Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies

Presenter: Ruming Liu[1]
Author: Sean Foley & Jonathan Karlsen & Talis J. Putniņš

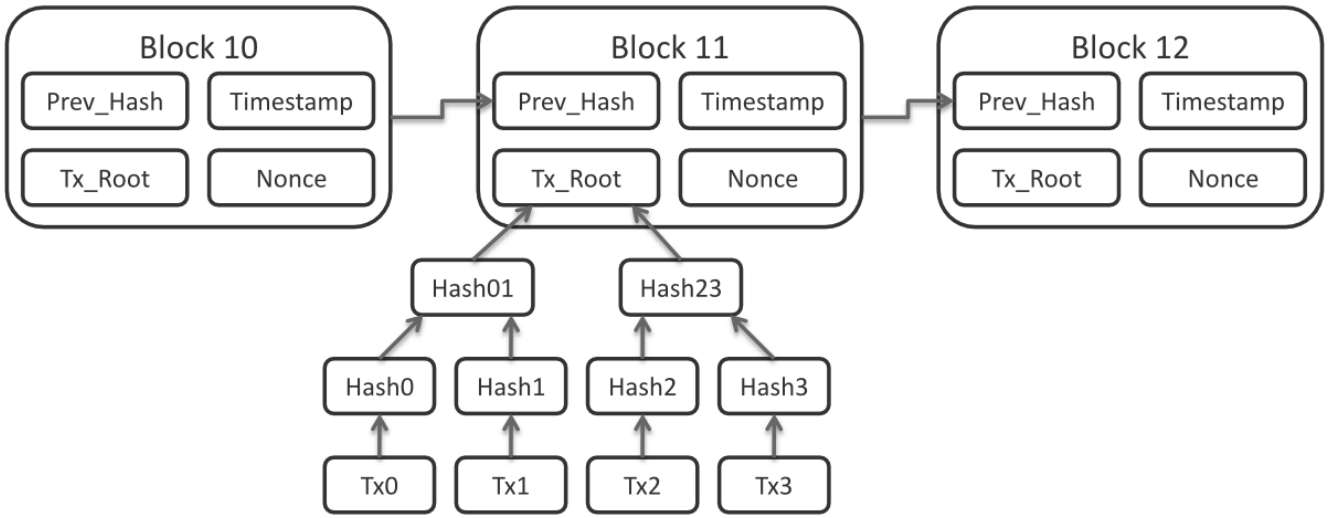
Stevens Institute of Technology[1]

MGT-719A Research Design
Nov 1st, 2022

Outline

Bitcoin Payment System

- Bitcoin system is defined in the white paper **"A Peer-to-Peer Electronic Cash System"** by an assumed name Satoshi Nakamoto.



- Contrast to the centralized banking currency system, a decentralized blockchain system does not have a central authority and the network is distributed. And it can ensure the data integrity.
- Blockchain derived from several ideas in academia: Distributed system, consensus protocol and zero knowledge proof in computer science. Smart contract, P2P finance, Behavior economics and game theory in finance.

What can blockchain do in the real world?

- Bitcoin was introduced as a digital currency in bitcoin blockchain, so it can be used as an "anonymous" payment method. (Be careful, it's not the really "anonymous", "pseudonymous" is a better definition)
- 

- Some other projects in the blockchain (e.g Ethereum, Dash) may have more interesting functions: smart contract, fully anoymous, etc. These functions is the ground for further projects: Decentralized Finance(Defi), Web 3.0, digital collection(NFT), Metaverse...

Bitcoin Literature Review

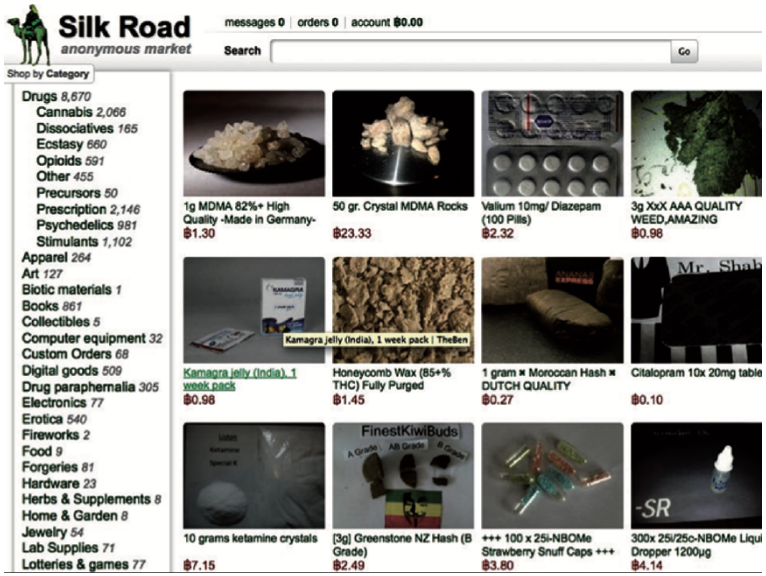
- Even though Bitcoin may not so fancy like other blockchains, it is still the first project to make the idea become real. It has the longest history and largest market capitalization. That's why a lot of researches in finance put some attention to bitcoin.
- There are several important research areas in bitcoin blockchain:
  - Asset pricing (e.g Pricing Cryptocurrency Options, 2020 <Journal of Financial Econometrics>)
  - Consensus (e.g The Blockchain Folk Theorem, 2019 <Review of Finance Studies>)
  - Reward protocol (e.g Blockchain without Waste: Proof-of-Stake, 2020 <Review of Finance Studies>)
  - Supplychain Management (e.g On the Financing Benefits of Supply Chain Transparency and Blockchain Adoption, 2019 <Management Science>)
  - ...
  - Illegal trade in blockchain (e.g Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies, 2019 <Review of Finance Studies>)

Illegal activity in bitcoin system

- A natural question is: what kinds of transactions are involved in bitcoin system?
- 1. Miners' rewards: miners will get some bitcoins as the reward of verifying transactions and maintaining the bitcoin ledger.
- 2. Some honest users may use bitcoins as an alternative payment method in the real world, like cross-border transfer (instead of using bank system protocol: VISA, MASTERCARD...).
- 3. However, bitcoins also offer a "safer" way for criminal transactions in dark net. (Drugs, money laundry, smuggling...)

Illegal activity in bitcoin system - Silk Road

- Silk Road was an online black market and the first modern darknet market, launched in February 2011



- In October 2013, the Federal Bureau of Investigation (FBI) shut down the website and arrested its founder Ross Ulbricht. In November 2020, the United States government seized more than $1 billion worth of bitcoin connected to Silk Road.
- End day of black market? No way, Silk Road 2.0...

