

Cryptocurrency Investigations Concepts and Tracing

OECD June 2025

Mike Lovell

michael.lovell@cra-arc.gc.ca

Canada Revenue Agency

Senior Computer Forensics Analyst

The Birth of Bitcoin

Ancient Ideas



Rai and Cryptocurrency

There are several concepts in Rai that match modern Cryptocurrencies.

- **Proof of Work**

The amount of work is inherent with the size of the coin.
Cryptocurrencies typically need an amount of work to be created.

- **Rarity**

Once the coins were moved, no more collected. Cryptocurrencies has a limit on amount.

- **Shared Ledger**

Everyone keeps record of values and transactions. No one authority.

History of Digital Currencies

- **1983: Blind Signatures for Untraceable Payments**
David Chaum publishes a paper cryptography for signing certificates without a central authority.
- **1990: DigiCash**
Bankrupt and liquidated.
- **1996: E-Gold**
Digital currency backed by gold. Indictments for Money laundering and Child pornography purchases.
- **2006: Liberty Reserve**
Often used to convert Dollars to Euros.
Shut down because of money laundering.

History of Digital Currencies (con't)

- 2007: M-Pesa Vodafone

Used primarily in Kenya and Tanzania. Phone credits can be used for purchases. Credits exchanged via text messages.

- 2008: Bitcoin white paper published

“Satoshi Nakamoto” publishes a 7 page white paper outlining a new cryptocurrency.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

- 2009: Bitcoin network launched on January 3rd

The Satoshi Paper: What is Bitcoin?

- **Bitcoin allows direct exchange**
Direct person to person transactions.
- **Digital signatures provide security of funds**
Decentralized authority.
- **Resolved the double-spending problem**
Created a distributed verifiable ledger in the “Blockchain”.
- **Third party trust is removed**
Transactions are irreversible.
- **Changes to network are made by consensus**
No central governing entity.

Bitcoin (BTC) Basics (May 13, 2025)

- Maximum number of BTC: 21 Million
- Number of BTC in circulation: ~19.86 Million
- 1 BTC = \$104,260 USD
- Volatile: \$53,991 - \$106,147 USD this year
- Market capitalization: \$2.18 Trillion USD
- Maximum transactions per day: 361,000
BTC = 4-7 per second (Visa = 24,000 per second)

A recent studies suggest that about 3% of transactions are associated with illegal activity

Key Concepts

Addresses, Private Keys, Wallets, The Blockchain, Nodes, Mining

Addresses

- A Bitcoin Address can be thought of as envelopes or bank accounts that contain bitcoins.
- It is usually represented as a string of digits and characters.
- To send/transfer your bitcoins to another person, you need to know their address.



This Is Your Bitcoin Address
1XKp7DsovCSS7RstXwkpNqFsJfwmaYLvX

Share this with anyone and they can send you payments.

Different types of Addresses

- Legacy Address Format (P2PKH)

Example: **1BvBMSEYstWetqTFn5Au4m4GFg8xJaNVN2**

This is the traditional format Bitcoin started with. Always start with **1**.

- Compatibility Address Format (P2SH)

Example: **3J98t1WpEZ73CNmQviecrmyiWrnqRhWNLy**

This address type is widely supported and a usual choice for a user that is generating their own address. Always start with **3**.

- Bech32 or Segwit Address Format

Example: **bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq**

Not compatible with legacy format, but using Segwit can lower transaction fees. Always start with **bc1**.

Private Keys

- Every **bitcoin address** has a **private key** (similar to how a credit card has a PIN).
- To spend bitcoins you use your private key to unlock access to the bitcoins associated with their address.
- Using your private key and the recipient's address, you broadcast a message to the Bitcoin Network that you want to send coins to that address.



Summary: Private Keys and Addresses

- **Private keys**

Control the ability to spend your bitcoins

- **Addresses**

Where your bitcoins are stored

Each **Address** has a unique **Private Key**

The **Address** is generated from the **Private Key**.

Wallets: Manage Addresses & Transactions

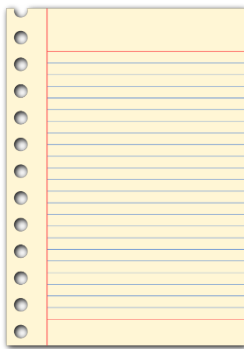
Wallets are more like keychains than wallets

- Digital wallets are hardware or software that manage keys, addresses, and transactions.
- There are no coins in a wallet. Coin ownership is stored on the Blockchain.
- Wallets broadcast your transactions to “nodes” on the bitcoin network.

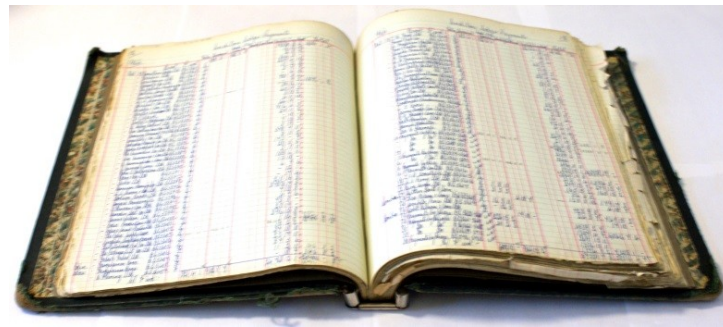


The Blockchain

- The **Blockchain** is a large ledger that contains every Bitcoin **transaction** that has ever taken place.
- The Blockchain holds all BTC address balances.
- Every **10 minutes** a new block (a new page of the transaction ledger) is added to the blockchain through a process called **Mining**



Block

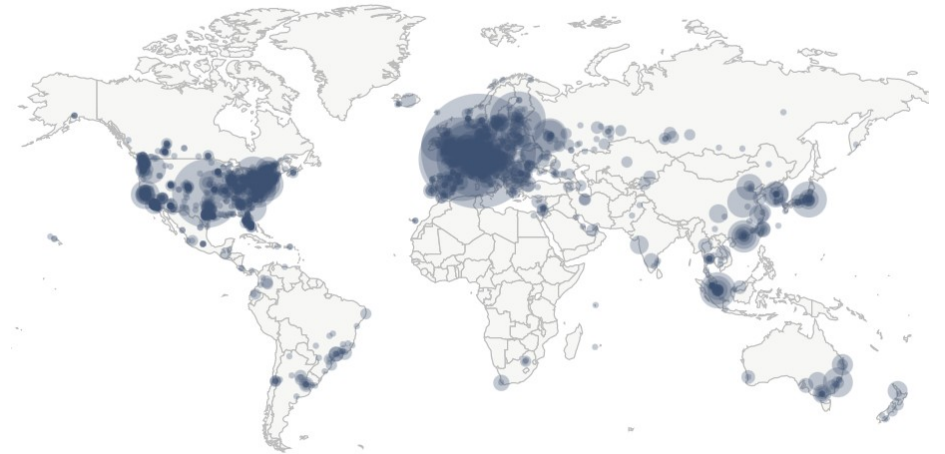


Blockchain

Nodes

- Identical copies of the **Blockchain** are kept on computers all over the world.
- These computers are called **Nodes**
- Several hundred nodes are located in Canada.
- Bitcoin nodes constantly update their **copies** of the **Blockchain**.

