DIGITAL ASSET RESEARCH

Industry Report – 7.15.19

Greg Cipolaro
gregory.cipolaro@digitalassetresearch.com

Lucas Nuzzi
lucas.nuzzi@digitalassetresearch.com

2Q19 REVIEW OF CRYPTO MARKETS

AT LEAST ONE OF THE ANALYSTS PARTICIPATING IN THE PREPARATION OF THIS REPORT OWNS BITCOIN, ETHEREUM, AND ZCASH. YOU ARE RESPONSIBLE FOR DETERMINING WHETHER ANYTHING CONTAINED HEREIN IS SUITABLE FOR YOUR PARTICULAR CIRCUMSTANCES, AND FOR SEEKING PROFESSIONAL TAX, LEGAL, AND/OR INVESTMENT ADVICE AS APPROPRIATE. PLEASE SEE THE OTHER DISCLOSURES AT THE END OF THIS REPORT.

SUMMARY

- The story of the quarter was the resurgence in crypto markets driven by price appreciation in the largest asset, Bitcoin.
- While the rally was initially sparked by a breach of technical barrier for BTC and subsequent short covering, we believe the rally has been sustained by new money coming into the ecosystem using Tether outstanding as a proxy.
- There has been a growing thread of macro-economic factors that should be a tailwind for the price of Bitcoin, but short-term correlations are weak in our opinion.
- We think our work around drawdowns and halving cycles that are specific to Bitcoin and crypto are much more powerful explanations for the recent market upturn.
- In addition, there were several notable events, like mainnet launches and partnership announcements, that drove returns in the quarter. Our work in this area continues to show that events drive alpha in this industry.
- Looking ahead, we don't see anything to change the narrative in the favor of alts as a category but are watching closely the Litecoin halving, Ycash fork of Zcash, Ethereum Classic Atlantis update as well as legal updates on NYAG and iFinex.

OVERVIEW

Without a doubt, the story of the quarter was the resurgence over overall digital asset prices following a tough 2018 and a rocky 1Q19. It started right at the beginning of the quarter on April 2nd, with Bitcoin punching through some widely believed technical resistance levels and ended with 30% sell off after Bitcoin rallied all the way to $13,868, a level not seen since the end of 2017. Make no doubt about it, this was a Bitcoin dominated quarter, with the blue-chip digital asset outpacing nearly every digital asset we track, except for five. While the media scrambled to backfill a reason for the rally from

quantitative trading algorithms to the upcoming (May 2020) reward halving to incoming institutional capital, a few threads seem to have merit: increasing expectations of interest rate cuts at central banks around the world, correlations with Bitcoin and other positive risk carry trade investments, and the amount of Tether in circulation as a measure of fiat coming into the ecosystem.

But the quarter wasn't all Bitcoin. We had numerous legal and regulatory developments, both encouraging and worrisome, a retrenching of digital asset exchanges that serve US based clients, the launch of a digital asset by the world's large social network, Facebook, and numerous individual project updates.

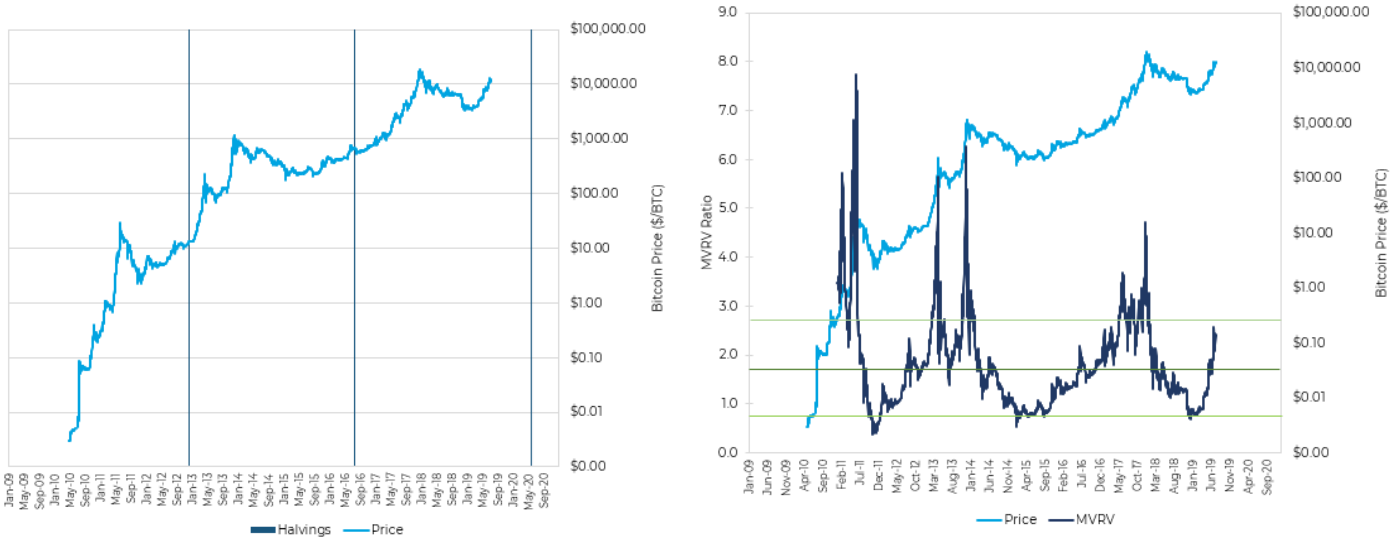
MARKET RALLY AND CYCLES

Without a doubt, the story of the quarter has been the price appreciation in crypto markets lead by Bitcoin. A jump through the $4,200 level, a price viewed as a ceiling by many investors, on April 2nd brought with it significant trading volume and talk of "a cyclical bottom had been formed." We wrote about it in-depth and concluded that while no new fundamental events had occurred, indeed the cycle low had likely been put in and that were most likely entering a new price cycle that has coincided with halving events.

We think about investing in digital assets in three different time intervals: short (< 1 month), intermediate (1 month – 12 months), and long-time horizons (1-4 years).

On the **long-term** horizon, prices appear to be parabolically cyclically determined by Bitcoin halving events that occur roughly every 4 years (210,000 blocks). In addition, the Market-Value-to-Realized Value (MVRV) ratio, a measure of current market cap to the cumulative value of all on-chain transaction priced at the point they last moved, appears to give ballpark estimates of over and "under valudeness".

FIGURE 1 – *LONG TERM INDICATORS: HALVINGS AND MVRV*



Source: Digital Asset Research, Coin Metrics

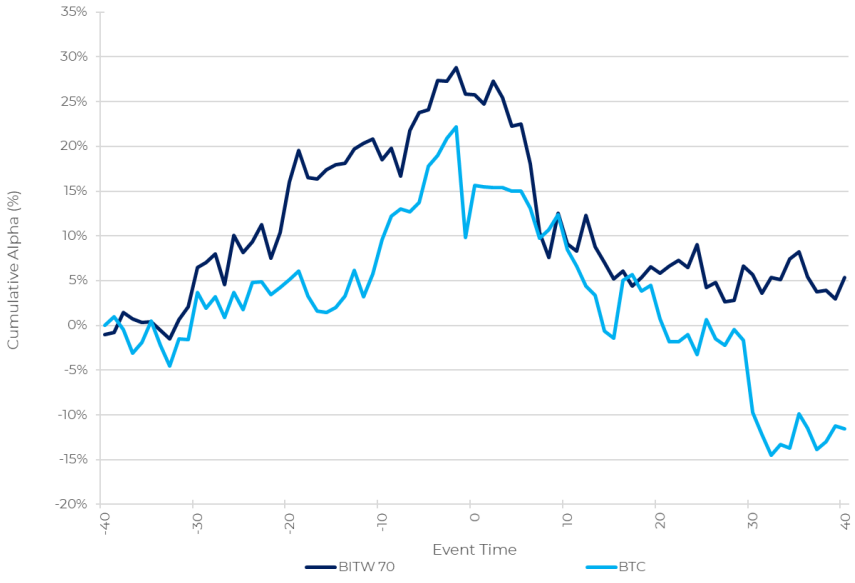
On the **intermediate term** horizon, returns appear to be driven by capital flows, in and out, and narratives. Currently, the narrative of Store-of-Value appears to be driving Bitcoin price, while Capital Formation and Exchange appear to be driving exchange tokens, like Binance Coin. In comparison, the dominant narrative in 2017 was Capital Formation (i.e. ICOs) enabled by Ethereum. For capital flows, we track the amount of Tether outstanding as a proxy for fiat coming into crypto.

FIGURE 2 – *INTERMEDIATE TERM INDICATOR, TETHER OUTSTANDING*

Source: Digital Asset Research, TradingView

On the **short term,** we have found that news and events have been significant sources of returns, like mainnet launches. We suspect there are other short-term price momentum (1-3 days) factors but have not unearthed any conclusive proof.

FIGURE 3 – *MEDIAN RETURNS FOR MAINNET LAUNCHES*



Source: Digital Asset Research

COMP SHEET UPDATE

We have updated our comp sheet to better reflect current market dynamics, removing digital assets below $20M in network value, adding new launches, and creating a new stablecoin segment.

