

CBDC Part 5: Comparing Corda, Fabric, and Quorum

WEEKLY RECAP

- Total market cap. reached \$123.4bn (a 0.3% increase), and 7 day trading volume rose 24% for top 100 crypto

THOUGHTS OF THE WEEK

Privacy: Corda only seeks to achieve consensus among parties of an agreement on the state of that specific agreement as it evolves, as opposed to seeking agreement on the state of a globally distributed ledger. Hyperledger Fabric offers the ability to set up shared channels (each one being a ledger) between parties, with transactions (txs) within the channel being private to outside parties. Regulators can be included in channels for compliance purposes. Quorum achieves privacy via public & individual private state trees, with the public state tree storing vanilla Ethereum txs and hashes of encrypted private smart contract changes. Quorum thus offers and requires both private and public smart contract txs.

Scalability & Performance: Corda does not rely on a proper blockchain. This not only alleviates privacy concerns, but also makes scaling significantly easier compared to traditional DLTs. In Fabric, $[N \times (N-1) / 2] + M$ channels are required to operate, with N = number of participating nodes, and M = number of multilateral channels. The network complexity rises with each new participant, and participants need to maintain and move funds between individual channel-level accounts for each channel. Quorum vastly improves upon the performance of Ethereum, yet there is further room for improvement with regards to the speed of running zero knowledge proofs.

Resiliency: While Corda can continue to operate should individual bank nodes go offline, the use of a single notary node (e.g. central bank) to achieve consensus over uniqueness is a potential point of weakness. This can be rectified with a notary node operated by multiple parties, although at the expense of added complexity. Fabric involves a blockchain, but an orderer is required to order txs into blocks. The Ubin 2 prototype is built on a single orderer, which introduces a single point of failure. A multi-node ordering service could solve this issue. Propagating hashes of private transactions to the global ledger improves resilience in Quorum. This use of a central ledger ensures significant resilience, and under the tested Raft consensus method the consensus leader could be rotated with each tx for added resilience. This may or may not be possible in the usage scenario of CBDC, and could thus constitute a point of weakness.

Finality: Crucial in a financial services context. The use of a notary node ensures tx finality in Corda, with a notary signature indicating that input states are thus far unspent. Fabric's orderer node orders transactions into a block, and sends it out to channel participants for commitment to the shared channel ledger. The tx is finalized upon commitment. The Raft consensus method tried alongside Quorum relies on a consensus leader to commit blocks to the chain after verification. Once a block has been committed the chain cannot be reversed and finality is thus achieved.

TOP CRYPTO PERFORMANCE SUMMARY

Name	Price	7D%	Vol.	7D%	Mkt Cap.	% Total Mkt
BTC	\$3,673.84	0.33%	42.37bn	19.88%	65.45bn	52.21%
ETH	\$133.60	10.81%	22.52bn	34.28%	14.01bn	11.35%
XRP	\$0.30	-0.77%	3.15bn	9.32%	12.50bn	10.13%
LTC	\$43.93	-3.74%	6.69bn	0.45%	2.66bn	2.15%
EOS	\$2.88	4.42%	6.70bn	50.73%	2.61bn	2.12%
BCH	\$124.69	-0.42%	1.84bn	16.29%	2.20bn	1.78%
USDT	\$1.00	-0.50%	35.24bn	29.47%	2.02bn	1.64%
TRX	\$0.02	-7.58%	0.83bn	-30.64%	1.59bn	1.29%
XLM	\$0.08	0.12%	0.98bn	28.09%	1.53bn	1.24%
BNB	\$9.22	-0.57%	0.46bn	-27.46%	1.30bn	1.05%

CHART OF THE WEEK

A Brief Summary and Comparison of Corda, Fabric, and Quorum

Aspect	Corda	Fabric	Quorum
Privacy	Consensus only on individual agreements, Not on whole ledger	Channels as data partitioning mechanism	Private state trees and zero knowledge proofs
Scalability & Performance	Not a proper blockchain, thus easier to scale	Number of channels required increases with each new participant	Vastly superior to Ethereum, but zero knowledge proofs possible bottleneck
Resiliency	Use of a single notary node (e.g. central bank) can be point of weakness	Use of single ordering node is possible point of weakness	Strength of a global distributed blockchain, yet Raft leader possible point of weakness
Finality	Achieved via notary node	Finality achieved within channels	Finality achieved by Raft consensus leader
Notable Prototypes	Jasper 2, Jasper 3, Ubin 2, Stella 2	Stella 1, Stella 2, Ubin 2	Ubin 2, Khokha, Stella 2, JPMorgan Coin

NETWORK FUNDAMENTALS

	BTC	ETH
Hashrate	43,887,003 TH/s (-1.3%)	138,734 GH/s (+0.5%)
# Wallet Users	33,225,824 (+0.5%)	56,955,494 (+0.5%)
Top 3 Miners	BTC.com (20%) AntPool (11%) F2Pool (11%)	Ethermine (29%) SparkPool (16%) NanoPool (14%)

TOP CRYPTO NEWS AT A GLANCE

Bitmain announces BM1397, the next generation of 7 nanometer ASIC mining chips: The new mining hardware can mine Bitcoin and Bitcoin Cash, and promises energy savings of 28.6% during mining. The chip will be manufactured by Taiwan Semiconductor Manufacturing Company (TSMC), and will be featured in the new Antminer devices S17 and T17. Expect more details on these in the future.

