UNDERSTANDING LIBRA

Professor Jamiel Sheikh
Introduction to Libra

Professor Paul Johnson
Market Analysis of Libra

Youwei Yang
Quantitative Analysis of Cryptos and Libra

Elliot Chun
Moderator

Introduction to Libra

Professor Jamiel Sheikh, CEO Chainhaus

jamiel@chainhaus.com

http://jamiel.io

What is Libra?

- Libra Coin
- Libra Protocol
- Libra Blockchain
- Libra Association
- LibraBFT
- Libra Core
- Move Programming Language
- Libra Authorized Resellers
- Calibra

chainhaus

Two Minute History of Blockchain

- Bitcoin –
  - Blockchain + Rigid Data Structures
- Ethereum –
  - Blockchain + Rigid + Arbitrary Logic
- Enterprise Blockchains
  - Blockchain + Arbitrary Logic
- Libra
  - Arbitrary Logic Define Blockchain

chainhaus

Libra Coin

- Global, borderless currency
- Low volatility coin
  - Stablecoin? Maybe
- “basket of bank deposits and treasuries from high-quality CBs”
  - Low inflation
  - Stable assets
  - Not confirmed
- Tokenized basket
  - Ask Paul Johnson On Quants for This

chainhaus

Libra Coin

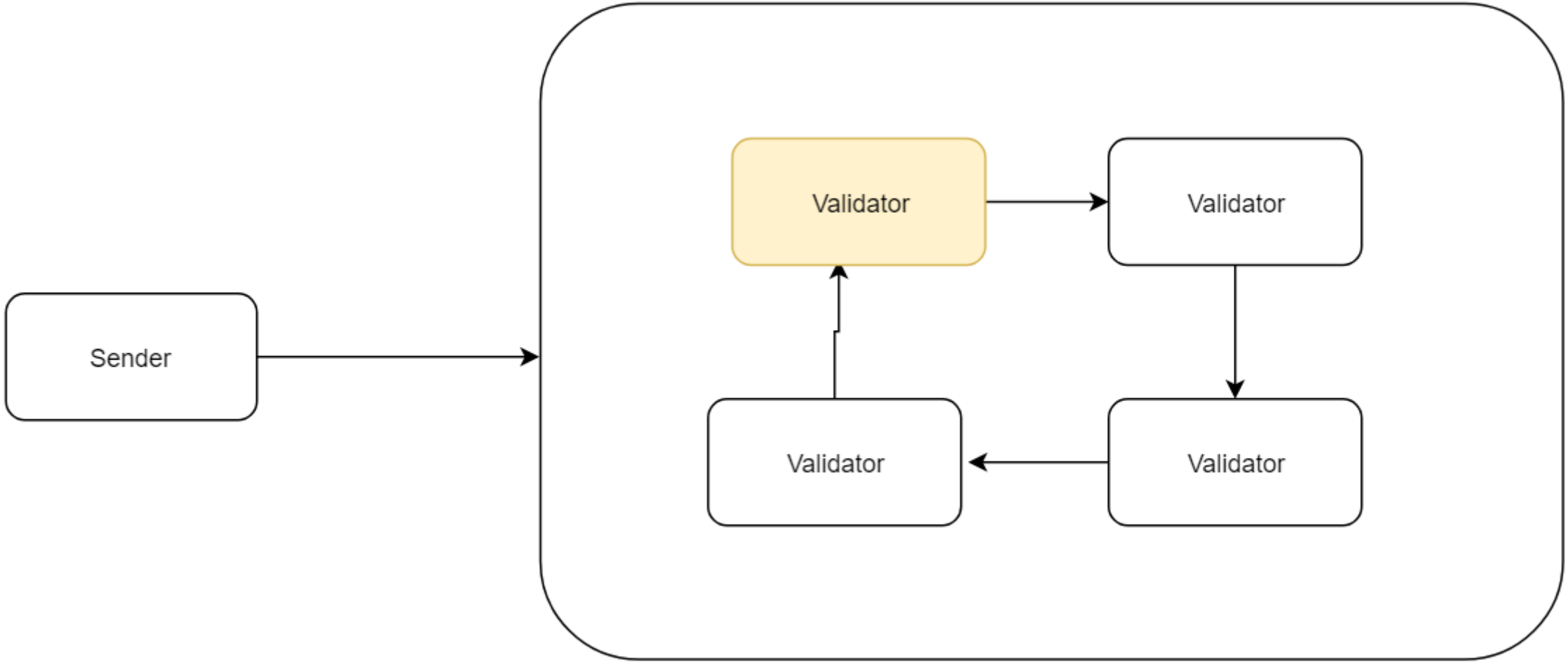
- Supranational?
  - So is Bitcoin
- Central Bank Buster?
- It is / isn't a cryptocurrency?
- Decentralized?

chainhaus

Libra Protocol

- Node operators = Validators
  - Intra-validator Network
  - Trusted and known entities
  - Founding members
- Clients
  - Submit transactions
  - Query Validators

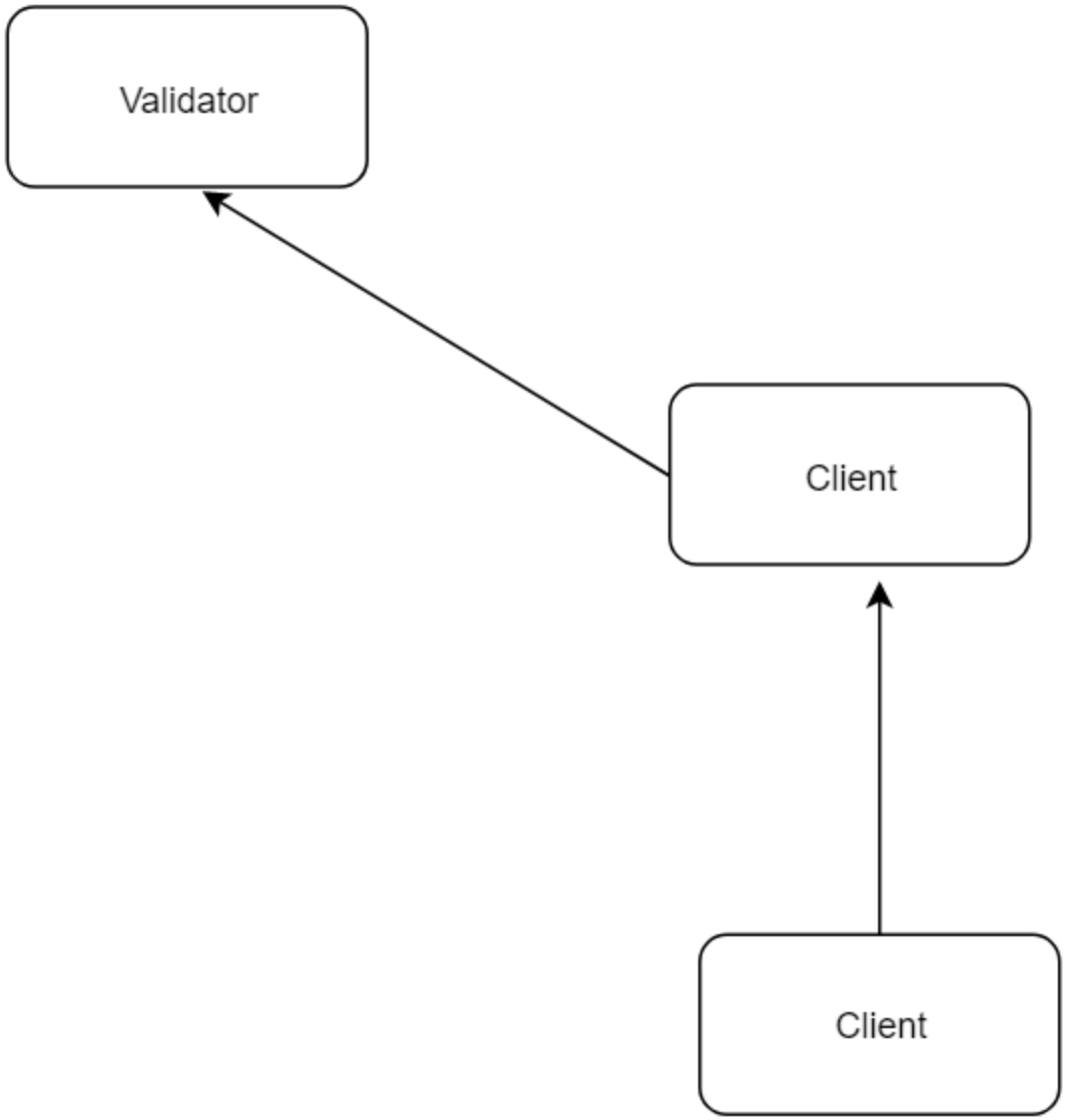
chainhaus



Libra Protocol

- Node operators = Validators
  - Intra-validator Network
  - Trusted and known entities
  - Founding members
- Clients
  - Submit transactions
  - Query Validators
  - Verify integrity of validators processing
- **Performance and scalability demands will be high**
  - **Hub & spoke**

chainhaus



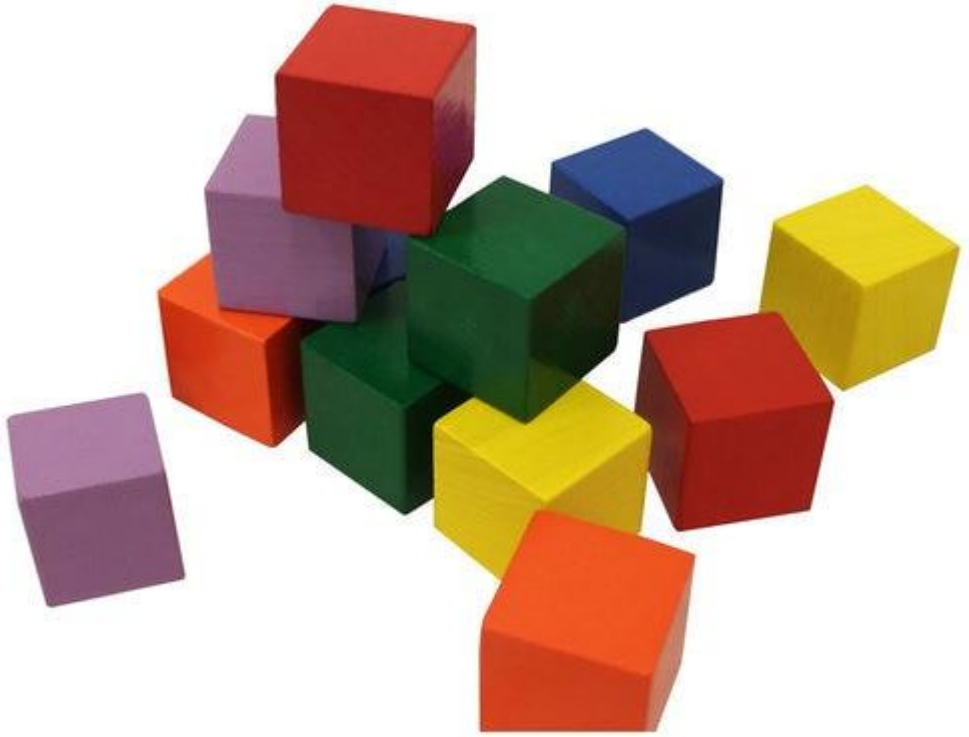
Leader Validator

- Can become a leader via random protocol
  - Effectively round robin
- Leaders propose transactions
  - Other enterprise chains any node can initiate and propose
  - Leader proposes on behalf of a client (i.e. sender)
- Leader proposes a new state of the ledger
- Other validators vote on the new state
  - Merkle trees

chainhaus

Ledger: No blocks

- Why do we need blocks anyway?
- Validation does occur in blocks
- Transactions not chained by blocks
  - There is no prev_hash in a block



chainhaus

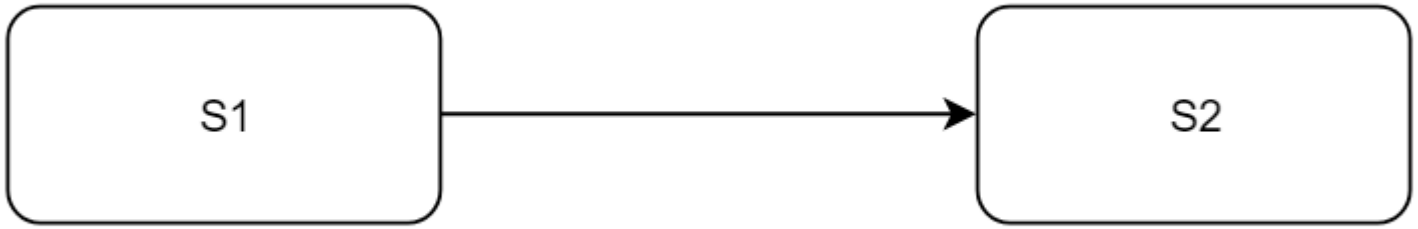
Ledger: Account-centric

- Key / Value
  - Hashmap
  - Dictionary
  - Lookup table
- Key = Account address
- Value = Account contents

chainhaus

Transactions

- Transactions change the state of a ledger



chainhaus

Transactions are dispatched by clients

- Input parameters
- Transaction script (Smart contract)
- Gas & Max Gas
- Bytecode (i.e. Solidity, JVM)
- Output
  - Transactions produce output plus metadata (events list)

chainhaus

Ledger: Versioning

- Each transaction produces new version of ledger
- Each version has an id

chainhaus

Transaction Gas

- Variable Fee
- Execution time may be probabilistic
- Halted transactions appear in transaction log
  - But not ledger
- Transactions **may be dropped**
- No gas charged for storage

chainhaus

Ledger: Account-centric

- Key / Value
  - Hashmap
  - Dictionary
  - Lookup table
- Key = Account address
- Value = Account contents

chainhaus

Account

- Address: Hash of public key
  - SHA3-256
- EdDSA
  - Edwards25519 curve
- Hence pseudonymous
- Private signing key can be modified without changing address
- Authenticator component

chainhaus

Account

- Resources
  - Assets
- Modules
  - Code that create, manage assets
  - Structs that define assets
- Can expire
- Authenticator component
  - Hash of serialized representation of account content
- Local sequence number
  - Replay attack

chainhaus

Namespace Schema

- Python, Java, Go .. Etc..