FIGURE 4 – *DAR'S DIGITAL ASSET COMP SHEET*

DIGITAL ASSET RESEARCH – CAP COMP SHEET

($ per token price, M of USD)
6/30/2019

			Tokens Outstanding		Network Value										Performance			
Name	Ticker	Price	Free Float	Total	Free Float	Total	Protocol Phase	Avg Daily Volume	Target Block Creation Time	Annualized Inflation Rate	Blockchain Base	Consensus Mechanism	Hash Algorithm	Category	Subcategory	WTD	MTD	QTD	YTD
Digital Currencies																			
Bitcoin	BTC	$11,620.87	17.8	17.8	$206,832	$206,832	Released	$22,407	10 Minutes	3.7%	Bitcoin	Proof of Work	SHA-256	Currency	General	5.2%	26.2%	163.5%	189.0%
Ripple	XRP	$0.40	42,566.6	99,991.6	$16,833	$39,543	Released	$1,701	3.5 Seconds	0.0%	Ripple	Practical Byzantine Fault Tolerant	N/A	Currency	General	-3.2%	-9.6%	28.2%	12.4%
Litecoin	LTC	$123.18	62.5	62.5	$7,701	$7,701	Released	$4,496	2.5 Minutes	8.4%	Bitcoin	Proof of Work	Scrypt	Currency	General	7.1%	6.7%	101.2%	301.2%
Bitcoin Cash	BCH	$413.80	17.9	17.9	$7,396	$7,396	Released	$1,866	10 Minutes	3.7%	Bitcoin	Proof of Work	SHA-256	Currency	General	0.9%	-10.2%	136.5%	164.5%
Bitcoin SV	BSV	$201.88	17.9	17.9	$3,605	$3,605	Released	$494	10 Minutes	3.7%	Bitcoin	Proof of Work	SHA-256	Currency	General	3.2%	-0.8%	198.9%	128.6%
Stellar	XLM	$0.10	19,425.0	105,122.7	$1,989	$10,767	Released	$390	4 Seconds	0.0%	Stellar	Fed Byzantine Agreement	FBA	Currency	General	-4.8%	-21.9%	-3.1%	-7.5%
Dash	DASH	$158.83	8.9	8.9	$1,414	$1,414	Released	$330	2.6 Minutes	8%	Litecoin	Proof of Work	X11	Currency	General	2.5%	-5.3%	44.7%	97.9%
IOTA	MIOTA	$0.39	2,779.5	2,779.5	$1,097	$1,097	Beta	$30	N/A	N/A	Directed Acyclic Graph	Tangle	N/A	Currency	General	0.5%	-23.0%	27.5%	10.0%
Bitcoin Gold	BTG	$27.62	17.5	17.5	$484	$484	Released	$23	10 Minutes	3.8%	Bitcoin	Proof of Work	Equihash	Currency	General	5.3%	-11.9%	101.8%	107.0%
Dogecoin	DOGE	$0.00	120,205.3	120,205.3	$397	$397	Released	$54	1 Minute	4%	Litecoin	Proof of Work	Scrypt	Currency	General	0.0%	-5.3%	56.6%	38.9%
Decred	DCR	$31.41	10.0	10.0	$315	$315	Released	$8	5 Minutes	23%	Decred	Hybrid PoW/PoS	Blake 256	Currency	General	2.0%	8.2%	50.6%	84.1%
HyperCash	HC	$5.06	43.5	43.5	$220	$220	Alpha	$21	Unknown	Unknown	Unknown	Hybrid PoW/PoS	HSR	Currency	General	19.7%	152.7%	217.2%	417.5%
Nano	NANO	$1.23	133.2	133.2	$164	$164	Released	$10	N/A	N/A	Directed Acyclic Graph	N/A	N/A	Currency	General	-1.5%	-28.9%	11.8%	36.1%
MonaCoin	MONA	$2.39	65.7	65.7	$157	$157	Released	$21	1.5 Minutes	13%	Bitcoin	Proof of Work	Lyra2REv2	Currency	General	-2.7%	15.0%	385.9%	291.8%
DigiByte	DGB	$0.01	11,990.4	11,990.4	$144	$144	Released	$2	15 Seconds	14%	Bitcoin	Proof of Work	SHA-256, Scrypt	Currency	General	-1.8%	-20.9%	-4.6%	15.0%
Vertcoin	VTC	$0.46	50.2	50.2	$23	$23	Released	$2	2.5 Minutes	10%	Bitcoin	Proof of Work	Lyra2REv2	Currency	General	-8.2%	11.2%	-4.0%	101.8%
Privacy Currencies																			
Monero	XMR	$90.76	17.1	17.1	$1,549	$1,549	Released	$161	2 Minutes	10%	CryptoNote	Proof of Work	CrytpoNight	Currency	Privacy	-2.5%	-5.9%	57.0%	89.8%
Zcash	ZEC	$102.86	6.9	6.9	$710	$710	Released	$419	2.5 Minutes	38%	Zcash	Proof of Work	Equihash	Currency	Privacy	-1.0%	13.7%	75.8%	81.9%
Bytecoin	BCN	$0.00	184,066.8	184,066.8	$171	$171	Released	$0	2 Minutes	0%	CryptoNote	Proof of Work	CryptoNight	Currency	Privacy	-2.0%	-13.1%	24.1%	28.2%
Komodo	KMD	$1.54	114.9	114.9	$177	$177	Released	$5	1.33 Minutes	1%	Komodo	Proof of Work	Equihash	Currency	Privacy	38.4%	-4.9%	21.4%	66.6%
Verge	XVG	$0.01	15,803.6	15,803.6	$119	$119	Released	$3	30 Seconds	10%	Verge	Proof of Work	Multiple	Currency	Privacy	-3.7%	-22.3%	3.8%	13.1%
PIVX	PIVX	$0.64	56.8	56.8	$36	$36	Released	$3	1 Minute	5%	Dash	Proof of Stake	Quark	Currency	Privacy	5.3%	-13.4%	-33.9%	-27.8%
Smart Contract Platforms																			
Ethereum	ETH	$293.52	106.8	106.8	$31,337	$31,337	Released	$8,676	15 Seconds	5.9%	Ethereum	Proof of Work	Ethash	Platform	Smart Contract	-0.1%	8.4%	105.4%	118.0%
EOS	EOS	$5.89	921.9	1,018.6	$5,432	$6,002	Released	$2,505	0.5 Seconds	0.0%	EOS	Delegated Proof of Stake	N/A	Platform	Smart Contract	0.7%	-32.2%	38.0%	124.5%
TRON	TRX	$0.03	66,682.1	99,281.3	$2,136	$3,180	Released	$773	15 Seconds	0.0%	Ethereum	Delegated Proof of Stake	N/A	Platform	Smart Contract	0.2%	-3.3%	35.8%	69.7%
Cardano	ADA	$0.08	25,927.1	31,112.5	$2,057	$2,468	Beta	$174	2 Minutes	N/A	Cardano	Proof of Stake	Ouroboros	Platform	Smart Contract	-8.2%	-8.2%	17.7%	99.9%
NEO	NEO	$17.51	70.5	100.0	$1,235	$1,751	Released	$587	15 Seconds	N/A	NEO	Del Byz Fault Tolerance	N/A	Platform	Smart Contract	2.9%	23.1%	67.8%	121.9%
Ethereum Classic	ETC	$7.94	111.7	111.7	$887	$887	Released	$764	15 Seconds	7.5%	Ethereum	Proof of Work	Ethash	Platform	Smart Contract	4.2%	-10.7%	60.4%	53.1%
NEM	XEM	$0.09	9,000.0	9,000.0	$825	$825	Released	$34	1 Minute	0.0%	NEM	Proof of Importance	SHA-3	Platform	Smart Contract	3.0%	-7.7%	64.0%	41.4%
Tezos	XTZ	$1.27	657.9	799.8	$835	$1,015	Beta	$7	1 Minute	0%	Tezos	Delegated Proof of Stake	N/A	Platform	Smart Contract	31.7%	-38.1%	-11.9%	101.9%
Qtum	QTUM	$5.05	95.8	101.6	$484	$513	Beta	$322	2.42 Minutes	0.9%	Hybrid: Bitcoin / Ethereum	Proof of Stake	N/A	Platform	Smart Contract	16.2%	48.6%	67.9%	128.8%
Lisk	LSK	$1.69	118.3	133.4	$200	$225	Released	$10	10 Seconds	10.7%	Crypti	Delegated Proof of Stake	N/A	Platform	Smart Contract	-7.7%	-13.9%	3.5%	34.6%
Waves	WAVES	$1.87	100.0	100.0	$187	$187	Released	$25	1 Minute	0%	Waves	Leased Proof of Stake	N/A	Platform	Smart Contract	-1.1%	-30.7%	-34.4%	-43.3%
Zilliqa	ZIL	$0.02	8,687.4	12,533.0	$140	$202	Released	$43	Minutes, 24 Second	N/A	Zilliqa	Hybrid PoW/pBFT	Ethash	Platform	Smart Contract	-2.5%	-22.3%	3.8%	13.1%
Nexus	NXS	$0.30	63.5	63.5	$19	$19	Beta	$0	Variable	N/A	Peercoin	Hybrid PoW/PoS	SHA-256	Platform	Smart Contract	-6.6%	-18.3%	-26.8%	-11.5%
Platforms																			
Cosmos	ATOM	$5.59	190.7	237.9	$1,066	$1,330	Released	$72	6.5 Seconds	9.7%	Cosmos	Delegated Proof of Stake	N/A	Platform	Interoperability	1.6%	-6.9%	49.4%	0.0%
Bitshares	BTS	$0.06	2,731.6	2,731.6	$162	$162	Released	$8	3 Seconds	0%	Bitshares	Delegated Proof of Stake	N/A	Platform	General	-5.4%	-12.9%	1.1%	58.3%
Bytom	BTM	$0.17	1,002.5	1,407.0	$169	$237	Beta	$36	15 Seconds	0%	Bytom	Proof of Work	Ethash	Platform	Interoperability	8.3%	20.4%	40.7%	101.5%
ICON	ICX	$0.31	473.4	800.5	$148	$251	Beta	$13	5 Minutes	N/A	ICON	Fed Byzantine Agreement	LoopChain	Platform	Interoperability	2.2%	-23.3%	-11.5%	29.5%
AION	AION	$0.12	327.3	327.3	$41	$41	Beta	$3	10 Seconds	1%	AION	Proof of Work	Equihash	Platform	Interoperability	-2.4%	-46.2%	-27.9%	-12.3%
Nxt	NXT	$0.03	999.0	999.0	$30	$30	Released	$1	1 Minute	0%	Nxt	Proof of Stake	N/A	Platform	General	-12.6%	-8.5%	-0.7%	13.0%
Stablecoins																			
Tether	USDT	$1.00	3,664.0	4,020.1	$3,681	$4,039	Released	$21,697	N/A	N/A	Multiple	Varies	N/A	Currency	Stable	1.9%	-0.8%	-0.8%	-1.7%
USD Coin	USDC	$1.00	366.6	367.7	$366	$367	Released	$135	15 Seconds	N/A	Ethereum (ERC20)	Proof of Work	Ethash	Currency	Stable	-0.4%	0.0%	0.0%	-2.0%
TrueUSD	TUSD	$1.00	215.8	215.8	$216	$216	Released	$225	15 Seconds	N/A	Ethereum (ERC20)	Proof of Work	Ethash	Currency	Stable	-0.1%	0.0%	-1.0%	-1.0%
Paxos Standard	PAX	$1.00	158.6	158.7	$158	$159	Released	$163	15 Seconds	N/A	Ethereum (ERC20)	Proof of Work	Ethash	Currency	Stable	-0.4%	0.0%	0.0%	-1.0%

