DFIN-511

Introduction to Digital Currencies

Session 2

The Byzantine Generals' Problem & the Bitcoin Solution

Objectives of Session 2

- Recognize centralized asset & transaction ledgers
- Understand the Byzantine Generals' Problem
- Understand how Bitcoin addresses the Byzantine Generals' Problem
- Review some key Bitcoin metrics and developments in practice

This session will provide the basis for understanding the theoretical underpinnings of Bitcoin, thinking about their broader implications and the practical exercises that will follow in the later sessions.

Students new to Bitcoin will find this the most challenging session of the course. <u>It is important to invest as much time as is needed in understanding this part and to not be discouraged</u>. It took most of us many hours/days/weeks to understand this part! Be active in the forums and ask questions!

Agenda

1. Asset and Transaction Ledgers
2. The Byzantine Generals' Problem
3. The Bitcoin Approach to the Byzantine Generals' Problem
4. Bitcoin: Some Key Metrics
5. Further Readings

1. Asset and Transaction Ledgers

Centralized Ledgers

- We take centralized ledgers (with trusted record-keepers) for granted because we have never before had a practical alternative
- If we let any untrusted party enter transactions in an important traditional ledger, chaos is likely to ensue (would you, for example, let strangers keep track of your checking account balance?)
- Given this, a trusted party is in charge of all ledgers of importance in modern society, whether it is Citibank for your bank account, or your local land registry office for the title deeds for your house
- Centralized ledgers, however, are not perfect because record-keepers are not always trustworthy, act as gatekeepers and represent a Single Point of Failure (SPOF)
  - Record-keepers might not be trustworthy in practice. They may, for example, take a bribe to transfer a piece of land illegally
  - Record-keepers might exclude parties that they disapprove of (e.g., payment networks refusing to serve adult performers)
  - Record-keepers might lose important transaction records, even if they are well-intentioned, due to carelessness, natural disaster and so on

We are surrounded by centralized ledgers

Your bank account transactions

Your credit card transactions

The General Ledger underlying your company's financial statements

The ownership records of corporate securities

The list of title deed holders at your land registry office

The guest reservations at a hotel

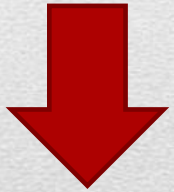
The names of lessees of cars leased by Toyota

The records relating to your citizenship, such as your national ID number

Decentralized Ledgers

A successful decentralized ledger that allowed parties that did not know or trust each other to transact together would have a wide range of advantages. In fact, it practically sounds like a fairy tale in traditional terms:

- Invulnerable to censorship and exclusion
- Invulnerable to malfeasance by record-keepers
- Invulnerable to loss of records



One of the reasons for the excitement of technologists about Bitcoin is that they believe Bitcoin is the first practical manifestation of an invention that could allow for the decentralization of all ledgers (not just currency)

Why Bitcoin Matters?

"A mysterious new technology emerges, seemingly out of nowhere, but actually the result of two decades of intense research and development by nearly anonymous researchers. Political idealists project visions of liberation and revolution onto it; establishment elites heap contempt and scorn on it. On the other hand, technologists – nerds – are transfixed by it. They see within it enormous potential and spend their nights and weekends tinkering with it. Eventually mainstream products, companies and industries emerge to commercialize it; its effects become profound; and later, many people wonder why its powerful promise wasn't more obvious from the start. What technology am I talking about? Personal computers in 1975, the Internet in 1993, and – I believe – Bitcoin in 2014….

The practical consequence of solving this problem is that Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. **The consequences of this breakthrough are hard to overstate.**

What kinds of digital property might be transferred in this way? Think about digital signatures, digital contracts, digital keys (to physical locks, or to online lockers), digital ownership of physical assets such as cars and houses, digital stocks and bonds … and digital money."

- Marc Andreessen, Founder of Netscape & well-known venture capitalist

Source: http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/

2. The Byzantine Generals' Problem

The Byzantine Generals' Problem (BGP)

- The problem of building a purely distributed but trusted system is not a new one in computer science. It is a common challenge in distributed systems with no central control to enforce trust and, is more generally, a sub-set of the study of fault tolerance. Imagine, for example, a computer system with distributed components that need to communicate information to each other, but that information might fail to communicate accurately (or at all) due to technical failures

- The Byzantine Generals' Problem, first proposed by Marshall Pease, Robert Shostak and Leslie Lamport in 1982, provides a stylized description of this problem

- Past attempts at solving the currency side of the problem include the following research :
  - Chaum, D., 1984. Blind Signature System, in: Chaum, D. (Ed.), Advances in Cryptology. Springer US, pp. 153–153.
  - Chaum, D., Fiat, A., Naor, M., 1990. Untraceable Electronic Cash, in: Proceedings of the 8th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '88. Springer-Verlag, London, UK, UK, pp. 319–327.
  - Okamoto, T., Ohta, K., 1992. Universal Electronic Cash, in: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '91. Springer-Verlag, London, UK, UK, pp. 324–337.
  - Wei Dai's B-Money (Wei Dai, 1998, http://www.weidai.com/bmoney.txt)

- Bitcoin, however, a system proposed in a white paper released in November 2008, under the pseudonym Satoshi Nakamoto, is the best solution to this problem that has been proposed to date and has had, by far, the broadest adoption

What is the BGP?

"We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement. The generals must have an algorithm to guarantee that (A) All loyal generals decide upon the same plan of action and (B) A small number of traitors cannot cause the loyal generals to adopt a bad plan"

- *The Byzantine Generals' Problem, 1982*

Should we stay or should we go (to battle)?