Nodes Worldwide



Total	11632
N/A	4299
United States	1833
Germany	1777
France	556
Netherlands	386
Canada	317

As of November 5, 2021

Mining (Proof of Work)



- Miners compete to solve a difficult mathematical task using the most recent list of transactions.



- Miners currently get **6.25 BTC + Transaction Fees**
- **Example: Hash of a Block** b8d43387d98f035e2f0ac49740a5af38
- If the difficulty is 4, then the first device to run the algorithm and get “b8d4” first is the winner. This may take millions or billions of tries. The block is then verified by that device and it will add that block to the blockchain.

















Other Cryptocurrencies

Forks, Alt-Coins, Sidechains

Other Popular Cryptocurrencies

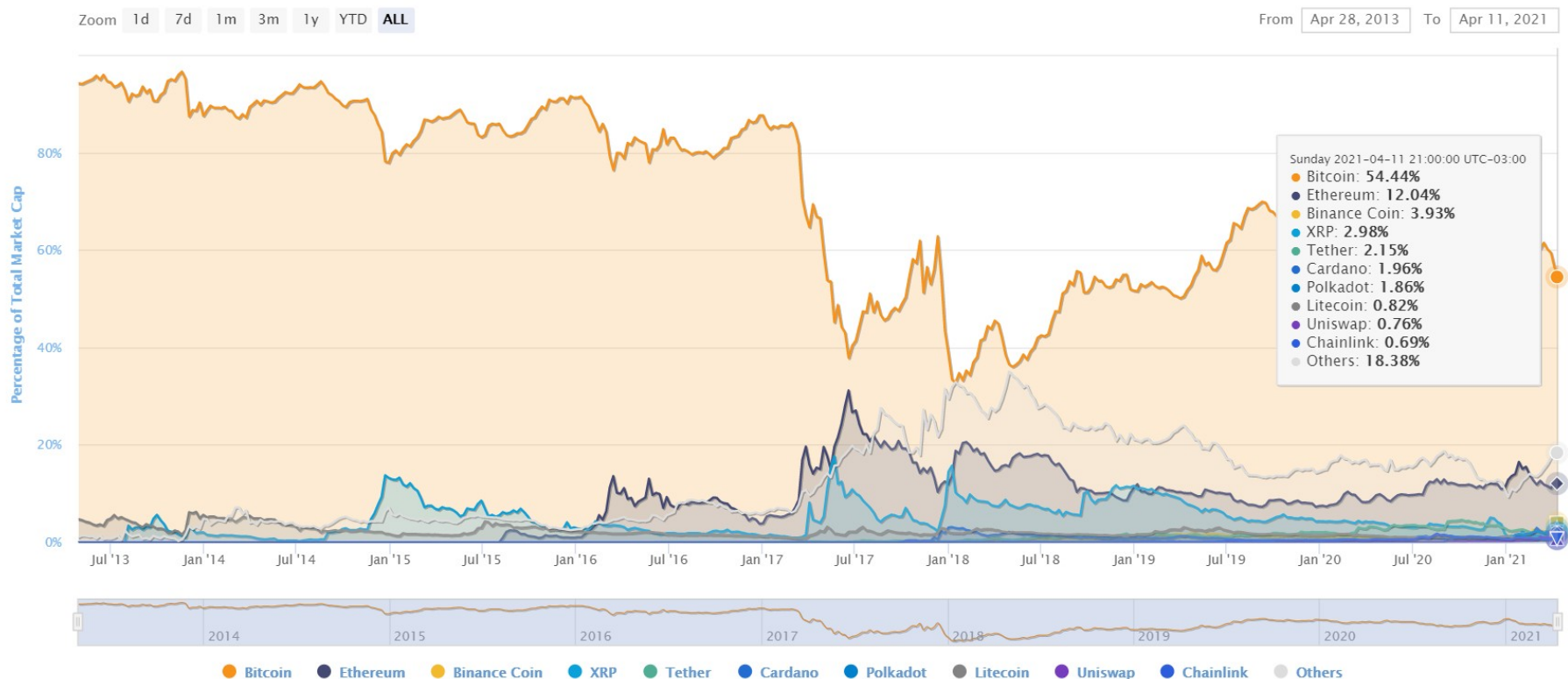
- **Bitcoin Cash (BCH):** A bitcoin fork with larger blocks for more transactions and lower fees.
- **Ethereum (ETH):** Utilizes smart contracts to facilitate more types of transactions on the blockchain than just currency.
- **Ripple (XRP):** RippleLab's global payment system that aims to replace the usual system of cross-border payments within the banking sector.
- **Cardano:** Allows metadata (identities) to be added to transactions to increase scalability.
- **Monero:** Privacy-centric that allows anonymous users hide transaction amounts.

Market Capitalization

# ▲	Name	Price	24h %	7d %	Market Cap ⓘ	Volume(24h) ⓘ	Circulating Supply ⓘ	Last 7 Days	
☆ 1	 Bitcoin BTC Buy	\$59,975.42	▼ 0.80%	▲ 2.36%	\$1,121,172,297,141	\$45,695,934,320 761,354 BTC	18,680,187 BTC		⋮
☆ 2	 Ethereum ETH Buy	\$2,151.78	▲ 0.41%	▲ 3.21%	\$248,467,606,966	\$19,638,331,609 9,123,450 ETH	115,431,483 ETH		⋮
☆ 3	 Binance Coin BNB Buy	\$523.19	▲ 12.85%	▲ 49.93%	\$80,870,061,736	\$5,719,181,320 10,928,655 BNB	154,532,785 BNB		⋮
☆ 4	 XRP XRP	\$1.35	▼ 8.38%	▲ 111.89%	\$61,420,734,532	\$19,290,288,534 14,259,953,414 XRP	45,404,028,640 XRP		⋮
☆ 5	 Tether USDT Buy	\$1.00	▼ 0.07%	▼ 0.11%	\$44,448,994,838	\$98,260,593,339 98,207,377,963 USDT	44,424,922,421 USDT		⋮
☆ 6	 Cardano ADA	\$1.28	▲ 4.71%	▲ 8.21%	\$40,978,545,542	\$3,696,445,887 2,881,878,687 ADA	31,948,309,441 ADA		⋮
☆ 7	 Polkadot DOT	\$41.08	▼ 1.22%	▼ 8.20%	\$38,164,521,470	\$1,475,664,579 35,909,750 DOT	928,719,457 DOT		⋮
☆ 8	 Litecoin LTC	\$255.19	▲ 0.43%	▲ 24.01%	\$16,902,986,798	\$6,424,043,512 25,369,505 LTC	66,752,415 LTC		⋮

<https://coinmarketcap.com/>

Market Capitalization Distribution



<https://coinmarketcap.com/charts/>

Sidechains

- Created primarily to increase the number of possible bitcoin transactions per second.
- Transactions are conducted off the main blockchain
- Transactions are then periodically reconciled onto the main blockchain
- Analogous to passing around IOUs which are eventually summed up and settled.



