UNIVERSITY *of* NICOSIA

Session 2

The Byzantine Generals' Problem & the Bitcoin Solution

MSc in Digital Currency

The Byzantine Generals' Problem

Session 2: Objectives

This session will provide the basis for understanding the theoretical underpinnings of blockchain technology and Bitcoin. We will look at the broader implications and introduce practical exercises in later sessions.

Students new to this technology will find this the most challenging session of the course. It is important to invest as much time as needed in understanding this material and to not be discouraged. It took most of us many hours / days / weeks to understand this part!

Objectives

- Identify centralized asset & transaction ledgers.
- Understand the Byzantine Generals' Problem.
- Understand how Bitcoin approaches the Byzantine Generals' Problem.
- Review some key Bitcoin metrics and developments.

The Byzantine Generals' Problem

Session 2: 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. Conclusions
6. Further Reading

1. Asset and Transaction Ledgers

Asset and Transaction Ledgers

Some Useful Definitions

Ledger

A **complete** record of a business' economic activities, usually to track of the transfer of money and asset ownership.

Blockchain

A list of validated blocks, each linking to its predecessor all the way back to the genesis block. Transactions in this global double-entry bookkeeping ledger encode the transfer of value between participants in a peer-to-peer network. (*Mastering Bitcoin*)

SHA-256

A cryptographic hash acts like a 'fingerprint' for a string of text or data file. Can be used to confirm integrity and authenticity. The **SHA-256** algorithm generates a 256-bit (32-byte) hash.

Hash Converter

Use an online hash converter, such as https://hash.online-convert.com and enter the text you want to convert. Then, try changing just a letter in the input text to see how the resulting hash varies significantly

Example: Try hashing the words 'Bitcoin' and 'bitcoin.'

Asset and Transaction Ledgers

The Role of Ledgers

Ledgers are used to record economic activities, such as the ownership of assets and the transfer of value, among various stakeholders such as consumers, distributors, suppliers, exchanges, and governments.

The assets recorded in a ledger can be:

- Tangible i.e. motor vehicles, houses
- Intangible i.e. money, stock certificates, digital rights