DIGITAL ASSET RESEARCH – COMP SHEET

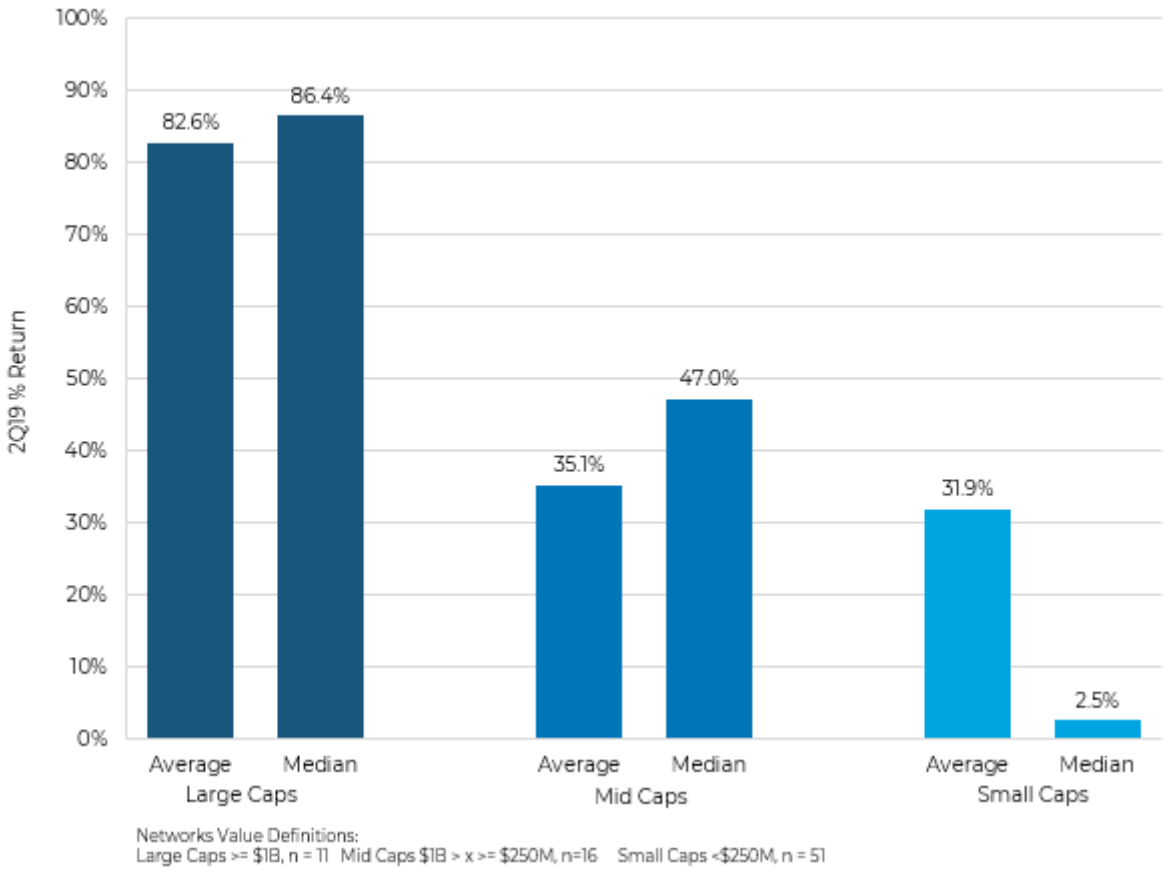
($ per token price, M of USD)
6/30/2019

Name	Ticker	Price	Tokens Outstanding		Network Value		Protocol	Avg Daily	Target Block	Annualized	Blockchain	Consensus	Hash	Category	Subcategory	Performance			
			Free Float	Total	Free Float	Total	Phase	Volume	Creation Time	Inflation Rate	Base	Mechanism	Algorithm			WTD	MTD	QTD	YTD
Advertising																			
Basic Attention Token	BAT	$0.30	1,273.0	1,500.0	$376	$443	Alpha	$43	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Advertising	3.3%	-15.5%	1.8%	129.6%
BaaS																			
Ontology	ONT	$1.43	120.1	1,000.0	$707	$1,429	Released	$168	10 Seconds	N/A	NEO	Del Byz Fault Tolerance	N/A	Platform	Blockchain-As-A-Service	-0.9%	-7.2%	9.2%	139.9%
VeChain	VET	$0.01	55,454.7	86,712.6	$414	$648	Beta	$50	15 Seconds	0.0%	Ethereum	Proof of Authority (pBFT)	N/A	Platform	Blockchain-As-A-Service	-2.5%	5.5%	32.9%	104.4%
Stratis	STRAT	$0.89	99.4	99.4	$88	$88	Released	$4	1 Minute	1%	Bitcoin	Hybrid PoW/PoS	SHA-256	Platform	Blockchain-As-A-Service	4.2%	-13.7%	-12.9%	-19.7%
Factom	FCT	$5.23	9.7	9.7	$50	$50	Beta	$1	10 Minutes	N/A	Bitcoin	Proof of Work	SHA-256	Application Specific	Blockchain-As-A-Service	-6.4%	-35.5%	-24.5%	-36.5%
Compute																			
Golem	GNT	$0.09	964.5	1,000.0	$92	$95	Alpha	$3	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Computation	9.5%	-3.6%	2.5%	37.9%
iExec RLC	RLC	$0.36	80.1	87.0	$29	$31	Beta	$1	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Computation	-0.2%	-14.9%	-22.0%	104.8%
DAO																			
DigiDAO	DGD	$24.94	2.0	2.0	$50	$50	Released	$3	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	DAO	-6.6%	-29.4%	34.6%	46.9%
Debit & Credit Card																			
Ark	ARK	$0.44	113.3	142.6	$50	$63	Released	$1	8 Seconds	7%	Lisk	Delegated Proof of Stake	N/A	Application Specific	Debit/Credit Card	0.2%	-27.0%	-37.3%	17.9%
TenX	PAY	$0.19	114.5	205.2	$22	$39	Beta	$1	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Debit/Credit Card	-3.9%	-17.6%	-33.8%	-18.4%
Metal	MTL	$0.56	45.1	66.6	$25	$38	Beta	$5	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Debit/Credit Card	4.3%	14.2%	-8.7%	112.1%
Exchange																			
Binance Coin	BNB	$33.32	141.2	189.2	$4,704	$6,304	Released	$402	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Exchange	-1.5%	-0.9%	86.4%	426.6%
Leo Token	LEO	$1.79	999.5	999.5	$1,788	$1,788	Beta	$11	15 Seconds	N/A	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Exchange	2.6%	17.3%	0.0%	0.0%
Raven Coin	RVN	$0.05	3,903.5	3,903.5	$209	$209	Released	$24	1 Minute	67%	Raven Coin	Proof of Work	X16R	Application Specific	Exchange	-0.8%	-13.3%	-13.9%	307.1%
0x	ZRX	$0.29	597.8	1,000.0	$175	$293	Beta	$24	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Exchange	-5.0%	-22.3%	3.8%	13.1%
Kyber Network	KNC	$0.24	168.5	214.3	$40	$51	Beta	$5	15 Seconds	N/A	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Exchange	-1.0%	-8.8%	-10.6%	62.3%
Bancor	BNT	$0.72	63.2	70.3	$45	$50	Released	$2	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Exchange	-0.7%	-4.5%	12.1%	14.4%
Polymath	POLY	$0.08	429.3	1,000.0	$35	$82	Beta	$7	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Exchange	1.0%	-17.5%	-27.4%	-39.5%
Populous	PPT	$0.64	53.3	53.3	$34	$34	Beta	$4	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Factoring	-8.2%	-40.8%	-60.7%	-58.8%
Fund Management																			
Iconomi	ICN	$0.27	98.9	98.9	$27	$27	Beta	$0	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Fund Management	-17.0%	1.2%	104.9%	26.6%
Gaming																			
FunFair	FUN	$0.00	6,548.9	10,999.9	$27	$45	Alpha	$2	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Gaming	-21.9%	-30.4%	-6.6%	17.3%
Identity Management																			
Metaverse ETP	ETP	$1.77	71.8	76.0	$127	$135	Beta	$49	24 Seconds	5%	Metaverse	Hybrid PoW/PoS	Ethash	Application Specific	Identity	-7.3%	53.4%	177.8%	204.5%
Civic	CVC	$0.07	342.7	1,000.0	$24	$71	Beta	$5	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Identity	0.8%	-16.1%	-17.0%	38.1%
Network Complements																			
Chainlink	LINK	$3.43	350.0	1,000.0	$1,199	$3,426	Released	$165	15 Seconds	N/A	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Network Compliment	54.5%	238.2%	579.7%	1091.9%
Ardor	ARDR	$0.12	999.0	999.0	$116	$116	Released	$4	1 Minute	0%	Nxt	Proof of Stake	SHA-256	Application Specific	Network Compliment	8.5%	31.8%	36.6%	119.5%
Gas	GAS	$3.12	10.1	17.2	$32	$54	Released	$4	15 Seconds	138%	NEO	Del Byz Fault Tolerance	DBFT	Application Specific	Network Compliment	-7.0%	-3.9%	8.5%	49.1%
Prediction Markets																			
Augur	REP	$14.62	11.0	11.0	$161	$161	Beta	$10	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Prediction Markets	-14.2%	-20.3%	1.6%	100.4%
Gnosis	GNO	$23.18	1.1	10.0	$26	$232	Beta	$0	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Prediction Markets	7.0%	-12.9%	45.6%	109.5%
Social																			
Steem	STEEM	$0.35	322.8	339.8	$114	$119	Released	$2	1-3 Seconds	0%	Steem	Delegated Proof of Stake	N/A	Application Specific	Social	-3.5%	-11.4%	-22.2%	36.3%
ReddCoin	RDD	$0.00	28,808.7	28,808.7	$57	$57	Beta	$1	1 Minute	0%	ReddCoin	Proof of Stake Velocity	N/A	Application Specific	Social	-4.2%	7.7%	46.3%	49.8%
Storage																			
BitTorrent	BTT	$0.00	212,116.5	990,000.0	$289	$1,349	Beta	$66	15 Seconds	N/A	TRON (TRC10)	Delegated Proof of Stake	N/A	Application Specific	Storage	12.1%	-16.1%	75.2%	0.0%
Siacoin	SC	$0.00	41,343.1	41,343.1	$129	$129	Beta	$2	10 Minutes	20%	Siacoin	Proof of Work	Blake (2b)	Application Specific	Storage	1.2%	-8.7%	15.2%	20.0%
Maidsafe	MAID	$0.22	452.6	452.6	$100	$100	Beta	$1	N/A	8%	Omni	Proof of Resource	N/A	Application Specific	Storage	8.8%	-4.7%	69.6%	60.6%
Storj	STORJ	$0.25	135.8	425.0	$34	$108	Released	$7	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Storage	7.4%	-6.8%	-19.2%	82.7%
Videogames																			
Enjin	ENJ	$0.12	775.7	1,000.0	$92	$119	Released	$8	15 Seconds	N/A	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Gaming	1.8%	-22.7%	-18.9%	224.6%
Wallet																			
Status	SNT	$0.03	3,470.5	6,804.9	$95	$186	Beta	$20	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Wallet	-0.7%	-6.4%	7.6%	56.7%
Other																			
MakerDAO	MKR	$643.15	1.0	1.0	$643	$643	Released	$3	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	Governance	0.3%	-10.9%	-7.5%	44.0%
Walton	WTC	$1.98	41.7	70.0	$83	$139	Pre-Alpha	$7	15 Seconds	0%	Ethereum (ERC20)	Proof of Work	Ethash	Application Specific	RFID	39.9%	-40.9%	-15.2%	23.0%

RETURNS BY NETWORK VALUE

We segment the crypto universe into three buckets; large caps (>= $1B network value), mid caps ($1B > x >= $250M in network value) and small caps (<$250M in network value). Interestingly, the market rally this quarter has been driven by large caps, predominately Bitcoin. This is something we saw in rally off the 2015 lows that lead into the 2017 market highs – Bitcoin lead tokens that survived the 2013 market highs (many did not survive) like Litecoin and Ripple/XRP. Observationally, it wasn't until gains were made in Bitcoin that money then spilled out into other digital assets so perhaps we will see something similar this cycle.

