

BITCOIN FORENSICS

BY- APURV SINGH GAUTAM

What is Bitcoin ?



- Bitcoin is a cryptocurrency
- An attempt to bring back a DECENTRALISED currency of people
- Not controlled by a Central Bank
- Works on Blockchain Technology



LOOKS



1NdvmVk4hvHo6RkmpRQrYQ4eBY2qMSWPfS

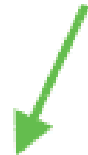


Example of Bitcoin

Bitcoin Address



Public Key



1M3RLrXve5wcT2ZcJu8WXoXjdh4WXcWQA9

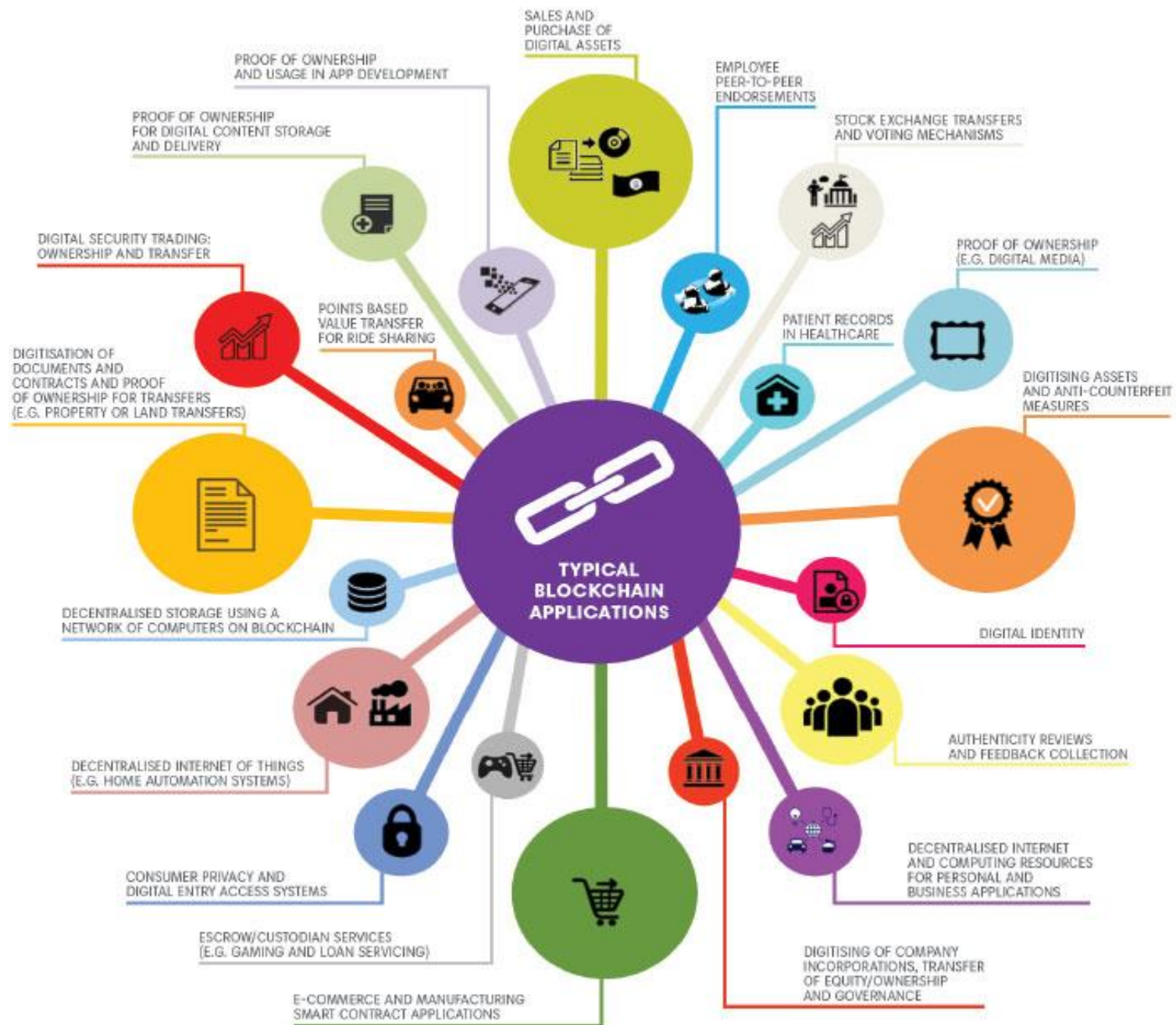
Private Key (Wallet Import Format)



Private key



5K8BwE76VsatiRa5wJpGng7758FAz4vLkMxAry8QnyZTdQJxPn



How to Perform Forensics ??