The Lightning Network: Sidechain which allows two people to send bitcoins to each other without inscribing their transactions in the Bitcoin blockchain. Only the final settling is “mined” and appears on the blockchain.

Cryptocurrencies like bitcoin are open source.
Therefore, anyone can make their own version based on the same blockchain.



Popular Bitcoin Forks

-  Bitcoin Cash: August 1, 2017
-  Bitcoin Gold: October 24, 2017
-  Bitcoin Diamond: November 24, 2017
-  Bitcoin Lightning: December 10, 2017
-  Bitcoin Hot: December 12, 2017
-  United Bitcoin: December 12, 2017
-  Super Bitcoin: December 14, 2017

Exercise: Create a Paper Wallet 1 of 2

Go to:

bitcoinpaperwallet.com/bitcoinpaperwallet/generate-wallet.html

<http://www.paperwalletbitcoin.com/>

<https://walletgenerator.net/>

Follow the Instructions.

Exercise: Create a Paper Wallet 2 of 2

Now go to blockchain.com/explorer

Question:

Can you see if your address is on the blockchain?

Why or why not?

Wallets

Cell Phone Wallets

- Wallet apps are quick and easy to install on cell phones.
- Cell phone wallets can only spend bitcoins if they have an Internet connection.
- If your cell phone gets hacked, the hacker can steal your bitcoins.
- Most cell phones are now strongly encrypted and password protected.



Bither



breadwallet



Electrum



GreenBits



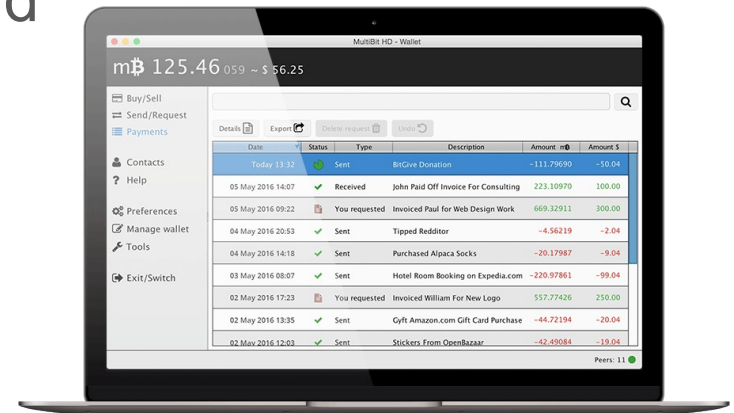
Mycellium



Airbitz

Computer Wallets

- Wallets can be installed on personal computers, laptops, and tablets.
- If your computer gets hacked, your bitcoins can be stolen.
- Can run from a program on the computer or a web application.



Green
Address



mSIGNA



Armory



ArcBit



Bitcoin
Core



Bitcoin
Knots



Electrum

Hosted wallets / Web Wallets

- Commercial services and exchanges offer wallet hosting
- Some manage the customer's private keys
- Some manage the customer's coins
- Web browsers or apps are used to access & manage
- Cryptocurrency traders often use hosted wallets
- Businesses may also use hosted wallets

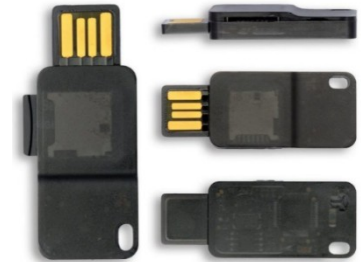


Beware!

- Wallet hosting services get hacked
- Wallet hosting services go out of business
- Wallet hosting services can run off with people's



Hardware Wallets



- Secure. Often used to protect large amounts of coins.
- Most wallets support Bitcoins as well as other coins.
- Wallet access is protected by password/PIN.
- Private keys never leave the wallet.

Popular Wallet Brands:

- Trezor
- Ledger
- KeepKey



Paper Wallets

- Paper wallets come from ATMs or regular printers
- The Private Key allows you to seize the coins
- The Public Key or Address allows you to view the wallet content and track the coins on the blockchain
- The ATM information indicates who may be holding KYC information



Multisignature Addresses and Security

- **Multisignature** (multisig) addresses are addresses which require more than one private key to authorize a Bitcoin transaction.
- **Multisig wallets** are used to share responsibility for possession and control over bitcoins.
- **M of N transactions:** requires “M of N” keys (e.g. 2 out of the 3 keys).



Cold Storage

- Offline Computer Wallets are referred to as “cold storage”
- Wallets hosted on computers which are not connected to the Internet
- Paper wallets
- Hardware wallets



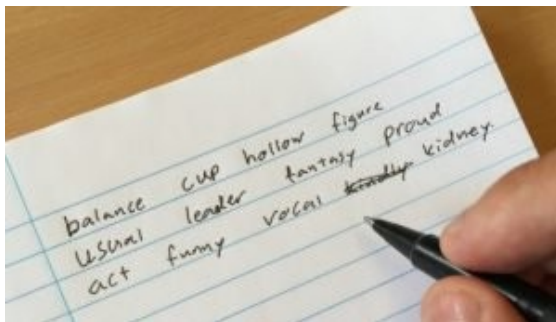
Wallet Backups

- A deterministic wallet is a system of deriving keys from a single starting point known as a seed
- The wallet seed allows users to recreate a wallet without needing any other information
- Wallet seeds are serialized into human-readable words in a Mnemonic phrase

These are called **Wallet Seed Word Lists**

Deterministic Wallets & Seeds

- Most hardware wallets, software wallets, and cell phone wallets allow you to recreate your wallet and its keys by using a seed word list.