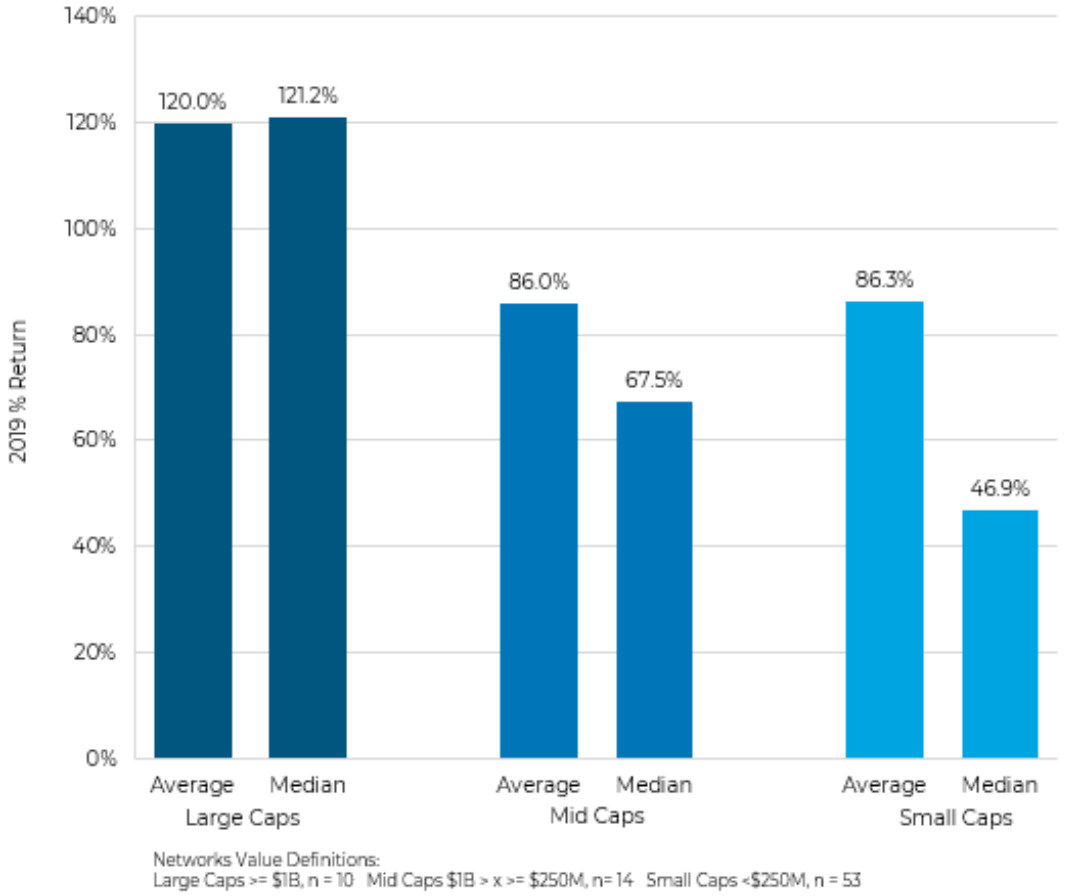
FIGURE 5 – *2Q19 RETURNS BY NETWORK VALUE*



Source: Digital Asset Research

2019 year to date returns look like 2Q19, with large caps outperforming mid caps, and mid caps outperforming small caps. One of our beliefs learned from the 2013 market peak and subsequent drawdown is that over the long term digital assets will exhibit VC style returns, whereby most digital assets will be worth very little or zero, some will exhibit some value capture, and the ones that really find product/market fit will generate significant returns and hold most of the value within the overall ecosystem.

FIGURE 6 – *2019 RETURNS BY NETWORK VALUE*

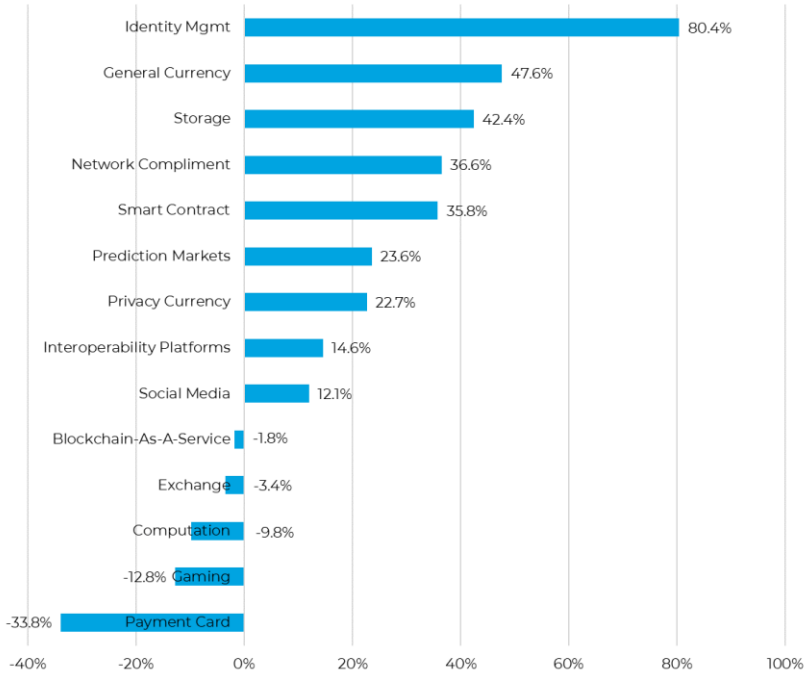


Source: Digital Asset Research

RETURNS BY SECTOR

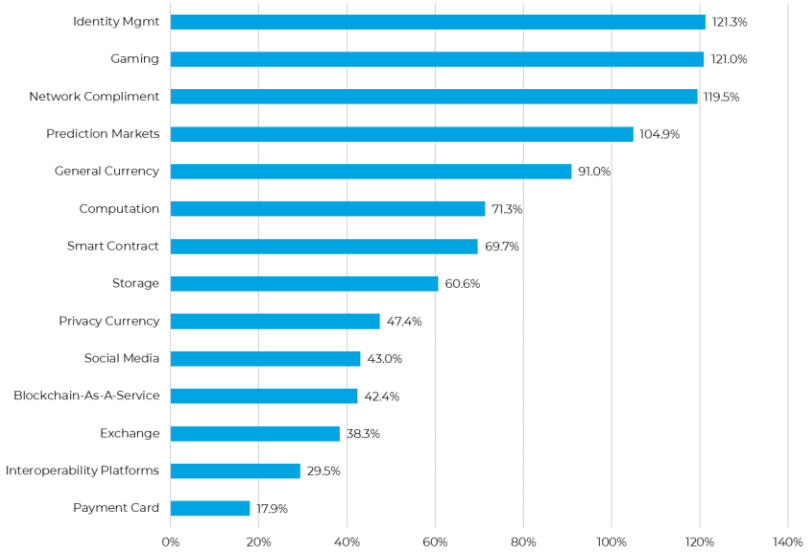
In 2Q19, Identity Management, General Currency and Storage sectors outperformed on a relative basis. Payment Card, Gaming, and Computation sectors underperformed during the quarter. For 2019, Identity Management, Gaming, and Network Compliment outperformed while Payment Card, Interoperability, and Exchange sectors underperformed. In the Exchange sector, Binance Coin and Raven Coin were notable outperformers but Polymath, 0x, and Bancor were significant drags on the sector.

FIGURE 7 – *2Q19 RETURNS BY SECTOR*



Source: Digital Asset Research

FIGURE 8 – *2019 RETURNS BY SECTOR*



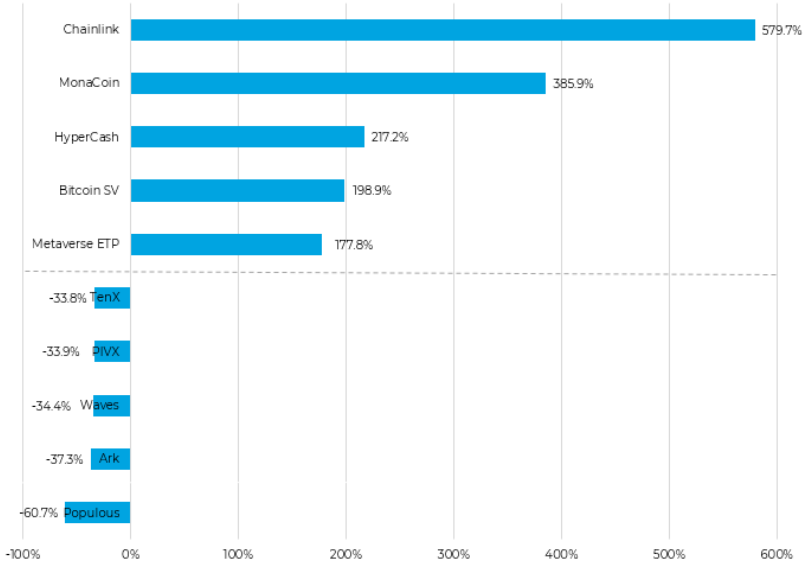
Source: Digital Asset Research

RETURNS BY INDIVIDUAL DIGITAL ASSETS

For 2Q19, Chainlink, which underwent a mainnet launch at the end of May and then was listed on Coinbase and integrated with Google's BigQuery on GCPcloud, was the best performer in the quarter. This was followed by MonaCoin, HyperCash, Bitcoin SV, and Metaverse ETP. Sixth in terms of 2Q performance but not pictured was Bitcoin. Underperformers were Populous, Ark, Waves, PIVX, and TenX.

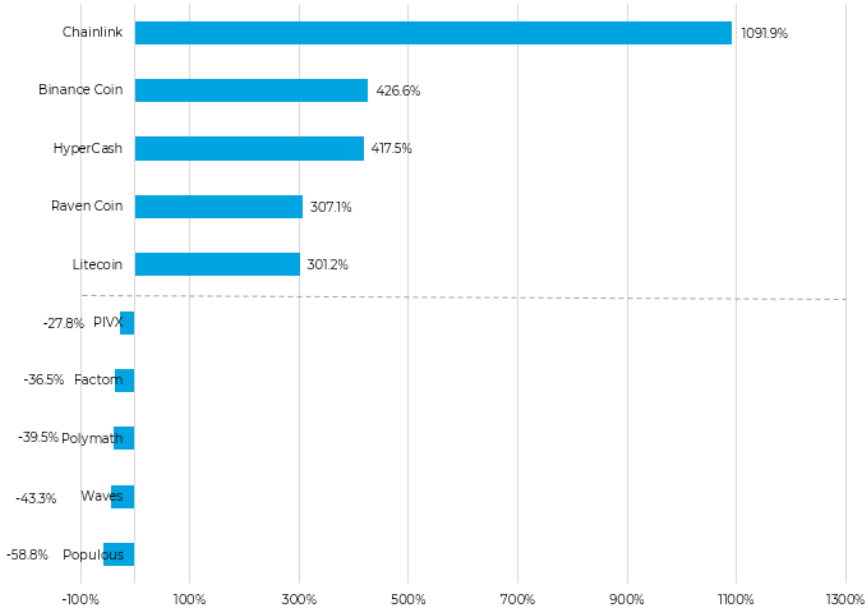
For 2019 year to date, once again Chainlink was the best performer followed by Binance, HyperCash, Raven Coin, and Litecoin. The worst performers were Populous, Waves, Polymath, Factom, and PIVX.

