EXPLICATING THE TRUST AND SCALING ISSUES IN THE BLOCKCHAIN CRYPTO CURRENCY ECOSYSTEM

Prof. Arivanantham Thangavelu, Prof. Poonam Deokar, Prof. Preeti Patil

Assistant Professor
Department of Information Technology
Dr. D. Y. Patil Institute of Technology, Pimpri, Pune, India

Abstract : The aim of this paper is to fill the gap in the current literature by investigating the trust-influencing factors (price manipulation, centrality, regulations, usability, etc.) as well as understanding the energy consumption and environmental impact and providing an in-depth explication of these factors and discuss the potential of the blockchain crypto currency ecosystem. Blockchain technology supports new ways of forming economic events, it helps to reduce time and a cost related with mediators, and strengthens the trust in an actor's ecosystem.

I. Introduction

Blockchain:

A blockchain is a public ledger dispersed over a network it records transactions performed between different network contributors. Every transaction is tested by network nodes according to a mainstream consensus mechanism before being added to the blockchain. At any time recorded data cannot be modified or deleted and each transaction history can be reconstructed at any time.

A blockchain system must provide some basic features in order to ensure a perfect and trustworthy platform for crypto currencies. These features include:

1. Trustless
2. Decentralization
3. Distributed Ledger Technology
4. Tamper-proof environment
5. Security & Privacy
6. Consensus Mechanism
7. Faster Transactions

Crypto Currency:

- A crypto currency is a virtual or digital currency that is protected using cryptography, which makes it nearly impossible to forgery or double-spend.
- Bitcoin was the first crypto currency introduced in the market by pseudonymous entity named Satoshi Nakamoto in 2008 but the real market for crypto currency started in 2013.

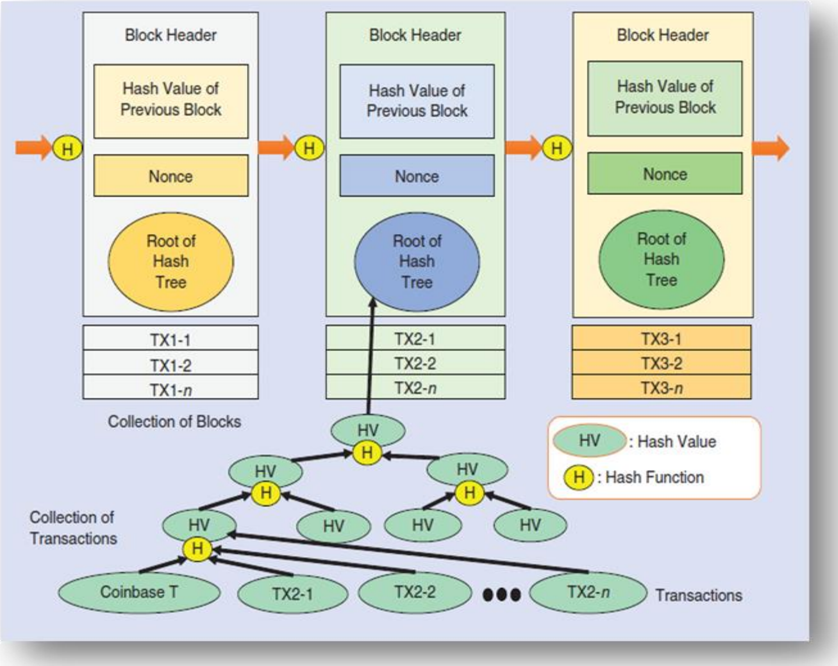
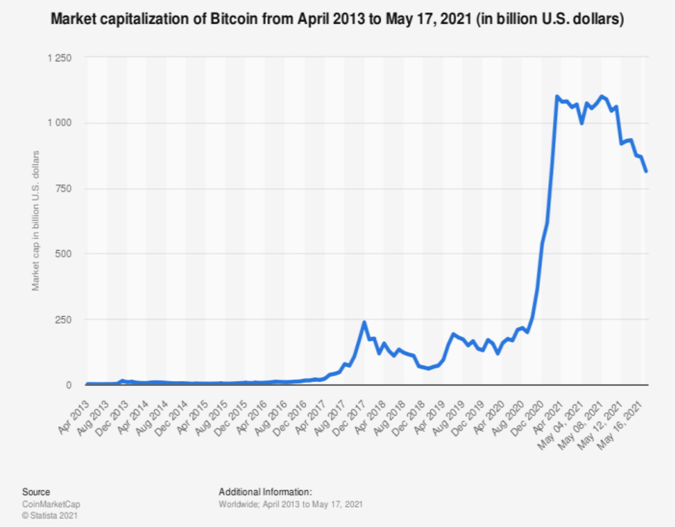