- A forensics investigator should know the Tech Architecture
- All about BLOCKCHAIN
- Currently no software tools is available
- Everything is in Public and Private Key (Cryptography)



Algorithm for Bitcoin

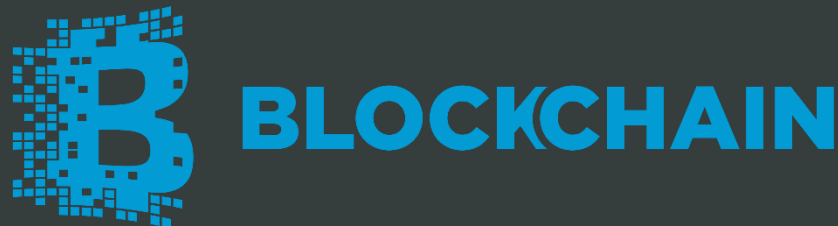
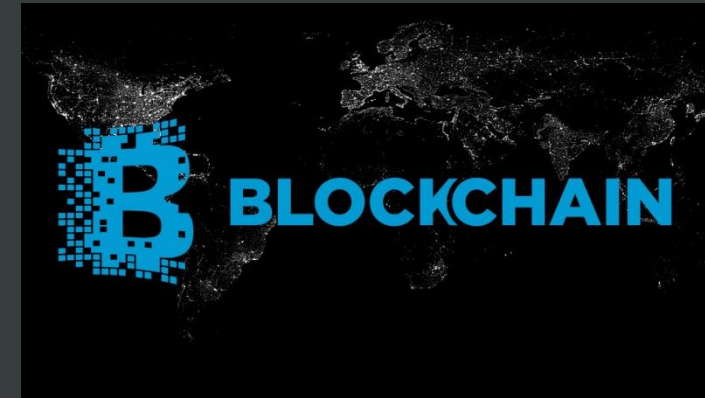


- Elliptic Curve Digital Signature Algorithm is used
- ECDSA is used to generate a public key from the PrivKey
- The PubKey can be used to verify transactions signed using the PrivKey
- 64-byte PubKeys are hashed down to 20-byte addresses
- 20-byte hash formatted using base58 check to produce either a P2PKH or P2SH Bitcoin address



What is BlockChain ??

- Type of distributed ledger
- Stored data in blocks
- Blocks contain digitally recorded data that is unchangeable
- Linked List is used in which each block contains hash of previous block



