Discussion Draft V1.1

Bitcoin: Contender for global currency or a haven for unethical agents?

Working Team
Matthew Ayres
Alvarez Pereira Brais
Shai Gorsky
Sean Hayes
Flávia Maria
Stefan Pfenninger
Zhi Qiao
Jessica Santana

23rd Jun 2014

Executive Summary

What exactly is Bitcoin?

- Bitcoin overview & history
- Bitcoin operating model & transaction flow
- Bitcoin data

Key Issues

- Disruption
- Trust
- Fraud

Research Focus Areas

- Network insights
- Timing insights
- Dynamics

Summary

What exactly is Bitcoin?

- Bitcoin is a consensus network that enables a new payment system and a completely digital money

- It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen

Value Proposition
1. 24 x 7 P2P payments
2. Simple mobile scan payments
3. Platform independent
4. Bank independent (decentralised)
5. Zero or low transaction fees
6. Identity independence

Questions
1. Can independence be trusted?
2. Can P2P disrupt core banking?
3. Does BTC reflect XR fundamentals?
4. Is BTC being used fraudulently?
5. Is the model robust?
6. Does anonymity optimise value?

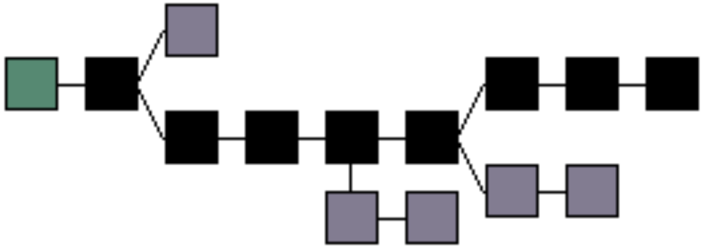
Summary

Definitions

What exactly is Bitcoin?

Term	Definition
Block	Data is permanently recorded in the Bitcoin network through files called blocks. A block is a record of some or all of the most recent Bitcoin transactions that have not yet been recorded in any prior blocks
Genesis block	A genesis block is the first block of a block chain. Modern versions of Bitcoin assign it block number 0
Blockchain	A block chain is a transaction database shared by all nodes participating in a system based on the Bitcoin protocol. A full copy of a currency's block chain contains every transaction ever executed in the currency
Mining	Mining is the process of adding transaction records to Bitcoin's public ledger of past transactions
Reward	When a block is discovered, the discoverer may award themselves a certain number of bitcoins, which is agreed-upon by everyone in the network. Currently this bounty is 25 bitcoins; this value will halve every 210,000 blocks