  Import package.class

- Move contracts
  - Account hash referenceable like namespace
  - 0x12/resources/0x56.MyCoinStruct

chainhaus

Bootstrapping

- Network - Like Bitcoin, seed peers required
- Heartbeat protocol
- Validaters stored in smart contract
  - Other chains use config files
  - Peers track smart contract changes

chainhaus

Genesis

- Empty state
- T0 special transaction (“genesis transaction”)
- Deploys modules / smart contracts / Libra Coin / base libraries
- Clients / Validators check for T0 transaction as one check of ledger integrity
- Future smart contracts use namespace to point back to modules / assets produced by t0

chainhaus

Hard Fork

- Possible
- By Smart Contract
- Epochs
  - Not really fork
  - Change in validator set

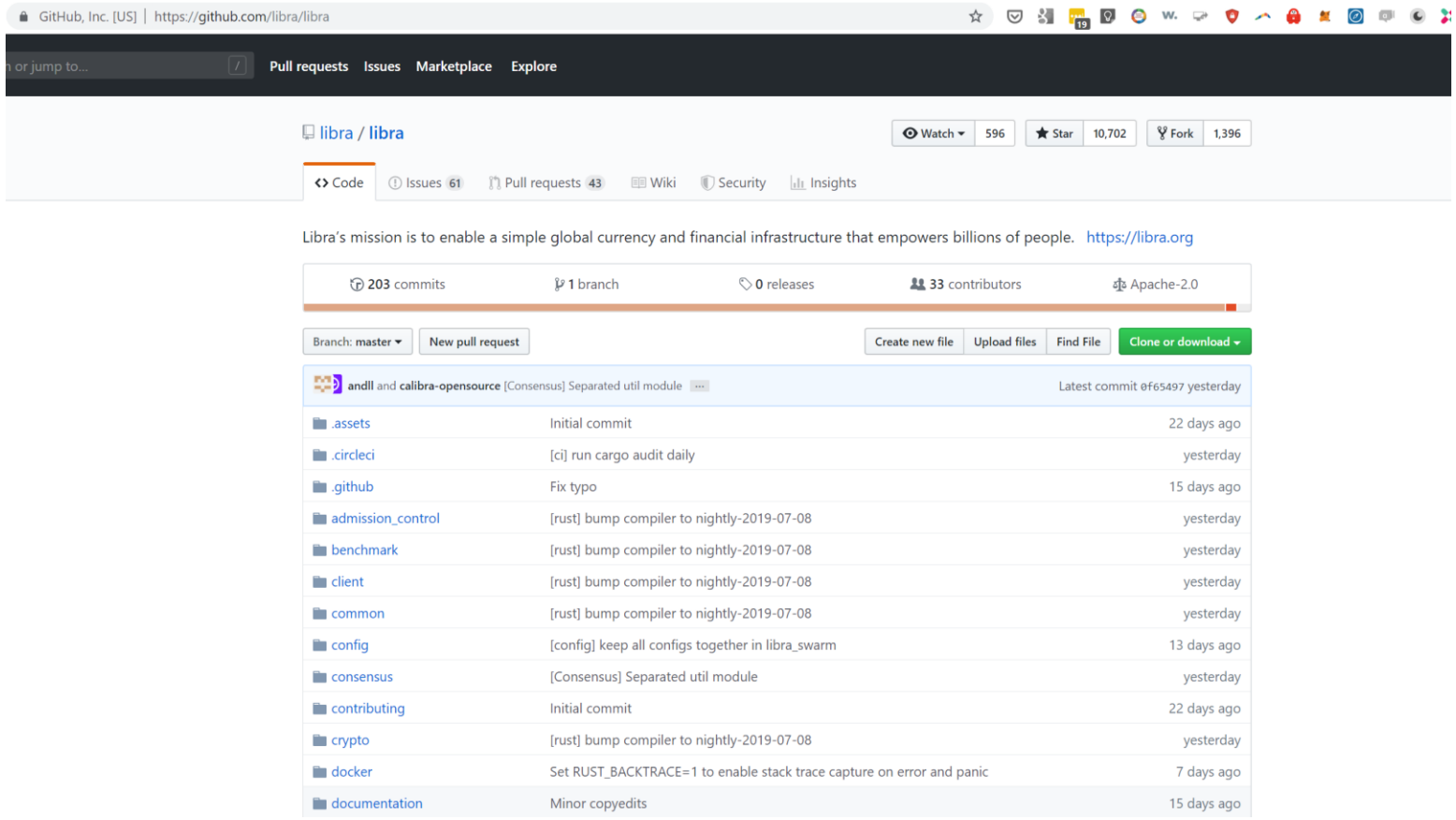
chainhaus

LibraBFT

- Based on HotStuff BFT algo
- Honest nodes all can go down and come back up with no impact
- Quorum Certificate is formed when validators sign-off on a transaction
- 3f + 1 , where f are Byzantine

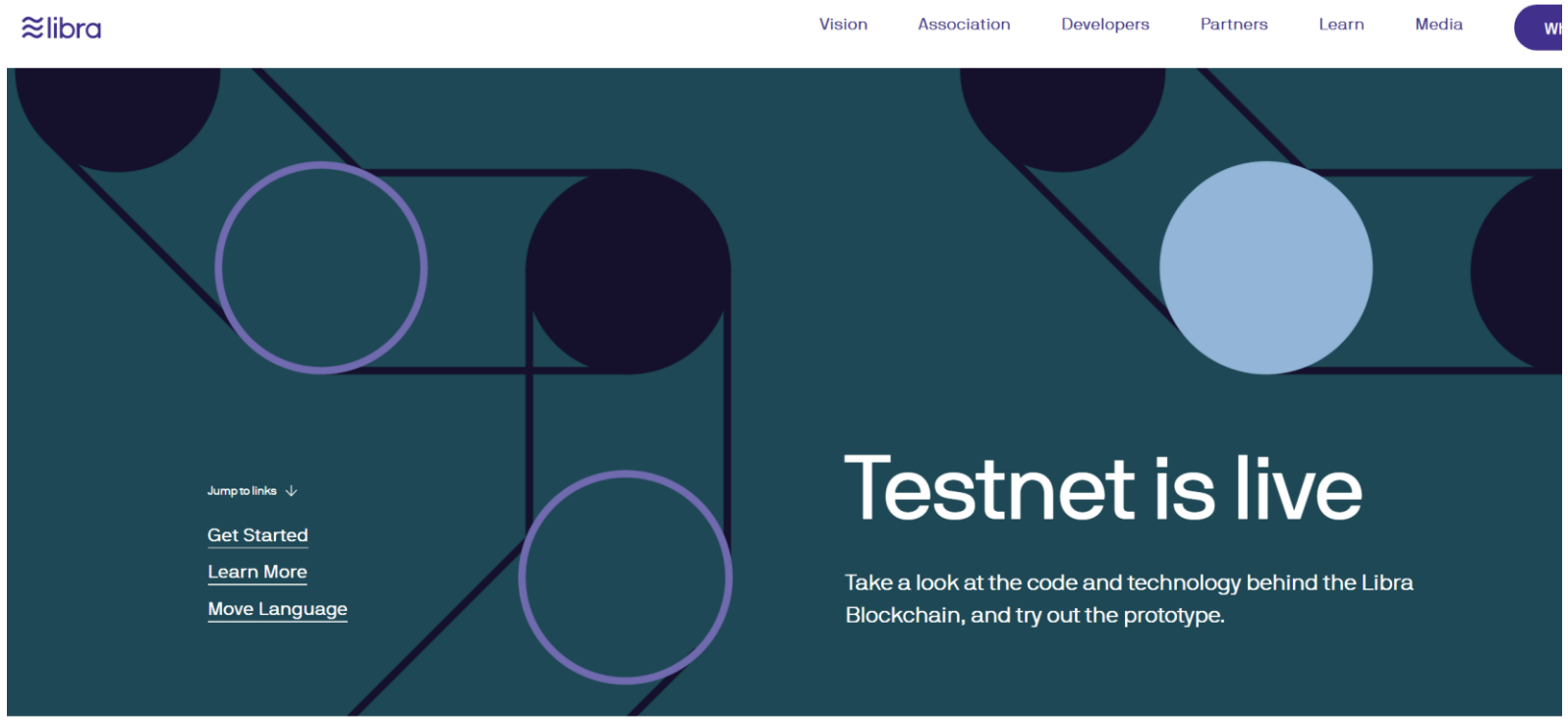
chainhaus

Libra Core



chainhaus

Libra Testnet



chainhaus

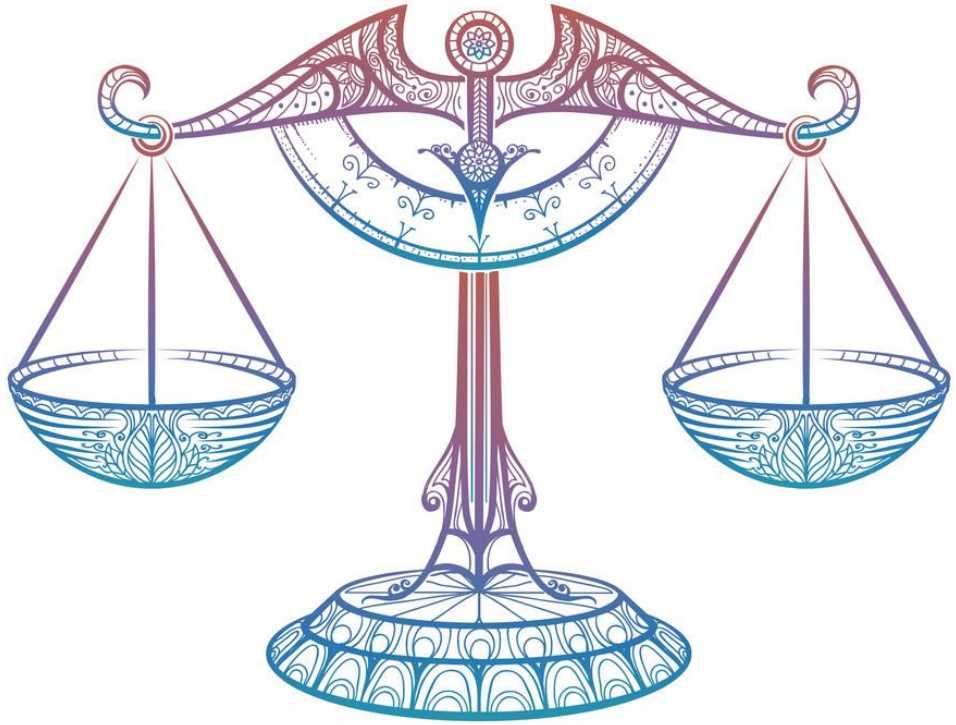
Paul Johnson

$1,000,000,000,000

What is Libra?