Block 51

Proof of work:
0000009857vvv

Previous block:
000000432qrza1

Transaction
lk54lfvx

Transaction
09345w1d

Transaction
vc4232v32

Block 52

Proof of work:
000000zzxvzx5

Previous block:
0000009857vvv

Transaction
dd5g31bm

Transaction
22qsx987

Transaction
001hk009

Block 53

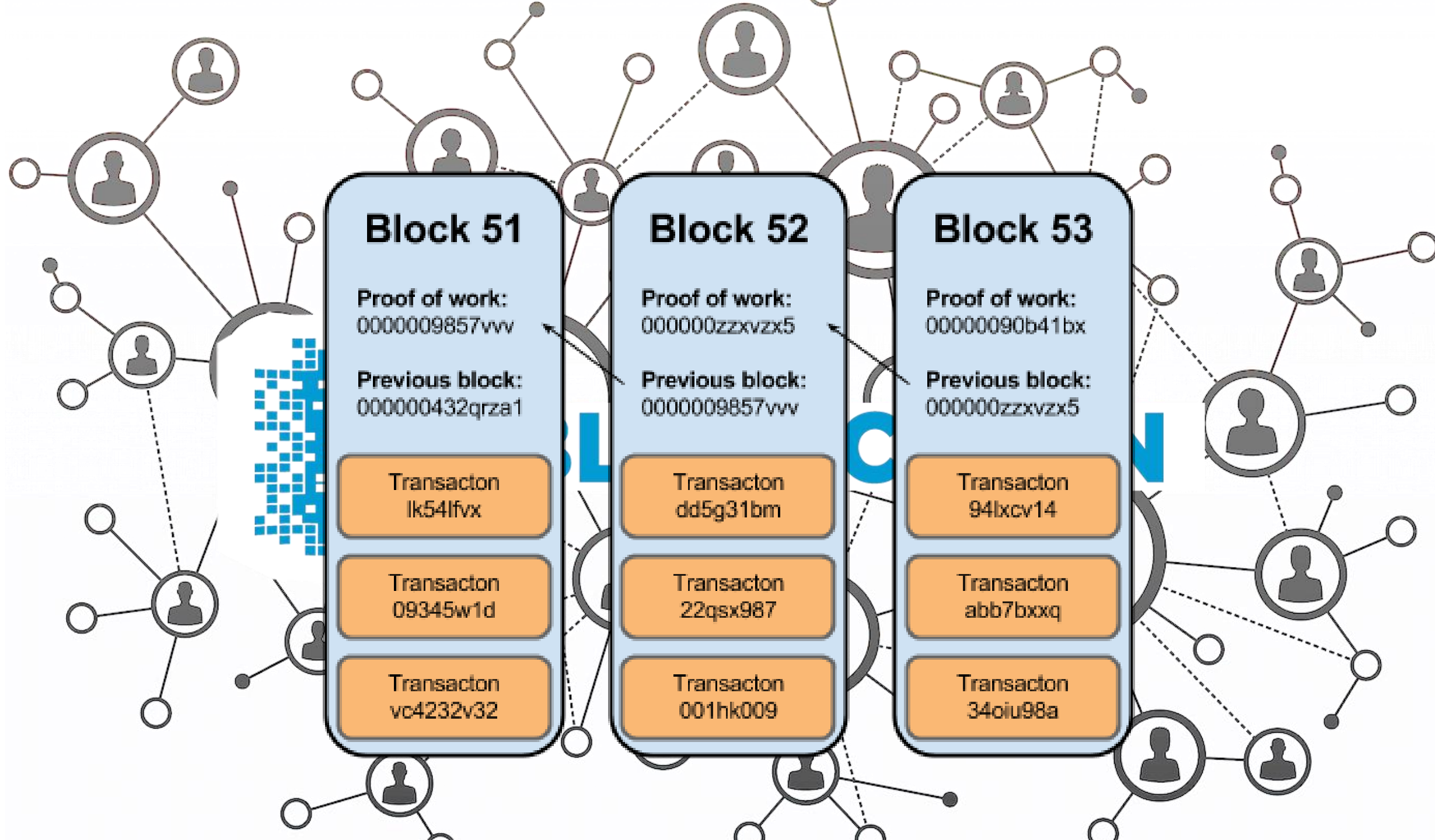
Proof of work:
00000090b41bx

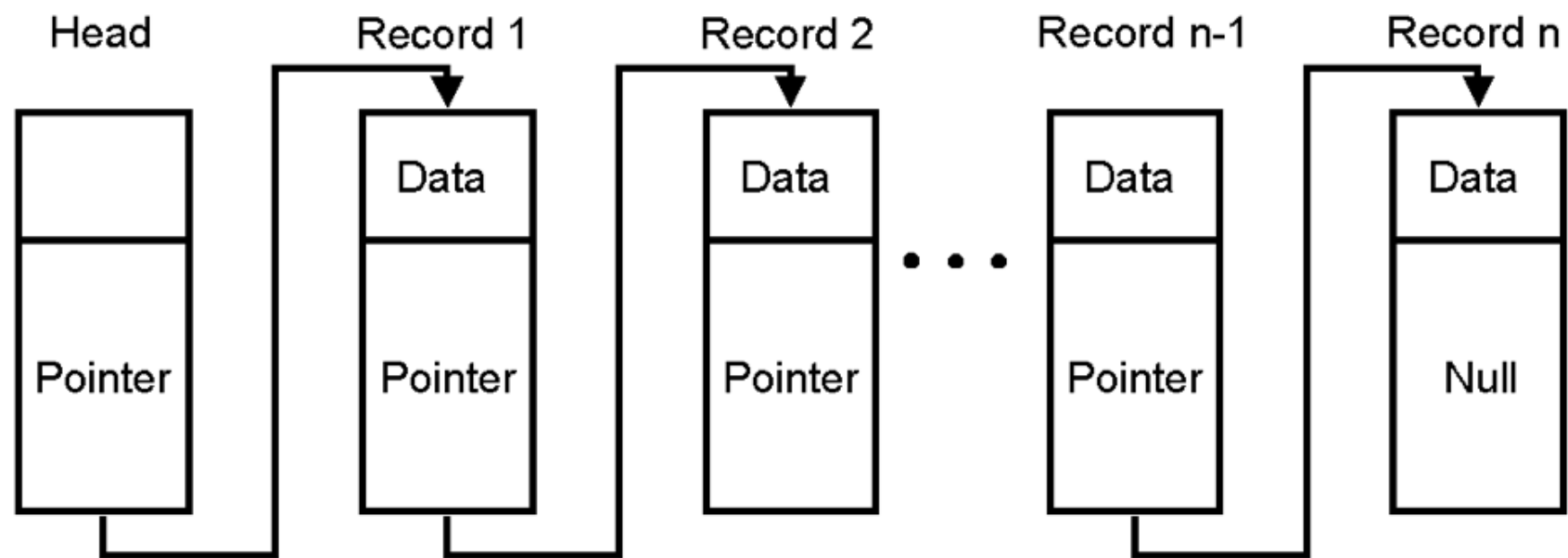
Previous block:
000000zzxvzx5

Transaction
94lxcv14

Transaction
abb7bxxq

Transaction
34oiu98a





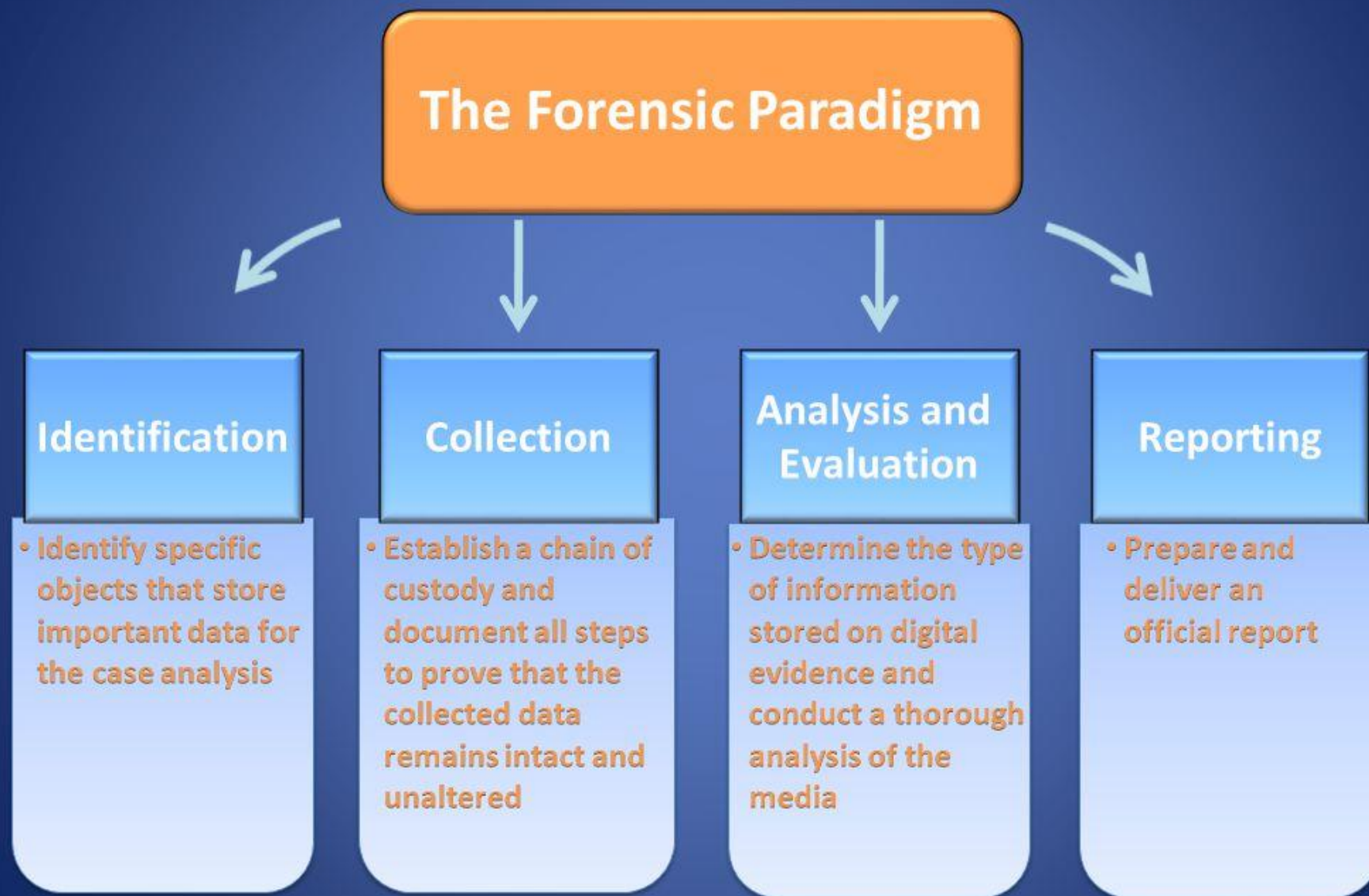


How Bitcoin Network Works ??

- Bitcoin network is composed of PEERS connected to other PEERS over unencrypted TCP channels
- Each peer attempts to maintain EIGHT outgoing connections to other peers
- These eight peers are called ENTRY NODES
- Transaction and Block messages are propagated in network by being Relayed through these ENTRY NODES to other peers



Computer Forensics Procedures





- Bitcoins don't EXIST ANYWHERE, not even on a hard drive
- For a Bitcoin Address there are no digital Bitcoins held against that Address
- One must reconstruct the balance of bitcoin by looking at the Blockchain
- Everyone on the network knows about the TRANSACTION and the history can be traced back to the point where the BITCOINS were produced



Blockchain

Block:

#1

Nonce:

11316

Data:

Prev:

00

Hash:

000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf

Mine

Block:

#2

Nonce:

35230

Data:

Prev:

000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf

Hash:

000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdafd043c19

Mine

Block:

#3

Nonce:

12937

Data:

Prev:

000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdafd043c19

Hash:

0000b9015ce2a08b61216ba5a0778545bf4ddd7c...