Motivation of this research

- From the story of silk road, we suspect there are lot of illegal users in bitcoin.
- Can we build a model to clarify whether a user in the blockchain system is a legal or illegal user?
- Of course, the training set is hard to collect, because no one is willing to admit that he/she is an illegal user in bitcoin.
- But fortunately, the FBI did a favor for us. They seized more than $1 billion worth bitcoin in Silk Road, that's a valuable data for us to start.

Identifying users in transaction-level bitcoin data

- Bitcoin special mechanics: unless a holding of bitcoin with a given address is exactly spent in a transaction, the "change" from the transaction is returned to a new address forming a new parcel of bitcoin.
- Say you want to buy a candy bar ($1) from a store. You open your wallet (fiat wallet) and inside there is a single $20 bill. What is the minimum amount you can pay? It isn't $1; you can't rip up 1/20th of the bill and give it to the cashier. You need to pay $20 and since you only owe $1, the cashier gives you back $19.
- Union-Find algorithm: If we detect change: A $\rightarrow$ B, B $\rightarrow$ C. Then we can say wallets A, B, C are controlled by the same user.
- The Union-Find algorithm might fail to cluster together two sets of addresses controlled by one user if that user never makes a transaction that uses an address from both sets. But it is a still suitable and conservative choice.

Transaction filters

- Remove transaction fees and block rewards.
- Remove currency conversion transactions.
- Remove transactions that reflect the "change" given back.
- Remove small amount ($< 1\$$) transactions.

Descriptive statistics for all users

Descriptive statistics for all users

Variable	Mean	SD	Min	P25	Median	P75	Max
A. Transactional characteristics							
Transaction count	5.70	1,622.74	1.00	2.00	3.00	3.00	11,410,691.00
Transaction size	5,207.61	56,939.00	1.00	22.06	111.91	668.44	92,504,688.00
Transaction frequency	29.88	659.27	0.12	7.20	24.00	36.00	3,077,978.00
Counterparties	4.18	553.71	0.00	2.00	3.00	3.00	4,385,500.00
Holding value	3,974.05	55,011.00	0.00	15.91	83.96	551.37	115,529,839.00
Concentration	0.10	0.28	0.00	0.00	0.00	0.00	1.00
Existence time	6.61	11.91	1.00	1.00	1.00	5.00	101.00
B. Characteristics associated with particular types of activity							
Darknet sites	17.14	5.10	0.00	15.00	18.00	20.00	27.00
Tumbling	0.45	0.05	0.00	0.00	0.00	0.00	181.82
Darknet shock volume	16.51	0.36	0.00	0.00	0.00	0.00	100.00
Bitcoin hype	28.29	15.44	0.00	19.00	24.00	38.00	100.00
Pre-Silk-Road user	0.07	0.26	0.00	0.00	0.00	0.00	1.00
Bitcoin market cap	9.82	0.49	5.14	9.71	9.94	10.09	10.40
Shadow coins	7.07	2.52	0.00	7.28	7.78	8.32	9.10
Alt coins	8.68	2.04	0.00	8.76	9.21	9.34	10.26

- Concentration takes values between zero and one, with higher values indicating a tendency to repeatedly trade with a smaller number of counterparties.

Descriptive statistics for all users

Descriptive statistics for all users

Variable	Mean	SD	Min	P25	Median	P75	Max
A. Transactional characteristics							
Transaction count	5.70	1,622.74	1.00	2.00	3.00	3.00	11,410,691.00
Transaction size	5,207.61	56,939.00	1.00	22.06	111.91	668.44	92,504,688.00
Transaction frequency	29.88	659.27	0.12	7.20	24.00	36.00	3,077,978.00
Counterparties	4.18	553.71	0.00	2.00	3.00	3.00	4,385,500.00
Holding value	3,974.05	55,011.00	0.00	15.91	83.96	551.37	115,529,839.00
Concentration	0.10	0.28	0.00	0.00	0.00	0.00	1.00
Existence time	6.61	11.91	1.00	1.00	1.00	5.00	101.00
B. Characteristics associated with particular types of activity							
Darknet sites	17.14	5.10	0.00	15.00	18.00	20.00	27.00
Tumbling	0.45	0.05	0.00	0.00	0.00	0.00	181.82
Darknet shock volume	16.51	0.36	0.00	0.00	0.00	0.00	100.00
Bitcoin hype	28.29	15.44	0.00	19.00	24.00	38.00	100.00
Pre-Silk-Road user	0.07	0.26	0.00	0.00	0.00	0.00	1.00
Bitcoin market cap	9.82	0.49	5.14	9.71	9.94	10.09	10.40
Shadow coins	7.07	2.52	0.00	7.28	7.78	8.32	9.10
Alt coins	8.68	2.04	0.00	8.76	9.21	9.34	10.26

- Darknet sites is the average number of operational darknet sites at the time of each of the user's transactions.

Descriptive statistics for all users

Descriptive statistics for all users

Variable	Mean	SD	Min	P25	Median	P75	Max
A. Transactional characteristics							
Transaction count	5.70	1,622.74	1.00	2.00	3.00	3.00	11,410,691.00
Transaction size	5,207.61	56,939.00	1.00	22.06	111.91	668.44	92,504,688.00
Transaction frequency	29.88	659.27	0.12	7.20	24.00	36.00	3,077,978.00
Counterparties	4.18	553.71	0.00	2.00	3.00	3.00	4,385,500.00
Holding value	3,974.05	55,011.00	0.00	15.91	83.96	551.37	115,529,839.00
Concentration	0.10	0.28	0.00	0.00	0.00	0.00	1.00
Existence time	6.61	11.91	1.00	1.00	1.00	5.00	101.00
B. Characteristics associated with particular types of activity							
Darknet sites	17.14	5.10	0.00	15.00	18.00	20.00	27.00
Tumbling	0.45	0.05	0.00	0.00	0.00	0.00	181.82
Darknet shock volume	16.51	0.36	0.00	0.00	0.00	0.00	100.00
Bitcoin hype	28.29	15.44	0.00	19.00	24.00	38.00	100.00
Pre-Silk-Road user	0.07	0.26	0.00	0.00	0.00	0.00	1.00
Bitcoin market cap	9.82	0.49	5.14	9.71	9.94	10.09	10.40
Shadow coins	7.07	2.52	0.00	7.28	7.78	8.32	9.10
Alt coins	8.68	2.04	0.00	8.76	9.21	9.34	10.26

- Tumbling is the percentage of the user's transactions that attempt to obscure the user's holdings (wash or tumbling trades).