- Libra blockchain
- Libra currency
- Libra Association
- Calibra

- Launch in 2020



Blockchain + smart contracts + low-vol cryptocurrency + wallet, integrated with some of the most popular GLOBAL (FB) apps

Libra blockchain

- Underpinning to the Libra coin (currency)
- Permissioned DLT (initially)
- Goal: thousands of transactions per second (target 10 sec settlement time)
- Libra supports “programmable resources” with smart contract (not just a stable coin)

Libra coin

- A stable coin
- Backed by a reserve of fiat money and low vol interest bearing financial assets *
- Held in custody by the Libra Association
- Goal to bring the 1.7 bn unbanked individuals of world into the financial system

* many low vol financial assets currently have negative yield

Libra Association

- Not-for-profit organization that governs the Libra DLT
- Based in Geneva
- Run by the Founding Members (including Facebook, although without a special status or role)
- Only entity that can burn or mint Libra currency – in response to market demand
- A 2/3 supermajority is required to make changes

Calibra

- Cryptocurrency wallet (stand alone app) based on public key cryptography
- Built and maintained by Facebook
- To be integrated into WhatsApp and FB Messenger
- Built-in fraud protection, password recovery options, and MFA with 24/7 customer support
- Fully regulated *:
  - KYC/AML verification
  - Applying for licenses (around the world)
  - Will operate only where legally allowed

* Contradicts the goal of bringing the unbanked into the financial system

Validators

- Will maintain the state of the blockchain – top-down and centralized
- Stake in bootstrapping the Libra ecosystem and investing resources towards its success
- “Interest * on the reserve assets will be used to cover the costs of the system, ensuring low transaction fees, while paying dividends to investors who provided capital to jumpstart the ecosystem and support further growth and adoption.”
- Criteria:
  - More than $1 billion USD in market value OR over than $500 million USD customer cash flow
  - Able to directly reach more than 20 million people a year, internationally
  - Recognized as an industry leader by a third-party association (in the top 100) – for example, be on the top 100 of the Fortune 500

* many low vol financial assets currently have negative yield

Key partners *:
Critical part of the adoption strategy

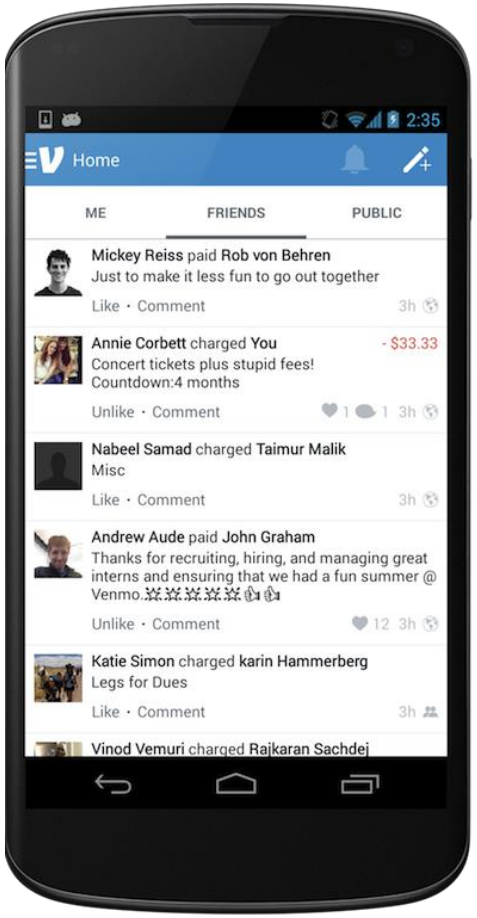
* Each partner commits to contribute a minimum of $10 mm

Missing

And every other bank!

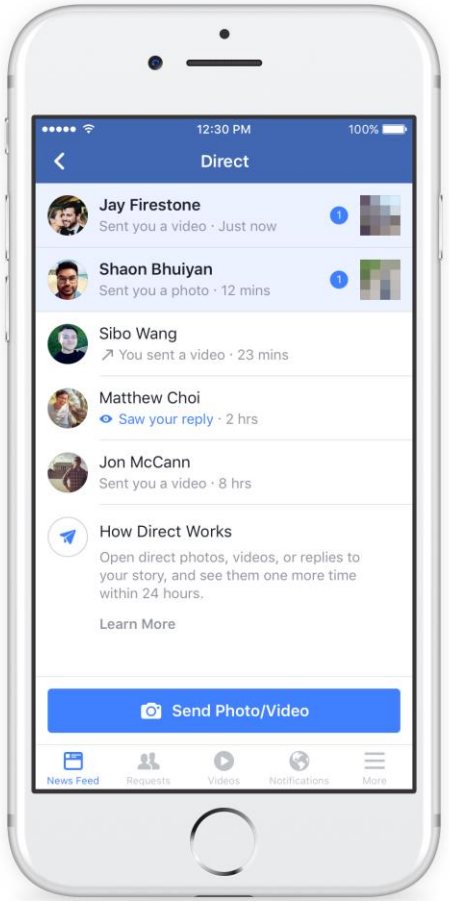
venmo

- 27.5 million users
- $19 billion transaction volume in the 4th quarter of 2018
- $80 billion per year
- ~$2,750 per user (annual)



- 2.38 billion monthly active users (MAU) – March 2019
- 15% penetration = 357 million
- At Venmo average, transaction volume would total =

$1,000,000,000,000 *



* International remittance market is roughly $500 bn per year

Western Union

Western Union

- $5.00 for transfers up to $50
- Price range - $5-$81 for $1,000 (depending on how money is sent) + a spread on F/X fees
- Can be close to instantaneous, for a fee

Libra

- Low transaction fees
- No limit to transfer amount
- Instantaneous transfer

Key challenges

- Regulatory response
- Emerging markets willingness to allow Libra to be successful *
- Facebook “trust” issues
- Validators – centralized versus decentralized governance
- Taxes – at least in the US
- Security
- Execution!
- Adoption!

* Most emerging market governments take currency management and capital controls very seriously

Reality

Libra

- is not a currency
- is not a blockchain
- is a modified ETF with a (potential) payment system bolted on top
- is not stable

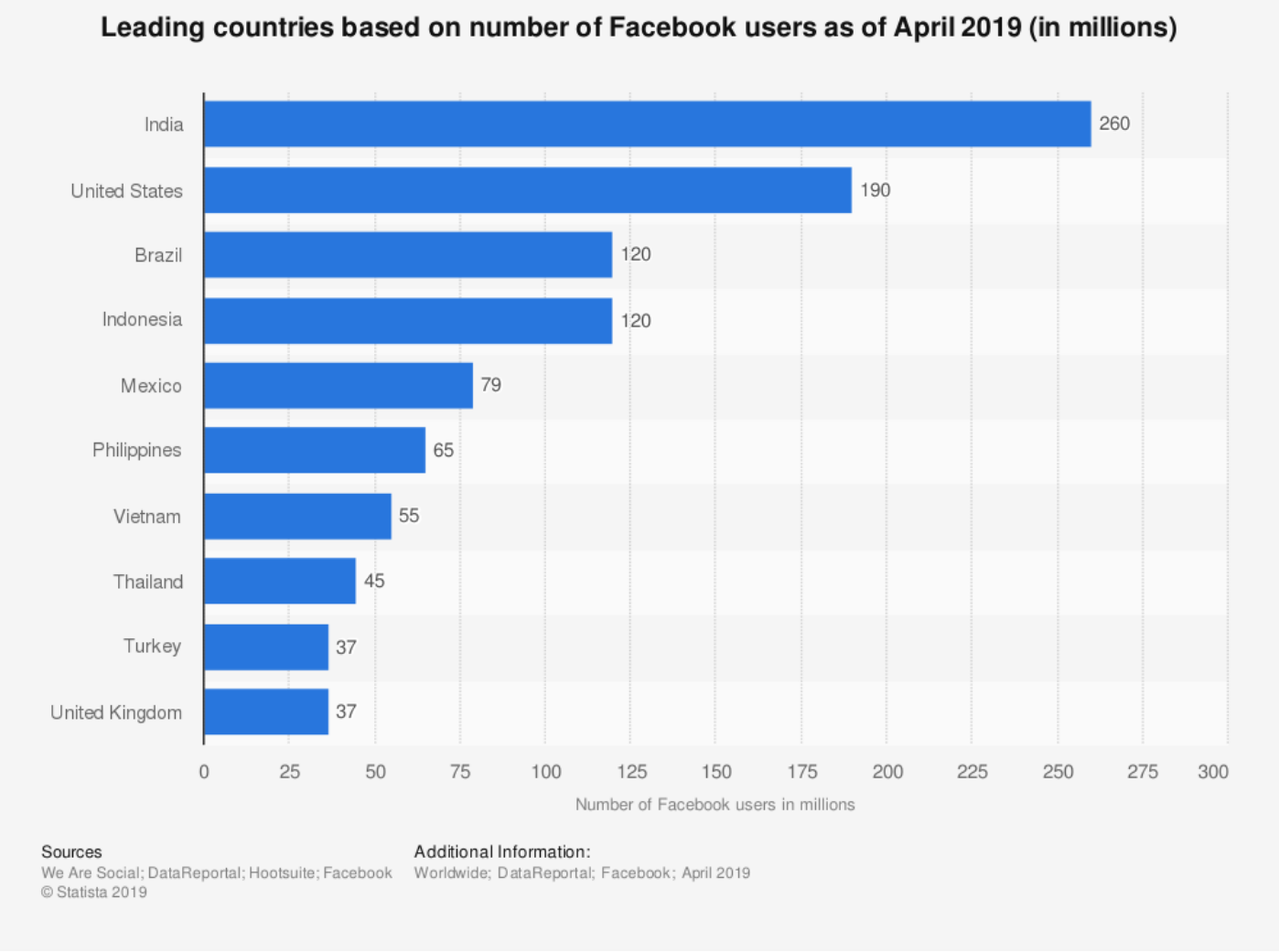
- is not done!

What's a stable coin?

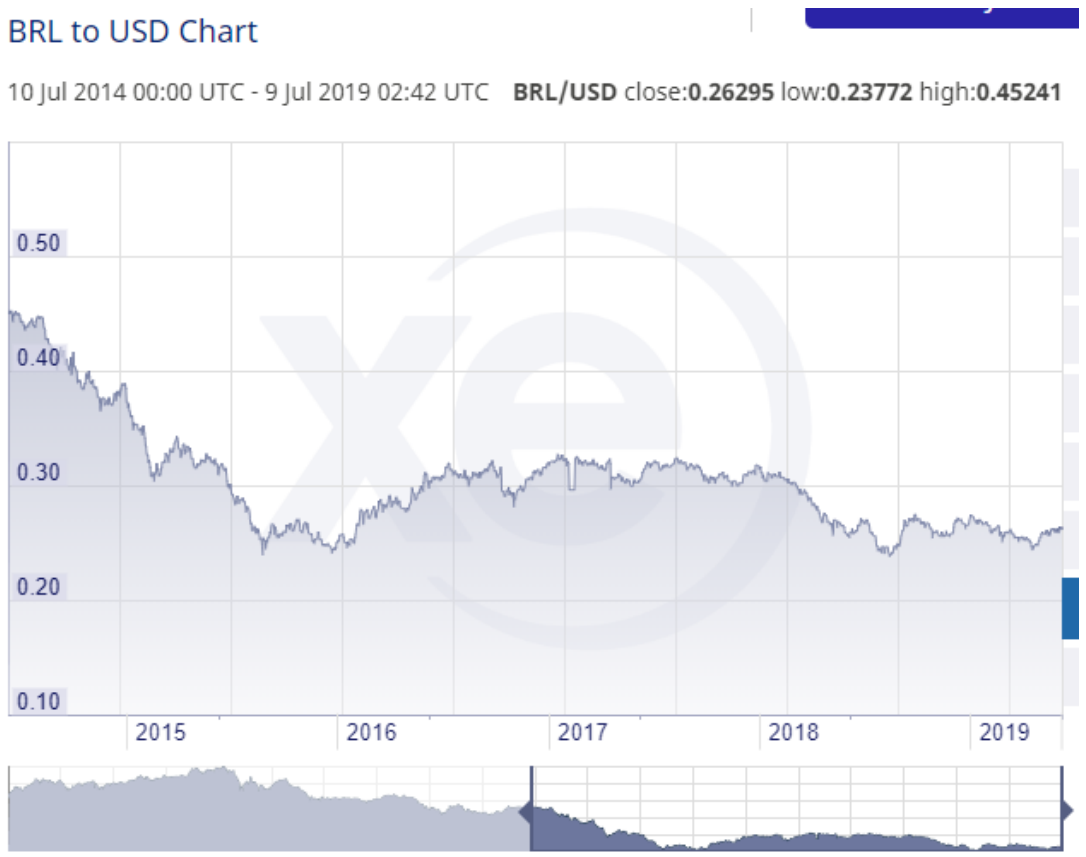
The [Libra coin] reserve is the key mechanism for achieving value preservation. Through the reserve, each coin is fully backed with a set of stable and liquid assets.