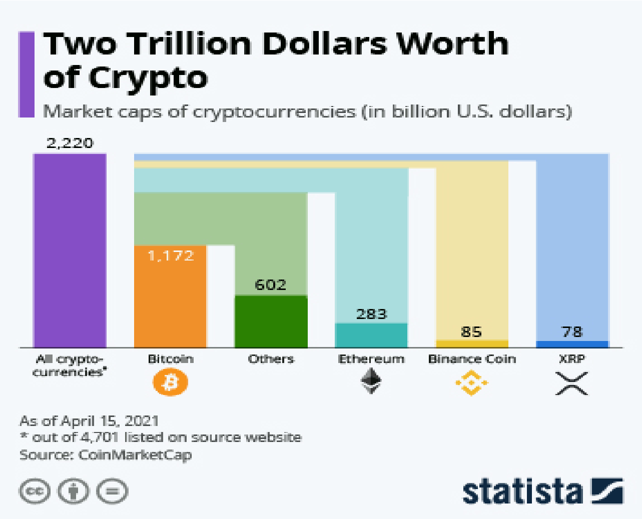
Figure: 1. Explicating the Trust & Scaling Issues in the Blockchain Crypto Currency Ecosystem

Crypto Currency:

- A crypto currency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend.
- Bitcoin was the first crypto currency introduced in the market by pseudonymous entity named Satoshi Nakamoto in 2008 but the real market for crypto currency started in 2013.
- In March 2021, the Bitcoin market cap reached an all-time high and had grown by over 600 billion U.S. dollars when compared to the summer months. The market capitalization briefly reached more than 1,000 billion USD in May 2021.


Market capitalization of Bitcoin from April 2013 to May 17, 2021 (in billion U.S. dollars)

Source
CoinMarketCap
© Statista 2021
Additional Information:
Worldwide; April 2013 to May 17, 2021


Two Trillion Dollars Worth of Crypto
Market caps of cryptocurrencies (in billion U.S. dollars)

As of April 15, 2021
* out of 4,701 listed on source website
Source: CoinMarketCap

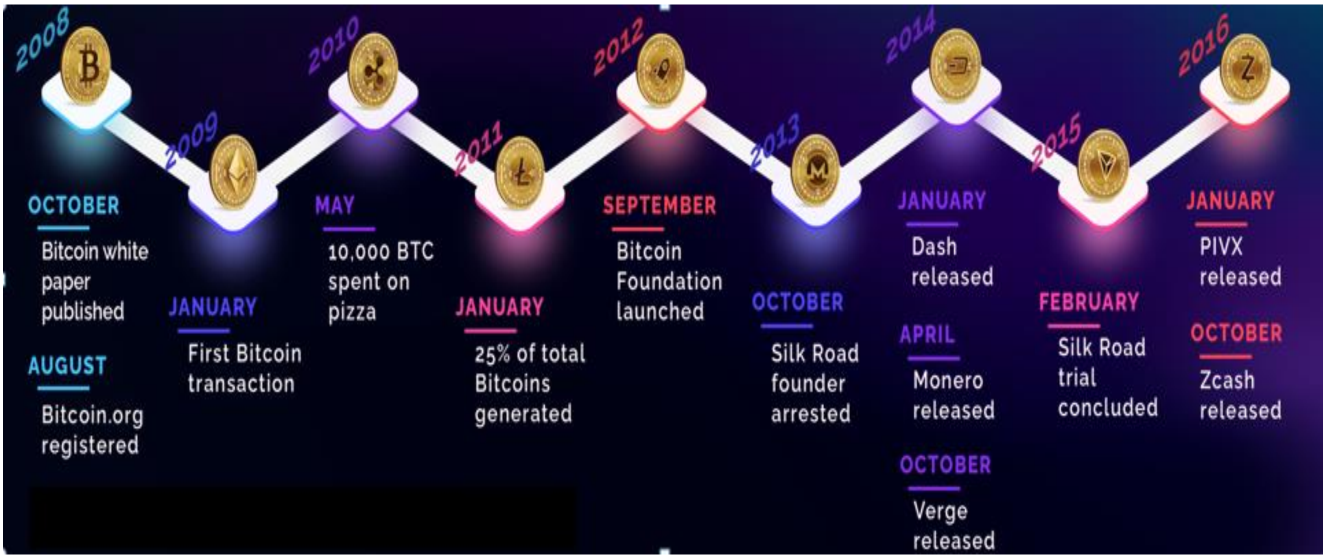


Figure: 2. Short history of Bitcoin and other crypto currencies

FIAT Currency:

- Fiat money is a government-issued currency that is not backed by a commodity such as gold.
- Fiat money gives central banks greater control over the economy because they can control how much money is printed.
- Most modern paper currencies, such as the Indian Rupee, U.S. dollar, are fiat currencies.
- One danger of fiat money is that governments will print too much of it, resulting in hyperinflation.