Descriptive statistics for all users

Descriptive statistics for all users

Variable	Mean	SD	Min	P25	Median	P75	Max
A. Transactional characteristics							
Transaction count	5.70	1,622.74	1.00	2.00	3.00	3.00	11,410,691.00
Transaction size	5,207.61	56,939.00	1.00	22.06	111.91	668.44	92,504,688.00
Transaction frequency	29.88	659.27	0.12	7.20	24.00	36.00	3,077,978.00
Counterparties	4.18	553.71	0.00	2.00	3.00	3.00	4,385,500.00
Holding value	3,974.05	55,011.00	0.00	15.91	83.96	551.37	115,529,839.00
Concentration	0.10	0.28	0.00	0.00	0.00	0.00	1.00
Existence time	6.61	11.91	1.00	1.00	1.00	5.00	101.00
B. Characteristics associated with particular types of activity							
Darknet sites	17.14	5.10	0.00	15.00	18.00	20.00	27.00
Tumbling	0.45	0.05	0.00	0.00	0.00	0.00	181.82
Darknet shock volume	16.51	0.36	0.00	0.00	0.00	0.00	100.00
Bitcoin hype	28.29	15.44	0.00	19.00	24.00	38.00	100.00
Pre-Silk-Road user	0.07	0.26	0.00	0.00	0.00	0.00	1.00
Bitcoin market cap	9.82	0.49	5.14	9.71	9.94	10.09	10.40
Shadow coins	7.07	2.52	0.00	7.28	7.78	8.32	9.10
Alt coins	8.68	2.04	0.00	8.76	9.21	9.34	10.26

- Darknet shock volume is the percentage of the user's total dollar volume that is transacted during the week after marketplace seizures or "exit scams."

Descriptive statistics for all users

Descriptive statistics for all users

Variable	Mean	SD	Min	P25	Median	P75	Max
A. Transactional characteristics							
Transaction count	5.70	1,622.74	1.00	2.00	3.00	3.00	11,410,691.00
Transaction size	5,207.61	56,939.00	1.00	22.06	111.91	668.44	92,504,688.00
Transaction frequency	29.88	659.27	0.12	7.20	24.00	36.00	3,077,978.00
Counterparties	4.18	553.71	0.00	2.00	3.00	3.00	4,385,500.00
Holding value	3,974.05	55,011.00	0.00	15.91	83.96	551.37	115,529,839.00
Concentration	0.10	0.28	0.00	0.00	0.00	0.00	1.00
Existence time	6.61	11.91	1.00	1.00	1.00	5.00	101.00
B. Characteristics associated with particular types of activity							
Darknet sites	17.14	5.10	0.00	15.00	18.00	20.00	27.00
Tumbling	0.45	0.05	0.00	0.00	0.00	0.00	181.82
Darknet shock volume	16.51	0.36	0.00	0.00	0.00	0.00	100.00
Bitcoin hype	28.29	15.44	0.00	19.00	24.00	38.00	100.00
Pre-Silk-Road user	0.07	0.26	0.00	0.00	0.00	0.00	1.00
Bitcoin market cap	9.82	0.49	5.14	9.71	9.94	10.09	10.40
Shadow coins	7.07	2.52	0.00	7.28	7.78	8.32	9.10
Alt coins	8.68	2.04	0.00	8.76	9.21	9.34	10.26

- Bitcoin hype is a measure of the intensity of Google searches for the term "bitcoin" around the time of the user's trades.

Descriptive statistics for all users

Descriptive statistics for all users

Variable	Mean	SD	Min	P25	Median	P75	Max
A. Transactional characteristics							
Transaction count	5.70	1,622.74	1.00	2.00	3.00	3.00	11,410,691.00
Transaction size	5,207.61	56,939.00	1.00	22.06	111.91	668.44	92,504,688.00
Transaction frequency	29.88	659.27	0.12	7.20	24.00	36.00	3,077,978.00
Counterparties	4.18	553.71	0.00	2.00	3.00	3.00	4,385,500.00
Holding value	3,974.05	55,011.00	0.00	15.91	83.96	551.37	115,529,839.00
Concentration	0.10	0.28	0.00	0.00	0.00	0.00	1.00
Existence time	6.61	11.91	1.00	1.00	1.00	5.00	101.00
B. Characteristics associated with particular types of activity							
Darknet sites	17.14	5.10	0.00	15.00	18.00	20.00	27.00
Tumbling	0.45	0.05	0.00	0.00	0.00	0.00	181.82
Darknet shock volume	16.51	0.36	0.00	0.00	0.00	0.00	100.00
Bitcoin hype	28.29	15.44	0.00	19.00	24.00	38.00	100.00
Pre-Silk-Road user	0.07	0.26	0.00	0.00	0.00	0.00	1.00
Bitcoin market cap	9.82	0.49	5.14	9.71	9.94	10.09	10.40
Shadow coins	7.07	2.52	0.00	7.28	7.78	8.32	9.10
Alt coins	8.68	2.04	0.00	8.76	9.21	9.34	10.26

- Bitcoin market cap, Shadow coins, and Alt coins are transaction-weighted average log market capitalizations of bitcoin, major opaque cryptocurrencies, and nonprivacy cryptocurrencies excluding bitcoin, respectively, at the time of each user's transactions.

1st approach: bitcoin seizures by law enforcement agencies

- Our first approach exploits bitcoin seizures by law enforcement agencies, such as the U.S. FBI. We manually identify bitcoin seizures from news articles (via searches using Factiva) and U.S. court records (via searches of the digital PACER records).
- In some cases (e.g., the U.S. FBI's seizure of Silk Road and Ross Ulbricht's holdings, and the Australian law enforcement's seizure of Richard Pollard's holdings) the law enforcement agency auctioned the seized bitcoin to the public. Then, we are able to identify the auction transactions on the bitcoin blockchain and work backwards to identify the seized bitcoin users.
- Using this approach we identify 1,016 known illegal users, which we refer to as "Seized users."

2nd approach: illegal darknet marketplaces and users

- We identify darknet marketplace users as individuals that send to and/or receive bitcoin from a known darknet marketplace.
- Using this approach we identify slightly over 6 million darknet marketplace users, which we refer to as "Black market users".

3rd approach: Users identified in darknet forums

- Our third approach exploits information contained in the darknet, in particular the bitcoin addresses of users identified in darknet forums as selling goods/services. We use systematic scrapes of darknet forums from 2013 to 2017. This allows us to identify users that might never have been caught by authorities and might not be otherwise identified in the data through transactions with known darknet marketplaces.
- Using this approach, we identify an additional 448 users that were not already identified in either of the previous two approaches. We refer to these as "Forum users."