Users do not need to worry about the association introducing inflation into the system or debasing the currency: For new coins to be minted, there must be a commensurate fiat deposit in the reserve.

Facebook by country

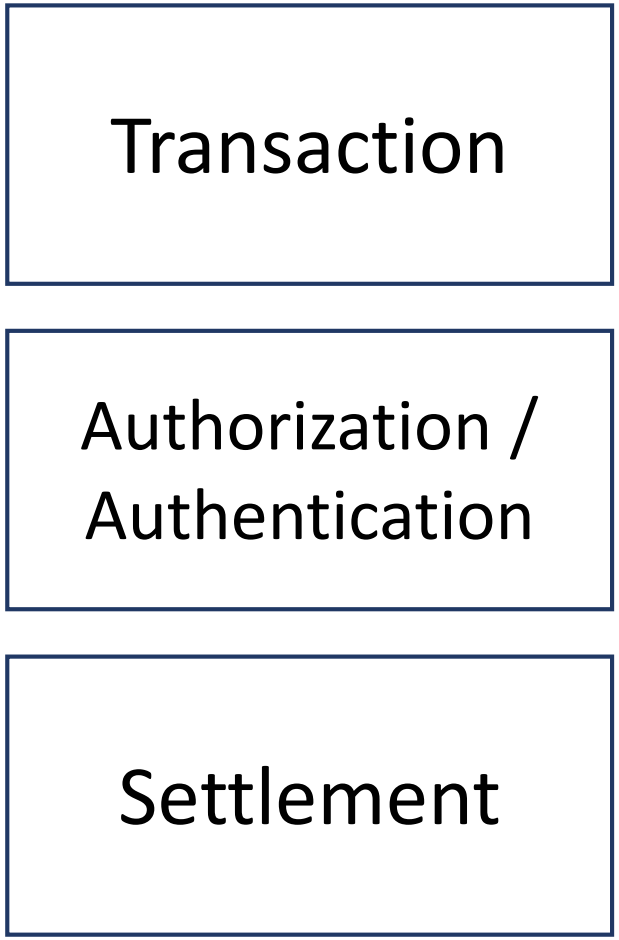


Stable to what *?