FIGURE 9 – *2Q19 RETURNS BY ASSET*



Source: Digital Asset Research

FIGURE 10 – *2019 RETURNS BY ASSET*



Source: Digital Asset Research

RETRENCH OF US EXCHANGES, BINANCE

One of the dominant threads throughout 2Q was the retrenchment of exchanges that service US-based customers, like Poloniex, Kraken, and Bittrex. In the most severe case, Bittrex, which filed for a BitLicense in 2015 (required to serve New York based customers) was forced to leave New York when its application was rejected by the New York Department of Financial Services (NYDFS). In its rejection, the NYDFS cited numerous deficiencies in the areas of BSA/AML/OFAC compliance, inadequate capital, and lack of due diligence tokens listed on its platform. While Bittrex vehemently denied the accusations in public response, they were forced to stop serving NY based customers within 24 hours of the announcement.

While not as severe as the NYDFS ejection, other exchanges, like Poloniex and Bittrex began to delist numerous assets available for trading to US based clients. From our vantage point, it appears as though the exchanges are ring fencing or geo fencing clients and assets in response to legal or regulatory uncertainty under US securities laws. This includes the world's largest exchange, Binance, which announced it will cease serving US based customer on September 12th. In a parallel track, Binance has created a US based entity and registered with FinCEN under the name BAM Trading. Our guess is that Binance's US based operation will be up and running and serving US based customers before the September 12th deadline. It's only registered as an MSB in the state of California indicating that either further state approvals are coming, or the service will be limited at the onset. Serving NY based customers may take even longer given the requirement to obtain a BitLicense.

NYAG, BITFINEX, AND TETHER

In April, the New York Attorney General's Office sought to obtain a court order against iFinex Inc, the parent of the Bitfinex exchange and Tether digital asset, to prevent them from violating New York State laws and defrauding New York customers. At issue were $850M of comingled assets that were no longer accessible by their payment provider, Crypto Capital Corp, which were most seized by authorities in Poland, Portugal, and the US. The NYAG sought to prevent the draw of credit facility between Bitfinex and Tether set up so that Bitfinex could continue to process client fiat withdrawals. Shortly after the filing, two individuals that have been connected to Crypto Capital Corp in the past were arrested on charges of opening numerous bank accounts and running a shadow banking operation. While the court battle between iFinex and the NYAG continues today, as a measure to tap liquidity and to take advantage of a novel use case, iFinex sold $1B worth of Leo tokens for use on the Bitfinex platform to access discounted services like reduced trading fees, something pioneered by Binance.

KIN ENFORCEMENT

On June 4th, the SEC sued Kik Interactive, creator of the Kin digital asset, in connection with its 2017 ICO. The SEC alleges that Kik sold the digital asset to US based investors without registering the offering. We warned clients about this offering ahead of the public sale in our pre-ICO report as there were numerous technical, legal, and valuation deficiencies and inaccuracies. While Kik was able to rally some well-known crypto service entities to its aid ahead of the lawsuit, including Coinbase, Circle and Union Square Ventures, that was not enough to ward off the SEC. It will be interesting to watch this legal battle unfold as it could set precedent for other token offerings in the future.

FATF RELEASES FINAL CRYPTO RULES

Intergovernmental organization the Financial Action Task Force (FATF) released final guidelines for digital asset service providers, or virtual asset service providers (VASPs). The FATF is supported by 37 member countries, including the US, and is focused on combating money laundering and terrorism financing so it's no wonder many of the guidelines include identifying real world participants in a digital asset transaction. These details include the sender's and recipient's real-world identity, nationality, and account details. The burden of that information gathering process is on VASPs, like an exchange, and are encouraged to share customer data. While the guidelines aren't binding, countries that fall out of compliance can get blacklisted from outside investment.

LEDGERX, ERISX RECEIVE CFTC APPROVALS, CME CHANGES ETHER REFERENCE RATE

The Commodity Futures Trading Commission (CFTC) approved LedgerX's designated contract market (DCM) license application, which paves the way for physically settled Bitcoin futures. ErisX also received a derivatives clearing organization (DCO) license from the CFTC. While there is still no word on timing of launch of futures products from either LedgerX or ErisX, we view both news items as positives. Finally, while there still is not a CME product launched around ETH yet, the organization did change its reference rate methodology to include itBit trading pairs.

CAPITAL FORMATION

The ICO boom of 2017 proved that capital formation was a new and important use case for crypto, primarily benefitting Ethereum, the substrate on which many of these funds were raised. And while many of the projects could be faulted for lack of basic disclosures and compliance with securities laws, we think capital formation as a crypto use case is here to stay. Case in point are the recent Security Token Offerings or STOs – legally compliant issuances of debt and equity instruments. While the rhetoric about the subject has likely exceeded real world execution, our math suggests $663M has been raised to date for STOs. While this is dwarfed by the tens of billions raised in ICOs, the trend has been on the rise, while ICO volume has dissipated. We expect this trend to continue and explored this in an in-depth report this past quarter. Also, on the rise are IEOs, or Initial Exchange Offerings. These are like 2017 ICOs, except they occur directly on an exchange, like Binance, and typically require the exchange's native token to participate. The dollar amounts of raises are small as well are the participant caps, but we also see this trend growing and believe is could we another value capture mechanism for exchange specific tokens.

TRADING, INVESTING AND SPECULATION

Centralized exchanges, like Binance and Coinbase, have been some of the most profitable businesses within the digital asset ecosystem. After all, the facilitation of trade for investment and speculation has been one of the strongest use cases within crypto. To capitalize on this opportunity in the form of a digital asset, several exchanges created their own tokens which gave owners of the token access to discount exchange services, like reduced margin rates and lower trading fees. We think this is a real-world example of product-market fit for a digital asset. As a further value capture method, many exchanges burn or destroy portions of their tokens' fixed supply in proportion with exchange revenue or profit. Binance has been on the forefront of this movement, and one of the reasons for the appreciation in the price of their token, but other exchanges have followed suit, like Bitfinex with its Leo token. Binance has even gone as far as to create a standalone network, rather than just an ERC20 token on Ethereum, and decentralized exchange for its token. While we won't necessarily see every exchange go to the lengths of Binance, we expect the exchange tokenization trend to continue.

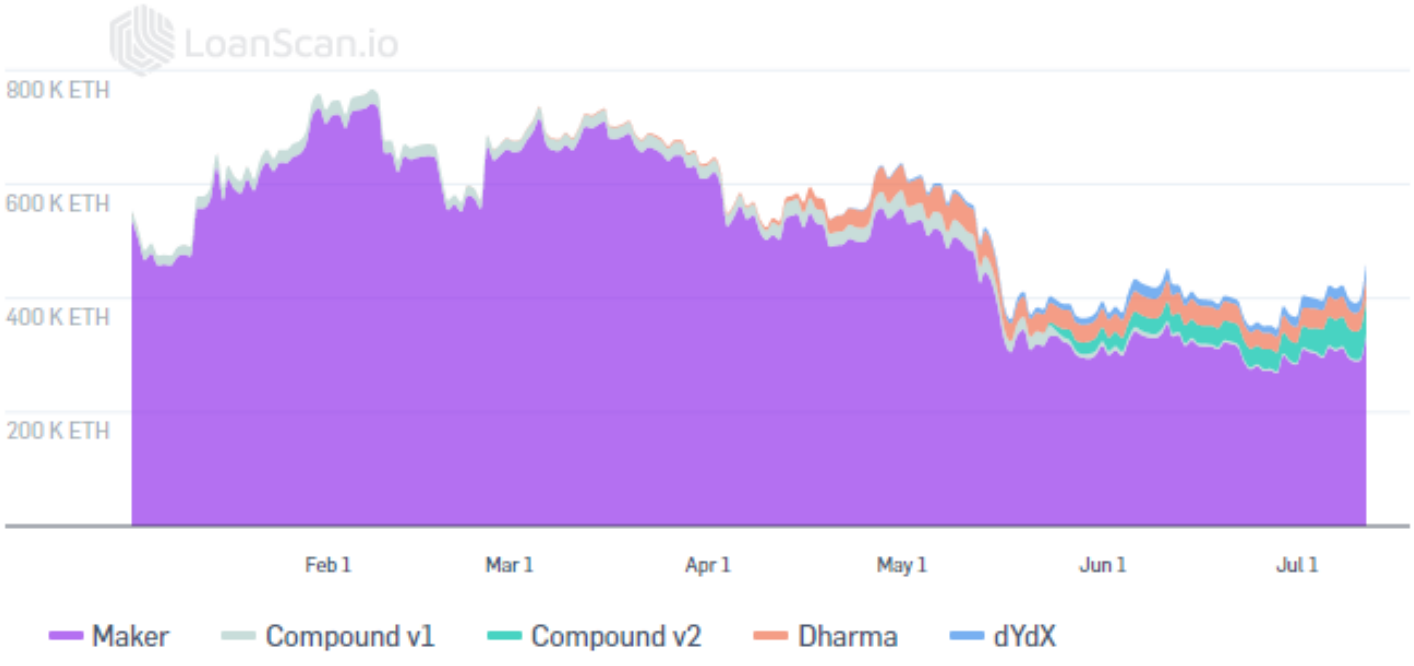
OPEN FINANCE

The Open Finance, or DeFi, stack that is being built mostly on Ethereum is an interesting use case for digital assets. It is essentially a replication of existing financial primitives, such as trading, lending, and borrowing, but on an open blockchain. Our observation is that directionally some of the larger projects, like MakerDAO, are going in the wrong direction and are shrinking in terms of staked capital. But the smaller, newer services, like Compound and Dharma, continue to grow.

LOANS DECLINE DRIVEN BY MAKER RATES

MakerDAO has been the dominant platform with which to obtain leverage on Ethereum. To slow credit creation and stabilize the supply and price of Dai, the output of the MakerDAO system, the stability fee (annual interest rate on borrowings) went from 0.5% at the beginning of the year all the way to 19.5% and now sits at 18.5%. This significant increase in borrowing rate significantly reduced the amount of credit in the system. Meanwhile, smaller lending and borrowing platforms, like Compound and Dharma, as well as derivatives platform dYdX have seen growth in their platforms, albeit from a small level.