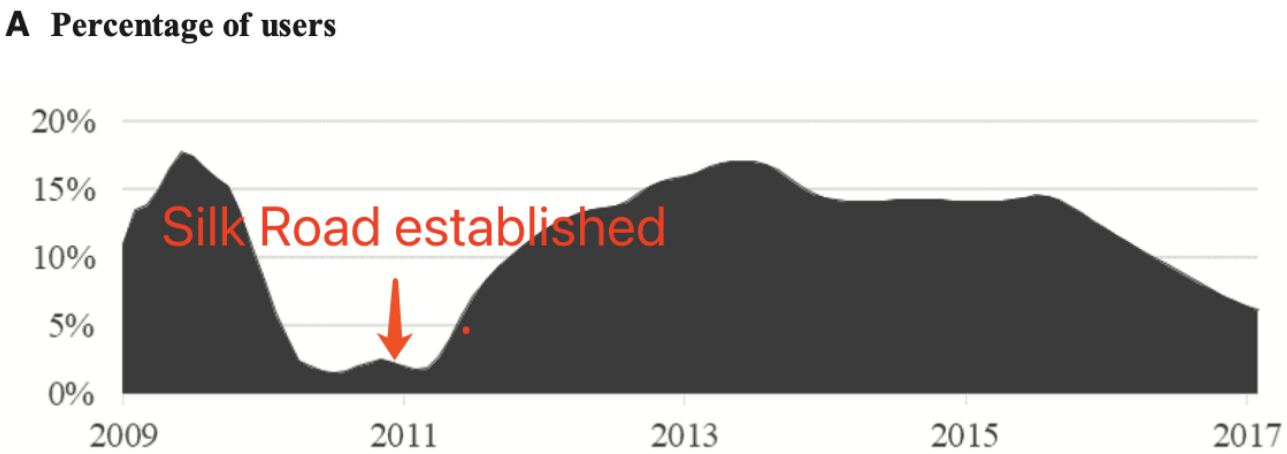
Size and activity of oberserved user groups

Size and activity of observed user groups

Group/subgroup	Users	Transaction count (mil)	Holding value ($mil)	Number of addresses (mil)	Volume ($bil)
1. All users	106,244,432 (100.00%)	605.69 (100.00%)	2,964.66 (100.00%)	221.71 (100.00%)	1,862.51 (100.00%)
2. Observed illegal users	6,223,359 (5.86%)	196.11 (32.38%)	1,342.43 (45.28%)	58.38 (26.33%)	241.46 (12.96%)
2A. Seized users	1,041 (0.00%)	23.83 (3.93%)	9.39 (0.32%)	8.30 (3.74%)	17.51 (0.94%)
2B. Black market users (not in 2A)	6,221,870 (5.86%)	157.30 (25.97%)	1,324.32 (44.67%)	49.71 (22.42%)	220.91 (11.86%)
2C. Forum users (not in 2A or 2B)	448 (0.00%)	14.98 (2.47%)	8.72 (0.29%)	0.38 (0.17%)	3.03 (0.16%)
3. Other users	100,021,073 (94.14%)	409.58 (67.62%)	1,622.23 (54.72%)	163.33 (73.67%)	1,621.05 (87.04%)

- Illegal users take more transactions, because they use bitcoin as payment method instead of long term investment.
- A limitation of the sample of observed illegal users is that: other forms of illegal activity, such as money laundering, payments in ransomware attacks, and bitcoin thefts, also involve bitcoin. Thus, our estimates are likely to underestimate some forms of illegal activity involving bitcoin.

Size and activity of oberserved user groups



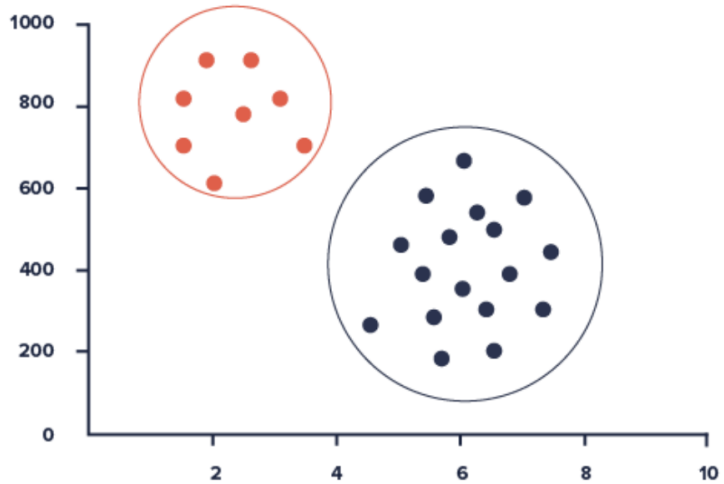
- Silk Road 1 was established in January 2011 and soon became a popular venue in which to buy and sell illegal goods and services. After Silk Road 1 was shut down by the U.S. FBI in October of 2013, a large number of other illegal darknet marketplaces commenced operating throughout 2013–2015.
- Peak activity of our sample of observed illegal users coincides with substantial darknet marketplace activity. However, we also observe a reasonable number of illegal users and illegal activity outside of this peak window.

Characterizing all illegal activity

- We used 3 approaches to identify a substantial sample of bitcoin users that are involved in illegal activity.
- Then our next step is to use the information in this sample to estimate the totality of illegal activity.
- We use two different methods to classify users into those that are primarily involved in illegal activity ("illegal users") and those that are primarily involved in legal activity ("legal users").

1st method: Network cluster analysis

- At an intuitive level, this method exploits the network topology— the information about who trades with whom. Trade networks reveal "communities" of users and can thereby identify other illegal users that were not part of our initial sample.
- E.g., if users A, B, and C are known to be involved in illegal activity (e.g., their bitcoin was seized by law enforcement agencies), a user X that trades exclusively or predominantly with users A, B, or C is likely to also be involved in illegal activity.

