

Blockchain Analysis of the Bitcoin Market

Igor Makarov Antoinette Schoar
LSE MIT Sloan, NBER, Ideas42

Bank of Canada, February 25th, 2022

Motivation

- Cryptocurrencies have grown significantly over the last decade



B Bloomberg.com
Bitcoin (\$BTC USD),
Ether (\$ETH) Lead
Crypto to \$3 Trillion
Market Cap

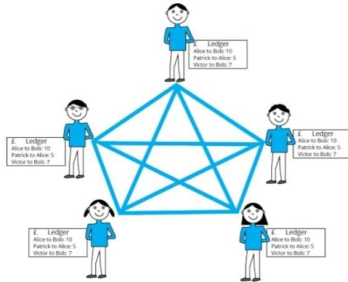
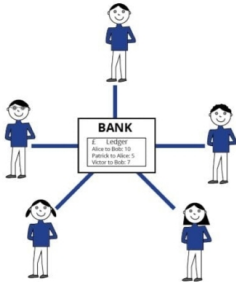


US Public Pension Fund for Firefighters Adds Bitcoin and Ether Worth \$25 Million to Portfolio



- Many calls for even wider Bitcoin adoption but there are still many open questions about the utilization of Bitcoin, its major players, potential risks, and spillover effects on the real economy

“Trustless” trust architecture



This Paper

- A systematic analysis of the Bitcoin market using the Bitcoin blockchain data
- Three major pieces of analysis:
 - **Network structure:** Analyze the transaction volume and network structure of the main market participants
 - Exchanges are central entities; 75% of volume is linked to exchanges
 - **Ownership concentration:** Document the ownership concentration of the largest bitcoin investors
 - High concentration: top 1K investors control 3M BTC, top 10K - 5M BTC
 - **Miners:** Study the concentration and regional composition of miners who ensure the integrity of the Bitcoin blockchain
 - High concentration: 50 miners often control 50% of the total market

Digital Footprint of Bitcoin Transactions

- Bitcoins are stored in Bitcoin addresses
- Bitcoin transactions record how bitcoins move between Bitcoin addresses

bc:a8178a7223372414ac060b4bba4b33b8b4847a756fa76a715af71d11bfd143d5		1,388.19794059 BTC	Fee: 0.001 BTC	
← prev tx	17A16QmavnUICW11DAApiJxp7ARnxN5pGX	-1,388.1984059 BTC		
			3QKAn2B1uDquujLZnoynVog1M9uac66Ysr	0.00795759 BTC
			1F81DpYbMLMaz11BEehqPJSN6XTL615TDz	0.01241030 BTC
			17A16QmavnUICW11DAApiJxp7ARnxN5pGX	1,388.1747294 BTC
bc:efb3f60304532ebc80163b5f375fa8a9a39a8b0807b99703b6b646c1f7af5bf		0.71061009 BTC	Fee: 0.001174 BTC	
← prev tx	3EocBKm4AgtX6Bb7P8HokjoVhCTZWNWP5q	-0.3229217 BTC		
← prev tx	3KA8RU8rmQEMVwXSQSPBkqgewZw63Upfwx	-0.30097999 BTC		
← prev tx	33QJiiYPkQzYf5BNbCzIHWowhco77sg18g	-0.08020333 BTC		
← prev tx	14J6bdZjJPeiJPEwcTgd7RWXRjUaMocqfN	-0.00310334 BTC		
← prev tx	3DqmyW4NLHgNOP7T32gstNe1sx88rKyaB	-0.00480385 BTC		
			3JGTTdXUwFSdmb6mWptD4CaXYm6KTdITPc	0.00302938 BTC
			3HLUD8a8C4wKlaNTj1n9D3NKpNMLMgjWkk	0.7106887 BTC

- Two main challenges:
 - Bitcoin addresses are easy to generate ⇒ potentially many addresses belong to the same entity
 - Link anonymous Bitcoin addresses to real-life entities