FIGURE 12 – *ETH LOANS OUTSTANDING*



Source: LoanScan.io

DECENTRALIZED EXCHANGE VOLUME UP AND TO THE RIGHT

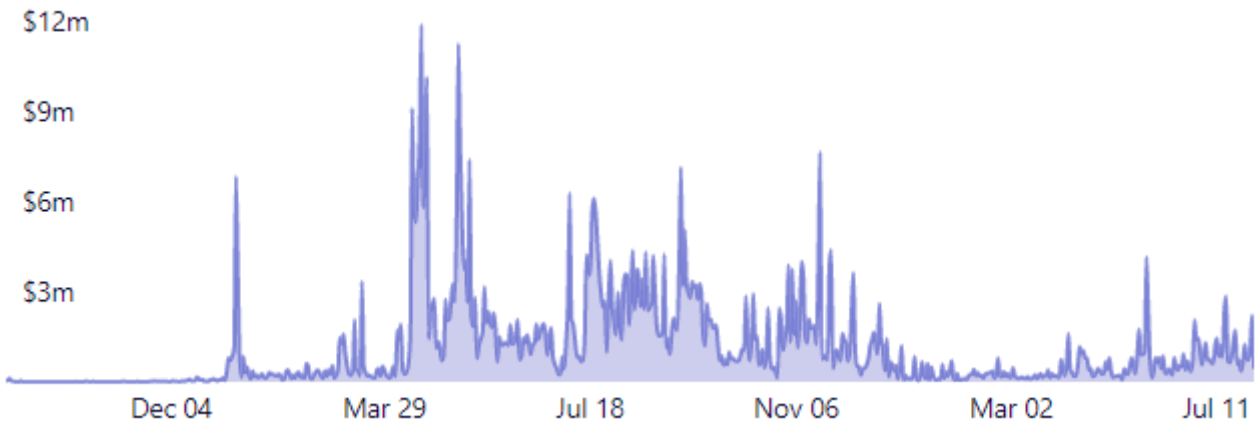
Decentralized exchanges (DEXes), like Uniswap, Bancor and Kyber, have been on the forefront of on-chain exchanges. Uniswap is by far the most dominant of the three, accounting for 65% of the ETH locked in DEXes. ETH locked in Uniswap and Kyber have been up and to the right, while Bancor took a big jump early in the quarter but has been declining since.

FIGURE 13 – *ETH LOCKED IN UNISWAP, BANCOR & KYBER*

Source: Defi Pulse

However, this comparison omits one of the longest standing DEX platforms, 0x, which is a protocol to build decentralized exchanges, called relayers. Unfortunately, transaction volume through relayers that use the 0x protocol are still small, although there has been growth off the early year lows.

FIGURE 14 – *TRANSACTION VOLUME THROUGH 0X RELAYERS*



Source: 0x Tracker

LIGHTNING CAPACITY STALLS

Most disappointing to us has been the decline in Bitcoin locked in the Lightning Network. While the total number of Lightning increased 9% in the quarter, network capacity has decreased by 10%. We believe this decline in capacity can be attributed to two factors. First, the overall rally in the price of Bitcoin may have increased demand for on-chain BTC, leading some speculators to close their channels. Since Lightning is still in beta, some users may have closed their channels to reduce their exposure to potential software bugs as BTC rallied. Second, the network's largest node operator, LNBIG, announced in June it would be closing some of its large, but then unused, Lightning channels. This may explain the sharp drop in capacity seen in early June.

FIGURE 11 – *BTC LOCKED IN LIGHTNING NETWORK*

Source: Defi Pulse

DIGITAL GOLD

Throughout Bitcoin's history there have been many narratives about what Bitcoin could be. The original whitepaper was titled "A Peer-to-Peer Electronic Cash System" and alluded to a medium of exchange for commerce, both offline and online. Also, of importance have been the narratives around international remittances, online tipping, machine-to-machine payments, privacy payments, and illicit or black-market purchases, and an open-source database for other services. While Bitcoin continues to be used in some of these use cases today, the reality is that they are still very small. We think there could be a couple of reasons for that, mostly the Bitcoin Pizza Day syndrome (why spend your BTC when you could've gotten fabulously wealthy?), that are not technical shortcomings of the protocol, which the community tends to focus on, rather they are human behavioral related to an asset that has a fixed supply. This has put Bitcoin today squarely in the narrative of censorship resistant digital gold. While we agree with this narrative, our opinion on what is driving it is a little more nuanced.

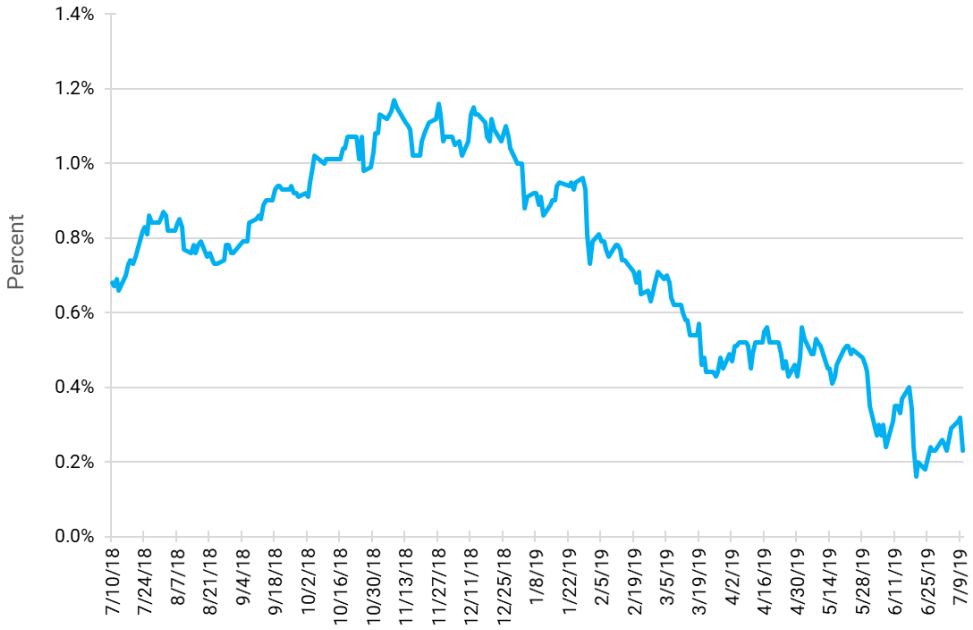
Because of this narrative of “digital gold” many look to the price of gold as an analogy for what drives the price of bitcoin. It doesn’t. The 90 day rolling correlations coefficient has only are now just approaching 0.3, not exactly high by any means. A regression will show similarly weak explanative powers.

FIGURE 15 – *CORRELATION OF BTC WITH GLD*

Source: Coin Metrics

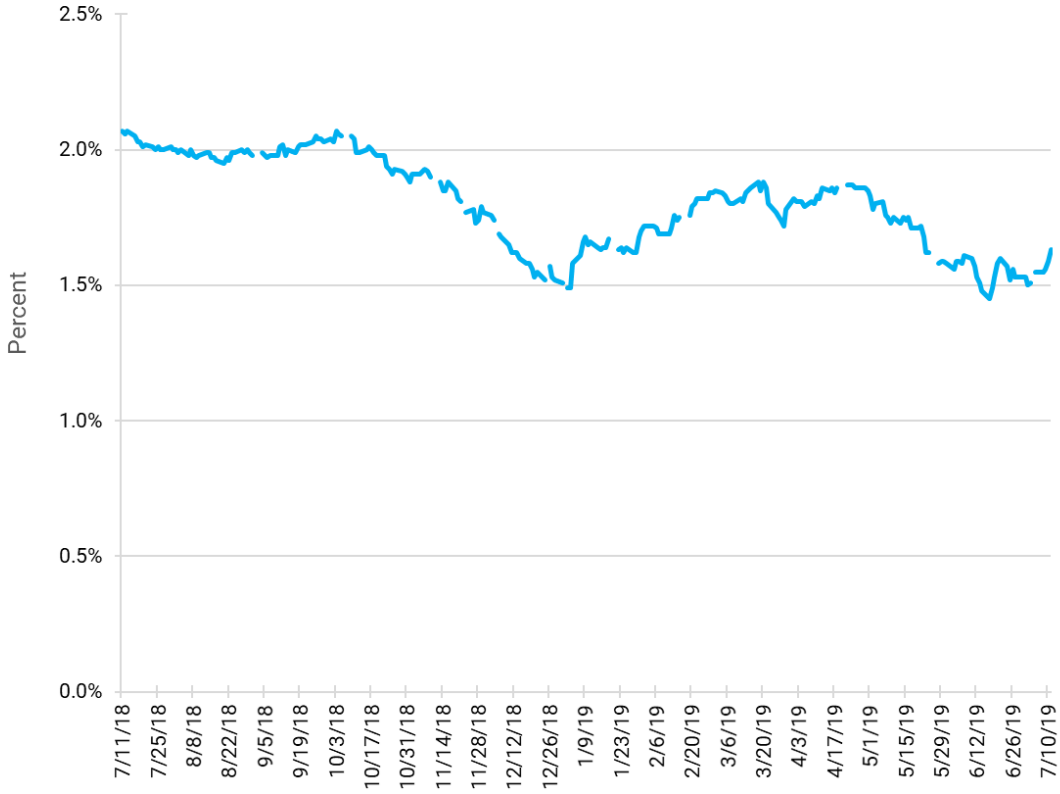
We do however think that there is something to be said about declining real yields and its correlation with risk assets, like Bitcoin and the stock market. As risk free real rates decline, investors are incentivized to put their money in non-riskless assets in order to earn a positive real rate of return, like Bitcoin and the stock market. As major central banks around to the world continue to signal their willingness to ease (i.e. reduce nominal rates) with inflation expectations steady and benign, we believe this has been a significant beneficiary to the asset class as money is “forced” to seek a positive rate of real return.