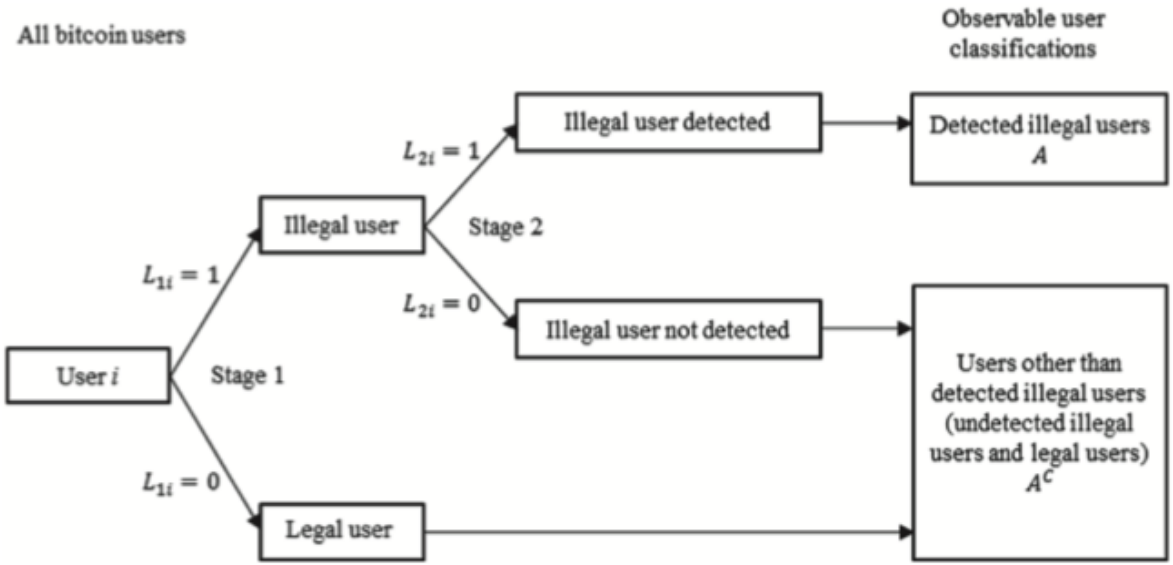


Smart local moving (SLM) algorithm

- The algorithm finds the underlying community structure in the network by moving nodes from one community to another, if such a move improves the model fit.
- Pseudocode
  step 1: Assign alltheobserved illegal users to the illegal community and all of the remaining users to the legal community.
  step 2: Loop through each user,performing the following action on each:
  – If the user disproportionately transacts with members of the user's currently assigned community, then leave the user in that community;
  – Otherwise, move the user to the other community (if the user is assigned to the illegal community, move the user to legal community, and vice versa).
  step 3: Repeat step 2 until the communities are stable.

2nd method: Detection-controlled estimation (DCE)

- At an intuitive level, this method exploits characteristics that distinguish illegal users from legal users (controlling for nonrandom detection).



2nd method: Detection-controlled estimation (DCE)

- where

$$\mathsf{Y}_{1i} = \beta_1 x_{1i} + \epsilon_{1i} \ (1)$$

$$L_{1i} = \begin{cases} 1 \ (Illegaluser) \ if \ \mathsf{Y}_{1i} > 0 \\ 0 \ (Legaluser) \ if \ \mathsf{Y}_{1i} \leq 0 \end{cases} \quad (2)$$

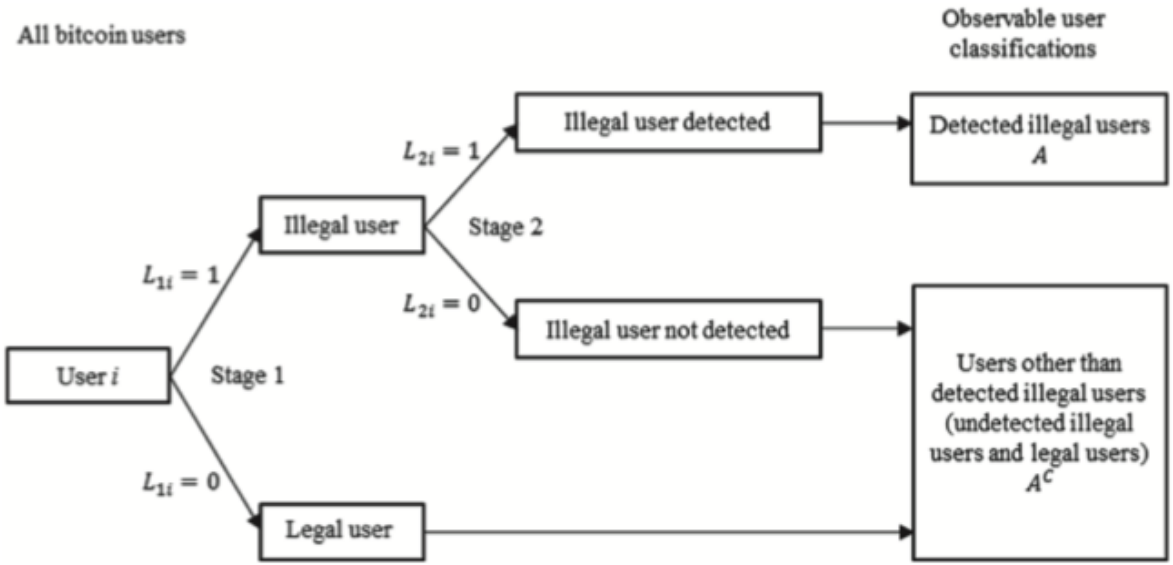
$$\mathsf{Y}_{2i} = \beta_1 x_{2i} + \epsilon_{2i} \ (3)$$

$$L_{2i} = \begin{cases} 1 \ (Detected) \ if \ \mathsf{Y}_{2i} > 0 \\ 0 \ (Notdetected) \ if \ \mathsf{Y}_{2i} \leq 0 \end{cases} \quad (4)$$

2nd method: Detection-controlled estimation (DCE)

- x_{1i} includes: Tumbling, Darknet shock volume, Bitcoin hype, Shadow coins, Alt coins...
- x_{2_i} includes: Pre-Silk-Road user, Darknet sites, Concentration...
- Notice: some characteristics work on both stages.

2nd method: Detection-controlled estimation (DCE) - MLE



- The first branch models whether a bitcoin user, i, is predominantly involved in illegal or legal activity.
- The second branch models whether or not an illegal user is "detected" (they enter our sample of observed illegal users).
- Both stages are simultaneously estimated using maximum likelihood to select parameter values that maximize the likelihood of the observable user classifications, A and A^C .

Estimated size and activity of legal and illegal user groups

Estimated size and activity of legal and illegal user groups

Group	Classification	Users (mil)	Transaction count (mil)	Holding value ($mil)	Number of addresses (mil)	Volume ($bil)
A. Values						
Illegal	SLM	30.94	276.63	1,394.76	87.95	436.78
	DCE	24.68	282.70	1,523.87	86.35	422.05
	Upper bound	34.22	308.72	1,782.44	99.67	558.23
	Midpoint	27.81	279.67	1,459.32	87.15	429.41
	Lower bound	21.39	250.62	1,136.20	74.63	300.60
Legal	SLM	75.31	329.06	1,569.90	133.76	1,425.73
	DCE	81.57	322.99	1,440.79	135.37	1,440.45
	Upper bound	84.86	355.07	1,828.47	147.09	1,561.91
	Midpoint	78.44	326.02	1,505.35	134.56	1,433.09
	Lower bound	72.02	296.97	1,182.22	122.04	1,304.28
B. Percentages						
Illegal	SLM	29.12%	45.67%	47.05%	39.67%	23.45%
	DCE	23.23%	46.67%	51.40%	38.95%	22.66%
	Upper bound	32.21%	50.97%	60.12%	44.96%	29.97%
	Midpoint	26.17%	46.17%	49.22%	39.31%	23.06%
	Lower bound	20.13%	41.38%	38.32%	33.66%	16.14%
Legal	SLM	70.88%	54.33%	52.95%	60.33%	76.55%
	DCE	76.77%	53.33%	48.60%	61.05%	77.34%
	Upper bound	79.87%	58.62%	61.68%	66.34%	83.86%
	Midpoint	73.83%	53.83%	50.78%	60.69%	76.94%
	Lower bound	67.79%	49.03%	39.88%	55.04%	70.03%

- The estimated number of illegal users is around four times larger than our sample of observed illegal users.

