e.g., 13'-4", 17'-0", 7'-0", 45'-8") and technical notes such as 'EXIST. BRICK WALL TO BE DEMOLISHED', 'EXIST. JOISTS', and 'WALK-IN CLOSET'. The word 'Parallelization' is centered over the plan in a large, white, sans-serif font.

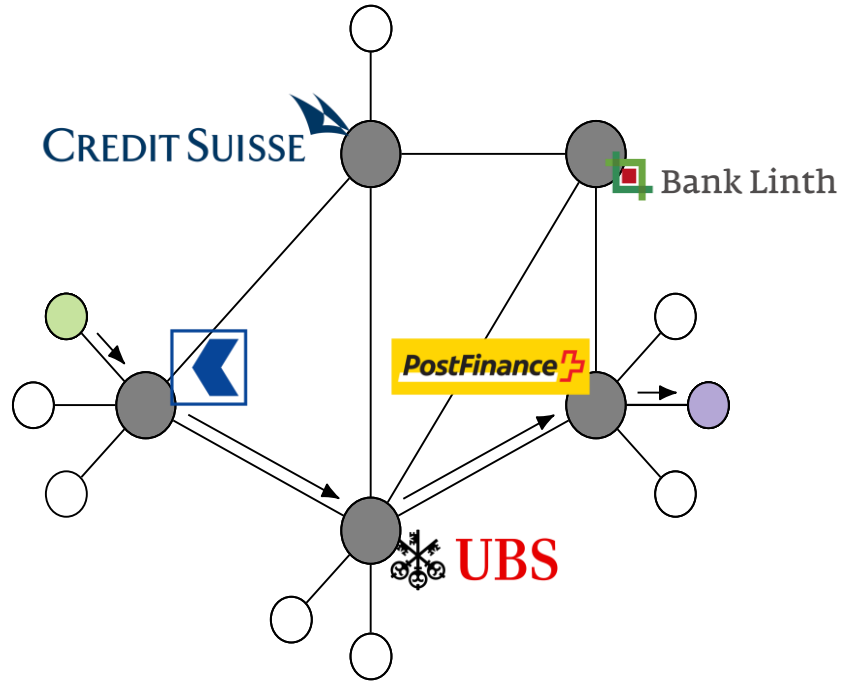
Sharded Signing



Sharded Signing



Second Layer





Short History of Cryptocurrencies



Buy 2 pizzas with 10k BTC



Buy 2 pizzas with 10k BTC

Smart Contracts! ...but why?





Buy 2 pizzas with 10k BTC

Smart Contracts! ...but why?

10k BTC = 30 million pizzas!





Buy 2 pizzas with 10k BTC

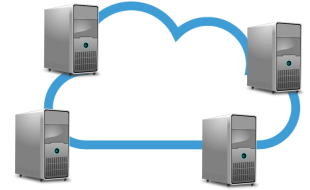
Smart Contracts! ...but why?

10k BTC = 30 million pizzas!

Smart Contracts: Uniswap...



Smart Contract Problem

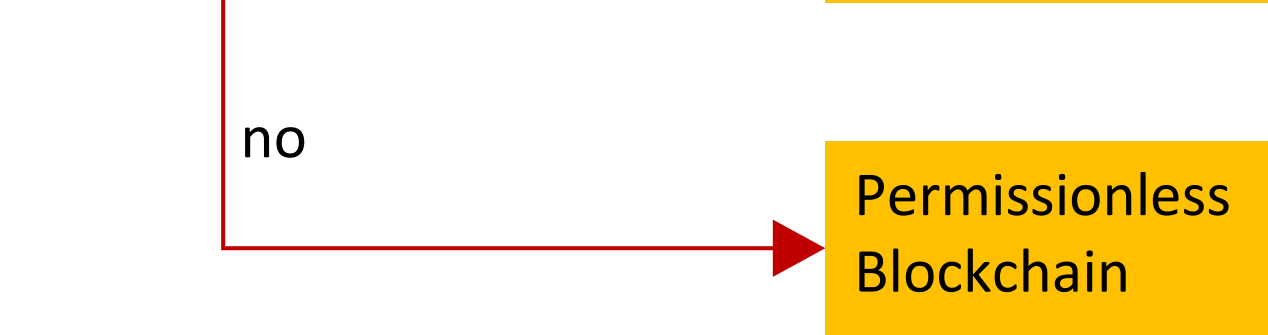
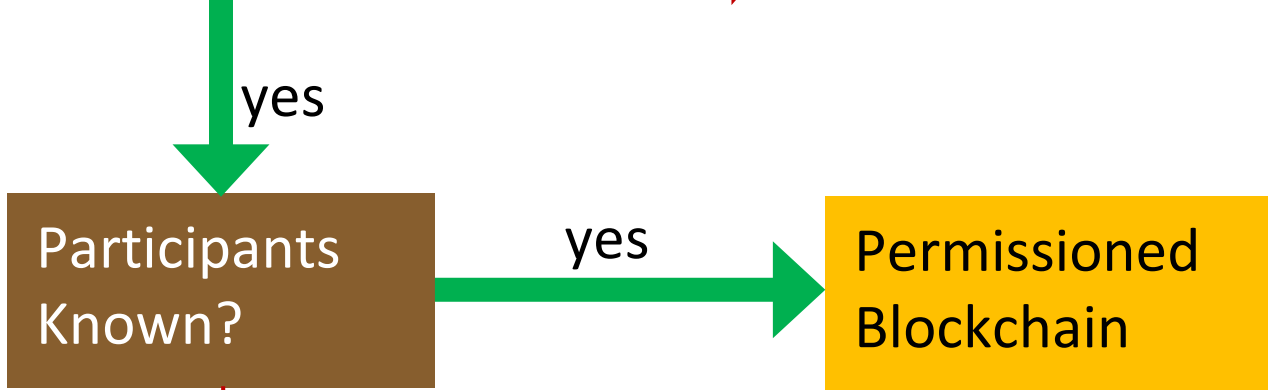
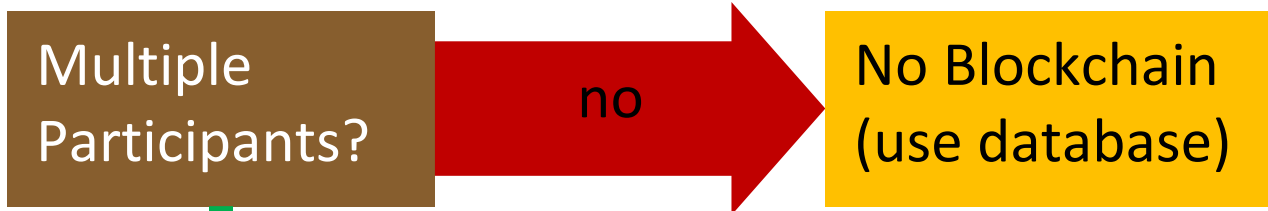