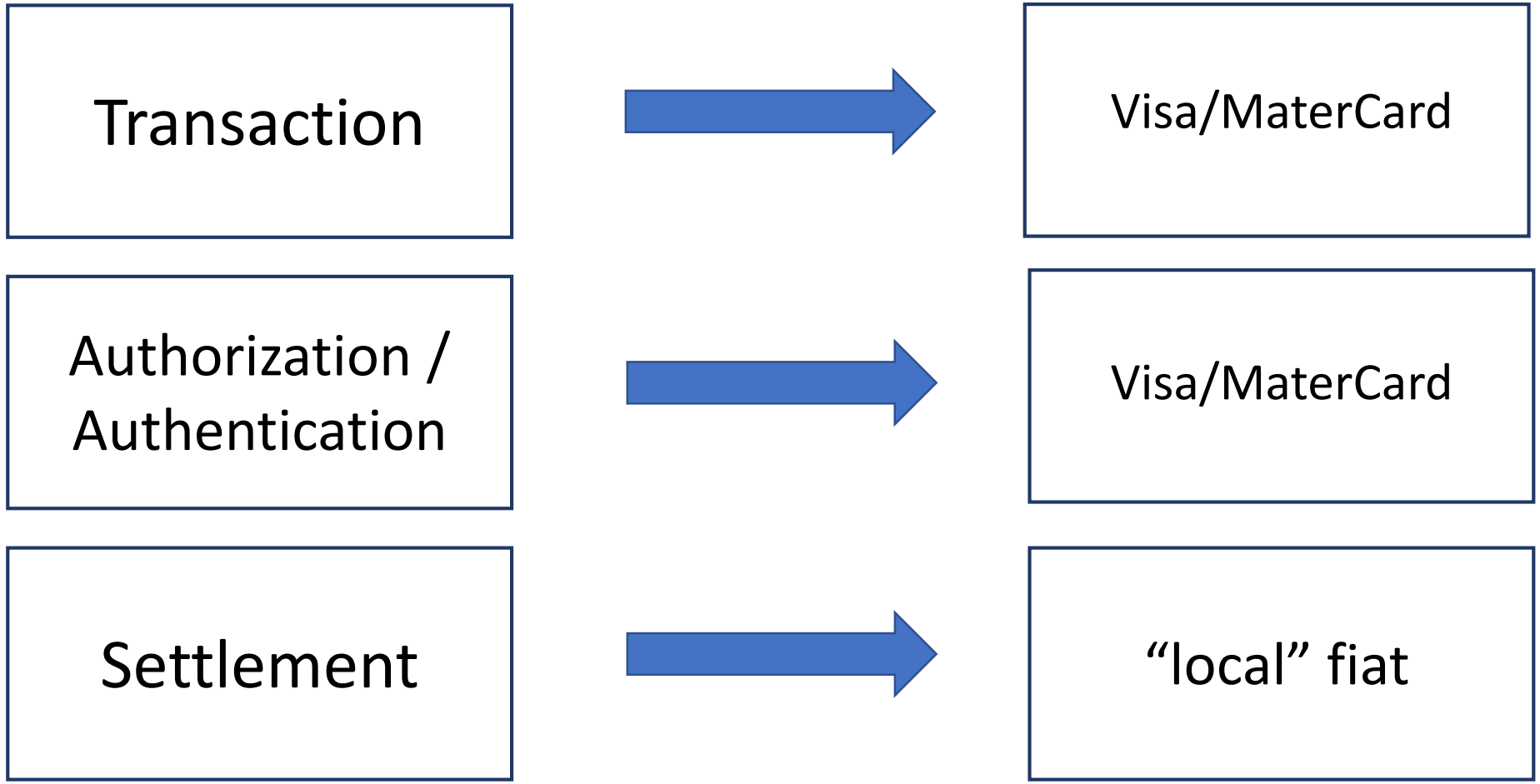


* Visa / MasterCard estimate that 85% of all transactions are still done in cash

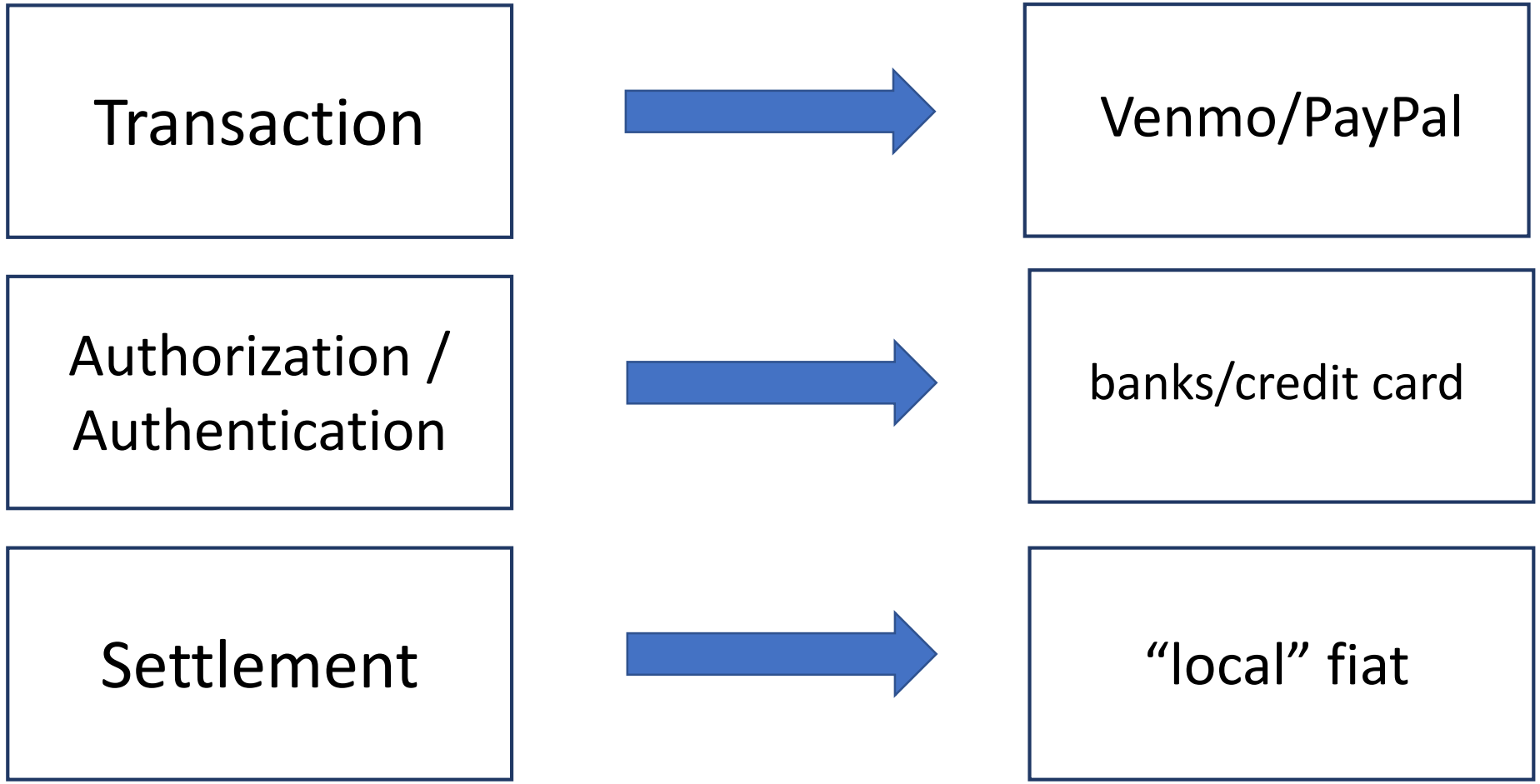
Payment stack



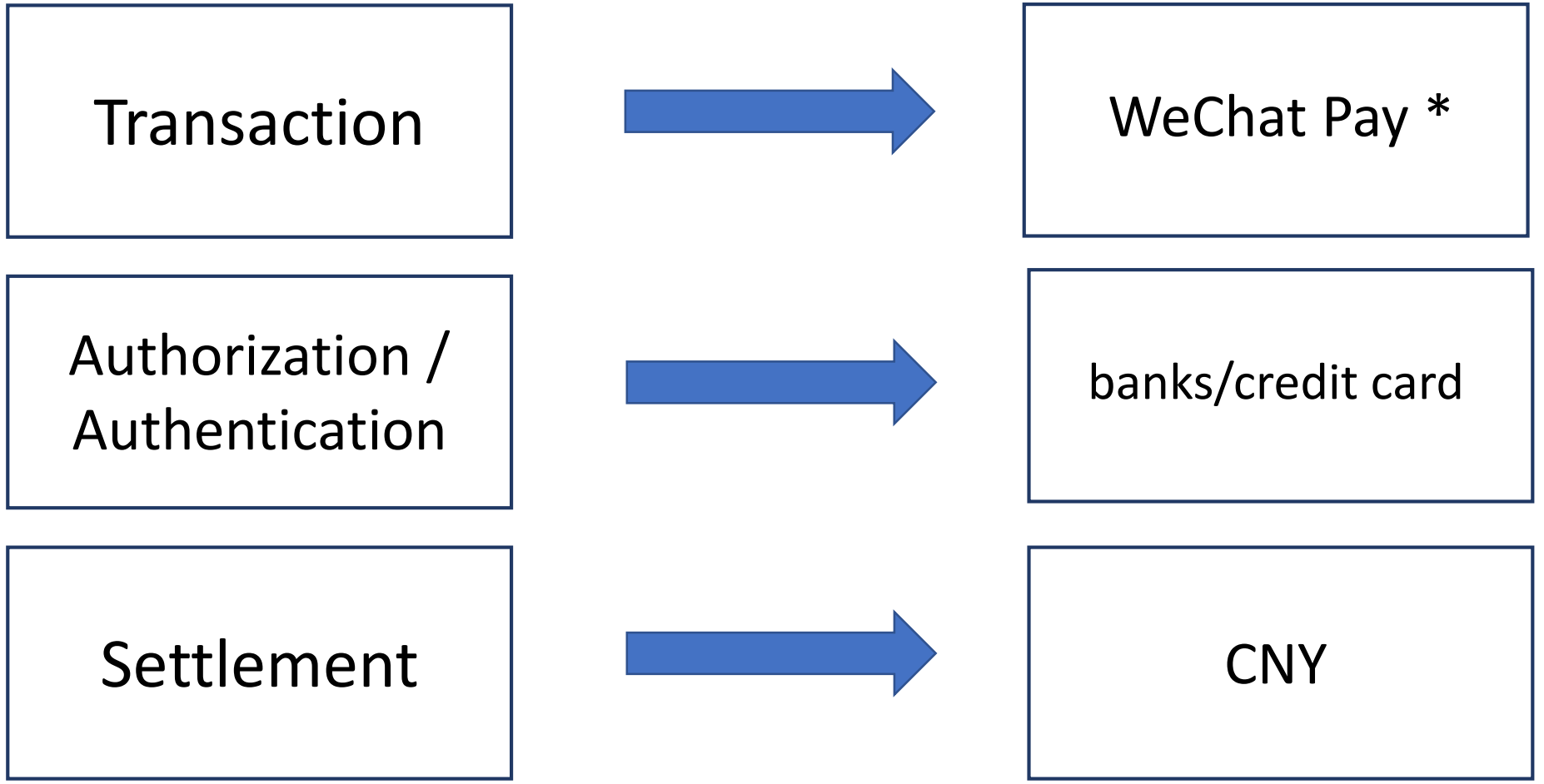
Traditional payment stack



FinTech payment stack

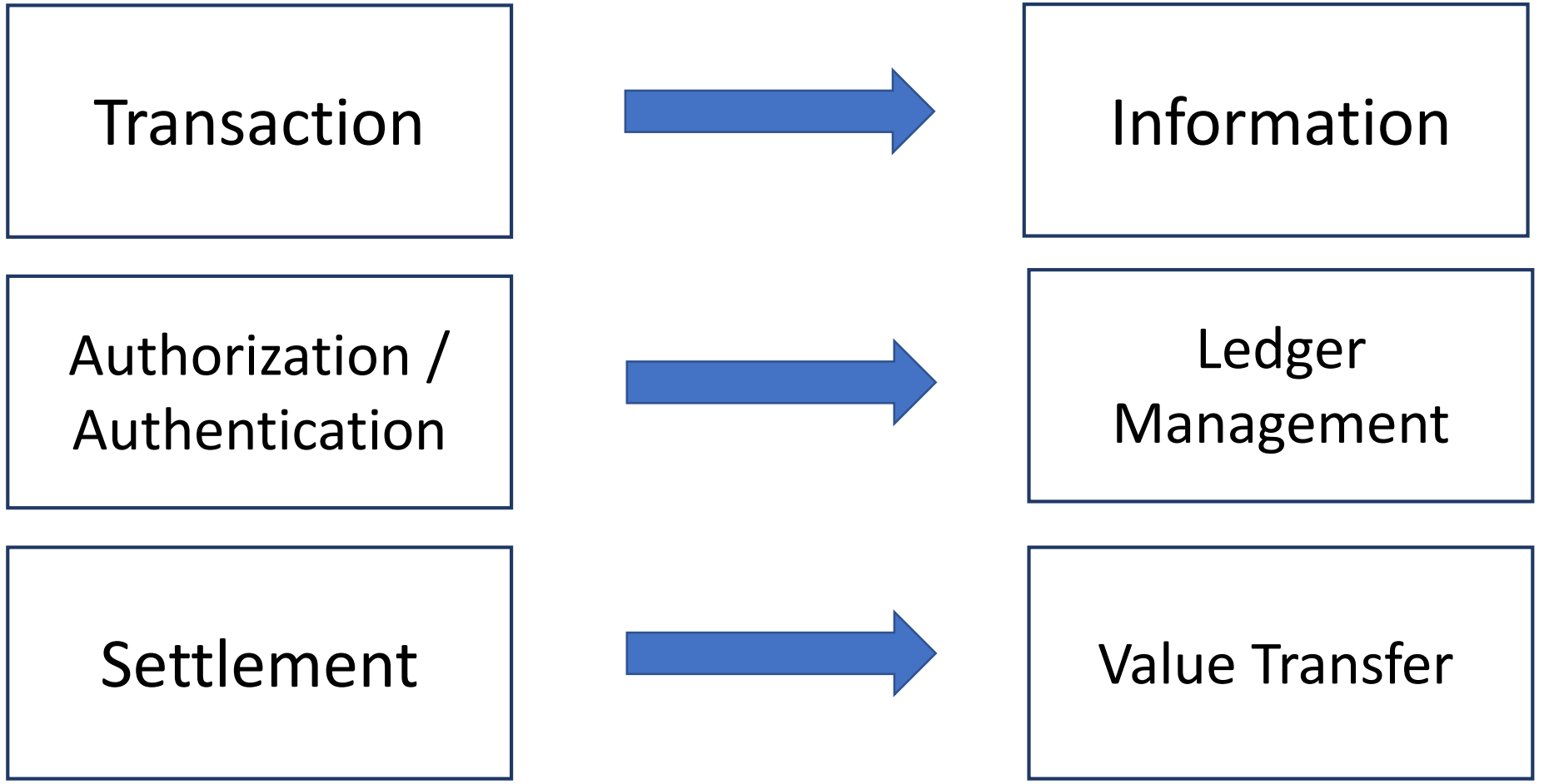


WeChat payment stack

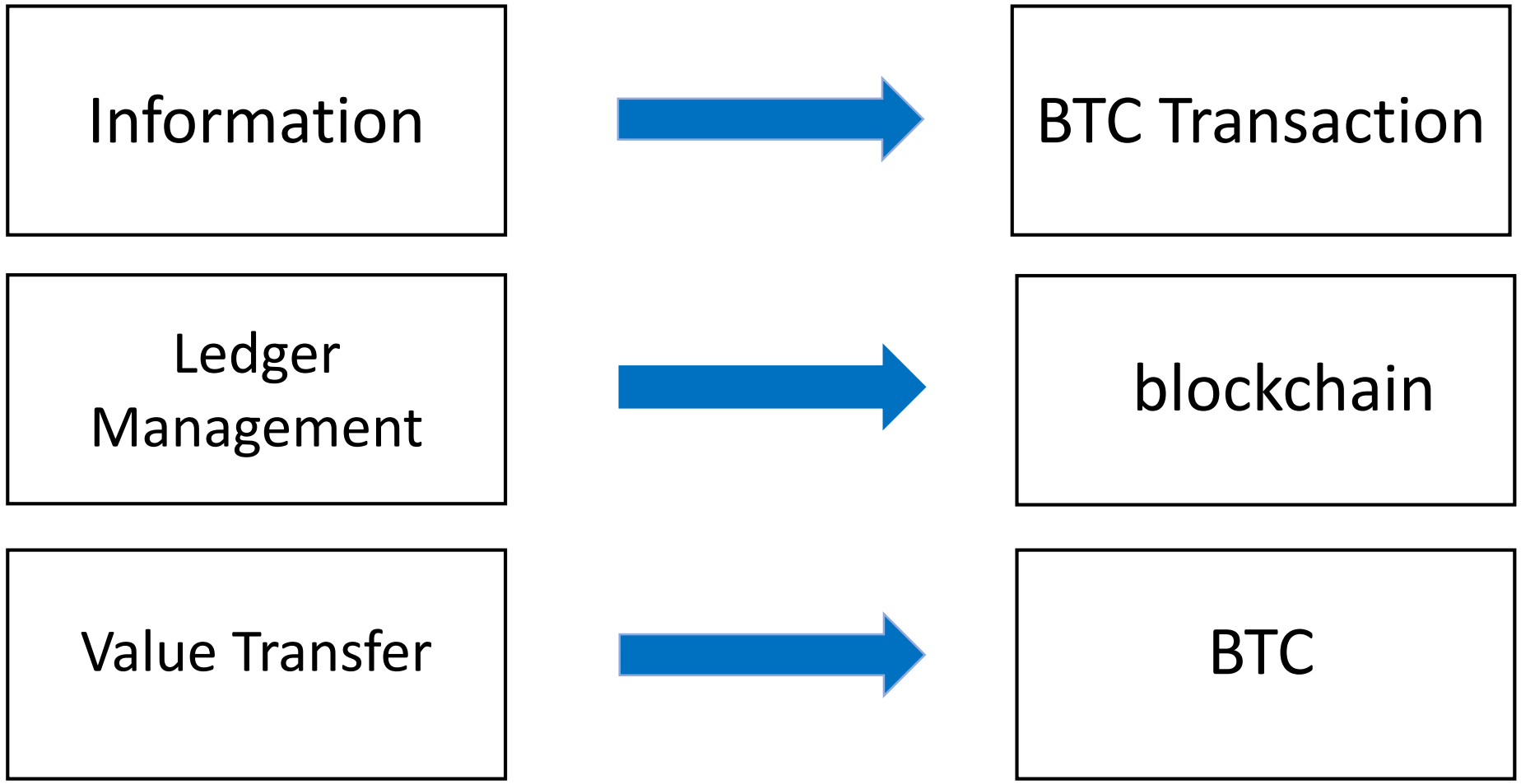


* 2017 mobile payments in China exceeded $16 trillion

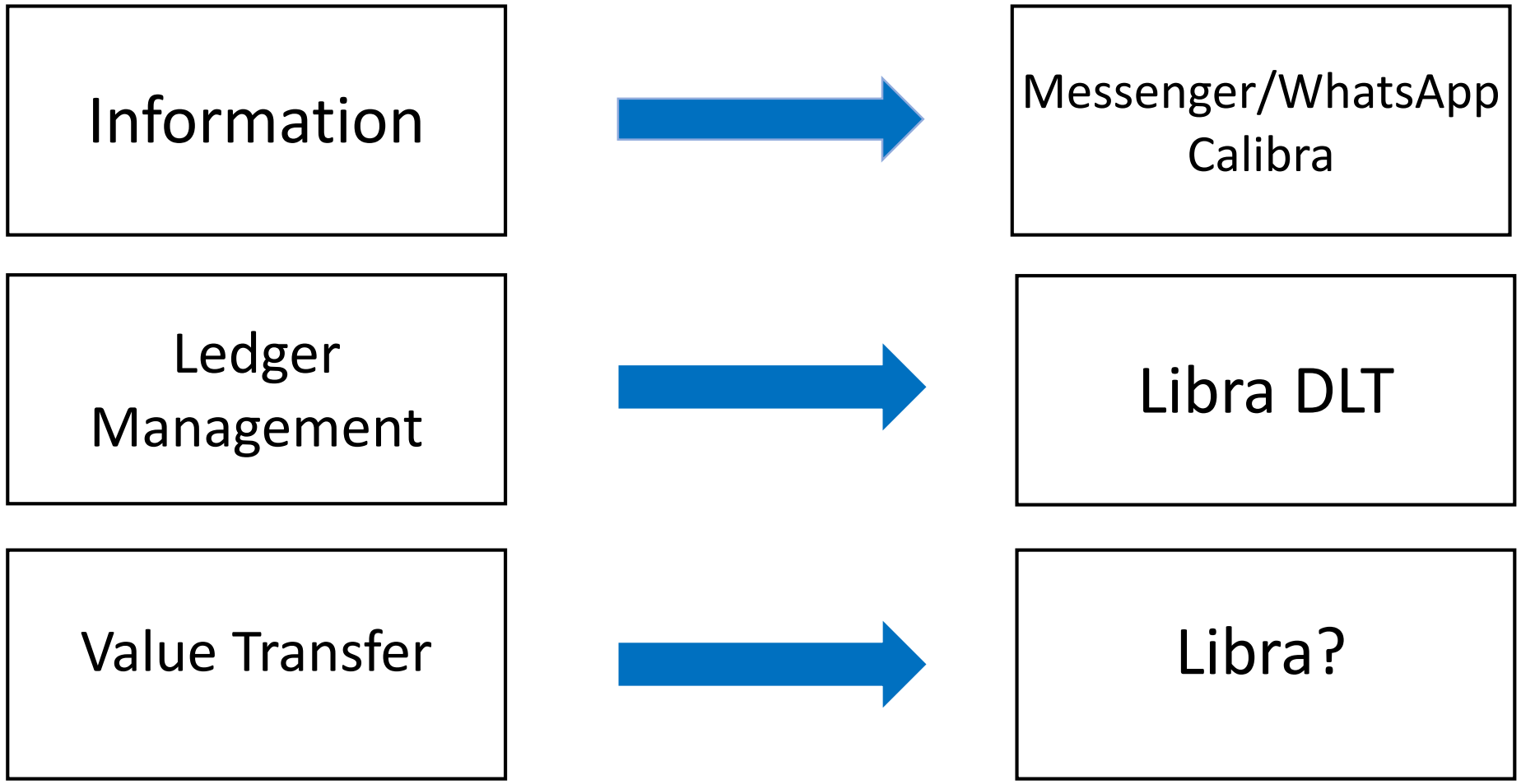
Payment stack (translated)