Mine

http://www.blockexplorer.com

Search based
On Block
Number, Address,
Block Hash,
Transaction
Hash or Public Key

Block Explorer

News

Market

Bitcoin cash

Zcash

Blocks

Status

Search for block, transaction or address

✓ Conn 89 • Height 505701

Scan

BTC

Buy Bitcoin with CCI

Latest Blocks


Height	Age	Transactions	Mined by	Size
505701	6 minutes ago	2302		975920
505700	33 minutes ago	121	SlushPool	995447
505699	34 minutes ago	1604	AntMiner	978675
505698	44 minutes ago	839	SlushPool	985071
505697	an hour ago	1917	BTCC Pool	938295

See all blocks


Latest Transactions

Hash	Value Out
db83748e58105b21ac6c3a0a7dc15a2709e803b11fd...	2.06477824 BTC
e705587a6b3ce9986812a8acb02ce9ef530a54ae75d...	0.12500596 BTC
9828e28e7c6c3fbd3bba58f61fdd37812dd00cb50c0...	0.48567328 BTC
a1f864678ec13ef54d54d1ab6081de222a7d07c8971...	169.03014083 BTC
907ec779d87ca3f796ac88995a41fa2ae9d22235bec8...	1.82892717 BTC
b41e94aa1fffaead7f3b69487d65253d262f91133286...	15.72372315 BTC
e0b26b1d8384a21c1ba0e4d5064f77dfc38ff8f5773...	0.00425 BTC
58f75fa9d66f1cc5de89bfa2c8884de78b602360c52b...	0.059831 BTC
d3e8566d7f5238c28d05c17a3265263dcde1e2ca759...	1.68403078 BTC
3e18454ed182ed2f69339eac713957c96186d0a4e82...	0.84414362 BTC


News



BlackWallet Hack Nets Thief \$400,000 in Stellar Lumens



I Gave: An Ethereum Smart Contract Based Charity Platform



Zk-starks White Paper Aims for Zcash-level Privacy Without the Trusted Setup

About Block Explorer

Bitcoin Block Explorer is an open source web tool that allows you to view information about [blocks](#), [addresses](#), and [transactions](#) on the Bitcoin blockchain. The [source code](#) is on GitHub.

What is bitcoin?

Public Bitcoin API: Machine readable stats & blockchain info can be accessed directly through the [REST](#) and [Websockets](#) APIs.

Testnet is Bitcoin's sandbox. Block Explorer supports viewing both the [testnet](#) and [mainnet](#) blockchains.

Thanks to [Private Internet Access](#) for hosting the site. They provide a [VPN Service](#) that accepts Bitcoin.

Blocks by date.

Height	Timestamp	Transactions	Mined by	Size
505701	Jan 23, 2018 4:55:06 PM	2302		975920
505700	Jan 23, 2018 4:27:46 PM	121	SlushPool	995447
505699	Jan 23, 2018 4:26:58 PM	1604	AntMiner	978675
505698	Jan 23, 2018 4:16:43 PM	839	SlushPool	985071
505697	Jan 23, 2018 4:11:00 PM	1917	BTCC Pool	938295
505696	Jan 23, 2018 3:57:20 PM	1588	AntMiner	979244
505695	Jan 23, 2018 3:46:44 PM	99		996648
505694	Jan 23, 2018 3:46:23 PM	420	SlushPool	994180
505693	Jan 23, 2018 3:43:35 PM	507		981073
505692	Jan 23, 2018 3:40:16 PM	1626		955968
505691	Jan 23, 2018 3:39:54 PM	2182		978691
505690	Jan 23, 2018 3:12:51 PM	858		980368
505689	Jan 23, 2018 3:12:18 PM	1557		981641
505688	Jan 23, 2018 2:55:47 PM	1905		961928
505687	Jan 23, 2018 2:50:44 PM	1652	AntMiner	991983
505686	Jan 23, 2018 2:46:50 PM	238	AntMiner	994981
505685	Jan 23, 2018 2:45:28 PM	1556		974149
505684	Jan 23, 2018 2:21:29 PM	556		992918