Blockchain Diagram

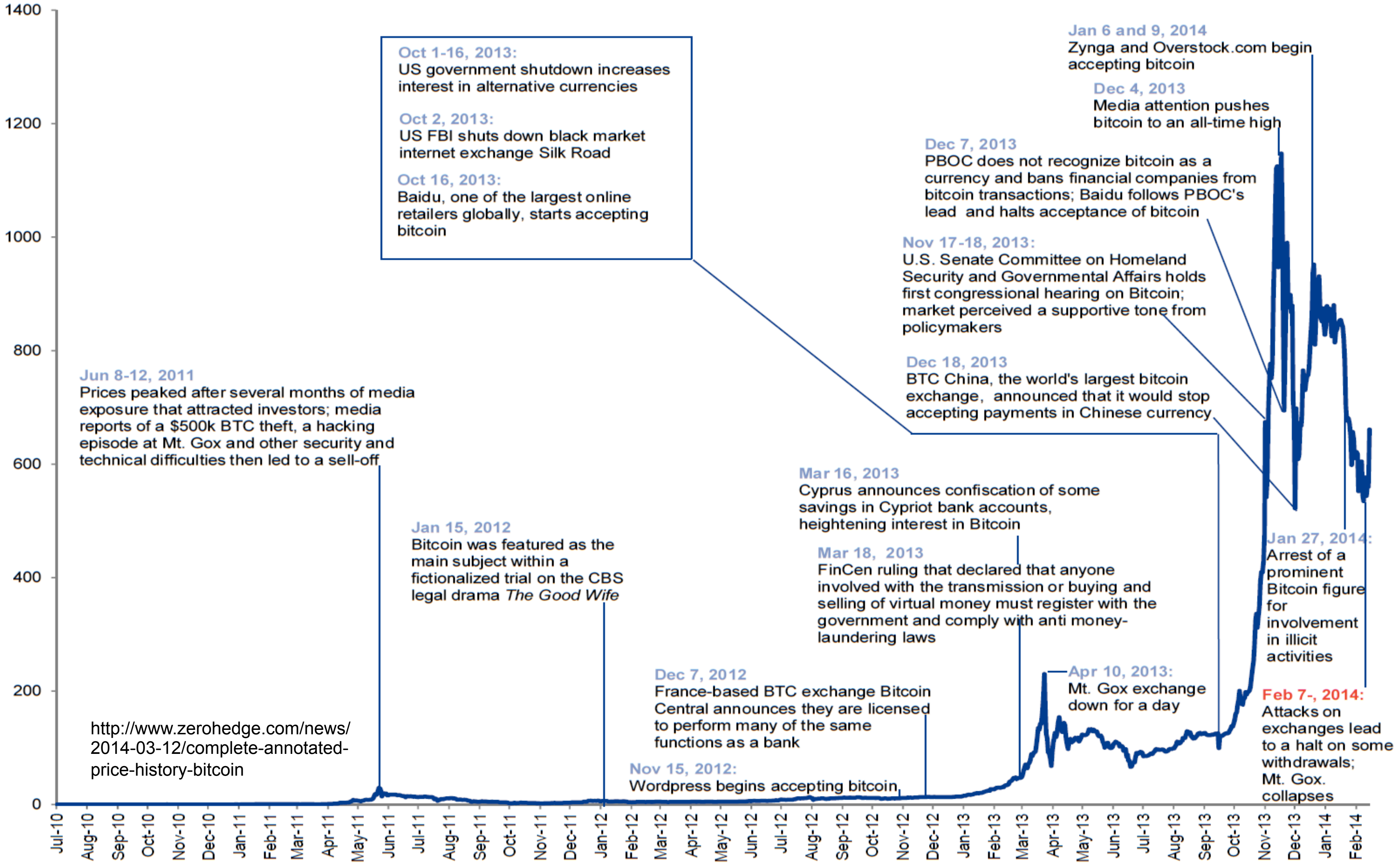


Blocks in the main chain (black) are the longest series of blocks that go from the genesis block (green) to the current block. Purple blocks are blocks that are not in the longest chain and therefore not used.

Source: https://en.bitcoin.it/wiki/File:Blockchain.png

Bitcoin has seen a rapid rise in price including significant volatility

COINDESK BITCOIN PRICE INDEX, BTC/$



Jun 8-12, 2011
Prices peaked after several months of media exposure that attracted investors; media reports of a $500k BTC theft, a hacking episode at Mt. Gox and other security and technical difficulties then led to a sell-off

Jan 15, 2012
Bitcoin was featured as the main subject within a fictionalized trial on the CBS legal drama *The Good Wife*

Nov 15, 2012:
Wordpress begins accepting bitcoin

Dec 7, 2012
France-based BTC exchange Bitcoin Central announces they are licensed to perform many of the same functions as a bank

Mar 16, 2013
Cyprus announces confiscation of some savings in Cypriot bank accounts, heightening interest in Bitcoin

Mar 18, 2013
FinCen ruling that declared that anyone involved with the transmission or buying and selling of virtual money must register with the government and comply with anti money-laundering laws

Apr 10, 2013:
Mt. Gox exchange down for a day

Oct 1-16, 2013:
US government shutdown increases interest in alternative currencies

Oct 2, 2013:
US FBI shuts down black market internet exchange Silk Road

Oct 16, 2013:
Baidu, one of the largest online retailers globally, starts accepting bitcoin

Nov 17-18, 2013:
U.S. Senate Committee on Homeland Security and Governmental Affairs holds first congressional hearing on Bitcoin; market perceived a supportive tone from policymakers

Dec 4, 2013
Media attention pushes bitcoin to an all-time high

Dec 7, 2013
PBOC does not recognize bitcoin as a currency and bans financial companies from bitcoin transactions; Baidu follows PBOC's lead and halts acceptance of bitcoin

Dec 18, 2013
BTC China, the world's largest bitcoin exchange, announced that it would stop accepting payments in Chinese currency