Data

- Obtain blockchain data using the open-source software of Bitcoin Core and use the BlockSci program to convert raw data into a database
 - As of June 28, 2021, there are about 650 million Bitcoin transactions and 850 million unique addresses
- Link addresses to real-life entities using public and proprietary sources
 - Scrape cryptocurrency blogs and websites, such as Reddit, Blockchain.info, bitcointalk.org, walletexplorer.com, and Matbea.com
 - State-of-the-art database of crypto entities from Bitfury Crystal Blockchain, one of the leading providers of anti-money-laundering tools

Data, continued

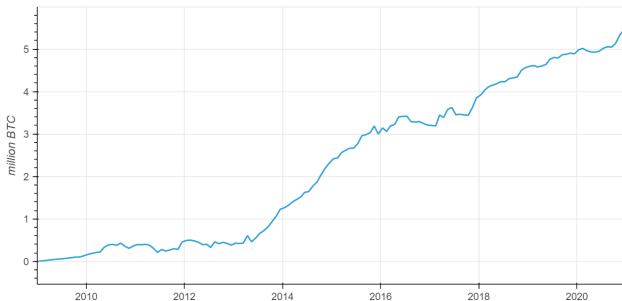
- Most complete information about crypto entities that have been used in academic research
 - We cover 1,043 of the largest entities
 - 393 exchanges, 86 gambling sites, 39 on-line wallets, 33 payment processors, 63 mining pools, 35 scammers, 227 ransomware attackers, 151 dark net marketplaces and illegal services

Ownership of Bitcoin

Ownership of Bitcoin

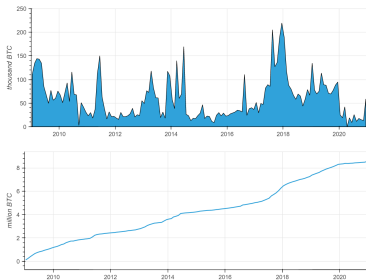
- Important to understand ownership and concentration of Bitcoin holdings
 - Determines who will benefit most from wider adoption. A select few investors or the general public?
- A challenging task:
 - More than just tracing “rich list” of addresses with large balances
 - Many addresses belong to exchanges and other intermediaries that hold bitcoins on behalf of many investors
- We use graph analysis and examine utilization pattern to separate intermediary and individual accounts

Intermediary Ownership

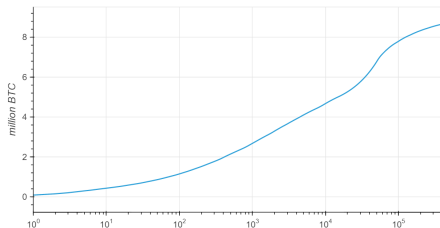


- As of Dec 2020, exchanges and other intermediaries held 5.5M BTC

Individual Ownership



early vs late adopters

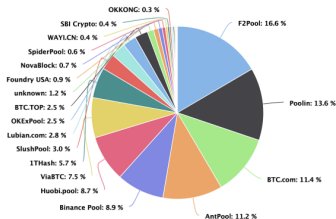


ownership concentration

- As of Dec 2020, individuals held 8.5M BTC
- High concentration of ownership:
 - top 1000 investors control 3M BTC
 - top 10,000 - 5M BTC

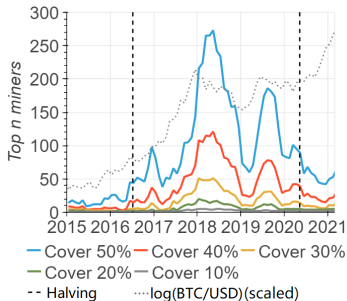
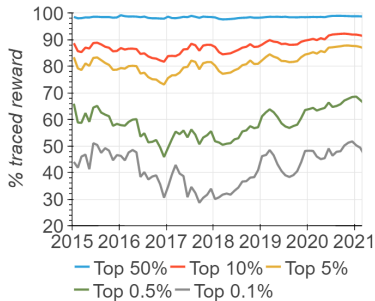
Miners