<< Previous Blocks mined on: 23/01/2018 Next >>

Height	Time	Relayed By	Hash	Size (kB)
505700 (Main Chain)	2018-01-23 10:57:46	SlushPool	000000000000000006359dd4e5d50437c32b4e8ef8c5b3efe7fc411d8a085a7	1,006.67
505699 (Main Chain)	2018-01-23 10:56:58	AntPool	000000000000000007765ecd0c3f435dc263b998f8fb58e438319a1378df568	1,057.16
505698 (Main Chain)	2018-01-23 10:46:43	SlushPool	00000000000000000736e886f0494928d58607387b98b3d209c02fbd2c4e2b9	1,037.95
505697 (Main Chain)	2018-01-23 10:41:00	BTCC Pool	000000000000000004810fe8f9fd57ebde2e3aa95d165565219c48fe912b2a5	1,178.25
505696 (Main Chain)	2018-01-23 10:27:20	AntPool	000000000000000005775a745652071378af39d3dff7ac3648cc30757d4fa2e	1,055.43
505695 (Main Chain)	2018-01-23 10:16:44	BTC.com	0000000000000000003d853ecc4958ed2c84d3932e9355982ba4a8bd07f3eb3	1,003.2
505694 (Main Chain)	2018-01-23 10:16:23	SlushPool	000000000000000006726bd49b1c3b1d0286f1168b7b50172c591d147ba3a5f	1,010.49
505693 (Main Chain)	2018-01-23 10:13:35	ViaBTC	000000000000000004e27ca1e23cee228ccf5005c0d5a52317768ca6fcea482	1,049.76
505692 (Main Chain)	2018-01-23 10:10:16	BTC.TOP	000000000000000007d488608b0b27bd43b4bf71ad30fd14389be229bc45770	1,125.29
505691 (Main Chain)	2018-01-23 10:09:54	F2Pool	000000000000000004057175a9ed480a17a87b700e8737ff7bfa08776039b71	1,062.28
505690 (Main Chain)	2018-01-23 09:42:51	BTC.TOP	0000000000000000012b15bbf4ec12fe410cc9197bd9b5b81541d9f4aab682b	1,052.12
505689 (Main Chain)	2018-01-23 09:42:18	Unknown	000000000000000006d8266d3ceb55ff29438b28913c01b36b01429df381554	1,047.73
505688 (Main Chain)	2018-01-23 09:25:47	Unknown	000000000000000004b7800ee30ef0750ea974be053166747f0a405cd7c422a	1,107.31
505687 (Main Chain)	2018-01-23 09:20:44	AntPool	00000000000000000567b7a4dd90b9ef51c4cc28963aa51dd5a06b4348eb1e6	1,016.83
505686 (Main Chain)	2018-01-23 09:16:50	AntPool	0000000000000000019cc464475978f26bc61cec8f1829fcca4db96718b3c00	1,007.9
505685 (Main Chain)	2018-01-23 09:15:28	BTC.TOP	000000000000000001635c2b1ebb05dae50a507d2063bb9327dd90ecd966c59	1,070.5
505684 (Main Chain)	2018-01-23 08:51:29	Bitcoin.com	00000000000000000142f3edc2e4d681a390352062bb3e832530c571ada131	1,014.23
505683 (Main Chain)	2018-01-23 08:46:11	BitClub Network	000000000000000007b2435fd163c5e0a25fd82656e3d000879bcd805d87469	1,024.61
505682 (Main Chain)	2018-01-23 08:35:35	BTC.com	0000000000000000040214f9354d5f7cb457560406db7a0ec010e2bba8441c7	1,030.54

Bitcoin Stats

Summary of bitcoin statistics for the previous 24 hour period.

BLOCK SUMMARY

Blocks Mined	182
Time Between Blocks	7.26 minutes
Bitcoins Mined	2,275.00000000 BTC

MARKET SUMMARY

Market Price	\$10,173.20	View Chart
Trade Volume	\$1,381,223,901.05	
Trade Volume	130,887.72387026 BTC	