Estimated size and activity of legal and illegal user groups

Estimated size and activity of legal and illegal user groups

Group	Classification	Users (mil)	Transaction count (mil)	Holding value ($mil)	Number of addresses (mil)	Volume ($bil)
A. Values						
Illegal	SLM	30.94	276.63	1,394.76	87.95	436.78
	DCE	24.68	282.70	1,523.87	86.35	422.05
	Upper bound	34.22	308.72	1,782.44	99.67	558.23
	Midpoint	27.81	279.67	1,459.32	87.15	429.41
	Lower bound	21.39	250.62	1,136.20	74.63	300.60
Legal	SLM	75.31	329.06	1,569.90	133.76	1,425.73
	DCE	81.57	322.99	1,440.79	135.37	1,440.45
	Upper bound	84.86	355.07	1,828.47	147.09	1,561.91
	Midpoint	78.44	326.02	1,505.35	134.56	1,433.09
	Lower bound	72.02	296.97	1,182.22	122.04	1,304.28
B. Percentages						
Illegal	SLM	29.12%	45.67%	47.05%	39.67%	23.45%
	DCE	23.23%	46.67%	51.40%	38.95%	22.66%
	Upper bound	32.21%	50.97%	60.12%	44.96%	29.97%
	Midpoint	26.17%	46.17%	49.22%	39.31%	23.06%
	Lower bound	20.13%	41.38%	38.32%	33.66%	16.14%
Legal	SLM	70.88%	54.33%	52.95%	60.33%	76.55%
	DCE	76.77%	53.33%	48.60%	61.05%	77.34%
	Upper bound	79.87%	58.62%	61.68%	66.34%	83.86%
	Midpoint	73.83%	53.83%	50.78%	60.69%	76.94%
	Lower bound	67.79%	49.03%	39.88%	55.04%	70.03%

- Illegal users account for an even larger share of all transactions. This result is consistent with the notion that illegal users are likely to use bitcoin as a payment system

Estimated size and activity of legal and illegal user groups

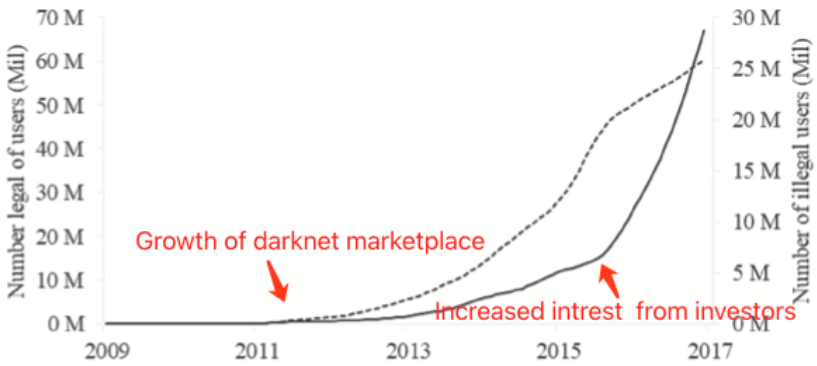
Estimated size and activity of legal and illegal user groups

Group	Classification	Users (mil)	Transaction count (mil)	Holding value ($mil)	Number of addresses (mil)	Volume ($bil)
A. Values						
Illegal	SLM	30.94	276.63	1,394.76	87.95	436.78
	DCE	24.68	282.70	1,523.87	86.35	422.05
	Upper bound	34.22	308.72	1,782.44	99.67	558.23
	Midpoint	27.81	279.67	1,459.32	87.15	429.41
	Lower bound	21.39	250.62	1,136.20	74.63	300.60
Legal	SLM	75.31	329.06	1,569.90	133.76	1,425.73
	DCE	81.57	322.99	1,440.79	135.37	1,440.45
	Upper bound	84.86	355.07	1,828.47	147.09	1,561.91
	Midpoint	78.44	326.02	1,505.35	134.56	1,433.09
	Lower bound	72.02	296.97	1,182.22	122.04	1,304.28
B. Percentages						
Illegal	SLM	29.12%	45.67%	47.05%	39.67%	23.45%
	DCE	23.23%	46.67%	51.40%	38.95%	22.66%
	Upper bound	32.21%	50.97%	60.12%	44.96%	29.97%
	Midpoint	26.17%	46.17%	49.22%	39.31%	23.06%
	Lower bound	20.13%	41.38%	38.32%	33.66%	16.14%
Legal	SLM	70.88%	54.33%	52.95%	60.33%	76.55%
	DCE	76.77%	53.33%	48.60%	61.05%	77.34%
	Upper bound	79.87%	58.62%	61.68%	66.34%	83.86%
	Midpoint	73.83%	53.83%	50.78%	60.69%	76.94%
	Lower bound	67.79%	49.03%	39.88%	55.04%	70.03%

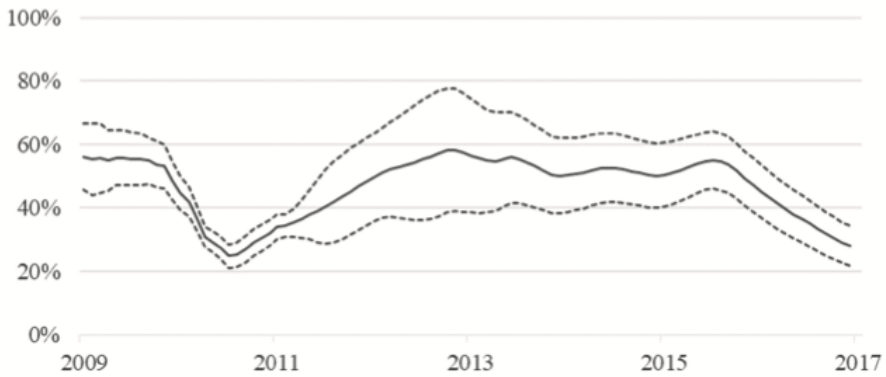
- Illegal users on average hold around one-half (49.22%) of all outstanding bitcoins. (In the bitcoin early stage, there is high fraction of illegal users)

Time series - number of illegal users

A Estimated number of illegal and legal bitcoin users

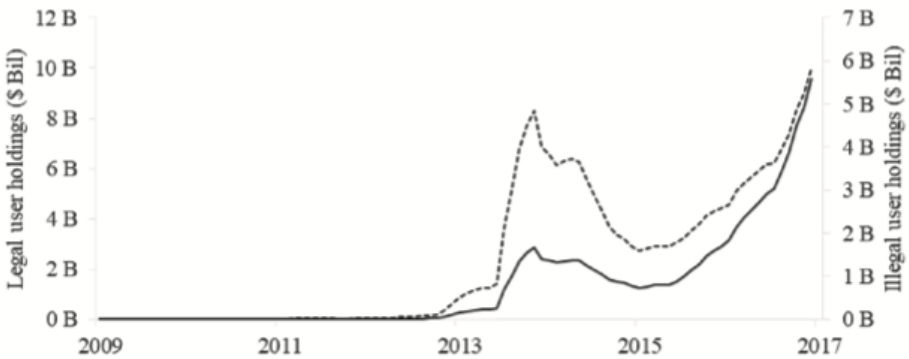


B Estimated percentage of illegal bitcoin users (plus 99% confidence bounds)