Image Source: Wikimedia Commons. Text: The Byzantine Generals' Problem, Lamport, Shostak, Pease, 1982

The BPG: Problem Formulation

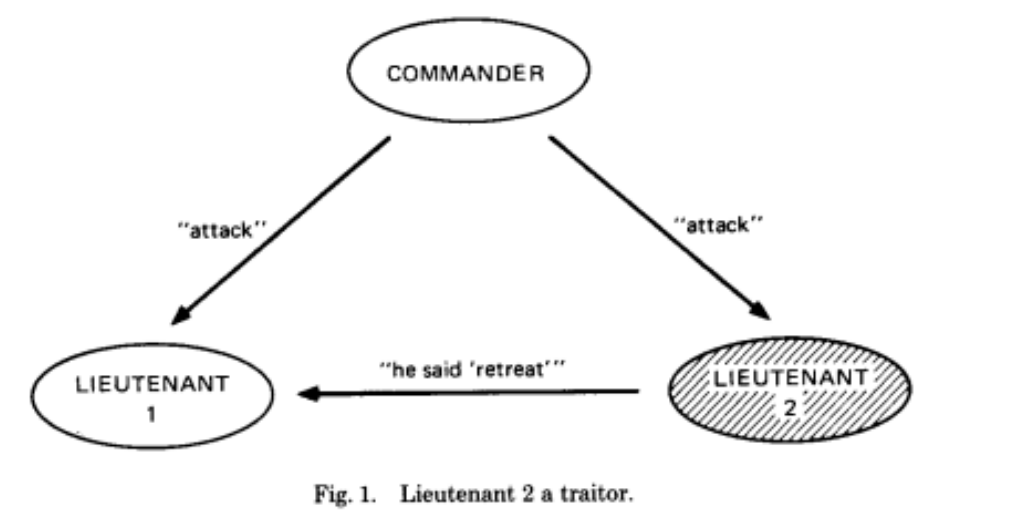


Fig. 1. Lieutenant 2 a traitor.

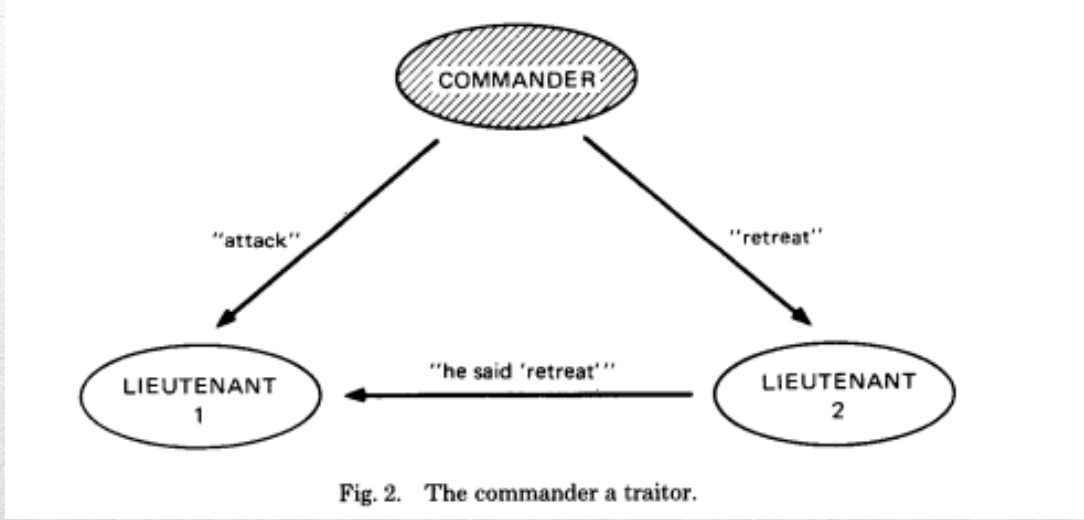


Fig. 2. The commander a traitor.

In this case, 1 traitor (1/3) could cause the attack to fail because one of the Lieutenants would retreat (or potentially retreat) when he should attack instead.

*The traitor prevents the group from **reaching consensus***

Image Source: The Byzantine Generals' Problem, Lamport, Shostak, Pease, 1982

The BPG: Problem Formulation

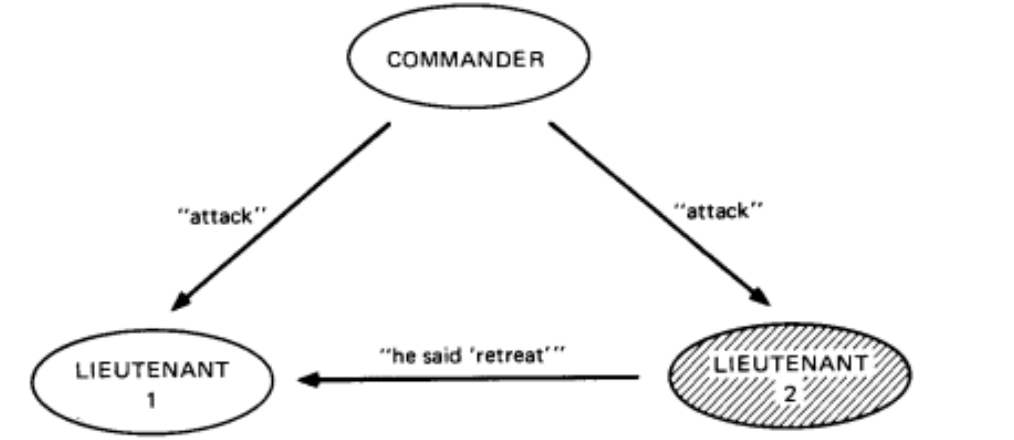


Fig. 1. Lieutenant 2 a traitor.

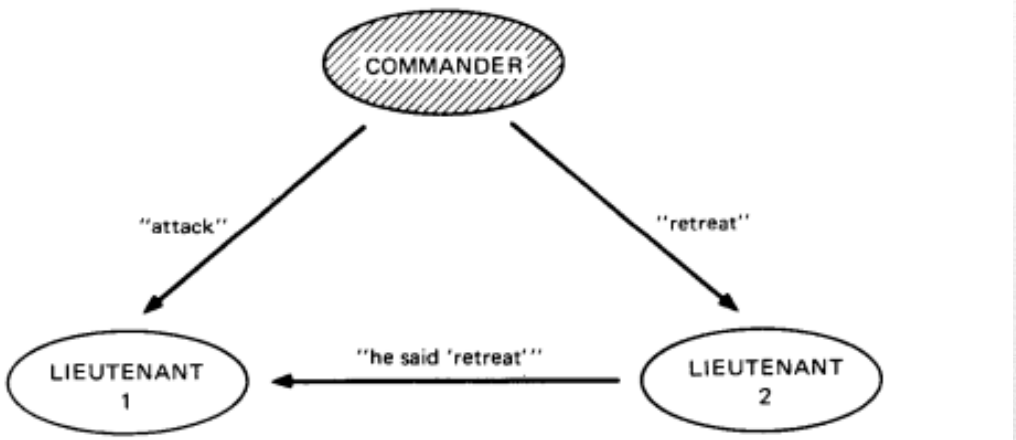


Fig. 2. The commander a traitor.

This slide is so important, we are including it twice. Stop for a few minutes and reflect upon it because this is the core issue underlying Bitcoin and other decentralized systems.