Jan 6 and 9, 2014
Zynga and Overstock.com begin accepting bitcoin

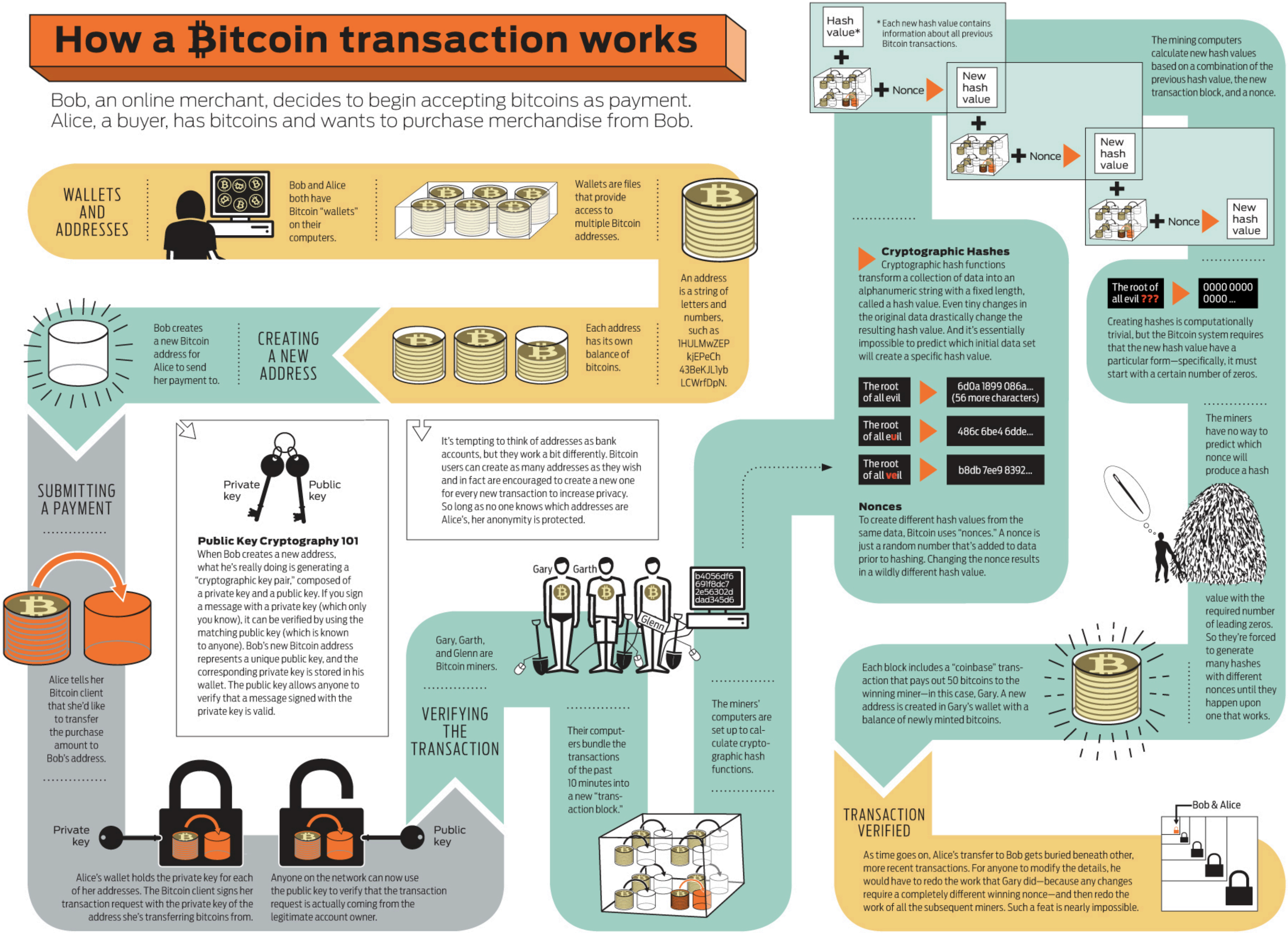
Jan 27, 2014:
Arrest of a prominent Bitcoin figure for involvement in illicit activities

Feb 7-, 2014:
Attacks on exchanges lead to a halt on some withdrawals; Mt. Gox. collapses

http://www.zerohedge.com/news/2014-03-12/complete-annotated-price-history-bitcoin
]

How a ₿itcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.



WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEPkjEPeCh43BeKJL1yb LCWrfDpN.

Each address has its own balance of bitcoins.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

Public Key Cryptography 101

When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.

Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil	6d0a 1899 086a... (56 more characters)
The root of all euil	486c 6be4 6dde...
The root of all veil	b8db 7ee9 8392...

Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

* Each new hash value contains information about all previous Bitcoin transactions.

The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

The root of all evil ??? → 0000 0000 0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

JOSHUA J. ROMERO, BRANDON PALACIO & KARLSSONWILKER INC.

Source: http://images.dailytech.com/nimage/Bitcoin_Transactions_Explained_Wide.png

Draft research Focus (V1.0)

Proposal for the Bitcoin group

Working definition of a research focus:

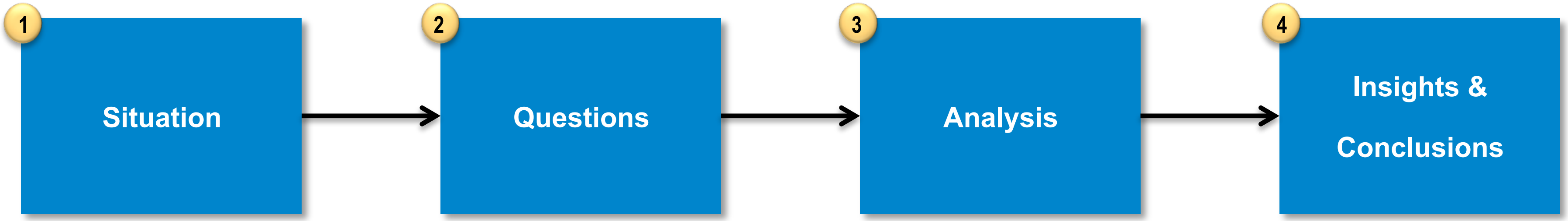
- The focus of periods of rapid change in exchange rate of Bitcoin in relation to U.S. dollars around notable peaks, which are the extreme maximum points (ups and down). Two possible approaches are: 1. examining the peaks by moving backwards and forwards in time (as much as computational efforts allow), or 2. defining narrower slices of the peak time period in discrete time steps.

What to measure/analyze?

- Average volume of Bitcoin transactions
- Actual distribution of Bitcoins per slice (which depends on computational effort)
- Average "days destroyed" per Bitcoin sold
- Short/long selling in Bitcoin
- Average days between peaks and heists
- In-degree and out-degree distribution (average degree of the nodes that are selling and buying)
- Average centrality of those nodes that are selling and buying
- Geographic location and any identity markers of addresses

Source:

Bitcoin overview and data analysis processes



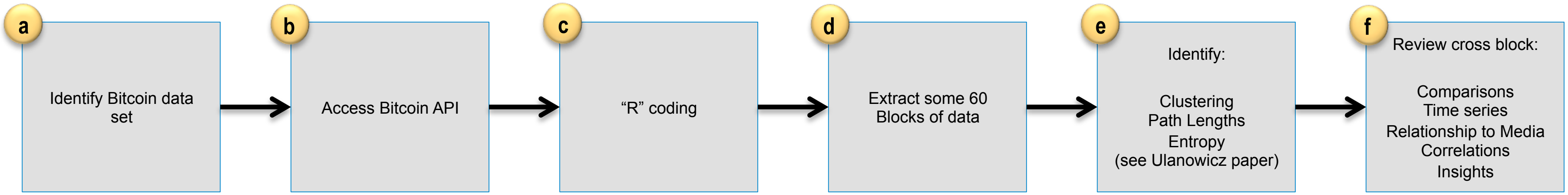
- Bitcoin is a rapidly growing virtual currency that has no central control
- There are cases of fraud and what appears to be gaming behaviors

- Can complex systems analysis find weaknesses in Bitcoin?
- Are periods prior to and post major changes in currency helpful to identify emerging network characteristics?