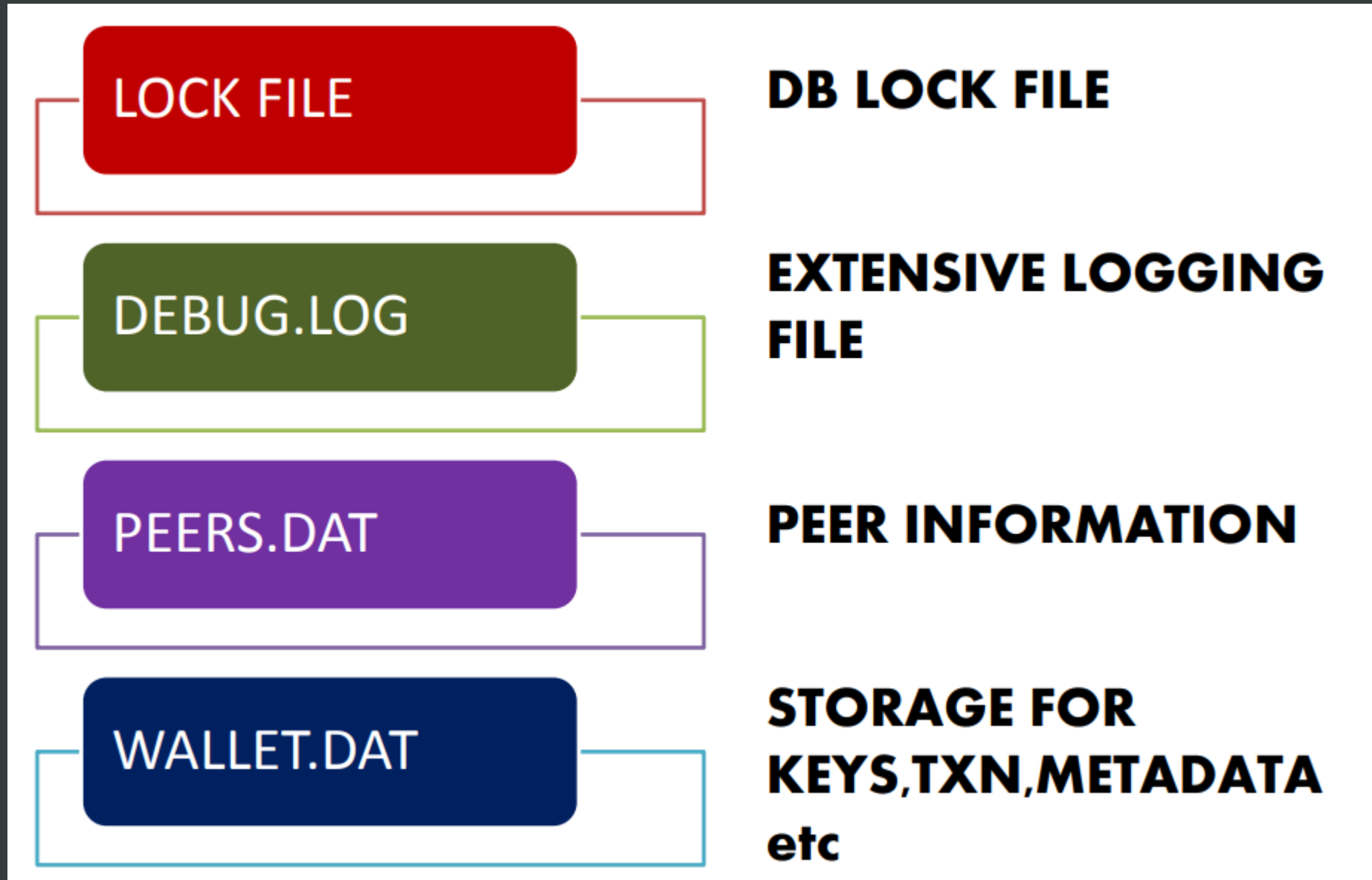
TRANSACTION SUMMARY

Total Transaction Fees (BTC)	299.29327400 BTC	View Chart
Number of Transactions	296,094	View Chart
Total Output Volume (BTC)	1,626,236.41495810 BTC	View Chart
Estimated Transaction Volume (BTC)	204,390.77492117 BTC	View Chart
Estimated Transaction Volume (USD)	\$2,156,882,365.49	View Chart