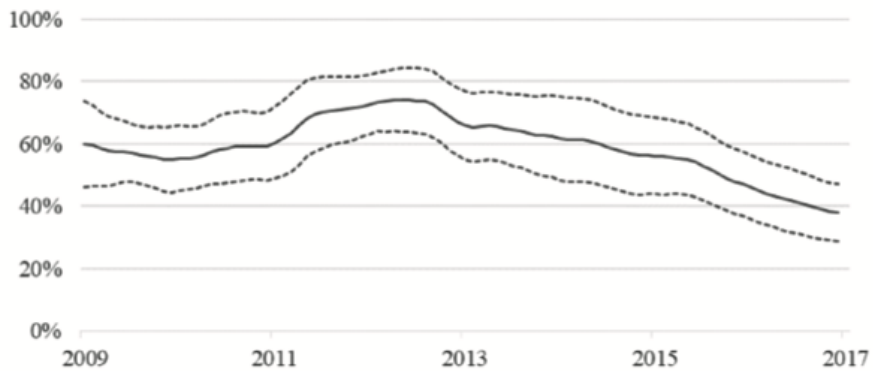


Time series - bitcoin holdings of illegal users

A **Estimated dollar value of illegal and legal users' bitcoin holdings**



B **Estimated percentage of illegal users' bitcoin holdings with 99% confidence bounds**



- At the early stage of bitcoin, bitcoin is cheap and number of users are small, illegal users held 60% volume of bitcoin. When bitcoin became more valuable and volatile since 2015, their holding mount is decreasing.

Differences in characteristics betwwen illegal and legal users

Table 5
Differences in characteristics between illegal and legal users

	Observed			SLM			DCE		
Variable	Other (1)	Illegal (2)	Difference (2-1)	Legal (1)	Illegal (2)	Difference (2-1)	Legal (1)	Illegal (2)	Difference (2-1)
Transaction count	4.09	31.51	27.42***	4.37	8.94	4.57***	3.96	11.46	7.50***
Transaction size	5,346.87	2,969.38	−2,377.49***	6,225.51	2,729.66	−3,495.85***	5,791.25	3,278.30	−2,512.95***
Transaction frequency	28.91	45.46	16.54***	29.77	30.16	0.39**	28.50	34.45	5.95***
Counterparties	3.53	14.61	11.08***	3.77	5.18	1.42***	3.57	6.19	2.62***
Holding value	4,021.77	3,207.06	−814.71***	4,625.45	2,388.31	−2,237.14***	4,359.86	2,698.71	−1,661.16***
Concentration	0.09	0.20	0.11***	0.08	0.13	0.05***	0.09	0.12	0.04***
Existence time	6.19	13.44	7.26***	5.91	8.31	2.40***	6.17	8.08	1.91***
Darknet sites	17.17	16.67	−0.50***	17.13	17.17	0.04***	16.87	18.04	1.18***
Tumbling	0.40	1.18	0.78***	0.37	0.64	0.27***	0.31	0.89	0.58***
Darknet shock volume	15.84	27.25	11.40***	14.51	21.39	6.88***	10.57	36.14	25.56***
Bitcoin hype	28.74	21.16	−7.58***	29.67	24.95	−4.72***	30.99	19.38	−11.60***
Pre-Silk-Road user	0.06	0.22	0.16***	0.06	0.12	0.07***	0.03	0.22	0.19***
Bitcoin market cap	9.85	9.45	−0.40***	9.88	9.68	−0.21***	9.96	9.36	−0.60***
Shadow coins	7.18	5.34	−1.84***	7.30	6.51	−0.79***	7.67	5.11	−2.56***
Alt coins	8.75	7.49	−1.26***	8.86	8.24	−0.62***	9.04	7.47	−1.57***

- Illegal users predominantly using bitcoin to buy and sell goods and services, whereas some legal users also use bitcoin for investment and speculation.

Differences in characteristics betwwen illegal and legal users

Table 5
Differences in characteristics between illegal and legal users

	Observed			SLM			DCE		
Variable	Other (1)	Illegal (2)	Difference (2-1)	Legal (1)	Illegal (2)	Difference (2-1)	Legal (1)	Illegal (2)	Difference (2-1)
Transaction count	4.09	31.51	27.42***	4.37	8.94	4.57***	3.96	11.46	7.50***
Transaction size	5,346.87	2,969.38	−2,377.49***	6,225.51	2,729.66	−3,495.85***	5,791.25	3,278.30	−2,512.95***
Transaction frequency	28.91	45.46	16.54***	29.77	30.16	0.39**	28.50	34.45	5.95***
Counterparties	3.53	14.61	11.08***	3.77	5.18	1.42***	3.57	6.19	2.62***
Holding value	4,021.77	3,207.06	−814.71***	4,625.45	2,388.31	−2,237.14***	4,359.86	2,698.71	−1,661.16***
Concentration	0.09	0.20	0.11***	0.08	0.13	0.05***	0.09	0.12	0.04***
Existence time	6.19	13.44	7.26***	5.91	8.31	2.40***	6.17	8.08	1.91***
Darknet sites	17.17	16.67	−0.50***	17.13	17.17	0.04***	16.87	18.04	1.18***
Tumbling	0.40	1.18	0.78***	0.37	0.64	0.27***	0.31	0.89	0.58***
Darknet shock volume	15.84	27.25	11.40***	14.51	21.39	6.88***	10.57	36.14	25.56***
Bitcoin hype	28.74	21.16	−7.58***	29.67	24.95	−4.72***	30.99	19.38	−11.60***
Pre-Silk-Road user	0.06	0.22	0.16***	0.06	0.12	0.07***	0.03	0.22	0.19***
Bitcoin market cap	9.85	9.45	−0.40***	9.88	9.68	−0.21***	9.96	9.36	−0.60***
Shadow coins	7.18	5.34	−1.84***	7.30	6.51	−0.79***	7.67	5.11	−2.56***
Alt coins	8.75	7.49	−1.26***	8.86	8.24	−0.62***	9.04	7.47	−1.57***

- Illegal users are more likely to repeatedly transact with a given counterparty. This characteristic might be a reflection of illegal users repeatedly transacting with a given illegal darknet marketplace or other illegal user once trust is established from a successful initial exchange.