Seed word list for all languages can be found here:

<https://github.com/bitcoin/bips/blob/master/bip-0039/bip-0039-wordlists.md>

Exercise: How Seed Lists Work (1 of 5)

128 bit string: 1011111010010101101100101101011100011101101101010001010111
0010111010000101001110101110011001101010010101001000111101111001001011

1												+1		
2												+1		
3												+1		
4												+1		
5												+1		
6												+1		
7												+1		
8												+1		
9												+1		
10												+1		
11												+1		
12												+1		

Exercise: How Seed Lists Work (2 of 5)

128 bit string: 1011111010010101101100101101011100011101101101010001010111
00101111010000101001110101110011001101010010101001000111101111001001011

1	1	0	1	1	1	1	1	0	1	0	0	+1		
2	1	0	1	0	1	1	0	1	1	0	0	+1		
3	1	0	1	1	0	1	0	1	1	1	0	+1		
4	0	0	1	1	1	0	1	1	0	1	1	+1		
5	0	1	0	1	0	0	0	1	0	1	0	+1		
6	1	1	1	0	0	1	0	1	1	1	0	+1		
7	1	0	0	0	0	1	0	1	0	0	1	+1		
8	1	1	0	1	0	1	1	1	0	0	1	+1		
9	1	0	0	1	1	0	1	0	1	0	0	+1		
10	1	0	1	0	1	0	0	1	0	0	0	+1		
11	1	1	1	1	0	1	1	1	1	0	0	+1		
12	1	0	0	1	0	1	1					+1		

Exercise: How Seed Lists Work (3 of 5)

128 bit string: 1011111010010101101100101101011100011101101101010001010111
0010111010000101001110101110011001101010010101001000111101111001001011

1	1	0	1	1	1	1	1	0	1	0	0	+1	1525	
2	1	0	1	0	1	1	0	1	1	0	0	+1	1389	
3	1	0	1	1	0	1	0	1	1	1	0	+1	1455	
4	0	0	1	1	1	0	1	1	0	1	1	+1	0476	
5	0	1	0	1	0	0	0	1	0	1	0	+1	0651	
6	1	1	1	0	0	1	0	1	1	1	0	+1	1839	
7	1	0	0	0	0	1	0	1	0	0	1	+1	1066	
8	1	1	0	1	0	1	1	1	0	0	1	+1	1722	
9	1	0	0	1	1	0	1	0	1	0	0	+1	1237	
10	1	0	1	0	1	0	0	1	0	0	0	+1	1353	
11	1	1	1	1	0	1	1	1	1	0	0	+1	1981	
12	1	0	0	1	0	1	1					+1	?	

Exercise: How Seed Lists Work (4 of 5)

128 bit string: 1011111010010101101100101101011100011101101101010001010111
00101111010000101001110101110011001101010010101001000111101111001001011

1	1	0	1	1	1	1	1	0	1	0	0	+1	1525	salon
2	1	0	1	0	1	1	0	1	1	0	0	+1	1389	
3	1	0	1	1	0	1	0	1	1	1	0	+1	1455	
4	0	0	1	1	1	0	1	1	0	1	1	+1	0476	
5	0	1	0	1	0	0	0	1	0	1	0	+1	0651	
6	1	1	1	0	0	1	0	1	1	1	0	+1	1839	
7	1	0	0	0	0	1	0	1	0	0	1	+1	1066	
8	1	1	0	1	0	1	1	1	0	0	1	+1	1722	
9	1	0	0	1	1	0	1	0	1	0	0	+1	1237	
10	1	0	1	0	1	0	0	1	0	0	0	+1	1353	
11	1	1	1	1	0	1	1	1	1	0	0	+1	1981	
12	1	0	0	1	0	1	1	1	0	0	0	+1	1209	

Exercise: How Seed Lists Work (5 of 5)

128 bit string: 1011111010010101101100101101011100011101101101010001010111
00101111010000101001110101110011001101010010101001000111101111001001011

1	1	0	1	1	1	1	1	0	1	0	0	+1	1525	salon
2	1	0	1	0	1	1	0	1	1	0	0	+1	1389	pulse
3	1	0	1	1	0	1	0	1	1	1	0	+1	1455	remind
4	0	0	1	1	1	0	1	1	0	1	1	+1	0476	derive
5	0	1	0	1	0	0	0	1	0	1	0	+1	0651	eyebrow
6	1	1	1	0	0	1	0	1	1	1	0	+1	1839	total
7	1	0	0	0	0	1	0	1	0	0	1	+1	1066	lunch
8	1	1	0	1	0	1	1	1	0	0	1	+1	1722	strong
9	1	0	0	1	1	0	1	0	1	0	0	+1	1237	once
10	1	0	1	0	1	0	0	1	0	0	0	+1	1353	poverty
11	1	1	1	1	0	1	1	1	1	0	0	+1	1981	wasp
12	1	0	0	1	0	1	1	1	0	0	0	+1	1209	novel

Buying, Selling, and Cashing Out

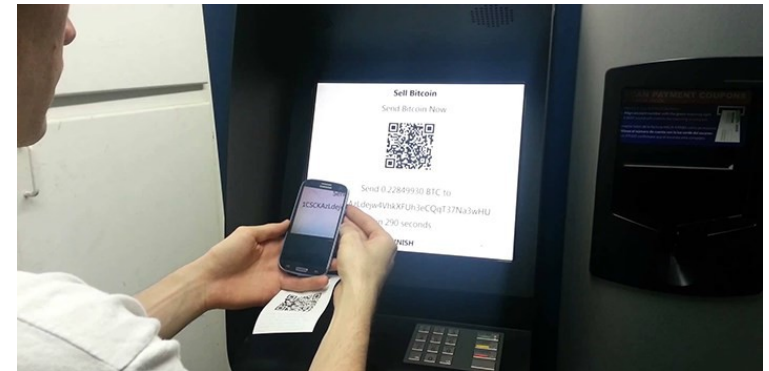
Bitcoin ATMs

Buying Bitcoins

- **Option 1:** Insert cash, receive a paper wallet
- **Option 2:** Insert cash, hold up your smart phone to ATM camera and show it your address

Selling Bitcoins

- **Option 1:** Hold paper wallet address up to ATM camera, receive cash
- **Option 2:** Hold your cell phone wallet address up to ATM, receive cash



Know Your Client (KYC):

- Code sent to your phone number
- Fingerprint scanner
- Telephone number
- Email address

Bitcoin Exchanges

Buying cryptocurrency from an Exchange:

- **Method #1:** Use your credit card (via a web page).
- **Method #2:** Set up an account and conduct a direct bank transfer.

Selling cryptocurrency at an Exchange:

- **Method #1:** Sell your currency on the exchange site and transfer the cash amount to your bank account.
- **Method #2:** Exchange your coins for other types of coins (e.g. Bitcoin for Ether).