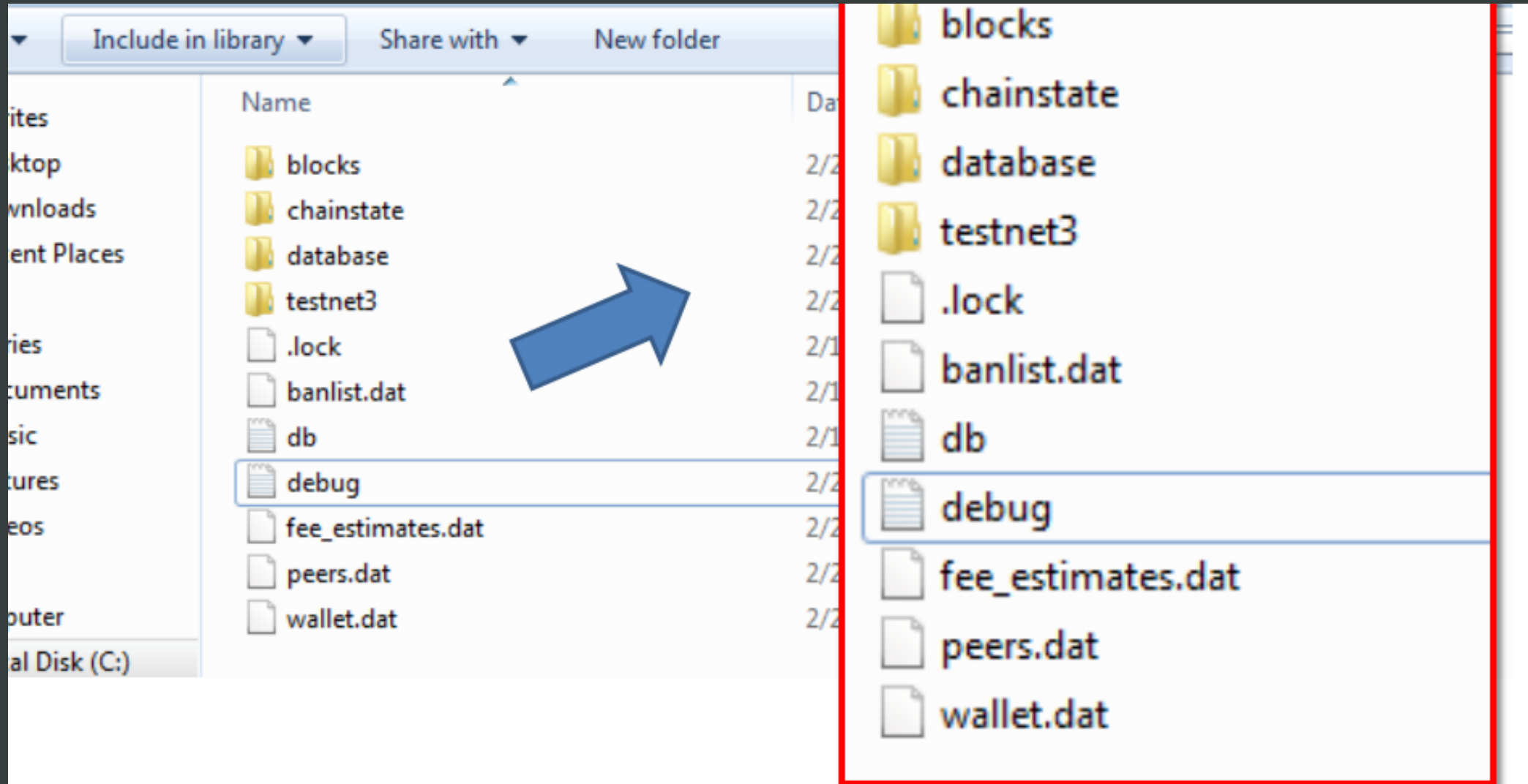
Bitcoin Core Wallet



Bitcoin Core/Bitcoin-Qt Folder Structure



Bitcoin Core/Bitcoin-Qt Folder Structure



Bitcoin Core/Bitcoin-Qt Folder Analysis

Organize ▾ Include in library ▾ Share with ▾ New folder				
★ Favorites				
Desktop				
Downloads				
Recent Places				
Libraries				
Documents				
Music				
Pictures				
Name	Date modified	Type	Size	
index	9/17/2017 8:35 AM	File folder		
blk00000.dat	9/10/2017 4:22 PM	DAT File	131,039 KB	
blk00001.dat	9/10/2017 4:31 PM	DAT File	131,036 KB	
blk00002.dat	9/10/2017 4:39 PM	DAT File	131,047 KB	
blk00003.dat	9/10/2017 4:45 PM	DAT File	131,059 KB	
blk00004.dat	9/10/2017 4:51 PM	DAT File	131,063 KB	
blk00005.dat	9/10/2017 4:56 PM	DAT File	131,068 KB	
blk00006.dat	9/10/2017 5:02 PM	DAT File	131,072 KB	
...
Name	Date modified	Type	Size	
index	9/17/2017 8:35 AM	File folder		
blk00000.dat	9/10/2017 4:22 PM	DAT File	131,039 KB	
blk00001.dat	9/10/2017 4:31 PM	DAT File	131,036 KB	
blk00002.dat	9/10/2017 4:39 PM	DAT File	131,047 KB	
blk00003.dat	9/10/2017 4:45 PM	DAT File	131,059 KB	



Bitcoin Core/Bitcoin-Qt Folder Structure



- Blocks subdirectory – This subdirectory contains blockchain data and contains a “blk.dat” file and a “blocks/index” subdirectory
- “blk.dat” stores actual Bitcoin block dumped in raw format
- The “blocks/index” subdirectory is a database that contains metadata about all known blocks
- chainstate subdirectory – It is a database with a compact representation of all currently up spent transactions and some metadata about where the transactions originated
- Database subdirectory – It contains database journaling files



Collection of Bitcoin Artifacts



- System Info
- Info about Logged Users
- Registry Info
- Remnants of Chats
- Web browsing Activities
- Recent Communications
- Info from Cloud Services



Few Tips for an Investigator

- Look thoroughly through the transactions happening on Blockchain
- Note down Bitcoin public addresses properly
- Seize any Physical object that can connect to the Internet in addition to the Hard Drive
- Bitcoins addresses can help in tracing the purchases



Thank You