Differences in characteristics betwwen illegal and legal users

Table 5
Differences in characteristics between illegal and legal users

	Observed			SLM			DCE		
Variable	Other (1)	Illegal (2)	Difference (2-1)	Legal (1)	Illegal (2)	Difference (2-1)	Legal (1)	Illegal (2)	Difference (2-1)
Transaction count	4.09	31.51	27.42***	4.37	8.94	4.57***	3.96	11.46	7.50***
Transaction size	5,346.87	2,969.38	−2,377.49***	6,225.51	2,729.66	−3,495.85***	5,791.25	3,278.30	−2,512.95***
Transaction frequency	28.91	45.46	16.54***	29.77	30.16	0.39**	28.50	34.45	5.95***
Counterparties	3.53	14.61	11.08***	3.77	5.18	1.42***	3.57	6.19	2.62***
Holding value	4,021.77	3,207.06	−814.71***	4,625.45	2,388.31	−2,237.14***	4,359.86	2,698.71	−1,661.16***
Concentration	0.09	0.20	0.11***	0.08	0.13	0.05***	0.09	0.12	0.04***
Existence time	6.19	13.44	7.26***	5.91	8.31	2.40***	6.17	8.08	1.91***
Darknet sites	17.17	16.67	−0.50***	17.13	17.17	0.04***	16.87	18.04	1.18***
Tumbling	0.40	1.18	0.78***	0.37	0.64	0.27***	0.31	0.89	0.58***
Darknet shock volume	15.84	27.25	11.40***	14.51	21.39	6.88***	10.57	36.14	25.56***
Bitcoin hype	28.74	21.16	−7.58***	29.67	24.95	−4.72***	30.99	19.38	−11.60***
Pre-Silk-Road user	0.06	0.22	0.16***	0.06	0.12	0.07***	0.03	0.22	0.19***
Bitcoin market cap	9.85	9.45	−0.40***	9.88	9.68	−0.21***	9.96	9.36	−0.60***
Shadow coins	7.18	5.34	−1.84***	7.30	6.51	−0.79***	7.67	5.11	−2.56***
Alt coins	8.75	7.49	−1.26***	8.86	8.24	−0.62***	9.04	7.47	−1.57***

- Illegal users tend to become involved in bitcoin earlier than legal users. Similarly, the differences in means also show a higher proportion of pre-Silk-Road users among the illegal users than the legal users.

DCE model estimates

DCE model estimates

	Model 1		Model 2	
Variable	I()	D()	I()	D()
Intercept	−1.147***	0.265***	−1.054***	0.066
	(−0.755)	(0.126)	(−0.677)	(0.033)
Darknet sites	1.005***		1.076***	
	(0.661)		(0.691)	
Tumbling	0.085***		0.103***	
	(0.056)		(0.066)	
Bitcoin market cap	−1.608***		−1.690***	
	(−1.059)		(−1.085)	
Shadow coins	−0.649***		−0.679***	
	(−0.428)		(−0.436)	
Alt coins	0.591		0.615	
	(0.389)		(0.395)	
Darknet shock volume	0.445***		0.496***	
	(0.293)		(0.319)	
Pre-Silk-Road user		0.430***		0.430**
		(0.204)		(0.213)
Transaction frequency	0.438***	0.477***	0.230	0.474
	(0.288)	(0.227)	(0.148)	(0.235)
Transaction size	0.005	−0.171***	−1.574***	−0.443**
	(0.003)	(−0.081)	(−1.011)	(−0.220)
Concentration	0.293***	0.542***	0.268***	0.500***
	(0.193)	(0.258)	(0.172)	(0.248)
Existence time	0.098	1.744***	−0.058	1.405
	(0.064)	(0.829)	(−0.037)	(0.697)
Holding value			3.602***	−0.537
			(2.312)	(−0.266)
Transaction count			7.900	−0.593
			(5.071)	(−0.294)
Pseudo R^2	21.92%		22.08%	

- Numbers not in parentheses are the coefficient estimates. Numbers in parentheses are the marginal effects (partial derivatives of the corresponding probability with respect to each of the variables, reported as a fraction of the estimated corresponding probability).
- Significance at the 1%, 5%, and 10% levels is indicated by ***, **, and *, respectively.

DCE model estimates

DCE model estimates

	Model 1		Model 2	
Variable	I()	D()	I()	D()
Intercept	−1.147***	0.265***	−1.054***	0.066
	(−0.755)	(0.126)	(−0.677)	(0.033)
Darknet sites	1.005***		1.076***	
	(0.661)		(0.691)	
Tumbling	0.085***		0.103***	
	(0.056)		(0.066)	
Bitcoin market cap	−1.608***		−1.690***	
	(−1.059)		(−1.085)	
Shadow coins	−0.649***		−0.679***	
	(−0.428)		(−0.436)	
Alt coins	0.591		0.615	
	(0.389)		(0.395)	
Darknet shock volume	0.445***		0.496***	
	(0.293)		(0.319)	
Pre-Silk-Road user		0.430***		0.430**
		(0.204)		(0.213)
Transaction frequency	0.438***	0.477***	0.230	0.474
	(0.288)	(0.227)	(0.148)	(0.235)
Transaction size	0.005	−0.171***	−1.574***	−0.443**
	(0.003)	(−0.081)	(−1.011)	(−0.220)
Concentration	0.293***	0.542***	0.268***	0.500***
	(0.193)	(0.258)	(0.172)	(0.248)
Existence time	0.098	1.744***	−0.058	1.405
	(0.064)	(0.829)	(−0.037)	(0.697)
Holding value			3.602***	−0.537
			(2.312)	(−0.266)
Transaction count			7.900	−0.593
			(5.071)	(−0.294)
Pseudo R^2	21.92%		22.08%	

- Model 2 adds further control variables, and finds that the main results do not change much in response to additional control variables.
- A risk of adding too many transactional control variables is co-linearity between such variables.

Network characteristics of legal and illegal user networks

Network characteristics of legal and illegal bitcoin user networks

	SLM		DCE	
Metric	Legal	Illegal	Legal	Illegal
Density (10^{-6})	0.04	0.13	0.04	0.17
Reciprocity	0.01	0.03	0.01	0.03
Entropy	1.50	1.75	1.53	1.73

- Density, takes the range [0,1] and indicates how highly connected the users are within a community.
- Reciprocity takes the range [0,1] and indicates the tendency for users to engage in two-way interactions.
- Entropy measures the amount of heterogeneity among users in their number of links to other members of the community.

Implications and Conclusion

- The paper can help to reduce the uncertainty about the negative consequences of cryptocurrencies, allowing for more informed decisions by policy makers that assess both the costs and benefits.
- A second contribution of this paper is the models can be applied by law enforcement authorities.
- Our finding that a substantial amount of illegal activity is facilitated by bitcoin suggests that bitcoin has contributed to the emergence of an online black market, which raises several welfare considerations.
- Our results also have implications for the intrinsic value of bitcoin.

Future Research

- Illegal activities on other blockchains.
- Fundamental value of cryptos.
- ...

Thanks!

E-mail: rliu38@stevens.edu