Exchange KYC (Know Your Client)

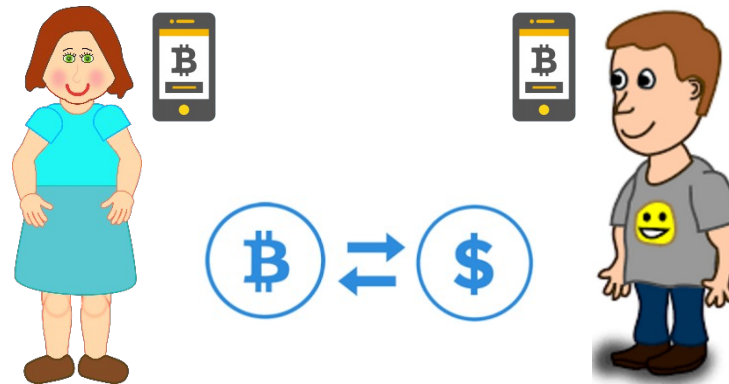
Most exchangers gather a significant amount of information about their clients

- Name
- Address
- Phone
- Email
- Government photo ID
- Photo of customer holding their photo ID
- Bank accounts
- Credit cards
- Transaction history

Buying and Selling Bitcoins

Person to Person / Cash

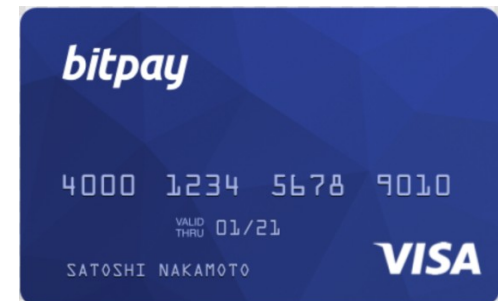
- Find someone who wants to sell or buy bitcoins (e.g. LocalBitcoins)
- Exchange cash
- Send bitcoins to the other person using an Internet-connected digital device (computer, cell phone, tablet)



Spending Bitcoins

Prepaid Bitcoin Debit/Credit Cards

- Order your card online
- Activate the card after you receive it
- Load your card with dollars using your bitcoin wallet.
- Spend or withdraw money from an ATM.



Exercise 3: Setup a Digital Wallet

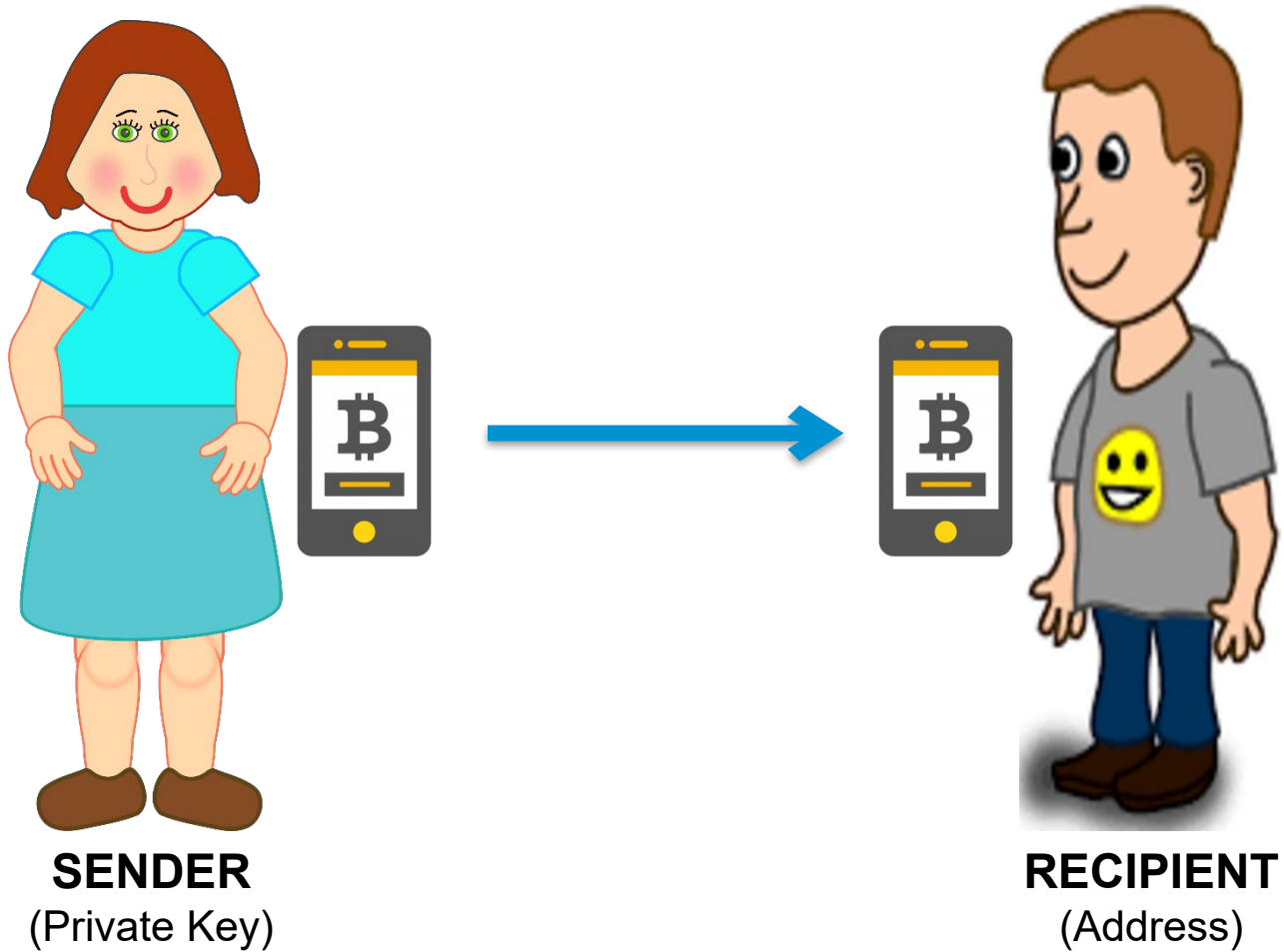
Follow along as we walk through the setup of a cryptocurrency wallet on a smartphone.

Be ready to write down some words!