Imagine you are Lieutenant 1 in Figure 1. How do you know which instruction to follow? If you find a new solution to that question, you might be the next Satoshi Nakamoto…

Image Source: The Byzantine Generals' Problem, Lamport, Shostak, Pease, 1982

The Byzantine Generals

As the number of the parties in the system increase, the number of channels for communication (and opportunities for mistrust) increase exponentially.

Imagine the complexity of ***building consensus*** in a truly decentralized system with thousands or millions of parties involved.

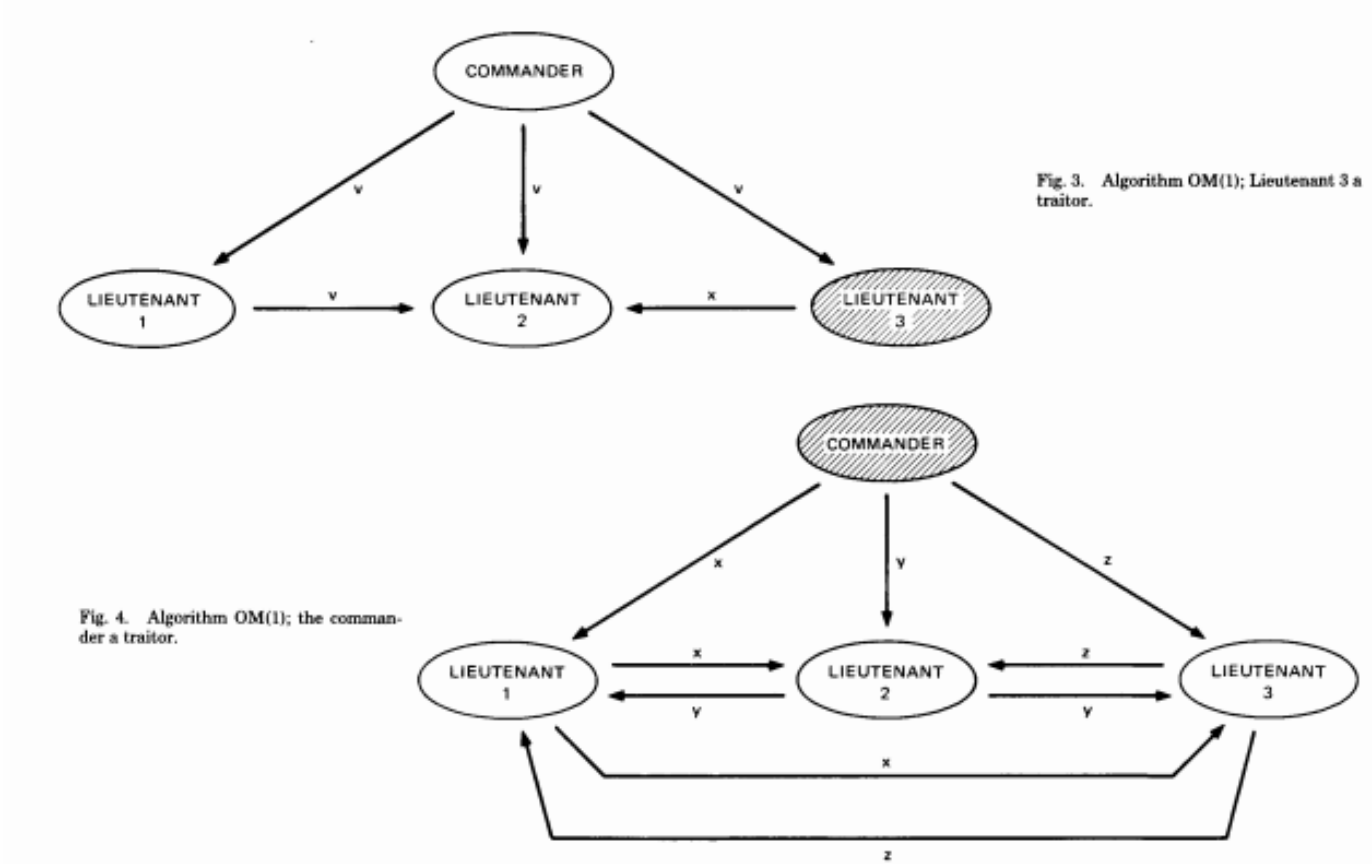


Image Source: The Byzantine Generals' Problem, Lamport, Shostak, Pease, 1982

2. Bitcoin's Approach To The Byzantine Generals' Problem

Bitcoin: Some Basic Definitions

- **bitcoin**: without capitalization, is used to describe bitcoins as a unit of account
- **Bitcoin**: with capitalization, is used when describing the concept of Bitcoin, or the entire network itself
- **Address**: a location that bitcoins have been sent to and reside at. Alternatively, can be thought of as an account of sorts that has a balance of bitcoins
- **Blockchain**: The complete transaction ledger of the Bitcoin network, showing how bitcoins have been transferred from one address to another over time. The blockchain is a public record of all bitcoin transactions in chronological order
- **Transaction**: The movement of bitcoins from one address to another address. In traditional terms, this can be thought of as a payment or money movement

The Bitcoin Ledger: The Blockchain

- The starting point:
  - A Bitcoin user downloads a piece of software (the Bitcoin "client" software)
  - This client software will initially download the blockchain, the ledger of all transactions in the history of Bitcoin
  - Each Bitcoin client stores the complete record of all bitcoin transactions of all time. There is no central record-keeper, just a set of copies distributed among all the clients

- Once the blockchain is on a client computer, the issue of synchronization emerges:
  - How are the blockchains (ledgers) that are on each client kept in sync with each other?
  - Or, in other words, how do the blockchains reach "distributed consensus" without a central party holding the definitive transaction ledger?
  - Or, in other words, when a client receives conflicting messages about a transaction, which one should it accept and which one should it ignore? Which one is truthful, which one is a traitor?