Major Trust Issues in the Ecosystem:

1. **Insider Trading**
   It is processes of sale or purchase of securities by someone with information.
   Insider trading laws claim critics should be legal because it offers useful information to markets and the laws against it cause harm normal people, while the wrongdoing itself causes little damage.
2. **Parallel & Shadow Economy**
   It also called as informal, parallel or underground economy; it includes illegal activities, unreported income from the creation of services and legal goods, either from exchange or monetary transactions.
3. **Reputation Systems**
   For example:
   Ethereum emphasizes that a reputation system must enable three functions: incentive mechanism to reduce cheating, filtration of honest stakeholders in the ecosystem, and a point-system for intrinsic value creation.
4. **Lack of Transparency:**
   Transparency can mean increased scope, not taking.

5. **Token Economy:**

ERC20 (a standard contract on Ethereum)

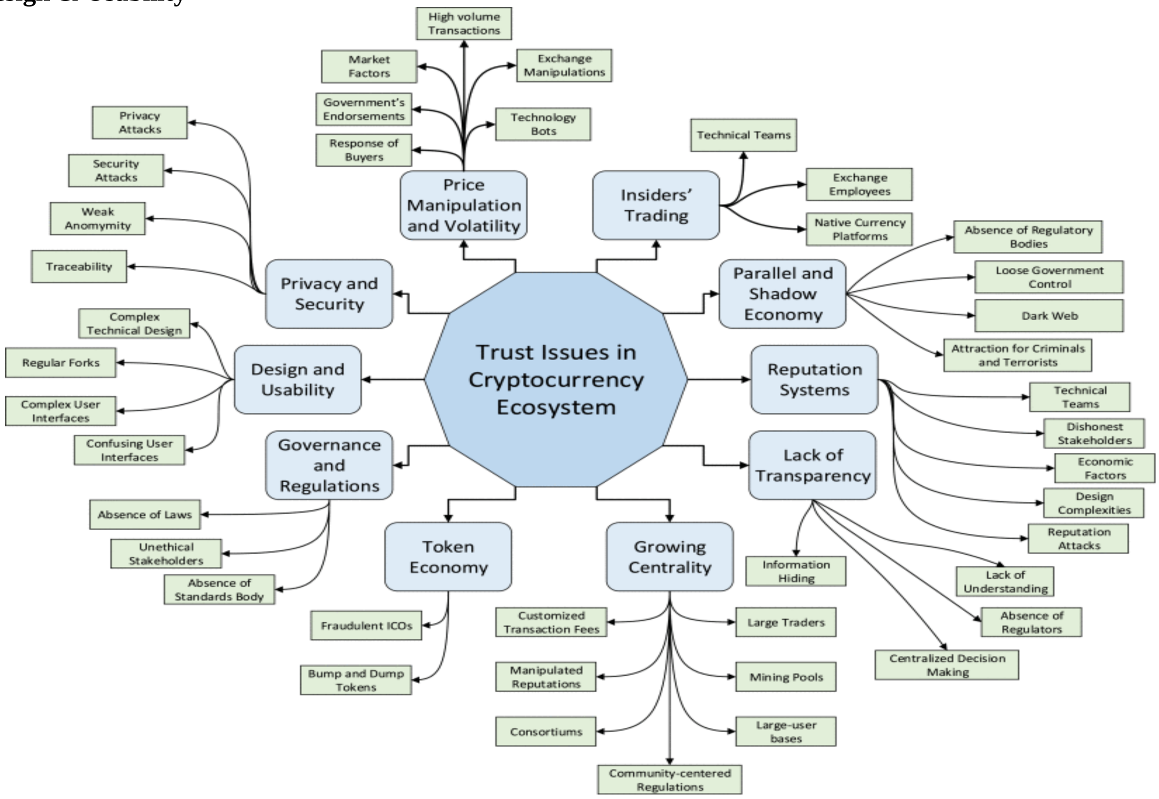
Fraudulent ICOs.

Top 10 scammers included Pincoin, Plexcoin, Bitcard, Opair, Benebit, Bitconnect, Confido, REcoin, Ponziecoin, and Karbon.