Bitcoin transaction fees hit 2014 level: Research firm Diar recently stated in a report that "Median Fees are also at levels not seen since 2015 despite the total monthly Bitcoins moved on-chain standing at higher levels than seen throughout most of 2018." Diar also reports that Binance's BTC/USD market has shrunk more than 40 percent since December 2018.

Luxembourg passes blockchain framework bill into law: The law aims to enhance the transparency and legal certainty in securities' circulation. Transfer of securities is expected to become more efficient, as the number of required intermediaries is reduced.

New regulations in trading crypto futures in Indonesia: Crypto futures exchanges must be registered and approved by the Indonesian Commodity Futures Trading Regulatory Agency prior to commencing operations.

Investor Tim Draper comments on fiat usage in Fox Business interview: Draper stated that he expects fiat money to be obsolete in five years, and that "criminals will still want to operate with cash, because they catch everybody who is trying to use Bitcoin."

Argentina uses Bitcoin to settle export deal with Paraguay: Paraguay purchased pesticides and fumigation products from Argentina, and Argentina used Bitex to facilitate the Bitcoin payments.

STANDARD KEPLER

WEEKLY SUMMARY | 11 – 17 FEBRUARY

DISCLAIMER

Abbreviations: ADA: Cardano; BCH: Bitcoin ABC; BSV: Bitcoin Satoshi Vision; bn: billion; BTC: Bitcoin; Central Bank Digital Currency: CBDC; crypto: cryptocurrencies; DLT: Distributed Ledger Technology; ETH: Ethereum; ICO: Initial Coin Offerings; Market Cap: Market Capitalization; mn: million; Trading Vol.: Trading Volume; tx: transaction(s); US\$: United States Dollars; USDT: USD Tether; XLM: Stellar Lumens; XMR: Monero; XRP: Ripple

Chart of The Week: Sources: Project Ubin Phase 2 whitepaper, Standard Kepler Research

Market Cap & Trading Vol.: Sources: Coinmarketcap, Standard Kepler Research
The horizontal axis represents the week number in 2018. For instance, W41 indicates the forty first week in 2018. W1 indicates the first week in 2019. The primary vertical axis represents total market capitalization; and the secondary vertical axis represents total trading volume.

Network Fundamentals: Sources: Blockchain.com, Blocktrail, Etherchain.org, Etherscan.io, Standard Kepler Research

Thought of The Week: Sources: Quorum whitepaper, Project Jasper 1 whitepaper, Project Jasper 2 whitepaper, Project Jasper 3 whitepaper, Project Ubin 1 whitepaper, Project Ubin 2 whitepaper, Stella 1 whitepaper, Stella 2 whitepaper, Project Khokha whitepaper, Standard Kepler Research

Top Crypto News At a Glance: Sources: Blockcast.it, CCN, Coindesk, Cointelegraph, Standard Kepler Research

Top Crypto Performance Summary: Sources: Coinmarketcap, Standard Kepler Research

Week Ahead: Sources: Cryptocalendar.pro, Standard Kepler Research

Weekly Recap: Sources: Coinmarketcap, Standard Kepler Research

Past performance does not guarantee future results.

Opinions and estimates offered constitute our judgment and are subject to change without notice, as are statements of financial market trends, which are based on current market conditions. We believe the information provided here is reliable, but do not warrant its accuracy or completeness. This material is not intended as an offer or solicitation for the purchase or sale of any cryptocurrencies. The views and strategies described may not be suitable for all investors. This material has been prepared for informational purposes only, and is not intended to provide, and should not be relied on for, accounting, legal or tax advice. Any forecasts contained herein are for illustrative purposes only and are not to be relied upon as advice or interpreted as a recommendation.

The price of Bitcoin and other cryptocurrencies are highly volatile in nature. It is suggested that clients should perform their own due diligence and consult a fully qualified independent professional financial adviser before making any investments in cryptocurrencies.

©Standard Kepler, February 2019.

Unless otherwise stated, all data is as of February 17, 2019 or as of most recently available.

ABOUT STANDARD KEPLER

Standard Kepler is Asia's leading blockchain financial services provider, offering market changing research insights, in addition to holistic advisory, brokerage, and custodian services. We take great pride in being able to offer professional services that are trusted for our honesty and driven by technology. Headquartered in Hong Kong, Standard Kepler's management team previously served in JP Morgan, Macquarie Capital, State Street, and KPMG.

Standard Kepler's research insights are distributed in collaboration with several partners, including Thomson Reuters, BTC.com, and Binance. If you are interested in exploring more of our research insights, or becoming one of our research distribution partners, visit www.standardkepler.com/research or contact us directly at research@standardkepler.com.