- By now, you should realize that keeping the blockchain copies in sync is a manifestation of the Byzantine Generals' Problem

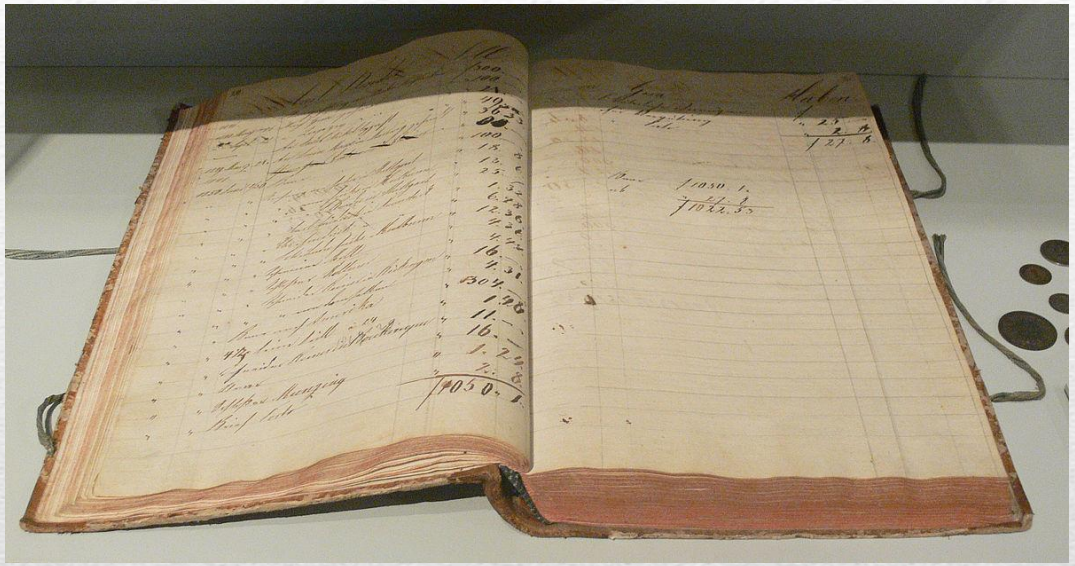
Syncing the Blockchain: Mechanics

1. When a Bitcoin client executes a transaction (sends bitcoins from one address to another), it broadcasts the transaction to all the users in the system. Within a few seconds, most of the clients in the world receive the transaction

2. At this point, however, the transaction is considered "unconfirmed" because it suffers from the Byzantine Generals' Problem. E.g., what if a rogue Bitcoin client sent out two transactions moving the same bitcoin to two different addresses? Which one should the clients accept?

3. The mechanism that Bitcoin uses to confirm transactions and resolve the Byzantine Generals' Problem is a process called "**mining**"

Syncing the Blockchain: Mining?



This

~~Not This~~

Mining is a largely misleading analogy for what 'miners' do.
Think of the miners as bookkeepers and they will make much more sense

Image Source: Wikimedia Commons. Ledger and Coal Strip Mine

Mining is a 3 step process

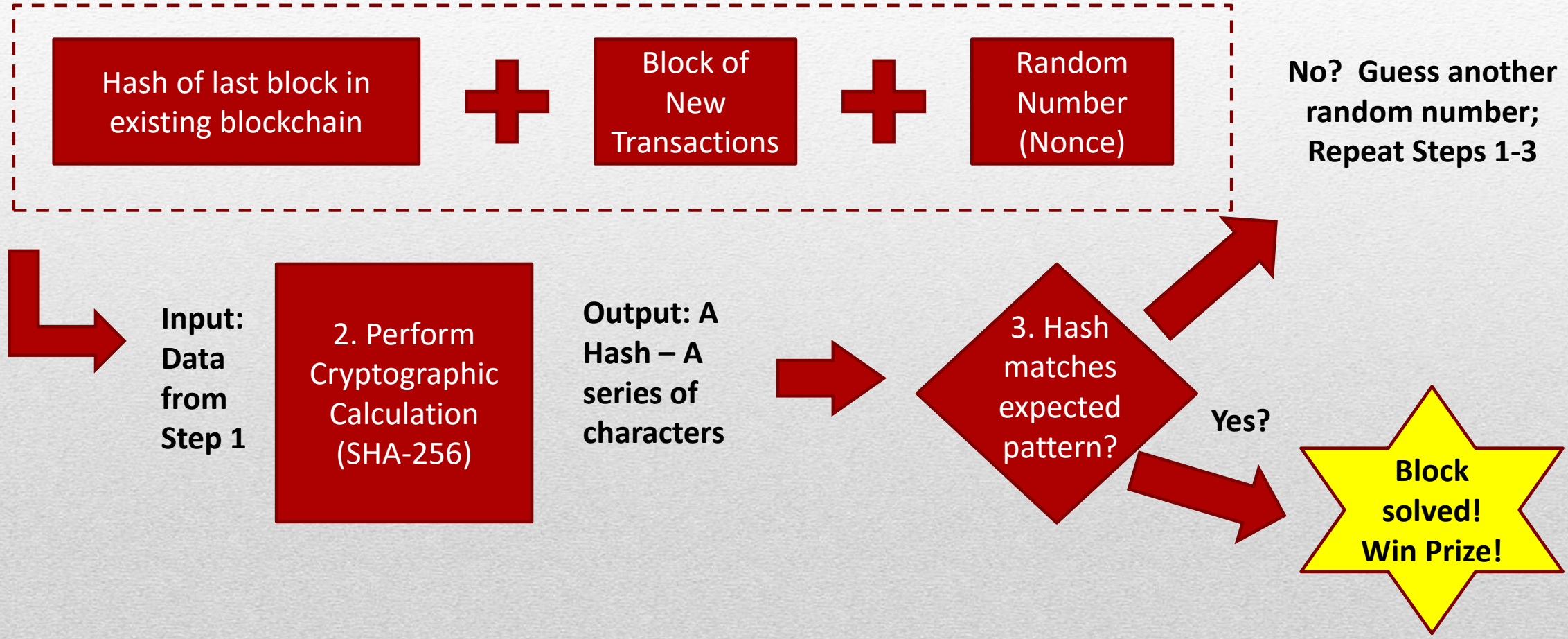
- **Step 1**: Miners create a file that contains (a) the hash of the last block in the existing blockchain, (b) a block of the new proposed transactions broadcast in the Bitcoin network and (c) a random number that the miner guesses (a "nonce"). The combination of (a) + (b) + (c) is the data used as the input for Step 2

- **Step 2:** Miners apply a cryptographic function to the data. The details of this function will be explained in detail in other sessions. Its most important function is that it produces a unique sting of characters which cannot be reversed (knowing the result does not allow you to retrace to the initial data). This new string of data is called the "data hash".

- **Step 3**: The hash is reviewed against a desired pattern (in the case of Bitcoin, how many leading zeros it has, an outcome that is effectively random). If the hash matches the pattern, the miner has a valid block and will win an economic prize (more on that later). If the hash does not match the pattern, the miner returns to step 1, guessing a new nonce and repeating the exercise

Mining in 3 steps

1. Compile Some Data To Be The Input To A Calculation



Mining: Winning a Prize?