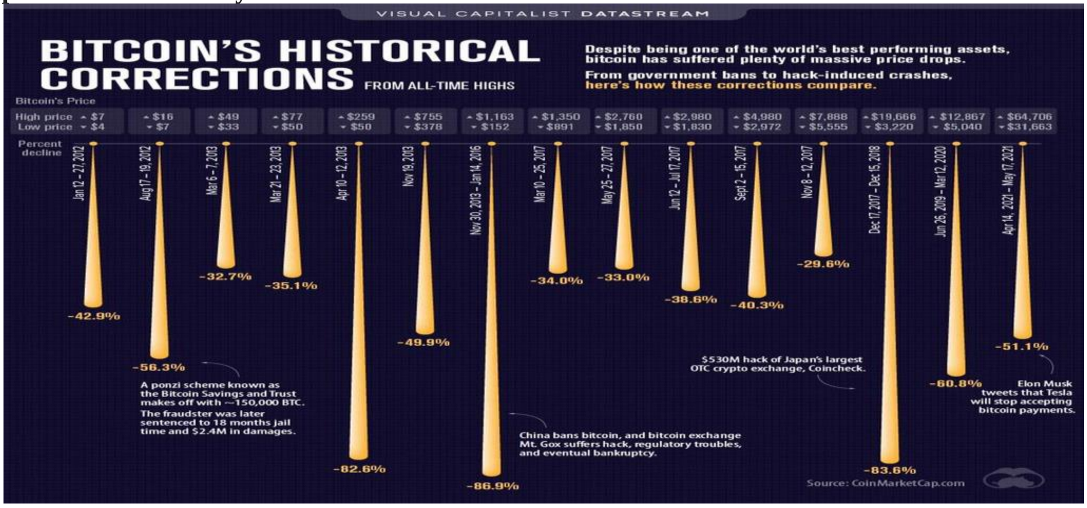
BurgerSwap $7.2 Million Flash Loan Attack –

The attacker eventually made off with
$1.6 million in Wrapped BNB,
$6,800 in ETH,
$3.2 million of BURGER coin,
$1 million of xBURGER, a synthetic version of BURGER,
95,000 ROCKS ($152,000),
$22,000 of Binance’s US dollar-pegged stablecoin, BUSD, and a further
$1.4 million of USD stablecoin Tether.

6. Design & Usability



7. Price Manipulations & Volatility:


VISUAL CAPITALIST DATASTREAM

BITCOIN'S HISTORICAL CORRECTIONS FROM ALL-TIME HIGHS

Despite being one of the world's best performing assets, bitcoin has suffered plenty of massive price drops.
From government bans to hack-induced crashes, here's how these corrections compare.

A ponzi scheme known as the Bitcoin Savings and Trust makes off with ~150,000 BTC. The fraudster was later sentenced to 18 months jail time and $2.4M in damages.

China bans bitcoin, and bitcoin exchange Mt. Gox suffers hack, regulatory troubles, and eventual bankruptcy.

$530M hack of Japan's largest OTC crypto exchange, Coincheck.

Elon Musk tweets that Tesla will stop accepting bitcoin payments.

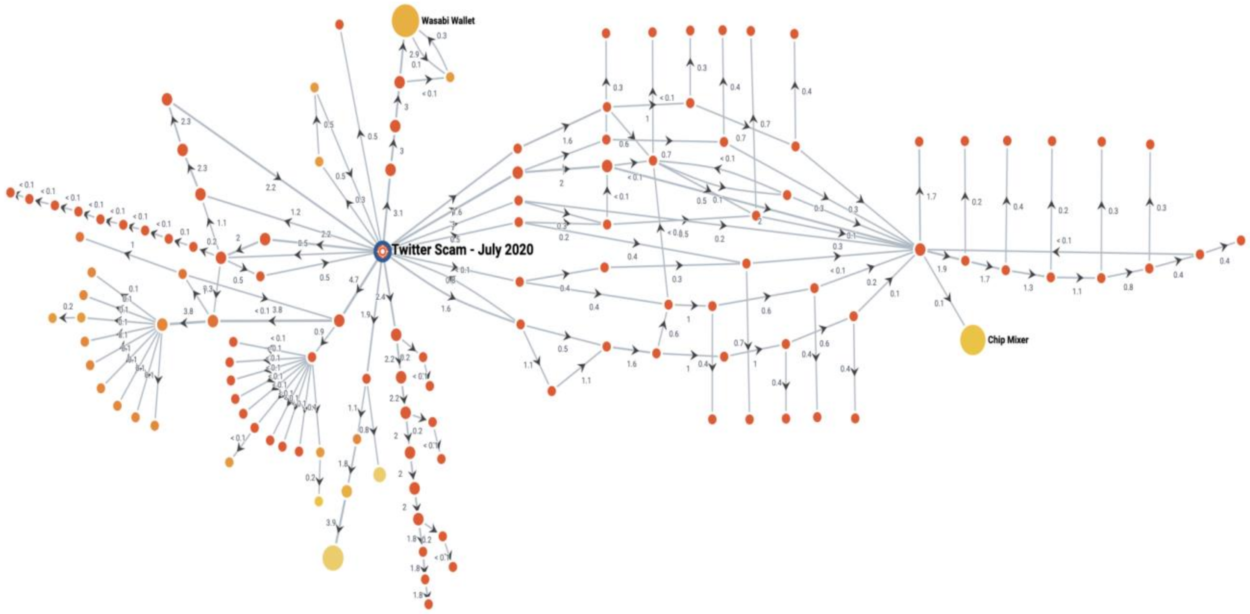
Source: CoinMarketCap.com
Bitcoin's Price
High price
Low price
Percent decline
Jan 12 – 27, 2012 ▲$7 ▼$4 -42.9%
Aug 17 – 19, 2012 ▲$16 ▼$7 -56.3%
Mar 6 – 7, 2013 ▲$49 ▼$33 -32.7%
Mar 21 – 23, 2013 ▲$77 ▼$50 -35.1%
Apr 10 – 12, 2013 ▲$259 ▼$50 -82.6%
Nov 19, 2013 ▲$755 ▼$378 -49.9%
Nov 30, 2013 – Jan 14, 2016 ▲$1,163 ▼$152 -86.9%
Mar 10 – 25, 2017 ▲$1,350 ▼$891 -34.0%
May 25 – 27, 2017 ▲$2,760 ▼$1,850 -33.0%
Jun 12 – Jul 17, 2017 ▲$2,980 ▼$1,830 -38.6%
Sept 2 – 15, 2017 ▲$4,980 ▼$2,972 -40.3%
Nov 8 – 12, 2017 ▲$7,888 ▼$5,555 -29.6%
Dec 17, 2017 – Dec 15, 2018 ▲$19,666 ▼$3,220 -83.6%
Jun 26, 2019 – Mar 12, 2020 ▲$12,867 ▼$5,040 -60.8%
Apr 14, 2021 – May 17, 2021 ▲$64,706 ▼$31,663 -51.1%