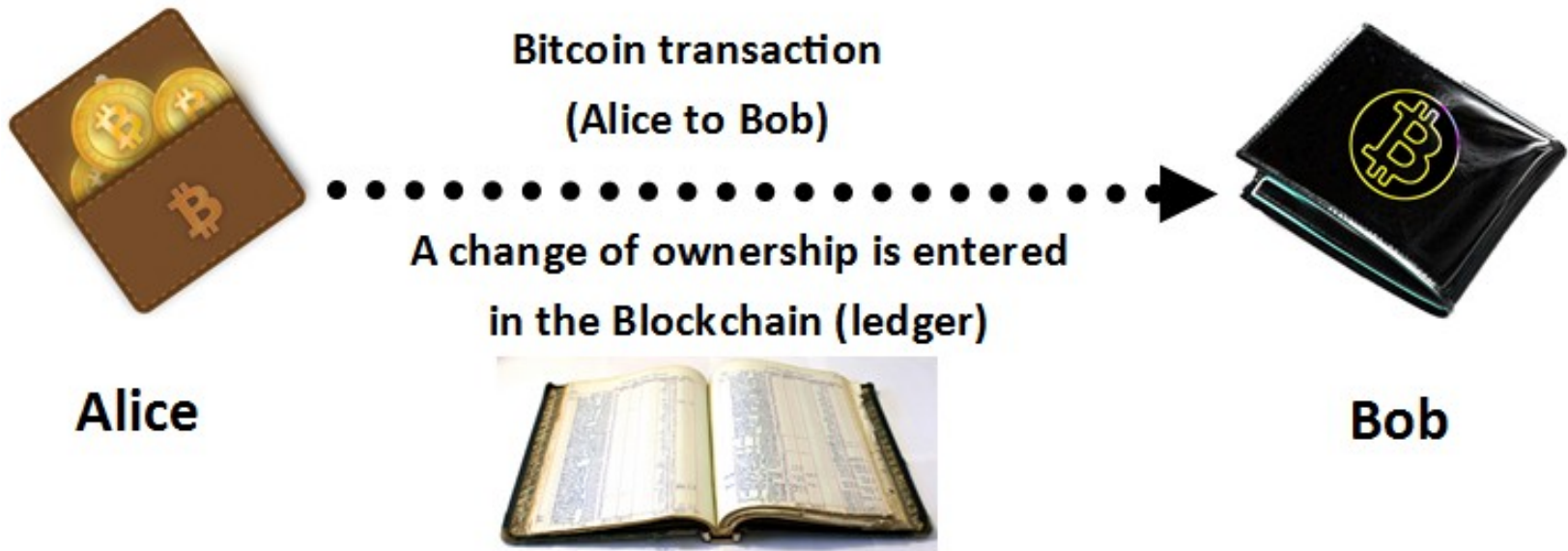
Tracing

Follow the Blockchain

Transactions



Transactions on The Blockchain



A Simple Transfer (1 of 5)

Alice's Wallet

Addresses	BTC
1FAvkeGMZsVSpTTwqb28YjtWqkyVkGZEKq	5
14NUMyJ1ZjBSkLRqC61EUMuhiVq42Rgbf9	2
19BLbQqr5C26NWfpVf4f6ntypRWdBiRgtg	2

Bob's Wallet

Addresses	BTC
1Kq6VCzmYPSs3JiafYSkWKHb8ZgHCPSuy9	1

A Simple Transfer (2 of 5)

Alice's Wallet

Addresses	BTC
1FAvkeGMZsVSpTTwqb28YjtWqkyVKGZEKq	5
14NUMyJ1ZjBSkLRqC61EUMuhiVq42Rgbf9	2
19BLbQqr5C26NWfpVf4f6ntyprWdBiRgtg	2



Bob's Wallet

Addresses	BTC
1Kq6VCzmYPSs3JiafYSkWKHb8ZgHCPSuy9	1
1AqsusDJmYXffydUWxFSsrKdqRfJtS1WMQ	0

A Simple Transfer (3 of 5)

Alice's Wallet

Addresses	BTC
1FAvkeGMZsVSpTTwqb28YjtWqkyVKGZEKq	0
14NUMyJ1ZjBSkLRqC61EUMuhiVq42Rgbf9	0
19BLbQqr5C26NWfpVf4f6ntyprWdBiRgtg	2



Bob's Wallet

Addresses	BTC
1Kq6VCzmYPSs3JiafYSkWKHb8ZgHCPSuy9	1
1AqsusDJmYXffydUWxFSsrKdqRfJtS1WMQ	6

A Simple Transfer (4 of 5)

Alice's Wallet

Addresses	BTC
1FAvkeGMZsVSpTTwqb28YjtWqkyVkGZEKq	0
14NUMyJ1ZjBSkLRqC61EUMuhiVq42Rgbf9	0
19BLbQqr5C26NWfpVf4f6ntyprWdBiRgtg	2



Bob's Wallet

Addresses	BTC
1Kq6VCzmYPSs3JiafYSkWKHb8ZgHCPSuy9	1
1AqsusDJmYXffydUWxFSsrKdqRfJtS1WMQ	6



A Simple Transfer (5 of 5)

Alice's Wallet

Addresses	BTC
1FAvkeGMZsVSpTTwqb28YjtWqkyVKGZEKq	0
14NUMyJ1ZjBSkLRqC61EUMuhiVq42Rgbf9	0
19BLbQqr5C26NWfpVf4f6ntyprWdBiRgtg	2
1JsAQPrXw2AaeR4mrzfbXzW3i8ohXg2otD	1



Bob's Wallet

Addresses	BTC
1Kq6VCzmYPSs3JiafYSkWKHb8ZgHCPSuy9	1
1AqsusDJmYXffydUWxFSsrKdqRfJtS1WMQ	6