- Once a miner has a winning block, it broadcasts it to the other clients as a "block" of confirmed transactions.
  - The client nodes verify that the hash matches the pattern needed and accept the new block, adding it to the existing blockchain that they all store. Note: Blockchain = a chain of blocks (!)
  - After that, all miners start working on finding the next block, incorporating the new, larger blockchain as their starting point in Step 1

- The miner is allowed to collect as part of having a winning block:
  - An allocation of new bitcoins (currently, 12.5 bitcoins per block) that is an increase in the total number of bitcoins
  - The transaction fees from all the transactions that were included in the block

- Block reward started from 50 bitcoins per block and is halving every 210,000 blocks, approximately every 4 years

- In September 2016, the block reward is 12.5 bitcoins. This amount far outweighs the reward from transaction fees. The last halving was this July and the next will take place in 2020. Block rewards will stop once the network reaches Block 6.930.000 (sometime around the year 2140). The total number of bitcoins issued by then will be about 21 million(https://en.bitcoin.it/wiki/Controlled_supply).

Mining: Winning a Prize?

Approximately 15.2M bitcoins have been issued so far through block rewards

This decelerating production function means that a total of 21 millions bitcoins will ever be created by 2140

The graph shows up to 2060 when more than 20,5 million will have been issued, and the rate will keep decreasing until the final issuance takes place in 2140

Mining: Auto-Adjusting Puzzles

- This winning of prizes sounds very pleasant. Why hasn't someone with a big computer mined all the bitcoins?

- Fortunately, the prizes (new blocks) auto-adjust their difficulty (leading zeros) to account for how much computing power is in the Bitcoin network.
  - The difficulty of guessing the correct random number (nonce) that produces the desired number of leasing 0s in the block hash, is adjusted every 2016 blocks (approximately two weeks) so that the network produces one successful block every 10 minutes or so.
  - While any given block might take less time or more time to create due to luck, if blocks start being produced too often or not often enough, the prize puzzle gets more difficult or less difficult so that blocks are formed every ten minutes or so again

- This means that, whether the Bitcoin network just has 20 old laptops doing mining or millions of super-computers mining, blocks will still be created every 10 minutes and anyone's expected reward from mining is their % of the total network's computing (mining) power. And since anyone can setup a mining node, if it is very profitable to mine because, say, the price of a bitcoin has gone up, more miners will come into the system (and vice-versa, if it is unprofitable, miners will drop out)

Back to the Byzantine Generals' Problem

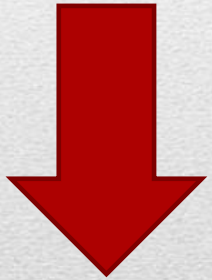
- An astute reader might say: "But, you have not yet solved the BGP, just moved it to the miners. What if two miners send out blocks with conflicting information? How do the clients choose?"
- The answer is that when a client is trying to decide which blockchain version to accept, it must choose the one that is "longest" (In Bitcoin terms), aka the one that has the "greatest combined difficulty" (of the hashes used to create it). In other words, the chain that took the most computation power to create
- The shorter blockchain is discarded (an "orphan block" and those transactions have to be re-processed if they were not in the longer blockchain)
- Given this, a traitor cannot keep entering bad signals into the blockchain (aka, spend money in one block, then erase the transaction in the next block) unless he or she can keep producing the longest block (the one with the most computation associated with it) which, statistically, the traitor can't do, given the essentially random nature of block creation

The Essentials Of The Solution

Random Work
(Guessing of the Nonce) To
Produce A Chain

+

Select The “Longest”
(Most Difficult) Chain



Solution to the Byzantine Generals’ Problem

Mining: Proof of Work

- The random number creation ("proof of work") is the subject of great confusion by laymen
- They often consider it (a) wasted effort or (b) an indication of poor system design ("why do they need to do so much work to enter a transaction when my database can just do it instantly?")
- In fact, it is the *key* aspect of providing ledger security, in that it prevents any one party from hijacking the ledger
- One might go as far as saying: "if you don't understand why the random number generation is there, you don't really understand how Bitcoin works."

  One useful mental model is to think of it as a lottery of sorts relating to who gets to enter the next transactions in the system to prevent one person from taking control of the ledger

Mining: 51% Attack

- To be more precise, Bitcoin solves the Byzantine Generals' Problem **so long as honest (or, at least, non-collaborating) miners consist of at least 50% of the hashing power in the system**

  (for theoretical attack scenarios, the latest research puts this threshold closer to 66.67%)

- Like a casino in Las Vegas always winning in the long-run, if one miner controls more than 50% of the hash power, in time, it can always produce a "longer" chain than all the other miners combined and therefore it can reverse its own past transactions and/or refuse to enter transactions from others. (It still can't spend the bitcoins of others, but it can prevent them from being spent).
  - This is known as a "51% attack"
  - In other words, a 51% miner becomes a centralized ledger-keeper like a bank or credit card company, eliminating the advantages of a decentralized system

- So, it is important for the ecosystem of any cryptocurrency that honest miners maintain 50% of the computational power in the system (alternatively, that no single dishonest miner, or coalition of miners, gains more than 50% of the computational power in the network).
  - At times, some mining pools (groups of miners) in Bitcoin have gained over 40% of the hashing power in the network, something that has raised concerns. These major pools have backed off from the 50% mark voluntarily in order to preserve confidence in the system)

