STANDARD KEPLER
WEEKLY SUMMARY | 15 – 21 APRIL

Tobias Mathiasen
DIRECTOR, RESEARCH
Tobias@standardkepler.com

Johnny AuYeung
CTO, STANDARD KEPLER
Johnny@standardkepler.com

Common Blockchain Misconceptions – Part 2 of 3

WEEKLY RECAP

- Total market cap. increased 1.2% to $178bn, and 7 day trading volume decreased 7.11% for top 100 crypto

THOUGHTS OF THE WEEK

My colleague and Standard Kepler CEO David Tang recently authored a few articles on the subject of blockchain and cryptocurrency misconceptions. Last week in part 1 we had a look at the first 4 of a total of 8, and this week we will continue by taking a slightly deeper look at misconceptions 5 and 6.

5. "Use of blockchain increases system security": I don't know the origin of this misconception, but we often hear our clients saying that they want to improve their system's security by "putting everything" on a blockchain. They fail to realize that blockchain does not equate absolute security. In fact, only some blockchains are secure, a lot of blockchains are not.

Before we discuss whether using blockchain improves system security, we need to know how blockchain secures itself and its limitations in doing so. Blockchain secures your data in two ways: Firstly, it maintains data integrity by making sure that the data recorded on it can neither be altered nor removed. Secondly, it secures the ownership of your account with public/private key cryptography. This means that your account is secure as long as your private key isn't exposed (normal password protection is significantly easier to crack compared to public/private key cryptography).

In the case of smart contracts, the above characteristics of blockchain makes it possible to achieve security on a new level: a program deployed on blockchain cannot be altered or removed, meaning that hackers cannot change your program code or make it misbehave. But there are also limitations. For example, if the deployed code has bugs then blockchain won't allow you to fix these bugs as the program code cannot be changed once launched. Also, the public/private key encryption adds an element of user unfriendliness to your system, since users cannot choose their private key and the keys can be long and hard to memorise. Back to the question, can blockchain helps improving your system security? The answer is that it depends.

If you just want to secure the data integrity: Yes, blockchain can help. Putting your data on a public blockchain can make your data largely immutable.

TOP CRYPTO PERFORMANCE SUMMARY

Name	Price	7D%	Vol.	7D%	Mkt Cap.	% Total Mkt
BTC	$5,314.53	3.02%	80.38bn	-0.33%	93.85bn	52.69%
ETH	$170.05	1.78%	37.15bn	-4.51%	17.98bn	10.10%
XRP	$0.32	-1.78%	6.30bn	-5.59%	13.53bn	7.60%
BCH	$290.48	-0.40%	7.33bn	-11.48%	5.15bn	2.89%
EOS	$5.25	-4.16%	11.73bn	-31.04%	4.75bn	2.67%
LTC	$77.33	-5.26%	15.20bn	-7.57%	4.75bn	2.67%
BNB	$24.19	23.23%	1.81bn	69.70%	3.42bn	1.92%
USDT	$1.01	0.07%	71.34bn	-11.83%	2.60bn	1.46%
XLM	$0.11	-4.37%	1.57bn	-11.17%	2.18bn	1.22%
ADA	$0.07	-11.97%	0.48bn	-29.36%	1.92bn	1.08%

If you want to make your program secure: Usually no, sometimes yes. Yes if your program is coded flawlessly; No if your program is not flawless, and most programs are far from perfect and do contain bugs.

If you want to hide your data from hackers: No, there are better ways to hide your data securely. Putting the data on a blockchain without lowering the data usability is impossible.

If you want to give your users the ability to store their encrypted data securely, and make sure that only they can decrypt their own data: Yes, you can do this with blockchain, but make sure you really need this level of security and that you are willing to make the relevant sacrifices in usability to users.

6. "Use of blockchain protects user privacy": Well, using Bitcoin can protect your privacy, and so can many other cryptocurrencies. But here lies a very common misconception that start-ups, VCs and a lot of laymen (non-laymen as well) have been reiterating. Blockchain protects privacy because it can verify a transaction without needing your personal information. However, it does not protect your privacy by preventing other parties from misusing your information without your permission. Consider the following example from a project:

> *"A user installs an application that uses our platform for preserving her privacy. As the user signs up for the first time, a new shared (user, service) identity is generated and sent, along with the associated permissions, to the blockchain in a Taccess transaction. Data collected on the phone (e.g., sensor data such as location) is encrypted using a shared encryption key and sent to the blockchain in a Tdata transaction, which subsequently routes it to an off-blockchain key-value store, while retaining only a pointer to the data on the public ledger (the pointer is the SHA-256 hash of the data). Both the service and the user can now query the data using a Tdata transaction with the pointer (key) associated to it. The blockchain then verifies that the digital signature belongs to either the user or the service. For the service, its permissions to access the data are checked as well. Finally, the user can change the permissions granted to a service at any time by issuing a Taccess transaction with a new set of permissions, including revoking access to previously stored data. Developing a web-based (or mobile) dashboard that allows an overview of one's data and the ability to change permissions is fairly trivial and is similar to developing centralized-wallets, such as Coinbase for Bitcoin."*

NETWORK FUNDAMENTALS

	BTC	ETH
Hashrate 7D Av.	44,958,820 TH/s (-2.2%)	146,963 GH/s (-0.7%)
Hashrate 30D Av.	45,808,205 (-0.4%)	143,958 GH/s (0.2%)
Wallet Users 7D Av.	35,601,091 (+1.1%)	61,687,013 (+1.0%)
Wallet Users 30D Av.	34,995,303 (+0.9%)	60,711,048 (+1.9%)
Top 4 Mining Pools	BTC.com (16%) Poolin (12%) F2Pool (11%) SlushPool (11%)	Ethermine (25%) SparkPool (23%) F2Pool (13%) Nanopool (12%)

What projects such as this one suggest is that all user data is uploaded and stored on a blockchain platform, and that services (apps) can only access this data with user permission. Most importantly, you can revoke the permission at any time. Does this not sound like Facebook login? Apps can only access your data with your consent, and you can revoke this permission at any time. So, can these apps "steal" your data? Yes! And all they have to do is to create a copy.

This most obvious point of failure of the above proposal. The data you generate in the app can only be uploaded to blockchain by the app itself, so the app can steal it in the middle of the upload, or it can even outright prevent the data from being uploaded. The only way to make it work is through something like TouchID: your fingerprint is collected by your iPhone, and the app cannot touch the data, it can only ask iPhone to check whether your fingerprint is correct. The data from the point of being collected, to being processed and stored is in a closed loop. This is how Apple protects your privacy from everyone except themselves.

In short, cryptocurrencies can protect privacy because they don't need your private information to verify transactions, nor do they require authorities that own your personal information to verify transactions. Blockchain can encrypt your data and store it securely and prevent anyone from using it, but it cannot protect your data from being misused.

DISCLAIMER

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

Chart of The Week: Sources:

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

Thought of The Week: Sources: Standard Kepler Research

Top Crypto Performance Summary: Sources: Coinmarketcap, 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.

Unless otherwise stated, all data is as of April 21, 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.