32b66b218d177b66ef0b3a8b6534e687fd401d5b2da2b887fea33172276bf156

2019-08-19 17:04:17

1PoNkvn8QNY2Bly3KQXZio9AkvkMK7UjtE



1ECeZBxCVJ8Wm2JSN3Cyc6rge2gnvD3W5K

1.48979 BTC

1.48979 BTC

7f3e4f56d5224d14a9622cb42fa1b7aaa87d0c3039929109257dcf002ac7275a

2019-08-19 17:02:22

17SdjxsJmTqddnnTkPpmZKesZ2vhPaT95D



1ECeZBxCVJ8Wm2JSN3Cyc6rge2gnvD3W5K

1.370738 BTC

1.370738 BTC

d533d7c4f2bbd0f5c5d514c4a4a86c21643dc3708955257a6fe51aab7bd5d8fc

2019-08-19 17:05:33

1LYiKXSgpgwK6qE2tCjuDGR6YuHyLNfqnax



1ECeZBxCVJ8Wm2JSN3Cyc6rge2gnvD3W5K
1LYiKXSgpgwK6qE2tCjuDGR6YuHyLNfqnax

1.440322 BTC
0.03 BTC

1.470322 BTC

Transaction View information about a bitcoin transaction

d533d7c4f2bbd0f5c5d514c4a4a86c21643dc3708955257a6fe51aab7bd5d8fc

1LYiKXSgpgwK6qE2tCjuDGR6YuHyLNfqnax



1ECeZBxCVJ8Wm2JSN3Cyc6rge2gnvD3W5K
1LYiKXSgpgwK6qE2tCjuDGR6YuHyLNfqnax

1.440322 BTC
0.03 BTC

SPONSORED

Crypto Credit

9 Confirmations

1.470322 BTC

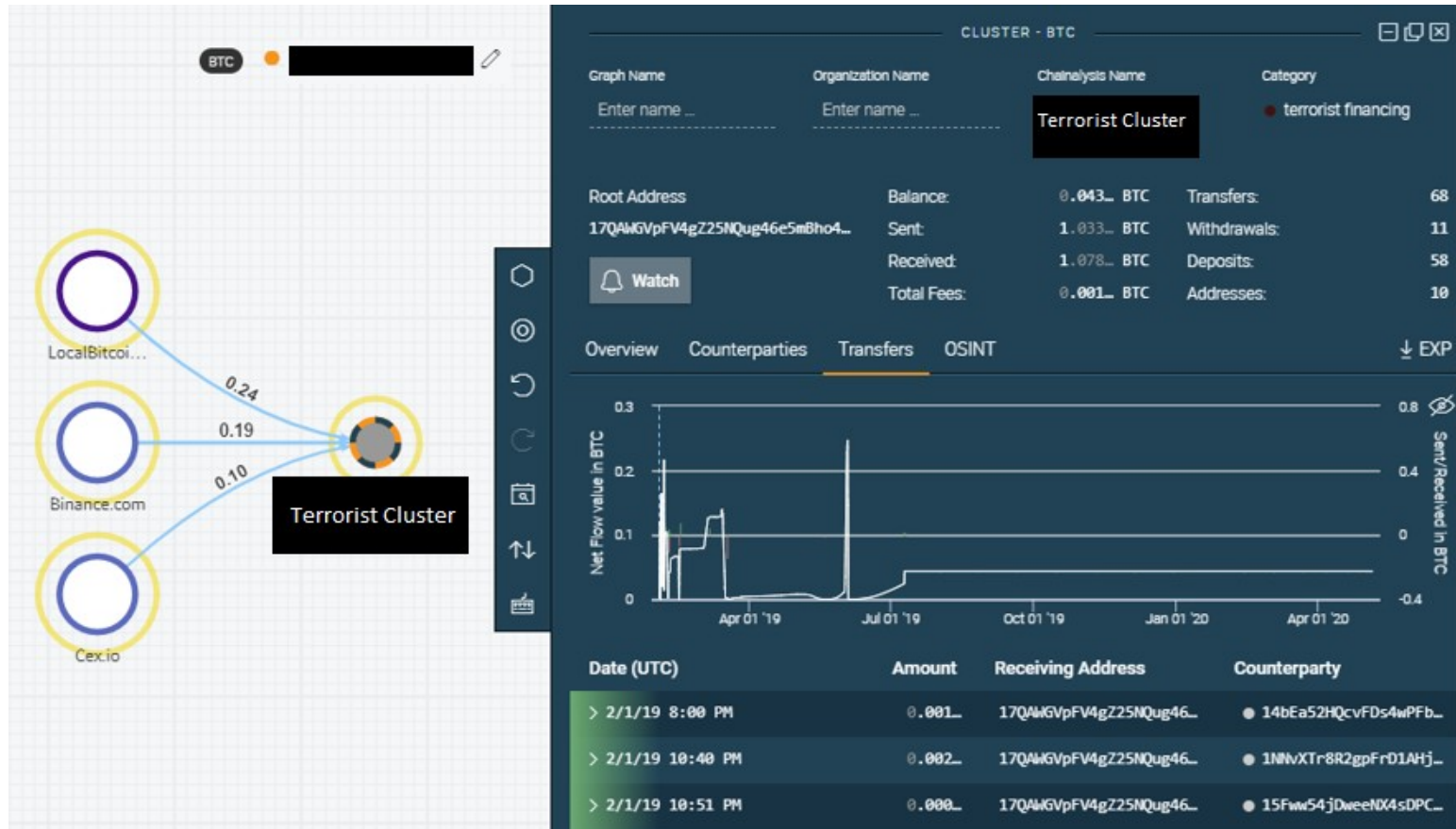
Summary

Size	225 (bytes)
Weight	900
Received Time	2019-08-19 17:05:33
Included In Blocks	590827 (2019-08-19 17:07:06 + 2 minutes)
Confirmations	9
Visualize	View Tree Chart