Payment (settlement) based on BTC

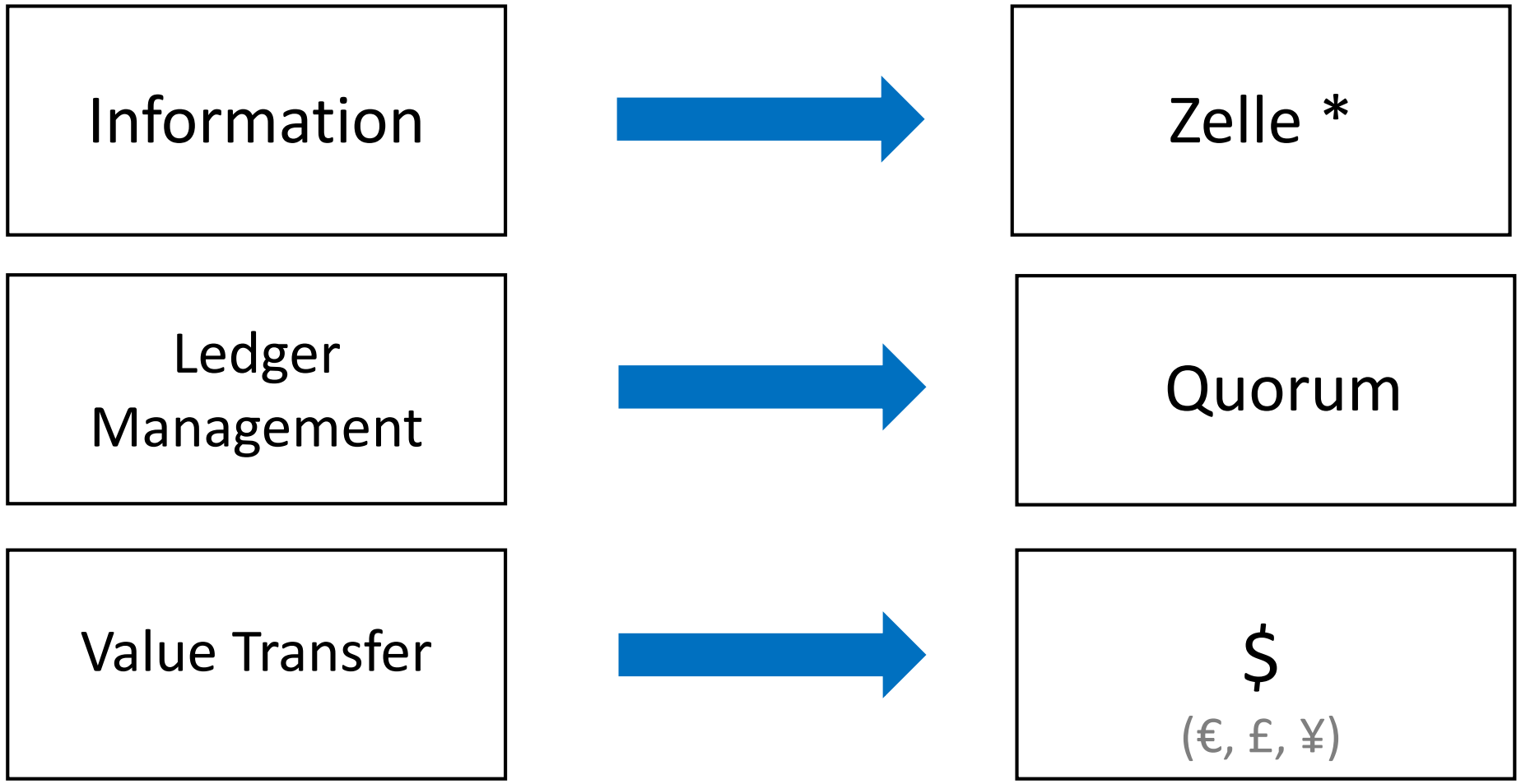


Based on Libra




J.P.Morgan

Integrated with other FinTech



* Zelle processed $122 bn in transactions in 2018

How to get government support?

- Central banks as validators!
- Provides control, access, and transparency

Facebook fiat – why keep reserves?

Dyson
Cornell
SC Johnson College of Business

Cornell CALS
College of Agriculture and Life Sciences

Financial Time Series Analysis of Cryptocurrencies and Discussion on Libra

libra

Youwei Yang, 7/9/2019

Mentors: Prof. Calum Turvey & Prof. Yongmiao Hong

Annual Meeting

About the Annual Meeting
Submissions
Webcasts
AEA Poster Session Videos
AEA Continuing Education
Exhibitors and Advertisers
Past Annual Meetings
2019
Program
Photos
2018
2017
2016
2015
2014
2013
2012

Economics of Financial Technology

Paper Session

Saturday, Jan. 5, 2019 · 10:15 AM - 12:15 PM

Hilton Atlanta, 405

Hosted By: CHINESE ECONOMIC ASSOCIATION IN NORTH AMERICA & AMERICAN ECONOMIC ASSOCIATION
Chair: Siu Fai Leung, Hong Kong University of Science and Technology

The Economics of Cryptocurrencies-Bitcoin and Beyond

Jonathan Chiu, Bank of Canada
Thorsten V. Koeppl, Queen's University

View Abstract | Download Preview (PDF, 1.17 MB)

Textual Factors

William Cong, University of Chicago
Tengyuan Liang, University of Chicago

View Abstract

Bitcoin as Decentralized Money: Prices, Mining, and Network Security

Emiliano S. Pagnotta, Imperial College London

Blockchain Economy and Cryptocurrency Markets

Paper Session

Friday, Jan. 4, 2019 · 2:30 PM - 4:30 PM

Hilton Atlanta, 203

Hosted By: ASSOCIATION OF FINANCIAL ECONOMISTS
Chair: Eric Ghysels, University of North Carolina

Volatility and Welfare in a Crypto Economy

Fahad Saleh, McGill University

View Abstract | Download Preview (PDF, 454.53 KB)

Tokenomics: Dynamic Adoption and Valuation

William Cong, University of Chicago
Ye Li, Ohio State University
Neng Wang, Columbia University and NBER

View Abstract

Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales

Sabrina T. Howell, New York University & NBER
Marina Niessner, Yale University
David Yermack, New York University & NBER

Economists' Comments on Bitcoin

- Robert Shiller
  - "I'm interested in bitcoin as a sort of bubble. It doesn't mean that it will disappear, that it'll burst forever. It may be with us for a while,"
  - "Financial theory says that if something is not shortable then it can be taken over by enthusiasts, and the doubters can no longer have an adequate way of betting against."
  - "It has no value at all unless there is some common consensus that it has value. Other things like gold would at least have some value if people didn't see it as an investment"
- Joseph Stiglitz
  - "[Bitcoin] ought to be outlawed," as it "doesn't serve any socially useful function."
- Paul Krugman
  - "Bubble, Bubble, Fraud and Trouble"

Issues for Applied Economists

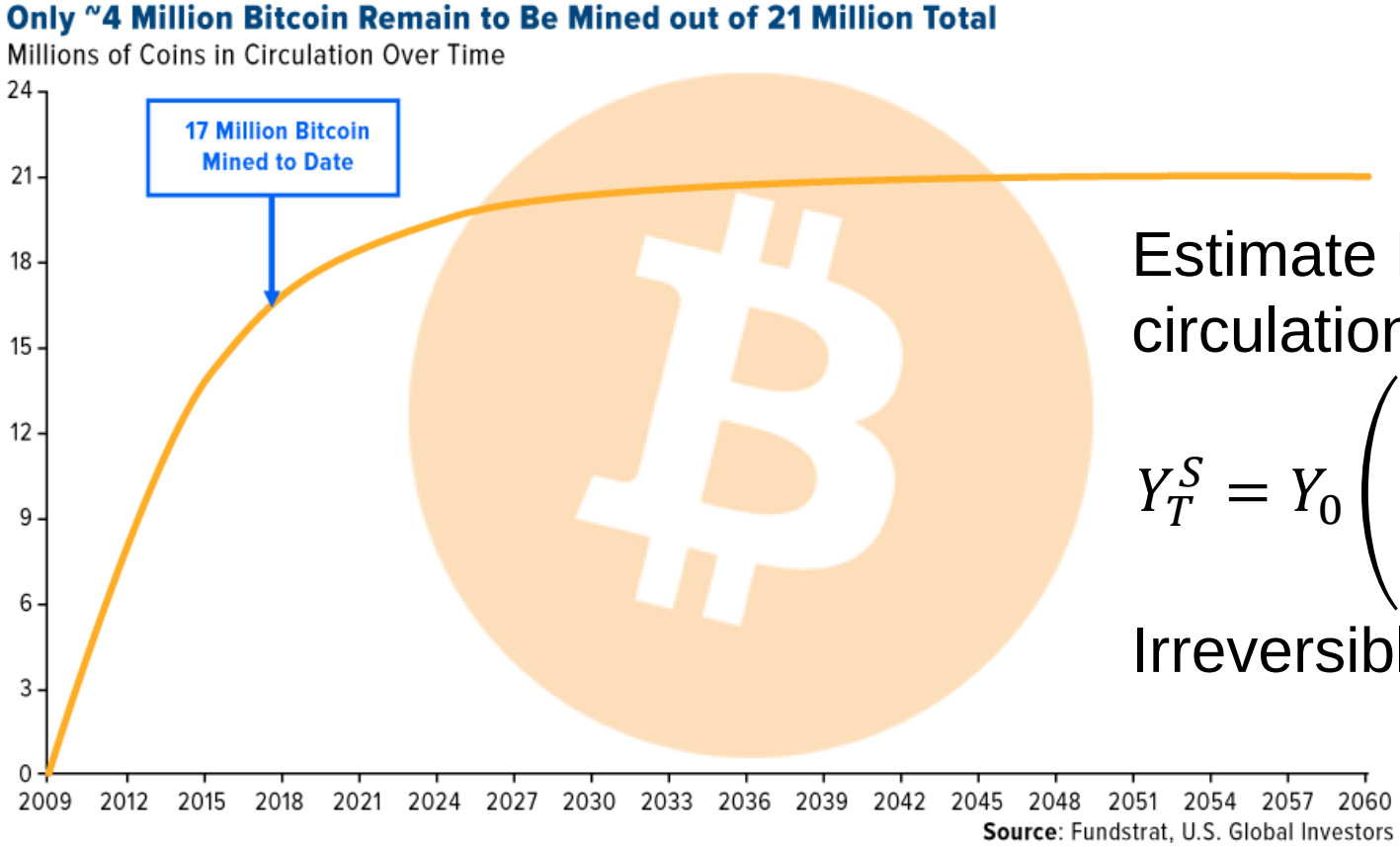
- Cryptocurrency and Blockchain are being promoted to improve efficiency in agricultural economics and finance
  - Fin-Tech: trade, transactions, and records keeping
  - Development finance: poverty reduction, Microloans
  - Food security: resource allocation
  - Biosecurity: traceability
  - Supply and value chain management
- In order to move forward on these issues, a greater understanding of market fundamentals is critical.
- This study reveals important market properties that contribute to the advancement of the Cryptocurrency and Blockchain community, also economics in general.

Research Question

- Investigating whether crypto coins follow a continuous random walk (e.g. geometric Brownian Motion) or some process such as a fractional Brownian Motion.
- Understanding the institutional structure of crypto currencies and explaining possible reasons for them appearing to be fBm.
- Mainly to see if these cryptocurrencies are traded in efficient way based on financial theories.

Bitcoin Supply: Releasing Mechanism

- Bitcoin has a limited total supply of 21 million and released in a decreasing rate: amount released in one period (e.g. 1 year) is ½ of the amount released in the previous period.