Implications

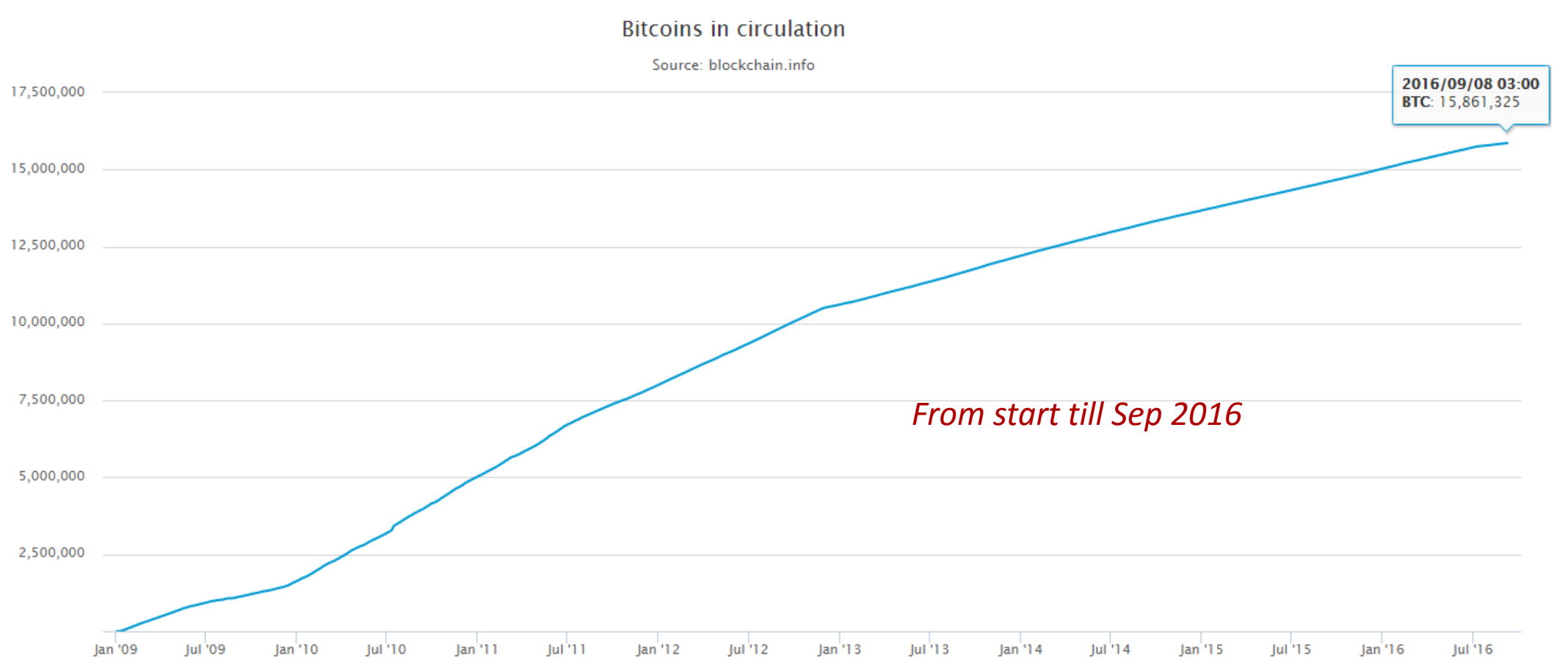
- The implications of this solution to the Byzantine Generals' Problem are the basis for the rest of this course so we are sure that the last few slides have raised a lot of questions

- In future sessions, we will discuss:
  - How you transact with bitcoin in practice
  - Strengths and weaknesses of Bitcoin specifically and relative to other related technologies
  - Implications in the area of currency and beyond

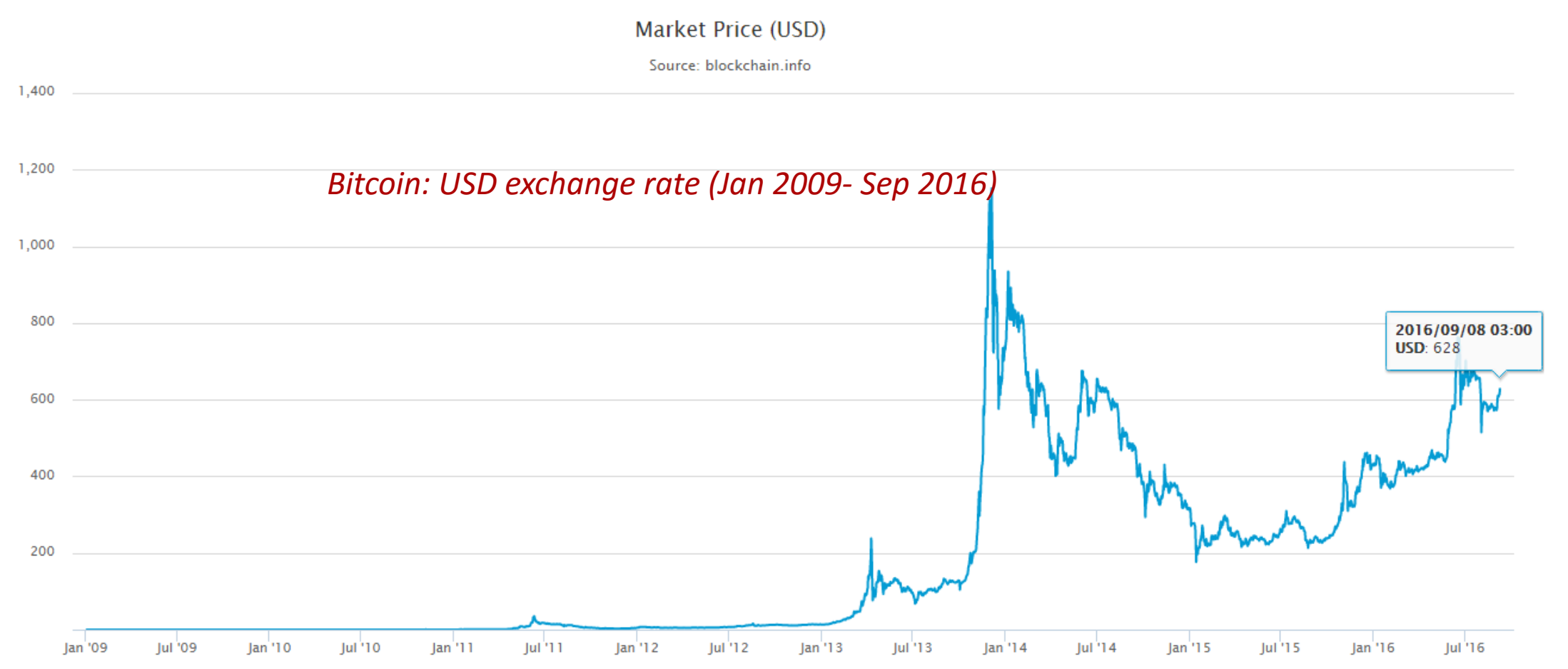
- For this session however, direct your attention primarily to understanding the underlying mechanics as well as possible, because it will strengthen your ability to participate in the rest of the course