8. Privacy & Security

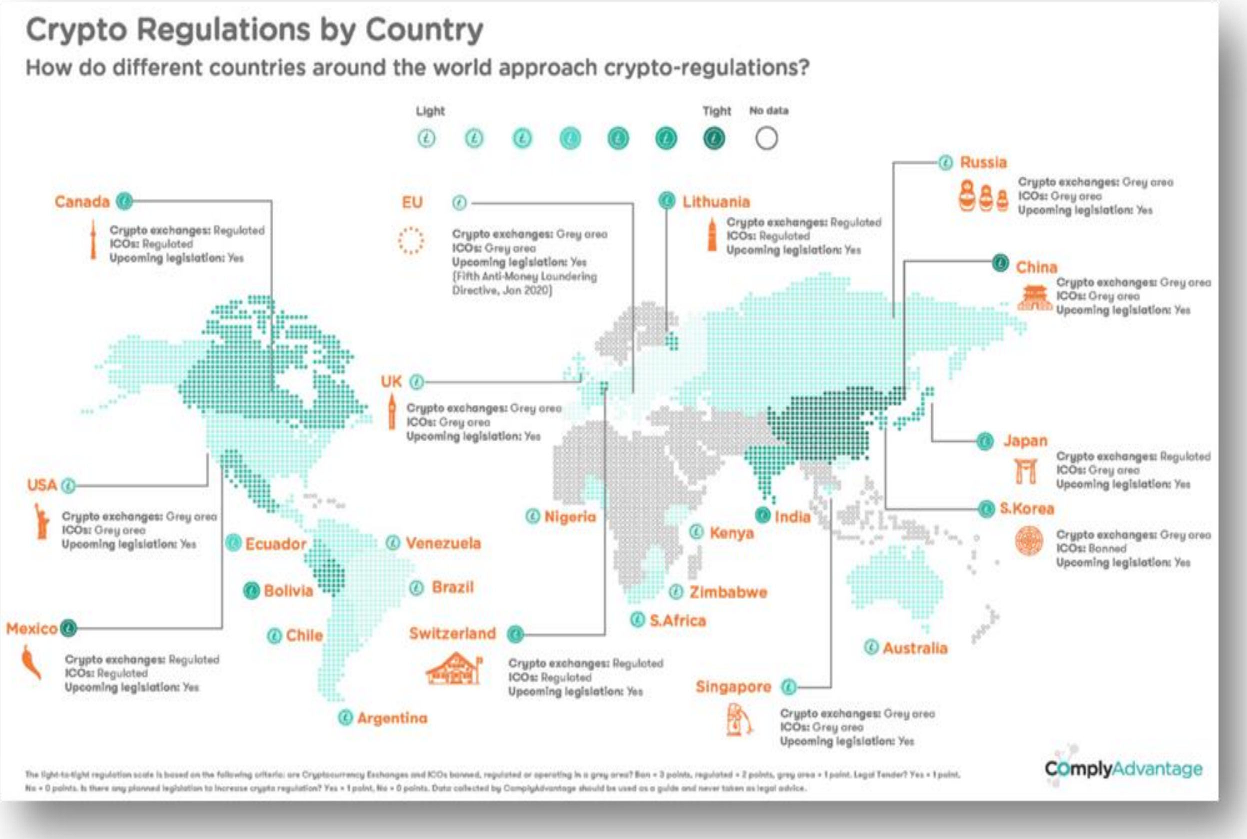
Crypto Scams:

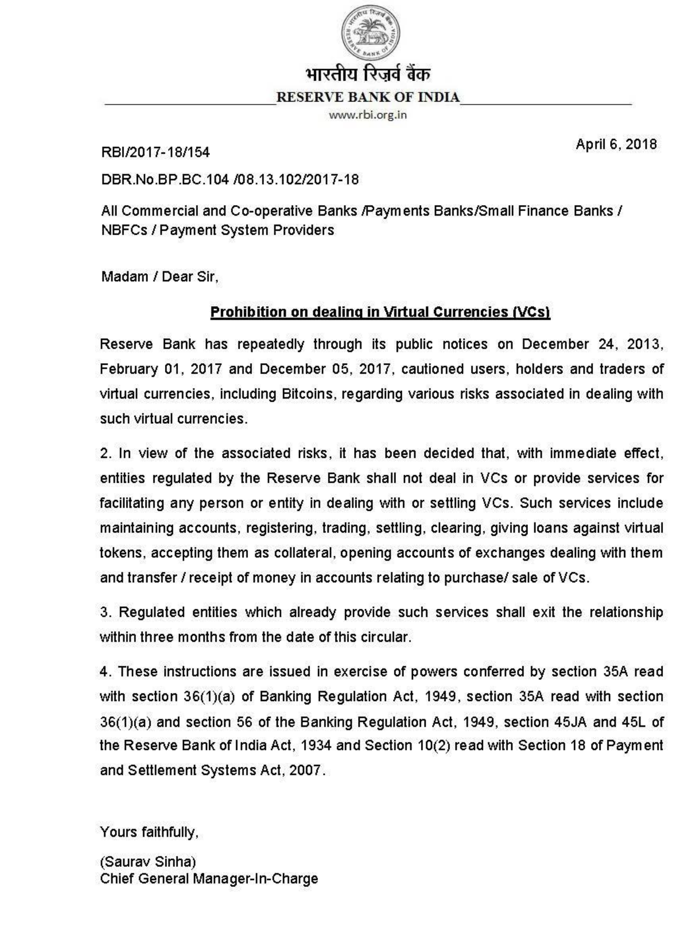
- Utilizing a common fraud technique known as a "giveaway scam", these accounts were used to defraud around 400 victims of a total of $121,000 in bitcoin.
- The addresses used were part of a larger wallet, which had previously received around $65,000 in bitcoin between May and July 2020. The New York Times reported that some of these funds may have come from selling stolen twitter accounts.

9. Representation of how the coins were transferred to multiple wallets:



10. Governance & Regulation:


Crypto Regulations by Country
How do different countries around the world approach crypto-regulations?
Light
Tight
No data
Canada
Crypto exchanges: Regulated
ICOs: Regulated
Upcoming legislation: Yes
EU
Crypto exchanges: Grey area
ICOs: Grey area
Upcoming legislation: Yes
(Fifth Anti-Money Laundering Directive, Jan 2020)
Lithuania
Crypto exchanges: Regulated
ICOs: Regulated
Upcoming legislation: Yes
Russia
Crypto exchanges: Grey area
ICOs: Grey area
Upcoming legislation: Yes
China
Crypto exchanges: Grey area
ICOs: Grey area
Upcoming legislation: Yes
UK
Crypto exchanges: Grey area
ICOs: Grey area
Upcoming legislation: Yes
Japan
Crypto exchanges: Regulated
ICOs: Grey area
Upcoming legislation: Yes
USA
Crypto exchanges: Grey area
ICOs: Grey area
Upcoming legislation: Yes
Nigeria
India
S.Korea
Crypto exchanges: Grey area
ICOs: Banned
Upcoming legislation: Yes
Ecuador
Venezuela
Kenya
Bolivia
Brazil
Zimbabwe
Mexico
Crypto exchanges: Regulated
ICOs: Regulated
Upcoming legislation: Yes
Chile
Switzerland
Crypto exchanges: Regulated
ICOs: Regulated
Upcoming legislation: Yes
S.Africa
Australia
Singapore
Crypto exchanges: Grey area
ICOs: Grey area
Upcoming legislation: Yes
Argentina
The light-to-tight regulation scale is based on the following criteria: are Cryptocurrency Exchanges and ICOs banned, regulated or operating in a grey area? Ban = 3 points, regulated = 2 points, grey area = 1 point. Legal Tender? Yes = 1 point, No = 0 points. Is there any planned legislation to increase crypto regulation? Yes = 1 point, No = 0 points. Data collected by ComplyAdvantage should be used as a guide and never taken as legal advice.
ComplyAdvantage



भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2017-18/154 April 6, 2018

DBR.No.BP.BC.104 /08.13.102/2017-18

All Commercial and Co-operative Banks /Payments Banks/Small Finance Banks / NBFCs / Payment System Providers

Madam / Dear Sir,

Prohibition on dealing in Virtual Currencies (VCs)

Reserve Bank has repeatedly through its public notices on December 24, 2013, February 01, 2017 and December 05, 2017, cautioned users, holders and traders of virtual currencies, including Bitcoins, regarding various risks associated in dealing with such virtual currencies.