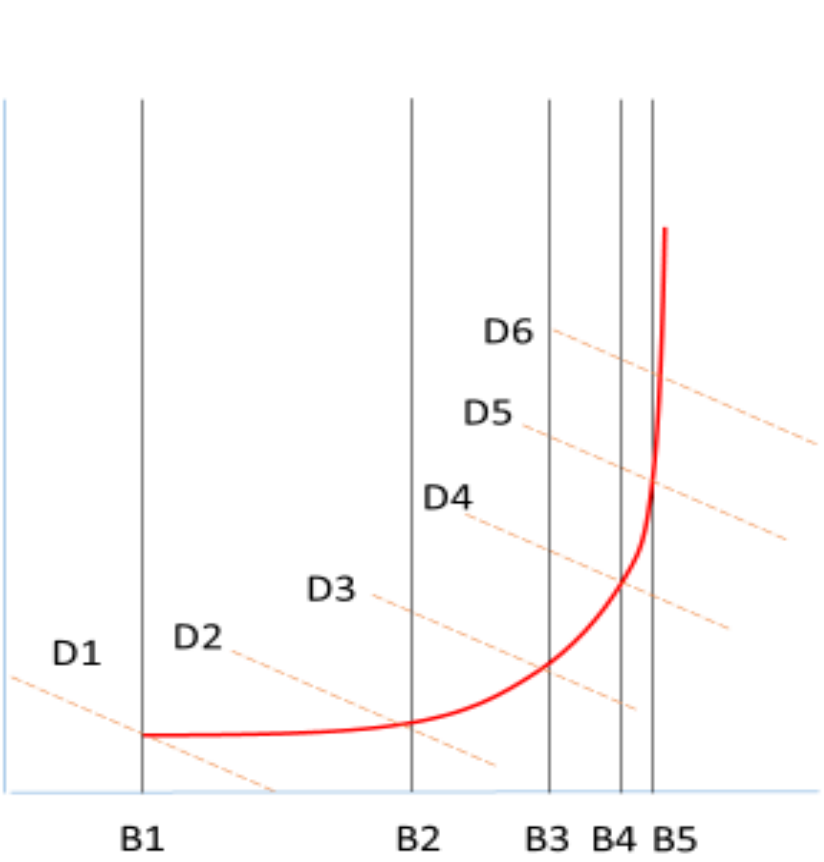
Estimate Bitcoins in circulation (Supply):

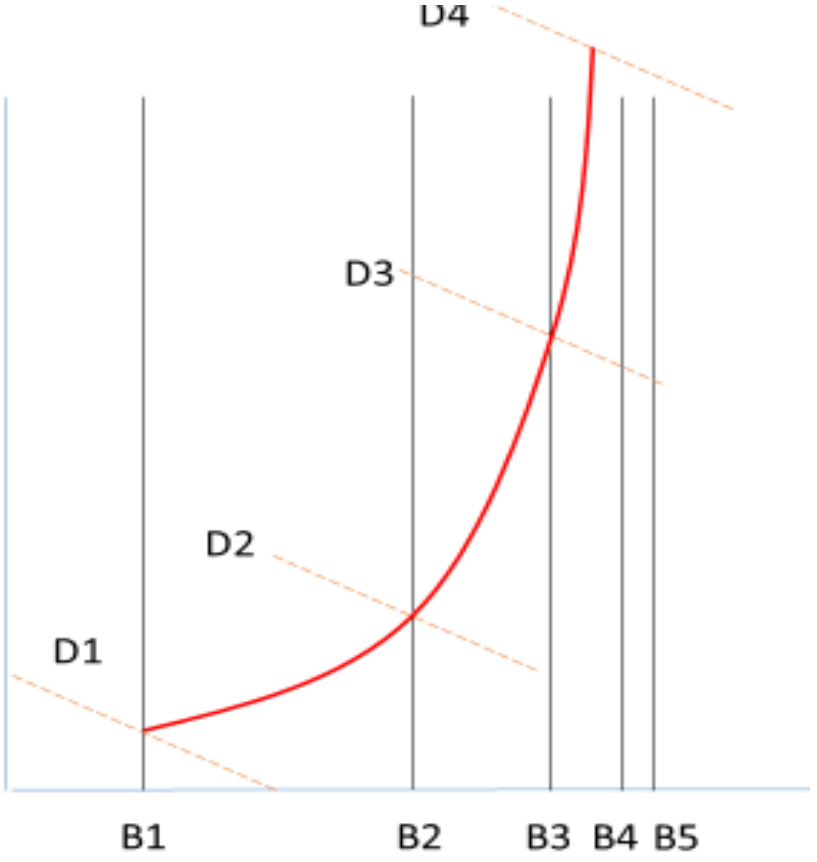
$$Y_T^S = Y_0\left(1 + \sum_{t=1}^{T} e^{-0.693t}\right)$$

Irreversible accumulation

Supply / Demand Equilibrium

This structure might be causing fractionality





e.g. Bitcoin: proportionally decreasing rate in supply increase

-Constant Rate Increasing Demand -Increasing Rate of Demand Increase

Hypothetical S / D Equilibrium

- Questionable as supply is pre-set and not variate.
- Bitcoin Supply: $Y_T^S = Y_0(1 + \sum_{t=1}^{T} e^{-0.693t})$
- Demand: $Y^D = A * P^{-B}$
- Supply Y_T^S = Demand Y^D , and get

$$P = (Y_0 / A) * (1 + \sum_{t=1}^{T} e^{-0.693t})^{-1/B}$$

- Empirically, I used semi-weekly Supply and Price data for 8 years run simple OLS linear form, find:

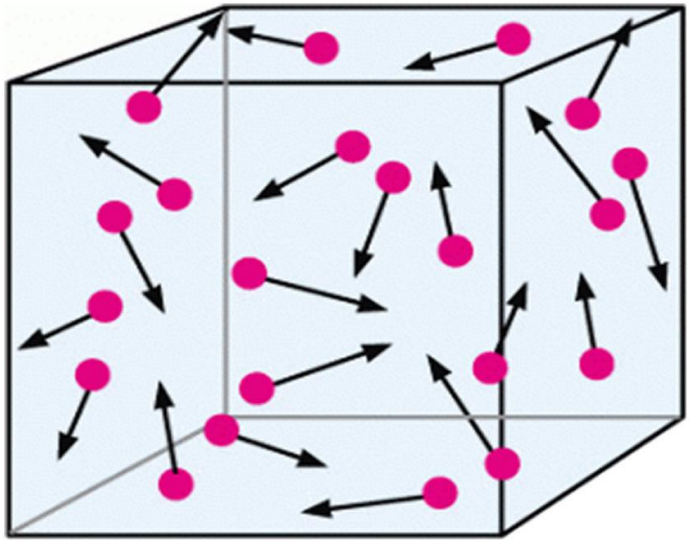
*Price = 0.00061*Supply -6495.11*

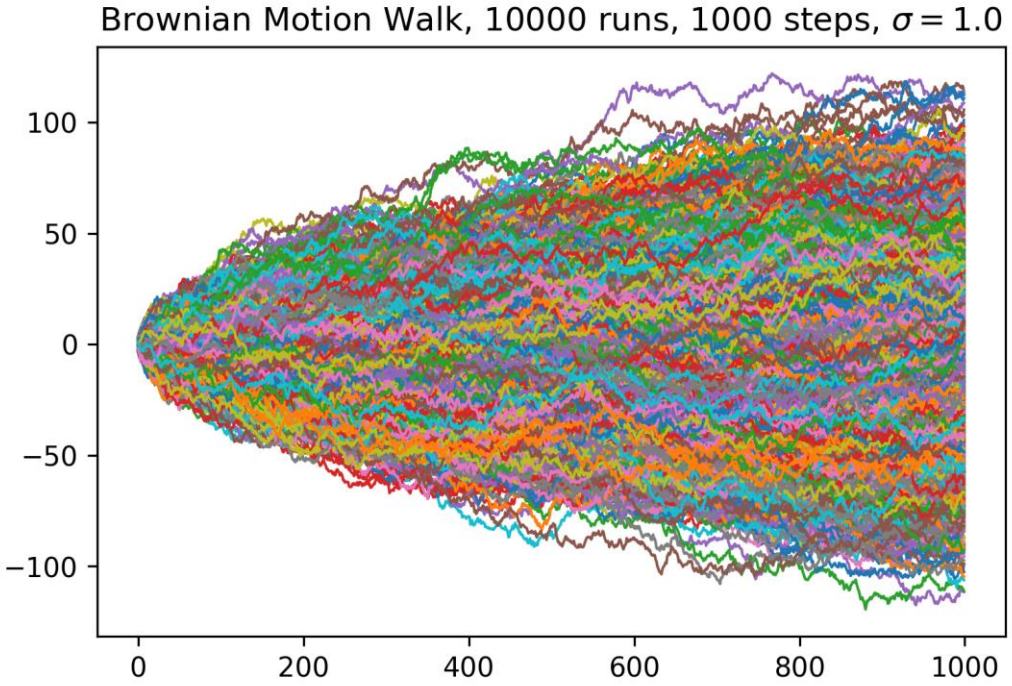
Methodology

- Estimating Hurst measures to examine the memory and indicate geometric / fractional Brownian motion in cryptos time series.
- Applying regression analysis to identify the impact of market structure factors on cryptos' fractionality (with Hurst coefficients measured in above analysis)

Brief Background on Brownian Motion - From Physics to Finance

- The erratic random movement of microscopic particles, as a result of continuous bombardment from molecules of the surrounding medium.





Why is it Important to See if Follow a Random Walk (gBm / fBm)

- Practical Implications of random walk:
  - Efficient market hypothesis (fully reflect all timely available information and memoryless system)
  - Predictiveness and arbitrage opportunities
  - Option-pricing (Black-Scholes is based on random walk gBm assumption)
  - Non-Brownian, i.e. fractional processes can be exploited to beat the market.

Hurst Coefficient (Math)

- H is commonly estimated by rescaled range (R/S) analysis, to examine the dependence of the rescaled range of N observations, divided into shorter periods.
- Variance and Covariance between time periods:

$$E[x(t_2) - x(t_1)]^2 = \sigma^2 (t_2 - t_1)^{2H}$$

$$E\{[x(t) - x(0)][x(t + \Delta t) - x(t)]\} = \frac{1}{2}\sigma^2[(t + \Delta t)^{2H} - t^{2H} - \Delta t^{2H}]$$

- Brownian motion Variance general form:

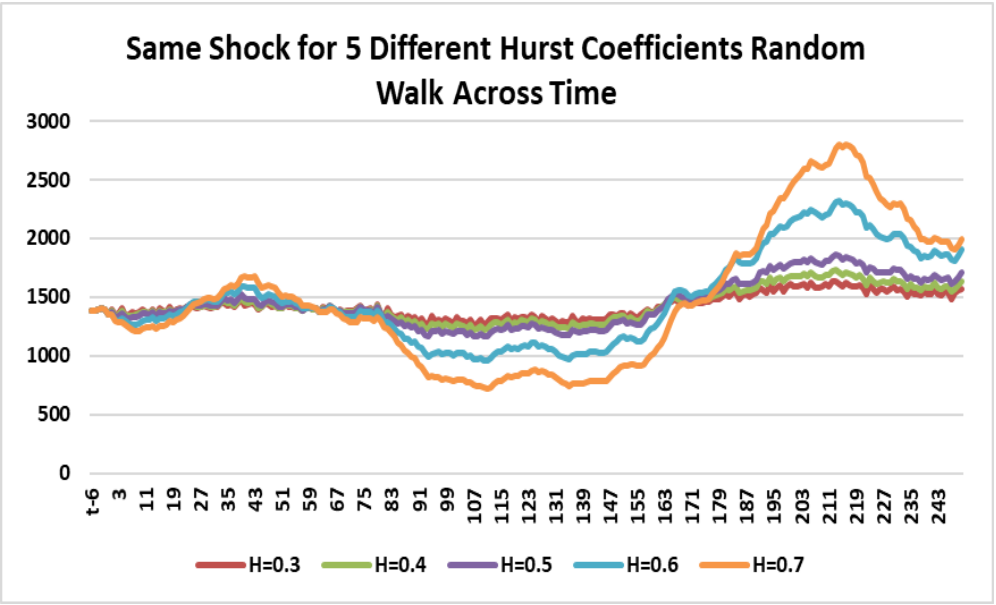
$$Var[x_{500} - x_1] = Var[x_t - x_{t-1}]T^{2H}$$