Miners: Provide Verification of Transactions



- Mining is done in pools
 - Provide coinsurance by pooling capacity of miners
 - Highly concentrated
 - Majority of pools are registered in China
- But mining pools are not miners!
- Pools' power depends on the size distribution of miners
- We identify miners by analyzing pool distributions ~ 250K miners

Concentration of Mining Capacity



- Mining capacity is concentrated
- Concentration varies with the Bitcoin price
- We estimate that about 70% of miners are located in China based on the geographic location of exchanges where miners cash out their rewards (pre June 2021)
 - Use Xinjiang mining incidence (April 17-18, 2021) to verify our results

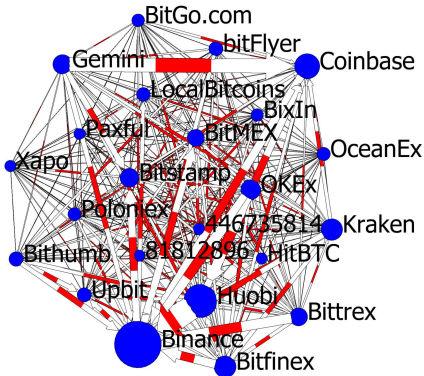
Network Structure

Volume Decomposition

- 75% of the blockchain volume is for trading activity
- Other transactions, e.g., gambling or illegal transactions are only a small share of total volume (< 3% combined)
- Exchanges are central entities on the blockchain and are highly interconnected

Largest Entities

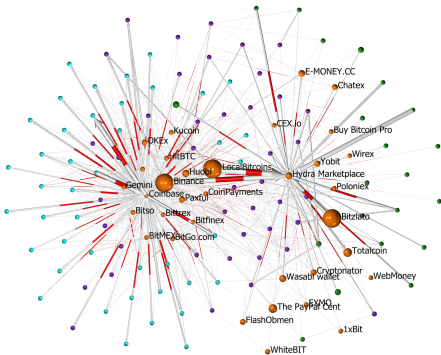
- Exchanges are central entities on the blockchain



- Ex: Network of entities that receive > 500K BTC over 2018-2020
 - 18 exchanges, 3 online wallets, 2 unknown entities — likely large OTC desks
 - Almost a complete graph
 - Large volume between KYC (e.g., Coinbase and Gemini) and non-KYC (e.g., Binance) exchanges

Illegal Transactions

- A small share of total volume (< 3%) but not a trivial amount ~ \$2.4B in 2020



Ex: Hydra network: Retain only nodes that send >1000 BTC within the network

- Highest volume entities interacting directly with dark net marketplaces are non-KYC exchanges
 - E.g. LocalBitcoins, Bitzlatto, Binance
 - But once the flows arrive to these exchanges they get mixed with other flows and become virtually untraceable, and so can be sent anywhere afterwards
- Direct interactions of dark net marketplaces with exchanges that enforce KYC norms are small, but their interaction with the neighboring “mixing” clusters is large

Implications for KYC regulation

- Current situation: KYC entities are allowed to accept flows from entities with lax-KYC norms. Digital footprint has limited effect on preventing tainted flows from entering into circulation
 - Even if KYC entities were restricted to deal exclusively with other KYC entities, preventing inflows of tainted funds would require placing severe restrictions on who can transact with whom
 - Every transaction would have to be subject to the approval of Bitcoin analytics companies e.g. Bitfury Crystal Blockchain and Chainalysis. They would be de facto trusted parties
- The wider the adoption of Bitcoin is, the easier it will become to use it for illegal transactions or tax evasion without ever having to touch regulated entities

Main Takeaways

- The majority of Bitcoin volume is for trading activity
- Exchanges are central entities on the blockchain
- Bitcoin ownership is concentrated
- Mining industry is concentrated
- The current KYC regulation has limited effect on preventing tainted flows from entering into circulation

Thank You!