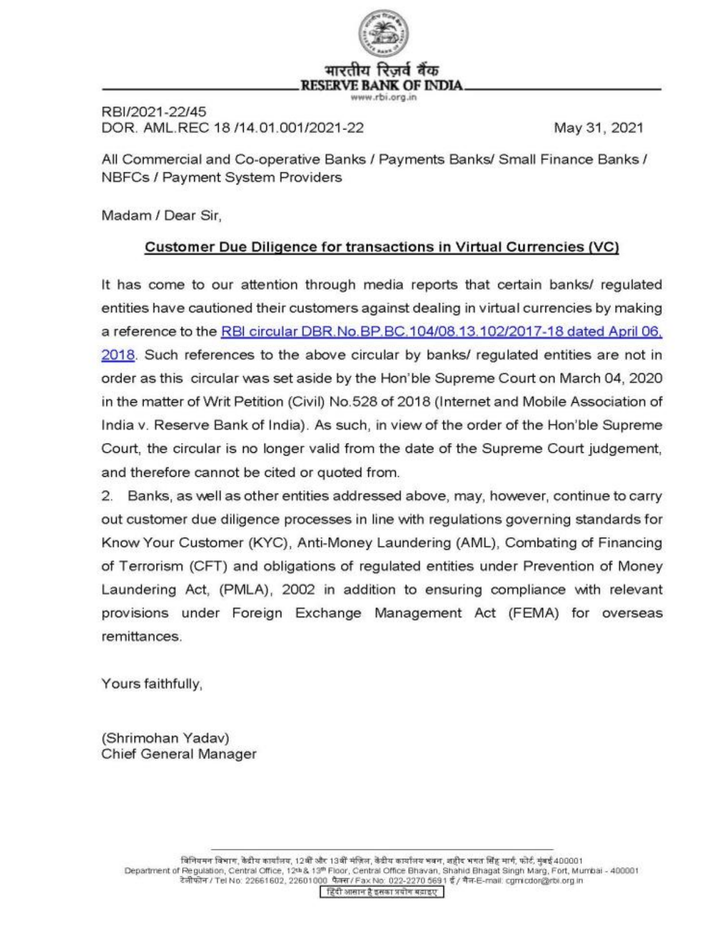
2. In view of the associated risks, it has been decided that, with immediate effect, entities regulated by the Reserve Bank shall not deal in VCs or provide services for facilitating any person or entity in dealing with or settling VCs. Such services include maintaining accounts, registering, trading, settling, clearing, giving loans against virtual tokens, accepting them as collateral, opening accounts of exchanges dealing with them and transfer / receipt of money in accounts relating to purchase/ sale of VCs.

3. Regulated entities which already provide such services shall exit the relationship within three months from the date of this circular.

4. These instructions are issued in exercise of powers conferred by section 35A read with section 36(1)(a) of Banking Regulation Act, 1949, section 35A read with section 36(1)(a) and section 56 of the Banking Regulation Act, 1949, section 45JA and 45L of the Reserve Bank of India Act, 1934 and Section 10(2) read with Section 18 of Payment and Settlement Systems Act, 2007.

Yours faithfully,

(Saurav Sinha)
Chief General Manager-In-Charge



भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2021-22/45
DOR. AML.REC 18 /14.01.001/2021-22 May 31, 2021

All Commercial and Co-operative Banks / Payments Banks/ Small Finance Banks / NBFCs / Payment System Providers

Madam / Dear Sir,

Customer Due Diligence for transactions in Virtual Currencies (VC)

It has come to our attention through media reports that certain banks/ regulated entities have cautioned their customers against dealing in virtual currencies by making a reference to the RBI circular DBR.No.BP.BC.104/08.13.102/2017-18 dated April 06, 2018. Such references to the above circular by banks/ regulated entities are not in order as this circular was set aside by the Hon'ble Supreme Court on March 04, 2020 in the matter of Writ Petition (Civil) No.528 of 2018 (Internet and Mobile Association of India v. Reserve Bank of India). As such, in view of the order of the Hon'ble Supreme Court, the circular is no longer valid from the date of the Supreme Court judgement, and therefore cannot be cited or quoted from.

2. Banks, as well as other entities addressed above, may, however, continue to carry out customer due diligence processes in line with regulations governing standards for Know Your Customer (KYC), Anti-Money Laundering (AML), Combating of Financing of Terrorism (CFT) and obligations of regulated entities under Prevention of Money Laundering Act, (PMLA), 2002 in addition to ensuring compliance with relevant provisions under Foreign Exchange Management Act (FEMA) for overseas remittances.