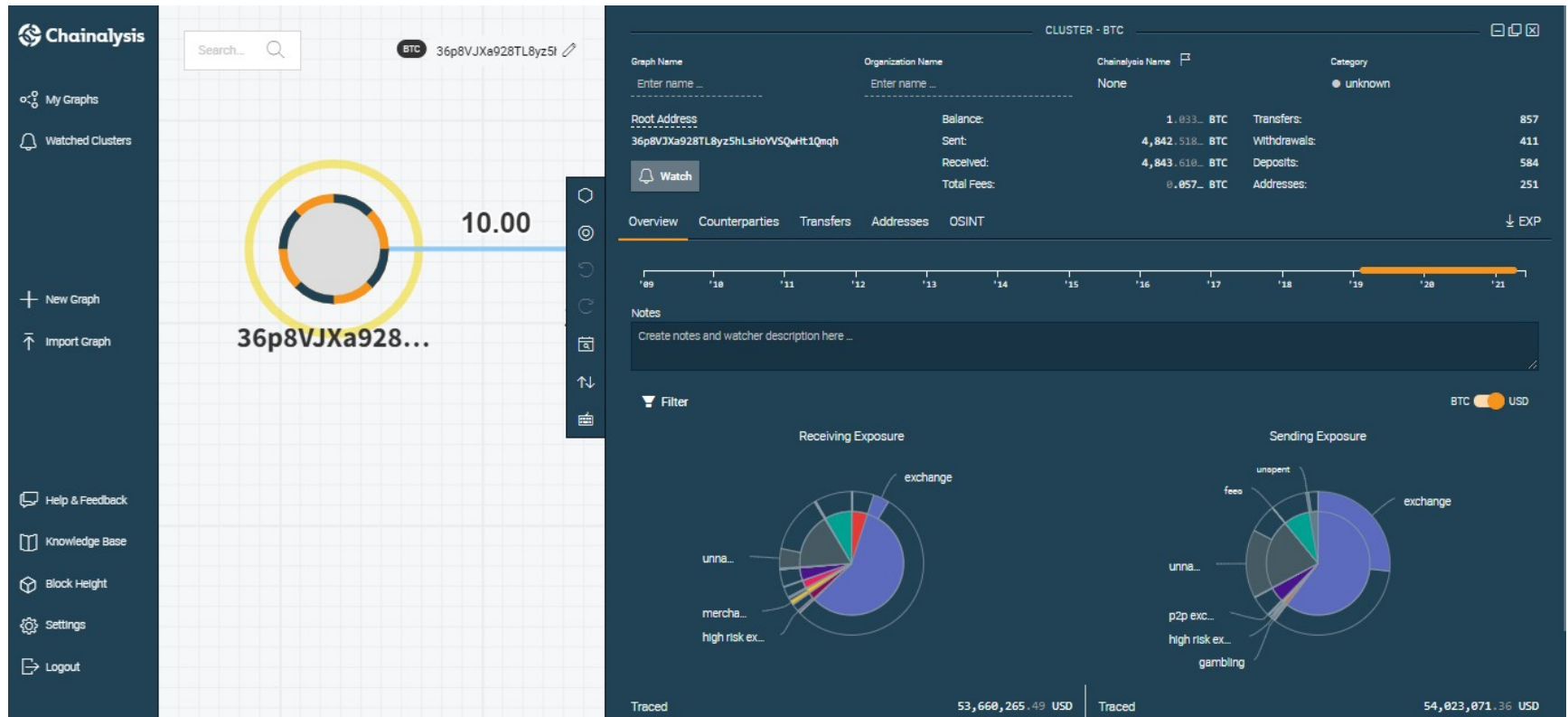
Inputs and Outputs

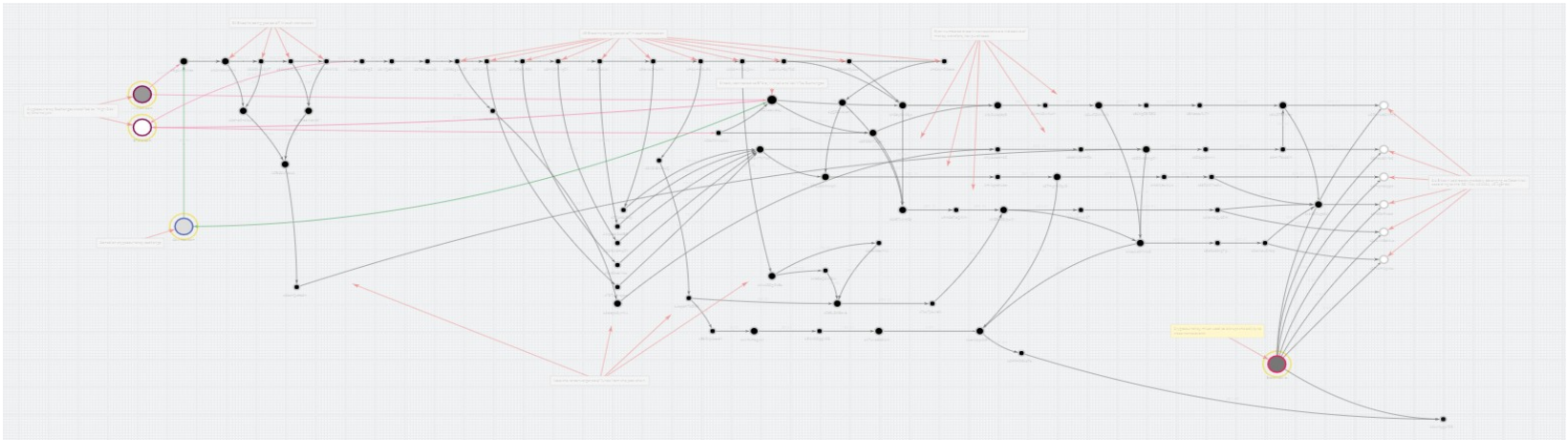
Total Input	1.472322 BTC
Total Output	1.470322 BTC
Fees	0.002 BTC
Fee per byte	888.889 sat/B
Fee per weight unit	222.222 sat/WU
Estimated BTC Transacted	1.440322 BTC
Scripts	Show scripts & coinbase

Crypto Tracing - Chainalysis

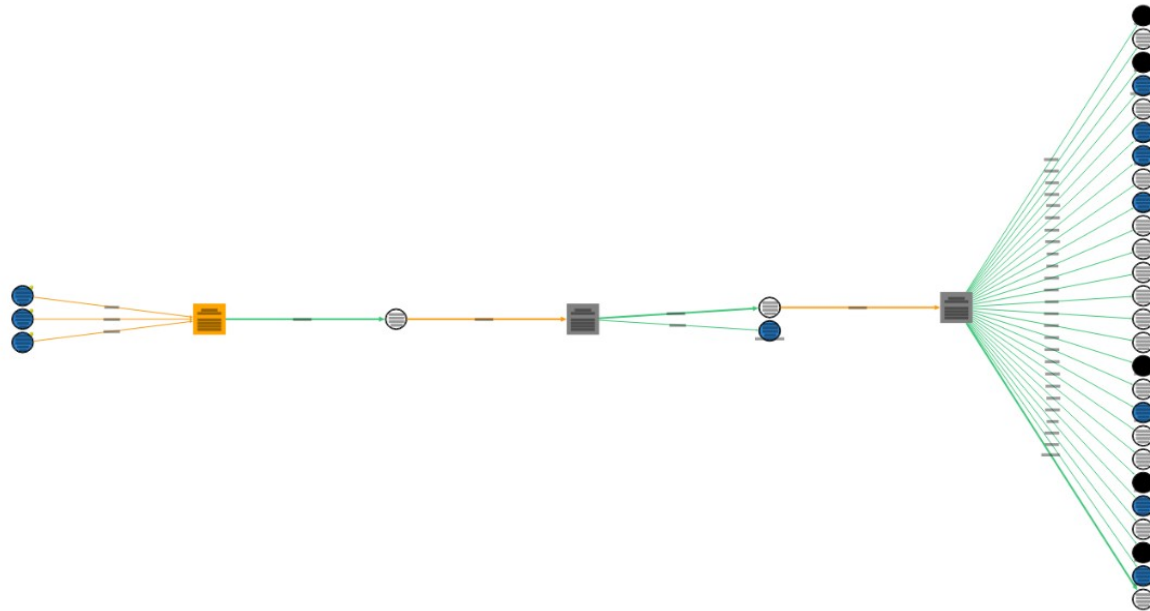


Crypto Tracing – Chainalysis (con't)





CipherTrace



Thank You!