- Bitcoin has transaction level data for Volume ($, #) and exchange rate
- The data source is very large so time slices will be used and accessed via API, using the below process

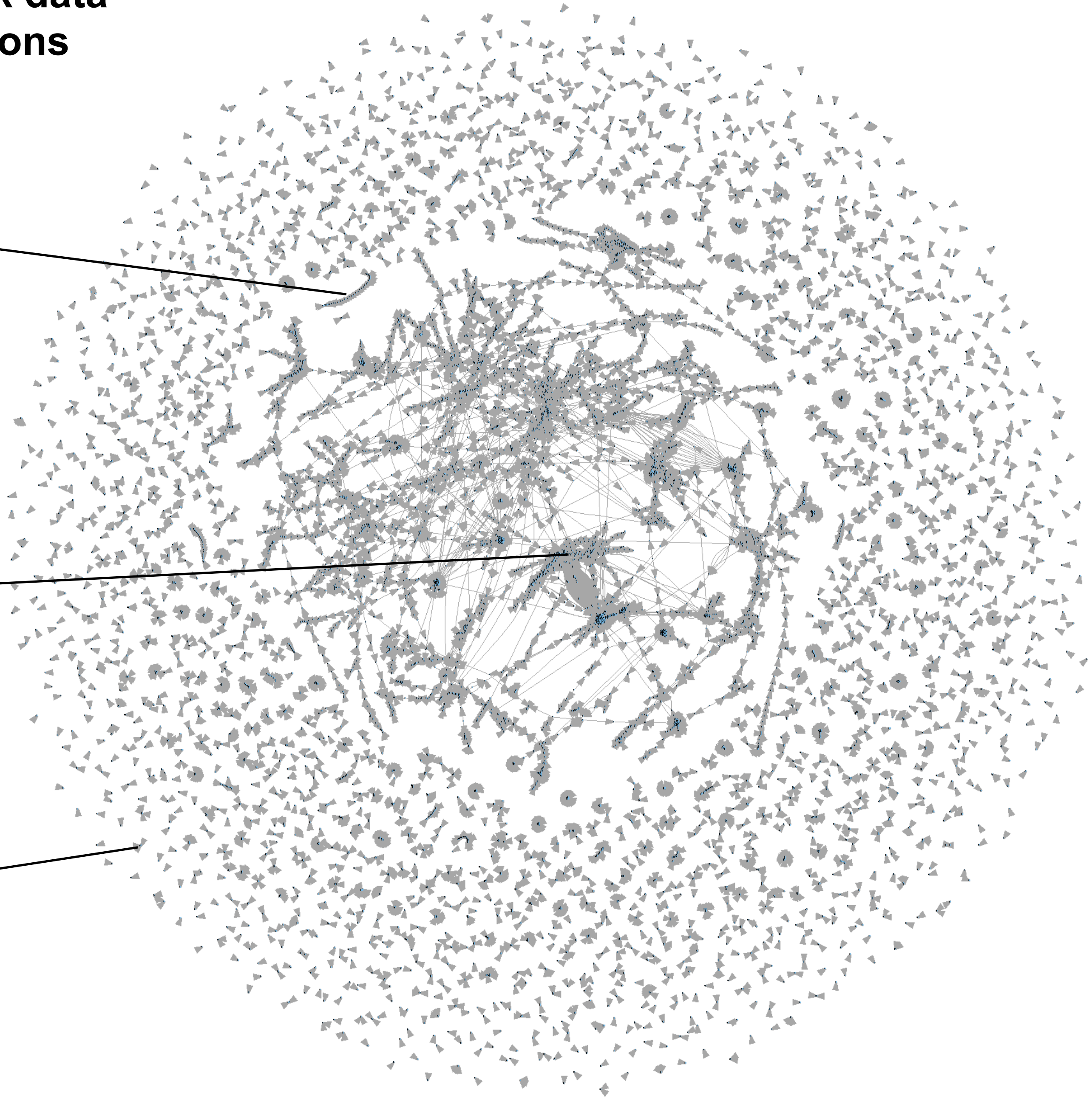
- Insights will be developed based on comparisons from pre and post event data
- A core focus of the work will be on functional and characteristic network change

Analysis Process



Support Paper: Quantitative methods for ecological network analysis, Ulanowicz,2004

First look at the network data raises a range of questions



Why do we see long “chains” in the network?

What is happening at critical network nodes?

What patterns are common across the network?

Source: Data extracted by Bitcoin.com, analysus by Sean Hayes