Yours faithfully,

(Shrimohan Yadav)
Chief General Manager

विनियमन विभाग, केंद्रीय कार्यालय, 12वीं और 13वीं मंज़िल, केंद्रीय कार्यालय भवन, शहीद भगत सिंह मार्ग, फोर्ट, मुंबई 400001
Department of Regulation, Central Office, 12th & 13th Floor, Central Office Bhavan, Shahid Bhagat Singh Marg, Fort, Mumbai - 400001
टेलीफोन / Tel No: 22661602, 22601000 फैक्स / Fax No: 022-2270 5691 ई / मेल-E-mail: cgmicdor@rbi.org.in
हिंदी आसान है इसका प्रयोग बढ़ाइए

Conclusion

A new technology to realize its full potential, a lot of circumstances need to co-exist before network effects can be realized. In order for the technology to bring in systemic efficiencies, a critical mass needs to be attained.

The block chain community is indeed witnessing unprecedented levels of industry collaboration between players who are otherwise competitors in the space. Because of the cost of moving from one infrastructure technology to the next, an open source collaborative approach is the most promising way forward.

This is the direction we insisted on in this paper, highlighting not only how to minimize the trust issues, but also what consensus mechanisms should be used and deployed to maximize the scaling and leading us towards an highly developed and sustainable operating environment.

References

1. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: May 17, 2021].
2. M. H. u. Rehman, K. Salah, E. Damiani and D. Svetinovic, "Trust in Blockchain Cryptocurrency Ecosystem," in IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1196-1212, Nov. 2020, doi: 10.1109/TEM.2019.2948861.
3. D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and G. Das, "Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems," in IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 6-14, July 2018, doi: 10.1109/MCE.2018.2816299.
4. M. Belotti, N. Božić, G. Pujolle and S. Secci, "A Vademecum on Blockchain Technologies: When, Which, and How," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3796-3838, Fourthquarter 2019, doi: 10.1109/COMST.2019.2928178.
5. S. Alzahrani and T. U. Daim, "Analysis of the Cryptocurrency Adoption Decision: Literature Review," 2019 Portland International Conference on Management of Engineering and Technology (PICMET), 2019, pp. 1-11, doi: 10.23919/PICMET.2019.8893819.
6. M. Mirtaheri, S. Abu-El-Haija, F. Morstatter, G. V. Steeg and A. Galstyan, "Identifying and Analyzing Cryptocurrency Manipulations in Social Media," in IEEE Transactions on Computational Social Systems, vol. 8, no. 3, pp. 607-617, June 2021, doi: 10.1109/TCSS.2021.3059286.
7. S. Alzahrani and T. U. Daim, "Analysis of the Cryptocurrency Adoption Decision: Literature Review," 2019 Portland International Conference on Management of Engineering and Technology (PICMET), 2019, pp. 1-11, doi: 10.23919/PICMET.2019.8893819.
8. Joseph Poon and Thaddeus Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,” 2016. [Online]. Available: 1https://lightning.network/lightning-network-paper.pdf. [Accessed: June 1 , 2021].
9. Colin LeMahieu, “Nano: A Feeless Distributed Cryptocurrency Network,” 2017. [Online]. Available: https://content.nano.org/whitepaper/Nano_Whitepaper_en.pdf. [Accessed: May 25, 2021].
10. Matt Hussey, Tim Copel and and Daniel Phillips, “What is Lightning Network? And How to Use It in 2020,” *Decrypt*, Sep. 3, 2020. [Online]. Available: https://decrypt.co/resources/bitcoin-lightning-network. [Accessed: May 20, 2021].

11. J. -H. Lee, "Rise of Anonymous Cryptocurrencies: Brief Introduction," in IEEE Consumer Electronics Magazine, vol. 8, no. 5, pp. 20-25, 1 Sept. 2019, doi: 10.1109/MCE.2019.2923927.
12. Benjamin Godfrey, “Ethereum 2.0 First Upgrade Altair Is Coming: Key Notes for Validators,” *Coinspeaker*, May 21, 2021. [Online]. Available: https://www.coinspeaker.com/ethereum-2-0-upgrade-altair-coming/. [Accessed: May 21, 2021].
13. “Tracing the Twitter Hack Bitcoins - An Update from Elliptic,” *Elliptic*, July 23, 2020. [Online]. Available: https://www.elliptic.co/blog/tracing-the-twitter-hack-bitcoins-an-update-from-elliptic#. [Accessed: July 25, 2020].
14. Josiah Wilmoth, “Think Coinbase Employees Engaged in Insider Trading? Deal With It.,” *CNN*, Dec. 20, 2017. [Online]. Available: https://www.ccn.com/think-coinbase-employees-engaged-in-insider-trading-deal-with-it/. [Accessed: June 2, 2021].