FIGURE 16 – *5-YEAR TREASURY INFLATION-INDEXED SECURITY, CONSTANT MATURITY (REAL RISK FREE YIELD)*



Source: Board of Governors of the Federal Reserve System

FIGURE 17 – *5-YEAR BREAKEVEN INFLATION RATE*

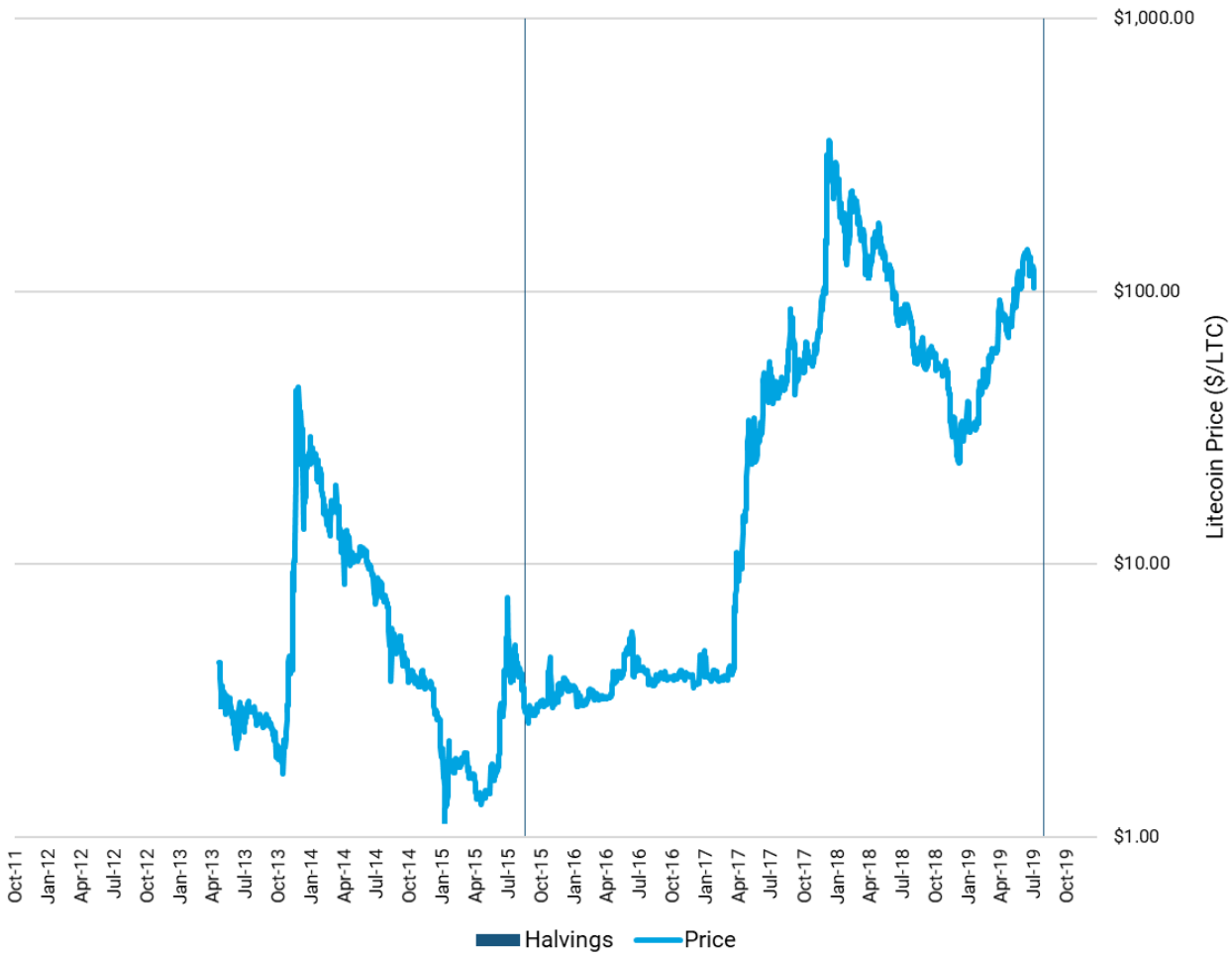


Source: Federal Reserve Bank of St. Louis

HALVINGS

Bitcoin's cyclical parabolic rise and fall appear to conspicuously coincide with halving events, or the every 210,000 block (~4 years) 50% reduction in mining (or coinbase) rewards. While our chart earlier showed Bitcoin's price charted logarithmically against prior halving events, another long-lived large cap is about to go through a halving as well – Litecoin. What we can tell from the 2015 halving is that it too experienced significant appreciation ahead of the halving while the rest of crypto was still at its lows from the 2013 peak. It subsequently lost much of those gains and didn't rally until Bitcoin once again attained a new all time high in 2017. With think that Litecoin's price appreciation and outperformance could be attributed to the halving. Now that the halving is upon us, we expect the digital asset to relinquish the alpha it generated vs Bitcoin. Litecoin's halving have been very much a "buy the news, sell the event" trade, while Bitcoin peak about a third of the way past a halving event.

FIGURE 18 – *PERFORMANCE OF LITECOIN VS HALVINGS*



Source: Digital Asset Research

STABLECOINS

If you aren't paying attention Tether, you should. We think that Tether is currently the most important crypto within the entire ecosystem, aside from Bitcoin. It is the quote currency (denominator) against hundreds of base (numerator) pairs (like BTCUSDT) across dozens of crypto only exchanges, like Binance and account for billions in daily exchange transaction volume. It is the primary source of fiat onramps for crypto only exchanges and represents a payment rail between exchanges to the tune of hundreds of millions of dollars per day. It also happens to be highly controversial and the subject of a lawsuit from the NYAG. Looking at the amount of Tether outstanding has been instructive as an indicator of the price of Bitcoin. Our theory is simple – investors convert fiat to Tether and Tether to Bitcoin. Because there are nearly 4B Tether outstanding, up from 1.9B at the beginning of the year, that represents inflow of capital of over $2B into the ecosystem. That seems paltry compared to the increase of Bitcoin from $65.4B to $207.6B today, but we think is only indicative of the amount of fiat that come in from existing exchange accounts and new fiat. Its no wonder that numerous stablecoins were launched to compete with Tether, many of which have obtained little traction against Tether.

Tether is a complicated digital asset comprised of 2 Omni Layer assets, 2 Ethereum assets, 1 on EOS and another on TRON. Most data providers get Tether's supply wrong and even Tether's own Transparency page fails to include balances of Omni tokens frozen.

FIGURE 19 – *TETHER OUTSTANDING*

Capitalization	
Omni Issued USDT Tokens (USD)	
Authorized Omni USDT	2,820,000,000
Treasury Omni USDT	249,592,849
Frozen Funds	39,404,629
Free Float USDT	2,531,002,522
Omni Issued USDT Tokens (EUR)	
Authorized Omni USDT	1,611
Treasury Omni USDT	167
Free Float USDT	1,444
Ethereum Issued USDT (USD)	
Authorized ERC20 USDT	1,400,057,493
Treasury ERC20 USDT	67,668,839
Free Float USDT	1,332,388,654
Ethereum Issued USDT (EUR)	
Authorized ERC20 USDT	50,000,050
Treasury ERC20 USDT	10,000,050
Free Float USDT	40,000,000
Tron Issued USDT (USD)	
Authorized TRC20 USDT	37,902,011
Treasury TRC20 USDT	490,816
Free Float USDT	37,411,195
EOS Issued USDT (USD)	
Authorized TRC20 USDT	1
Treasury TRC20 USDT	1
Free Float USDT	-
EUR/USD	1.13
USDT/USD	1.00
Total Authorized USDT Tokens	4,307,961,165
Total Free Float USDT Tokens	3,940,803,815
Free Float Network Value (USD)	**3,946,004,003**

Source: Digital Asset Research, 7/12/19

MAINNET LAUNCHES

THUNDERCORE

ThunderCore is a smart contract platform developed by Rafael Pass and Elaine Shi; two of the leading scientists behind Cornell's IC3 blockchain lab. During the 2019 Consensus conference the ThunderCore team announced it had successfully launched the first iteration of their mainnet, which intends to provide developers with a more scalable version of the Ethereum Virtual Machine (EVM). As such, Ethereum developers are now able to leverage ThunderCore's architecture to attain better transaction throughput. The next iteration of ThunderCore, which is expected to launch in 3Q19, will carry full functionality, such as the ability for users to stake tokens, and will better position us to fully evaluate its product-market fit.

ZILLIQA

Zilliqa is a smart contract platform experimenting with a sharded architecture, whereby transactions are processed in parallel for better scalability. On June 10, Zilliqa successfully performed the first mainnet test of a sharded smart contract on its blockchain. While its mainnet launch occurred in 1Q19, it was only until June that the network was able to launch its main functionality; sharded smart contracts.

CHAINLINK

ChainLink is an Ethereum-based oracle network that allows arbitrators to feed data to a smart contract. That data can then be used by smart contracts to trigger a transfer or update the contract's state. On June 1, the project broadcast its main set of smart contracts on the Ethereum network, effectively launching its main functionality. The first intended use-case for ChainLink's oracle network is simple; the feeding of pricing data of the ETHUSD pair for other Ethereum-based applications.

IOTEX

IoTeX is a project targeting the Internet-of-Things (IoT) segment. Much like Tron, the project has replicated an Ethereum client, in IoTeX's case the Go-Ethereum (Geth) client, and added a Delegated Proof-of-Stake (DPoS) engine that enables it to achieve higher transaction throughput. On April 22, IoTeX launched its mainnet with the goal of having a network "*where all physical and virtual "things" — humans, machines, businesses, and dApps — can efficiently exchange information and value at global scale.*"

KAKAO KLAYTN

Klaytn is a blockchain platform being developed by Kakao, South Korea's largest messaging app. On June 27, the company announced its blockchain had gone live after months of public testnet trials. While the messaging app does not currently offer any blockchain features, the company is currently developing specific applications on Klaytn, including a data marketplace, a video streaming app and a tipping plug in. We see the adoption of Klaytn as an interesting factor to keep track of ahead of the launch of its western counterparts, such as the Telegram and Libra blockchains.

SECURITY EVENTS

BINANCE HACK

On May 7, Binance disclosed a security breach that led to the theft of Binance's entire hot wallet with 7000 BTC, worth around $40M at the time. A discussion on social media ensued after a couple of developers suggested triggering a reorganization on Bitcoin's blockchain to revert the hack. In essence, this would be implemented a double spend attack whereby Binance double spends the stolen 7000 BTC and incentivize miners to revert the hack and all transactions that occurred thereafter. The suggestion was made hours after hack, making this a deep reorg with severe consequences and a potential contentious hard fork. Thankfully, Binance's CEO, CZ, announced on May 8 that they would not be pursuing this approach and all stolen user funds will be reimbursed.

THE STELLAR NETWORK HALT

The Stellar Consensus Protocol (SCP) is an interesting approach to distributed system consensus, as it allows network participants to select which entities they trust. Unfortunately, we have found that many users do not take the extra step to diversify the list of network participants they trust, and most default to the same selection as the Stellar Foundation. That makes it challenging to efficiently secure the network and mitigate the risk of consensus failures. In April, a study published by researchers at the Korea Advanced Institute of Science and Technology (KAIST), a national research university in Korea, described how an attacker could trigger a network-wide halt by targeting only two nodes. The attack, dubbed a "Cascading Failure" attack, was then performed on the Stellar mainnet a month after the paper was published, leading the network to halt for two hours. Given the reliance of the SCP on diversification, we believe this vulnerability will be difficult to be addressed and may negatively affect the adoption of Stellar soon.

ANOTHER LOOK AT ALGORAND

Algorand is a high profile blockchain project that received $64M in funding by high profile investors in 2018. Algorand's promising architecture was envisioned by Dr. Silvio Micali, an MIT scientist and Turing award winner. One of the main value propositions claimed by the system is that Algorand's consensus protocol has a property that makes it unforkable, thereby offering users instant transaction finality. In other words, upon receiving a balance, users do not need to wait for blocks to confirm to take that balance as valid. However, in May, a researcher at UNC Charlotte challenged that assumption and showed that, if a portion of users go rogue, Algorand can, nevertheless, be forked. While the paper provided an interesting perspective on the project's consensus system and at times challenged some of its assumptions, a Proof-of-Concept still needs to be developed to prove the attack vector.

FLASHBOYS 2.0

Michael Lewis's *Flashboys* introduced the world to high frequency trading, whereby traders buy and sell securities in milliseconds based on high assurance on short term trends. In April, a group of researchers published a white paper dubbed *Flashboys 2.0,* which applied similar concepts to Decentralized Exchanges (or "DEXes"). Like high frequency trading, the paper described strategies whereby an algorithm is able to front-run transactions on the blockchain in order to attain a guaranteed arbitrage profit. Given that unprocessed transactions on the blockchain are stored in a public database, the *mempool*, the paper makes the case that blockchains may further increase the profitability of high frequency arbitrage trades, as HFTs have full information on asset transfers before they are even confirmed. The paper also describes the so-called *time-bandit* attacks, a scenario where miners use their power to amend blocks to the blockchain to increase profitability by also engaging in arbitrage. In other words, miners in a Proof-of-Work network are able to rewind the blockchain to extract previous arbitrage opportunities.