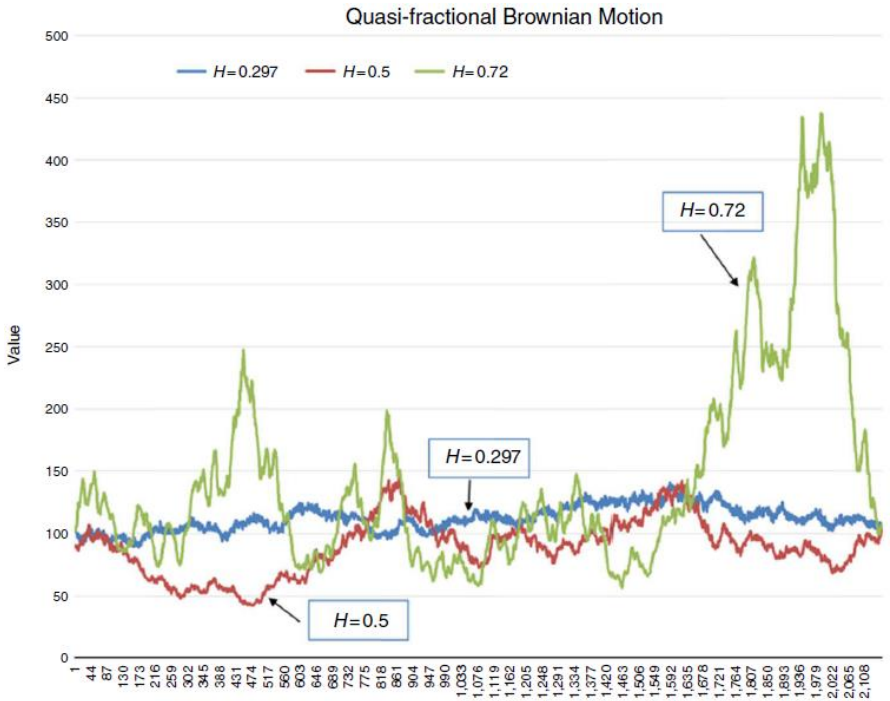
- Hurst coefficient estimation

$$H = \frac{1}{2}\frac{Log\left(\frac{Var[x_{500} - x_1]}{Var[x_t - x_{t-1}]}\right)}{Log(T)}$$

Hurst Coefficient (Interpretation)

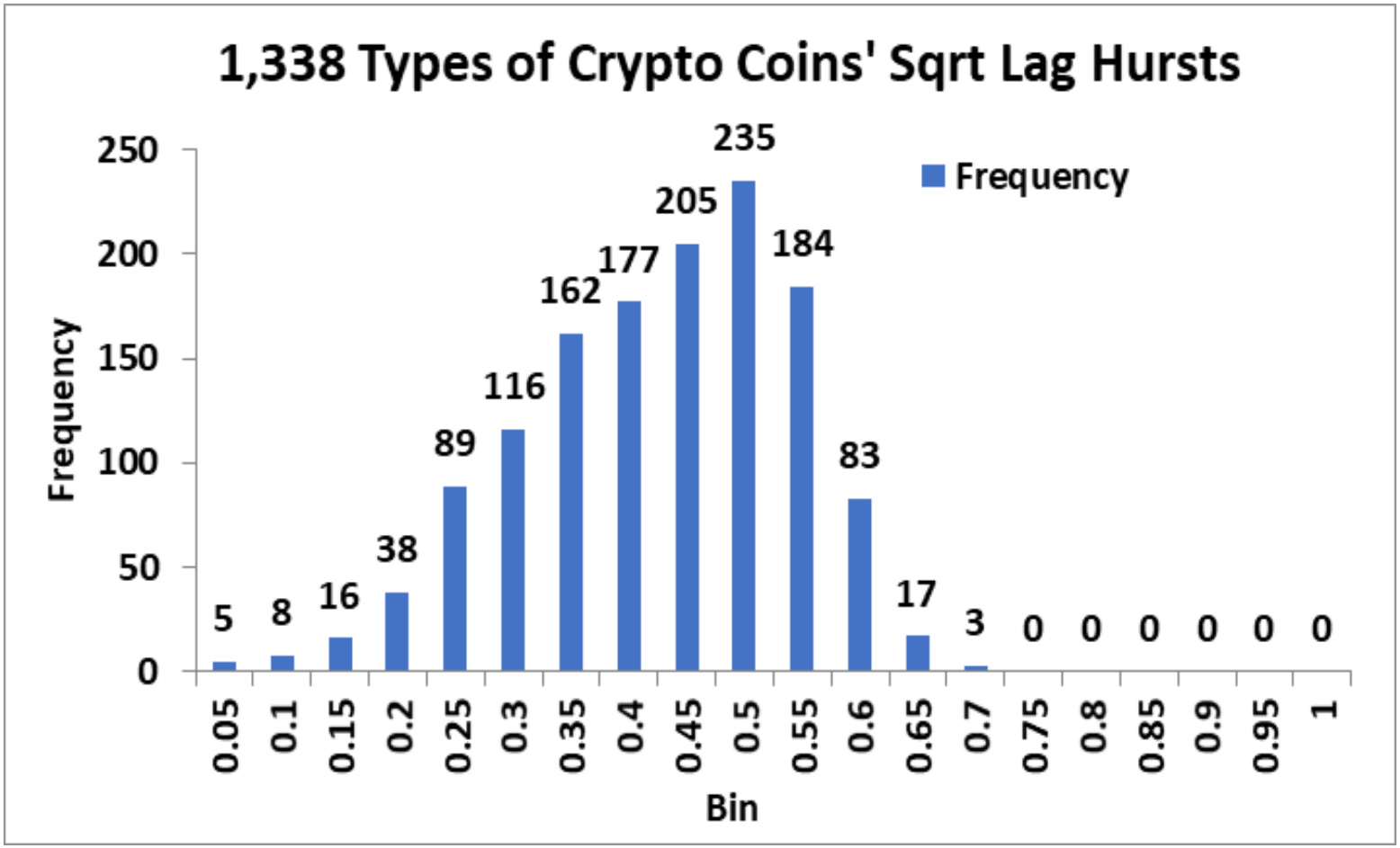
- H = 0.5 : geometric Brownian motion – no memory
- H > 0.5 : Persistence/long memory (Black noise)
- H < 0.5 : Anti-persistence/mean-reverting (Pink to White noise)





Hurst Coef. Estimates of Cryptos

- Estimated H for crypto currencies that are older than 6 months



*vs. Securities, stocks, and commodity futures time series all have H around 0.5.

Factors Influencing Memory of Cryptos

- To understand the underlying supply structure and factors influencing crypto prices' fractional property.
- Collected information on the top 100 crypto currencies for age (period since its release), estimated year 2050's supply or max supply, current supply issued ratio, type of supply, and market volatility, etc.
- We ran simple OLS regression of these variables against Hurst coefficients estimated earlier with various specifications of these variables.

$$Hurst_i = \beta_{0i} + \beta_1 * Age_i + \beta_2 * SupplyIssued_i + \beta_3 * S_i^2 + \delta * Control$$

- Control is supply type of currencies, 3 main types: Capped total, Perpetual inflation and Decaying inflation.

Hurst ~Supply Factors Regress Results

Hurst OLS Fit with Market Structure Influencing Factors			
Hurst (Sqrt n lag)	(1)	(2)	(3)
Intercept	0.524851***	0.527834***	0.535094***
	(0.024870)	(0.0287689)	(0.026443)
Age	0.006628 .	0.0044473	0.006644
	(0.003935)	(0.0111458)	(0.004094)
Age^2		0.0003073	
		(0.0014685)	
SupplyIssued%	-0.124696	-0.1267831	-0.157494 .
	(0.079850)	(0.0808486)	(0.084275)
SupplyIssued%^2	0.118355 .	0.1200127 .	0.140730*
	(0.061408)	(0.0622071)	(0.063894)
Supply Type (reference category = Capped total)			
Decaying inflation			0.017784
			(0.023957)
Perpetual inflation			-0.026986
			(0.026529)
Observations	105	105	105
R-squared	0.0728	0.0732	0.0888

. P < 0.1, * p < 0.05, ** p < 0.01, *** p < 0.001
Standard errors in parentheses.

- Supply issued % decreases Hurst at a decreasing rate (Convex). Meaning more portions of coins issued, less persistent the price series' memories are.
- Decaying inflation supply type contributes to more persistency, and Perpetual inflation supply type is opposite.

Analysis Findings Summary

- Our analysis of Cryptocurrencies shows overwhelming evidence of fractionality through Hurst estimation. This fractionality indicates most of these cryptocurrencies traded contain systematically memory and inefficiency.
- Our results confirm our conjecture that price movement in cryptocurrencies are demand driven along a prescribed deterministic supply, e.g. supply in each moment in time is perfectly inelastic.
- This is because supply structure with pre-determined and independent of price, along with the emotional hype, implies potential market inefficiency and fractional Brownian motion.
- Our study shows the major supply indicators: supply issued % and inflation structures show effects on Hurst estimates (indicator of the memory in the price series).

How About libra ?

- Compare with all other cryptocurrencies:
  - Similarity:
    - Digital, cryptography
    - Operated through blockchain
    - The feature of low volatility and minting/burning Libra coins ~ stable coins.
  - Difference:
    - Backed by a reserve of assets designed to give it intrinsic value
    - Governed by Libra Association with “Founding Members” in various industries: Payments, Technology, Venture Capital, Nonprofit, etc.
    - Libra is not a “peg” to a single currency with stable convert rate, unlike Tether (USDT) or other stable coins.
    - Comes with built-in market power and network influence. i.e. Facebook has 2.4 billion users globally, so does Libra’s other founding members: PayPal, eBay, Visa, Uber, etc. (Some economists in network effects and monetary policy serve on the consulting team of the Libra association.)
    - It links closer to the real world traditional finance.

How does my analysis on all cryptos helps understanding of libra ?

- We predict the Hurst coefficient of Libra will be around 0.5, meaning it will be more efficiently traded than most of the cryptocurrencies from a Financial theory Efficient Market Hypothesis standpoint.
- Why? It is backed by real assets! Thinking gold standards in 1930s.
- Having fundamental value helps to lower the volatility and rationalize the emotional hype and bubble value resulted from network belief in other cryptocurrencies, which we believe is the source of the fractionality or say the market inefficiency.
- As we can see from my analysis the supply structure is the key to the efficiency. The supply structure with minting and burning coins just like the Feds does will solve this end of the problem.
- So it should work!

What problems libra may face?

- Regulation
- Competition
- Governance

Facebook's **digital currency** may force **central banks** to create their own
MIT Technology Review - Jul 1, 2019
Just a few months ago, Augustín Carstens, the general manager for the Bank for International Settlements (BIS), the so-called **central bank** for ...
Morning Scan Deutsche mulling 'radical' job cuts; **Central bank digital** ...
American Banker - Jul 1, 2019
BIS will support **central banks** that issue their own **digital currencies**
Yahoo Finance - Jul 1, 2019
BIS: **Central Banks** May Issue **Digital Currencies** Soon
Bitcoin Magazine - Jul 1, 2019
Bitcoin Hater Agustin Carstens U-Turns to 'Support' **Digital Currencies**
CCN Markets - Jul 1, 2019
View all

Central banks should issue **digital currencies** of their own
Financial Times - Jul 1, 2019
Central banks should issue **digital currencies** of their own ... For governments and **central banks**, the digitalisation of money raises new ...
IMF Survey: Almost All **Central Banks** Plan To Issue **Digital Currencies**
KryptoMoney (press release) - Jul 1, 2019
View all

Central bank plans to create **digital currencies** receive backing
Financial Times - Jun 30, 2019
Global **central banks** may have to issue their own **digital currencies** sooner than expected, the general manager of the Bank for International ...
BIS Chief: **Central Banks** May Issue **Digital Currencies** 'Sooner Than ...
CoinDesk - Jul 1, 2019
View all

Bank of Japan: Adopting **Central Bank Crypto** Would Mean Dropping ...
CoinDesk - Jul 5, 2019
An official at the Bank of Japan (BoJ) has ruled out the use of **central bank digital currencies** because to do so may require the country to ...
Bank of Japan: Cash Prevents **Digital Currencies** With Negative Interest
Cointelegraph - Jul 5, 2019
View all

What else? libra

- Index fund. If we know the assets and weights of Libra. How different is it from a index with the same composition?
- Investing via Facebook with Libra, or investing via Merrill Lynch with Libra assets index? They should converge.
- Other derivatives or competition?

THE WALL STREET JOURNAL.

U.S. Edition ▾ | July 9, 2019 | Print Edition | Video

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate

MARKETS

Bitcoin Rally Fuels Market in Crypto Derivatives

New structured products draw concern as digital currency climbs back above $10,000

Forbes

Stop seeing this ad Why this ad?

4,628 views | Jul 8, 2019, 10:56am

Beijing Begins Imagining A WeChat China Cryptocurrency

Kenneth Rapoza Senior Contributor

Markets

I write about business and investing in emerging markets.

If China is ever going to allow for an officially sanctioned cryptocurrency, there's no better place to start than WeChat. TOMOHIRO OHSUMI/BLOOMBERG NEWS

Thank You!

Dyson
Cornell
SC Johnson College of Business

Cornell CALS
College of Agriculture and Life Sciences