4. Bitcoin: Some Key Metrics

Bitcoin Metrics: Number of bitcoins

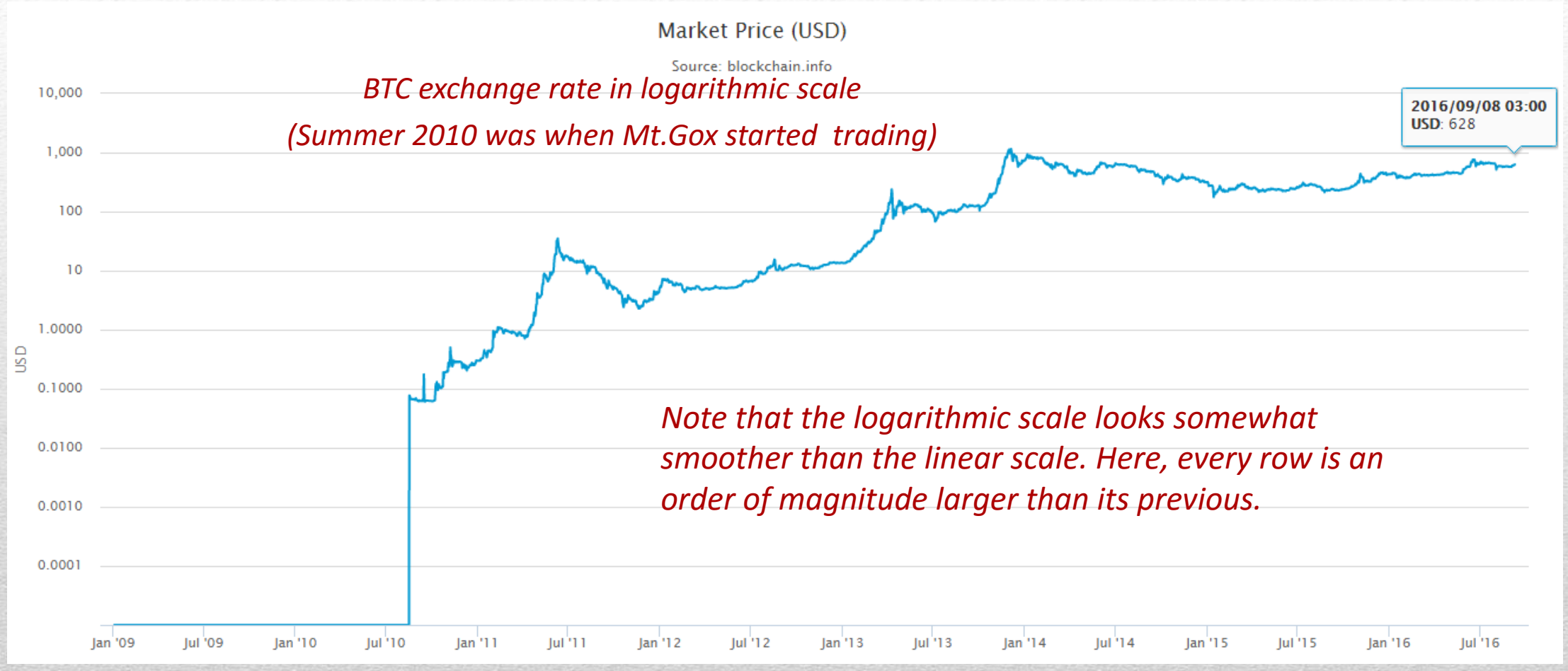


Bitcoin Metrics: Market Price



Bitcoin: USD exchange rate (Jan 2009- Sep 2016)