MICROSOFT ION

In May, Microsoft announced its Identity Overlay Network (ION); the first decentralized identity solution developed by a large tech firm. Much like a *layer 2* solution, the project is being developed on top of the Bitcoin blockchain using a structure that does not carry scalability concerns as the information effectively encoded on the blockchain is considerably reduced. According to the project's Github repository, ION makes it possible to anchor tens of thousands of Decentralized Identities (DID), as well as Decentralized Public Key Infrastructure (DPKI) using a single on-chain transaction. Through a set of APIs, this solution would enable users to validate and prove their identity to Bitcoin smart contracts, as well as log onto a plethora of online services (like Github) using a single identifier. We believe ION is one of the best-conceived designs for decentralized identity and look forward to reviewing the first uses of this technology.

BINANCE DEX

For months, Binance has been working on its own blockchain initiative, a project called BinanceChain, which was built using the Cosmos SDK. In addition to the issuance of tokens through IEOs, their objective with BinanceChain is the development of a DEX that complements their centralized exchange business. In April, the Binance DEX officially launched on BinanceChain, which marked the first step toward the migration of BNB tokens from Ethereum onto BinanceChain. Public information on the Binance DEX is thin, but we expect further details to be released in the next quarter.

Starkdex

Perhaps one of the most significant technical developments of 2Q19 was the alpha release of the StarkDEX; a joint project developed by 0x and Starkware. This decentralized exchange protocol utilizes cutting-edge cryptography, *STARKs*, in conjunction with transaction batching to achieve sidechain-like scalability. The result is over 550 transactions per second, and a 200x cost reduction in transaction fees. Although StarkDEX is still in early stages and has only been tested on the Ropsten testnet, we are looking forward to further developments in this area.

UTREEXO

One of the key aspects of any blockchain network is the determination of which accounts have a valid balance to spend at any given time. While the blockchain provides a strong validation engine, an auxiliary tool is often used to more swiftly assess the validity of a balance; a database called the *UTXO set*. Since full validating nodes are required to store this database, the convenience of maintaining such database imposes considerable

scalability concerns to all blockchains employing this structure. In June, Thaddeus Dryja, one of the co-creators of the Lightning Network, published a paper that describes a novel mechanism to address this problem; uTreeXo. Through the use of sophisticated cryptographic techniques, uTreeXo can considerably decrease the size of this database, thereby lowering hardware requirements to run a full node.

ZKVM

The Zero Knowledge Virtual Machine, or ZkVM, is a Stellar-based project that combines multiple technologies to provide a new approach to *layer 2*. By leveraging Bitcoin's uTreeXo and Taproot technologies, the ZkVM is able to provide an efficient way for transactions and contracts to be succinctly executed outside of the Stellar blockchain. The project also makes use of Bulletproofs, which is a privacy-preserving scheme that carries minimum trade-offs, such as trusted setups. As a generalized computation platform, the ZkVM is particularly interesting approach to layer 2 solutions. While there are no specific use-cases it targets at this point, we will continue to track the progress of the ZkVM, and the ways it may be applied to connect various blockchains to Stellar.

RINGCT 3.0

Ring Confidential Transactions, or RingCT, is a novel mechanism used in Monero to increase the privacy guarantees of its blockchain. It combines the concept of Ring Signatures, a type of signature that fuses multiple keys to hide the sender's identity, with the Confidential Transactions scheme, which encodes transaction amounts. In May, a paper describing a new approach to RingCT was published; the RingCT 3.0 scheme. Unlike RingCT 2.0, this new scheme does not rely on a trusted setup, but can still provide a 97% decrease in the ring signature size relative to RingCT 1.0, which is currently used in Monero. While still theoretical in nature, RingCT 3.0 is a promising new schema for private transactions, and we look forward to reviewing implementations of this schema.

SPARTAN

Cryptocurrencies like Zcash make use of a highly sophisticated cryptographic scheme, *zkSNARKs*, to eliminate traceability of senders and receivers of ZEC. For practicality and succinctness, the math behind zkSNARKS require a parameter to be created secretly by multiple entities. If compromised, an attacker who knows that secret parameter is able to create fake proofs and essentially print ZEC secretly out of thin air. Users joining the ZEC network must trust that the setup used to generate that parameter was flawless, which has resulted in a lot of criticism by the technical community. In May, however, a ground-breaking paper describing a new general-purpose zkSNARK scheme called *Spartan* was released. Unlike most approaches to zkSNARKs, Spartan does not require a trusted setup for efficiency, which may considerably decrease the risk of a compromised secret parameter. We have yet to see deployed Spartan implementations, but the technology looks promising, and could address many of the concerns arounds zkSNARKS.

ERLAY

As the proverb goes, Bitcoin's main value proposition is to enable its users to *be their own bank*. As such, they can maximize the security of their funds by storing their private keys in air-gapped environments, such as HSM wallets, and running their own full nodes. High availability of information on the most recent network events is a key aspect of user security, and users attain that by being highly connected to other network participants. Unfortunately, the current wire protocol used for nodes to communicate makes it difficult for users to optimize security and there is plenty of room for improvements. In May, a group of Bitcoin Core developers unveiled Erlay, a solution that greatly improves the connectivity of Bitcoin nodes. Erlay not only reduces the bandwidth consumption of Bitcoin nodes by 40%, but it also keeps the bandwidth use almost constant as connectivity increases. If implemented on Bitcoin Core, Erlay can considerably increase the overall security of the network and reduce the bandwidth requirements of running a node. Given its association with Core developers, we expect Erlay to be integrated to Bitcoin Core within the next couple of releases.

BITCOIN CORE 0.18

On May 8, Bitcoin Core released version 0.18 of its network client, which carried a number of performance and security improvements, as well as some bug fixes. The most significant update was native compatibility with hardware wallets such as Ledger and Trezor.

TELEGRAM

In December of 2017, Telegram announced it was working on its own implementation of a blockchain network. In May of this year, the project released its highly-anticipated testnet and enabled developers to publicly perform tests. We had the opportunity to briefly review the TON Virtual Machine (TVM) and its accompanying scripting language and were both surprised and impressed by the complexity of the entire system. The project is striving to learn lessons from Ethereum and improve upon the state of the industry on smart contracts. While we welcomed the flavors of functional programming in Telegram's smart contract scripting language, we ultimately believe the project's complexity will further delay its mainnet launch. As with any other project pursuing a broad and ambitious scope, the devil is in the details. Excessive, and perhaps unnecessary, complexity may further delay the adoption of the TVM on Telegram's messaging app. Nevertheless, given the sheer number of users on its platform, we look forward to reassessing the adoption of TON, once the TVM activates on Telegram's messaging app.

DISCLOSURES

ONE OR MORE OF THE ANALYSTS PARTICIPATING IN THE PREPARATION OF THIS REPORT HAVE HOLDINGS OF THE DIGITAL TOKEN LISTED AT THE TOP OF PAGE 1 AS OF THE DATE HEREOF. The employees of Digital Asset Research ("DAR") may purchase and use cryptocurrencies as part of the due diligence process. They may also own or hold them for any other reason.

This report is for clients of Digital Asset Research ("DAR") only. Use of this report, in any context, is governed by the Subscription Services Agreement and DAR's Terms of Use, both of which are incorporated here by reference. DAR is the sole and exclusive owner of this report and retains all right, title and interest to it and you do not have any right to the same except for the rights otherwise expressly granted herein or in the Subscription Services Agreement.

You are permitted to store, display, analyze, modify, and print this report, but only for your own use. You are not permitted to (a) reverse engineer, decompile, decode, decrypt, disassemble, or in any way derive source code from this report; (b) modify, translate, adapt, alter, or create derivative works from this report; (c) copy (except as expressly permitted in the Subscription Services Agreement), distribute, publicly display, transmit, sell, rent, lease or otherwise exploit this report or grant any third party access to it; (d) frame or scrape or in-line link to the this report or use web crawlers, web spiders or other automated means to access, copy, index, process and/or store any of the information herein; (e) create apps, extensions, programs or other products or services that use any of the information herein; or (f) make or have made a service or product using similar ideas, features, functions or graphics of or providing a similar benefit as that provided by this report.

DAR DOES NOT MAKE AND HEREBY EXPRESSLY DISCLAIMS ALL WARRANTIES, ORAL OR WRITTEN, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. WITHOUT LIMITING THE FOREGOING, YOU AGREE THAT YOUR USE OF THIS REPORT IS AT YOUR SOLE RISK AND ACKNOWLEDGE THAT THIS REPORT IS PROVIDED "AS-IS" AND DAR DOES NOT MAKE ANY WARRANTIES WITH RESPECT TO THE OPERATION, AVAILABILITY, RELIABILITY, ORIGINALITY OR ADEQUACY OF THE SAME. THIS REPORT (INCLUDING ANY INFERENCES OR CONCLUSIONS DRAWN HEREIN) IS BASED ON INFORMATION DAR CONSIDERS RELIABLE, HOWEVER, DAR DOES NOT REPRESENT IT AS ACCURATE OR COMPLETE, AND IT SHOULD NOT BE RELIED ON AS SUCH. THIS REPORT (INCLUDING ANY INFERENCES OR CONCLUSIONS DRAWN HEREIN) IS PROVIDED FOR GENERAL INFORMATIONAL PURPOSES ONLY AND YOU ARE RESPONSIBLE FOR DETERMINING WHETHER ANYTHING CONTAINED HEREIN IS SUITABLE FOR YOUR PARTICULAR CIRCUMSTANCES, AND FOR SEEKING PROFESSIONAL TAX AND/OR INVESTMENT ADVICE AS APPROPRIATE. DAR DOES NOT GIVE TAX, LEGAL OR INVESTMENT ADVICE OR ADVOCATE THE PURCHASE OR SALE OF ANY SECURITY, INVESTMENT, CRYPTOCURRENCY OR DIGITAL ASSET. NONE OF THE INFORMATION CONTAINED IN THIS REPORT CONSTITUTES OR IS INTENDED TO CONSTITUTE A RECOMMENDATION BY DAR TO ACQUIRE, HOLD, INVEST IN, OR USE ANY PARTICULAR COIN, TOKEN, CRYPTOCURRENCY, PROTOCOL, COMPANY OR FOUNDATION.

You assume the entire risk of any use you make or permit to be made from this report. Without limiting the foregoing and to the maximum extent permitted by applicable law, in no event shall DAR have any liability regarding this report for damages, even if notified of such possibility.

The information contained herein is as of the date hereof and is subject to change without prior notice. We may provide oral or written market commentary or trading strategies to our clients that reflect opinions that are contrary to the opinions expressed in this research. Information containing any historical information, data or analysis should not be taken as an indication or guarantee of any future performance as past performance does not guarantee future results. None of DAR's products or services recommend, endorse, or otherwise express any opinion regarding any "coin", "token", "cryptocurrency" "protocol", "company" or "foundation" and none of DAR's products or services are intended to constitute investment advice or a recommendation to make (or refrain from making) any kind of investment decision and may not be relied on as such.