A Posteriori Consensus

$$3f + 1 \quad \rightarrow \quad 5f + 1$$

The image shows a detailed architectural blueprint of a house, rendered in white lines on a dark blue background. The blueprint includes various rooms such as a Family Room, Bathroom, and Bedroom, along with structural elements like joists and beams. Handwritten notes and dimensions are scattered throughout the drawing. Overlaid on the center of the blueprint is the text "Permissionless?" in a large, white, sans-serif font.

Permissionless?



The image shows a detailed architectural blueprint of a house, rendered in a blue-tinted style. The blueprint includes various rooms and structural elements, with handwritten annotations and dimensions. Key areas labeled include a 'FAMILY ROOM' at the top, a 'BEDROOM' at the bottom, a 'BATH' on the right, and a 'KITCHEN' on the left. There are also labels for 'EXIST. BRICK RIPUP TO BE DEMOLISHED', 'EXIST. JOISTS', 'EXIST. BLINDS', 'EXIST. GUARD', 'WALK-IN CLOSET', and 'WIND ROOM'. Dimensions such as '13'-4"', '7'-0"', '7'-2"', '45'-8"', '9'-5"', '47'-0"', and '17'-0"' are scattered throughout. The text 'Decentralized Finance' is prominently displayed in the center in a large, white, sans-serif font. The overall aesthetic is technical and professional, typical of architectural drawings.

Decentralized Finance

POLL

The image shows the word "POLL" written on a corkboard. Each letter is on a separate piece of paper, pinned at the top. The 'P' is on a red paper with a white pushpin. The 'O' is on a white paper with an orange pushpin. The first 'L' is on a white paper with a red base and a blue pushpin. The second 'L' is on a white paper with a green pushpin.

The image shows a detailed architectural blueprint of a house, rendered in white lines on a dark blue background. The blueprint includes various rooms such as a Family Room, Bathroom, Bedroom, and a Walk-in Closet. It also features technical annotations like 'EXIST. BRICK RIPUP TO BE DEMOLISHED', 'EXIST. JOISTS', and 'EXIST. GUARD'. Dimensions and structural notes are scattered throughout the drawing. Overlaid on the center of the blueprint is the text 'Account Types' in a large, white, sans-serif font.

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



The background of the image consists of a detailed architectural blueprint for a residential renovation project. The blueprint is drawn in white lines on a dark blue background. It shows various rooms including a Family Room, a Bathroom, a Bedroom, and a Hallway. The drawing includes numerous annotations such as 'EXIST. BRICK RIPUP TO BE DEMOLISHED', 'EXIST. JOISTS', 'EXIST. GUARD', and 'EXIST. CURB'. Dimensions are provided for various elements, such as '13'-4"', '7'-0"', '7'-2"', '45'-8"', '6'-0"', '3'-2xID', '5'-0"', '47'-0"', and '45'-0"'. There are also notes about materials like 'EXIST. BRICK RIPUP TO BE DEMOLISHED' and 'EXIST. BRICK RIPUP TO BE DEMOLISHED'. The text 'Offline Payments' is centered over the drawing in a large, white, sans-serif font.

Offline Payments

No Electricity, No Internet, No Computer?

Known (Returning) Customer



Registered Account



Security Token



Small Amount



WISHING
YOU A

**HAPPY
BIRTHDAY**



POLL

The image shows the word "POLL" written on a corkboard. Each letter is on a separate piece of paper, pinned at the top with a pushpin. The 'P' is on a red paper with a white pushpin. The 'O' is on a white paper with an orange pushpin. The first 'L' is on a white paper with a blue pushpin. The second 'L' is on a white paper with a green pushpin.



A hand-drawn architectural floor plan on blue paper, showing various rooms and structural details. The plan includes a Family Room, Kitchen, Bathroom, and Bedroom. Key features include a shower, a walk-in closet, and a bedroom with a window. The drawing is annotated with numerous dimensions, notes, and structural markers such as 'EXIST. JOISTS', 'EXIST. BRICK', and 'EXIST. WALK-IN CLOSET'. The word 'Summary' is overlaid in large white text across the center of the plan.

Summary



Uncommon

Handling Costs

Slow Transactions

Not Automatable EMP

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



Final

P

O

L

L

Thank You!

Questions & Comments?





Ene, mene,
eins, zwei, drei,
Bitcoins bringe
mir herbei.
Hash Hash.

@grauhut