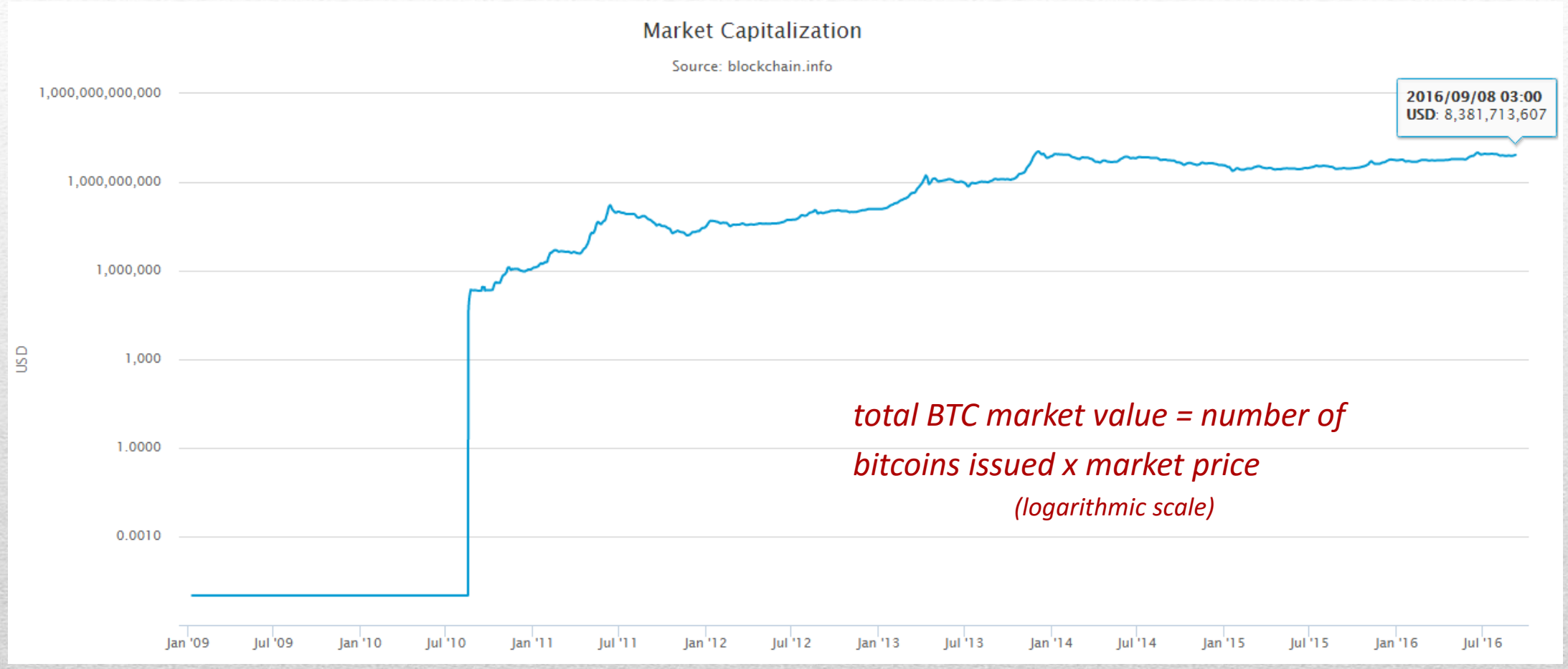
Bitcoin Metrics: Market Price



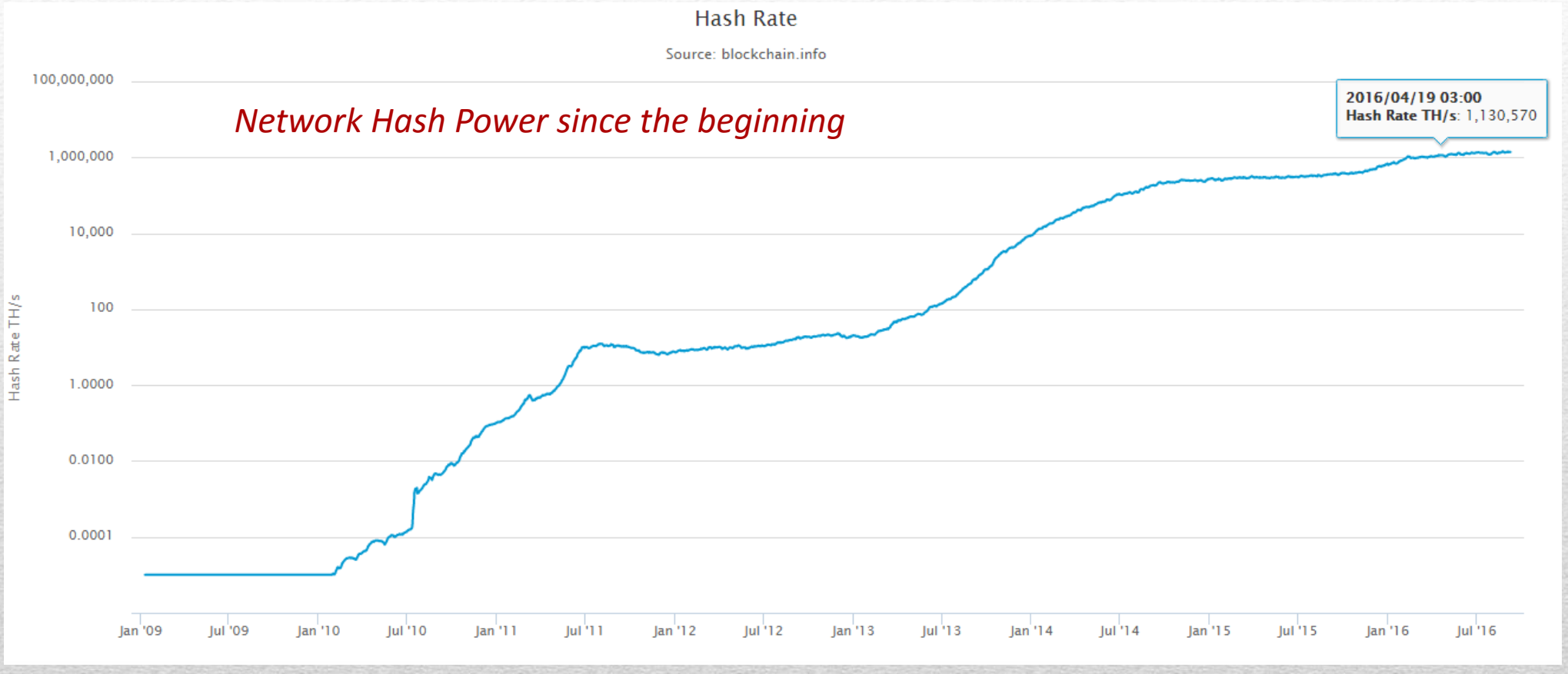
Bitcoin Metrics: Market Capitalization

total BTC market value = number of bitcoins issued (x) market price

Bitcoin Metrics: Market Capitalization



Bitcoin Metrics: Total Mining Power



Conclusions

- Historically, all ledgers of importance have been centralized. While giving a measure of security, central record-keepers have weaknesses in the areas of:
  - Corruption
  - Inclusion
  - Technical failures
- The Byzantine Generals' Problem, a matter of study in the area of fault tolerance, describes why decentralized ledgers have historically been infeasible
- Bitcoin has presented the best solution to-date for solving the Byzantine Generals' Problem and, subject to certain conditions, has made widespread decentralized asset and transaction ledgers possible
- Leading technologists believe that the implications of this technical breakthrough will be far-reaching, extending far beyond digital currency

Some Further Reading (1/2)

These readings cover technical aspects of Bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System (Satoshi Nakamoto)
https://bitcoin.org/bitcoin.pdf
(the paper that started it all)

Bitcoin Series (Khan Academy)
https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it
(9 part video series by Khan Academy that is relatively non-technical, about 101 minutes in total. Watch if you are still confused after this presentation and the papers, it is a different approach to explaining the topic that might help)

By reading this article, you're mining bitcoins (Ritchie King, Quartz)
http://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins/
(A non-technical explanation of mining)

Optional / Advanced:

- The Byzantine Generals' Problem (Leslie Lamport, Robert Shostak, Marshall Pease)
https://www.andrew.cmu.edu/course/15-749/READINGS/required/resilience/lamport82.pdf
(the first paper that defined the Byzantine Generals ' Problem in those terms)
- Majority is not Enough: Bitcoin Mining is Vulnerable
https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf

Some Further Reading (2/2)

These readings cover some implications of Bitcoin

Why Bitcoin Matters (Marc Andreessen, Andreessen Horowitz)
http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/

Bitcoin As Protocol (Albert Wenger, Union Square Ventures)
http://www.usv.com/posts/bitcoin-as-protocol

Circle, Bitcoin and Global Digital Currency (Jeremy Allaire, Circle)
https://www.circle.com/2013/10/30/circle-bitcoin-global-digital-currency/

The Bitcoin Model for Crowdfunding (Naval Ravikand, Angellist)
http://startupboy.com/2014/03/09/the-bitcoin-model-for-crowdfunding/

Bitcoin Series (Antonis Polemitis, Ledra Capital)
http://ledracapital.com/blog/2014/1/4/bitcoin-series-14-our-robot-overlords-will-use-bitcoin
http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list
(a group brainstorming of different places blockchain based technologies can be used)

Questions?

Contact Us

Email:

digitalcurrency@unic.ac.cy

Twitter:

@MScdigital