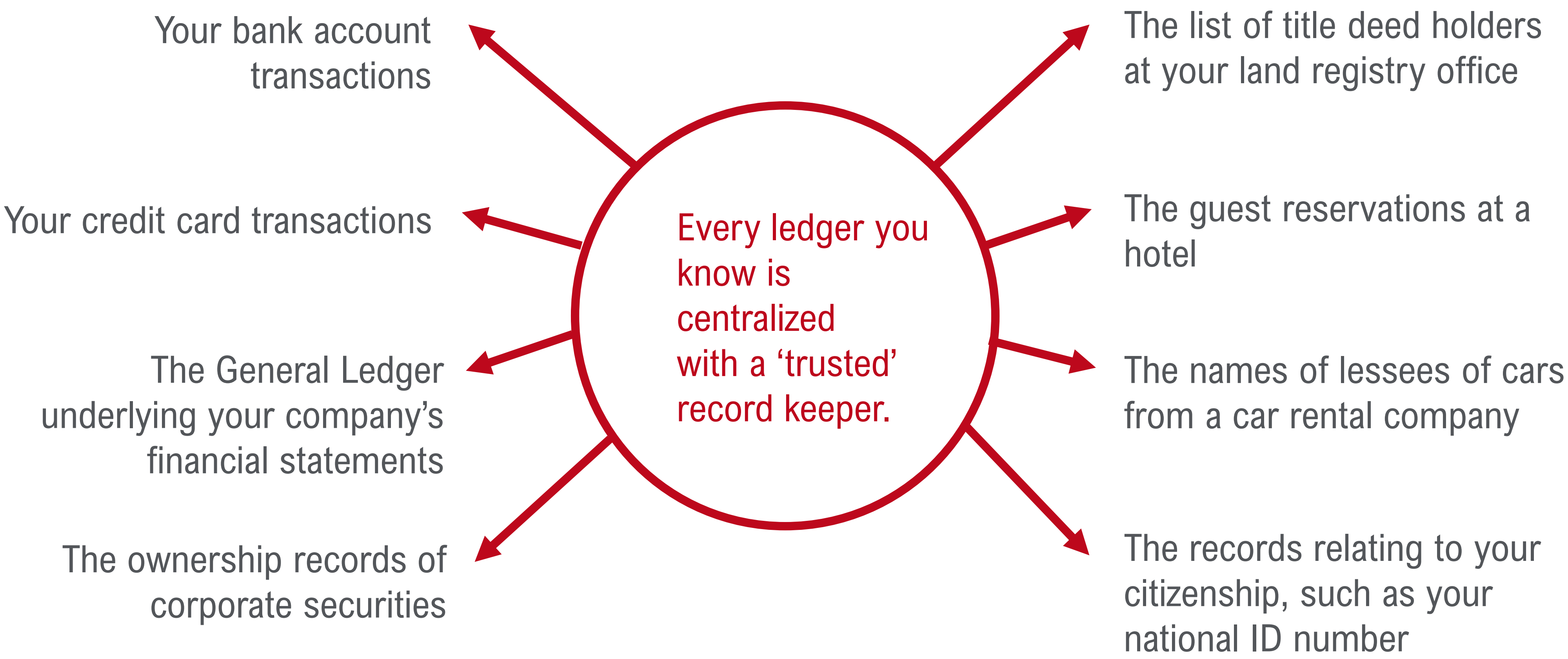
Asset and Transaction Ledgers

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 third party make entries 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 third party is in charge of all ledgers of importance in modern society, whether it is the bank which "stores" your funds, or your local land registry office for the title deeds to your house.
- Centralized ledgers, however, are fallible. Record-keepers are not always trustworthy, act as gatekeepers, and represent a Single Point of Failure (SPoF).
    - Record-keepers might not be trustworthy. They may, for example, take a bribe to transfer a land deed illegally.
    - Record-keepers might exclude parties who they disapprove of (e.g. banks blocking transactions to/from cryptocurrency exchanges and businesses).
    - Record-keepers might lose important records due to carelessness, technical failure, natural disaster and so on.

Asset and Transaction Ledgers

We are surrounded by centralized ledgers



Every ledger you know is centralized with a ‘trusted’ record keeper.

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

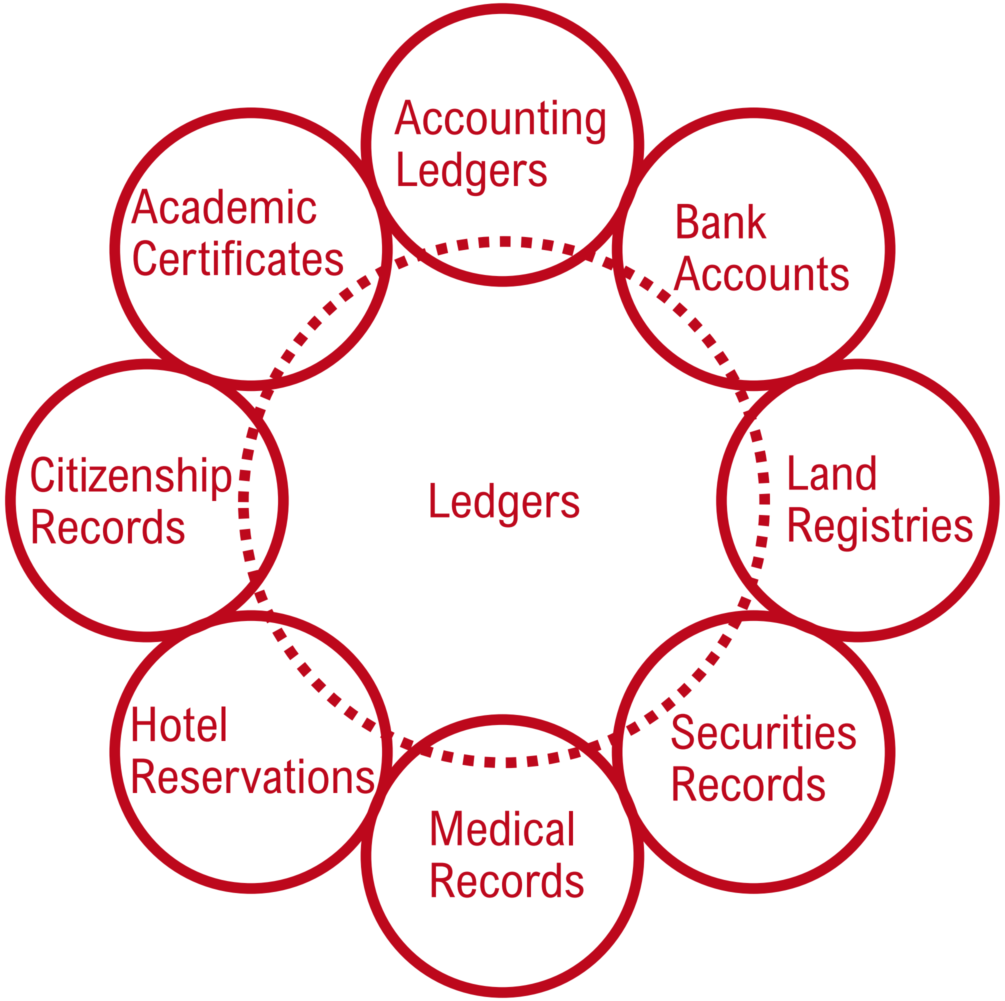
The guest reservations at a hotel

The names of lessees of cars from a car rental company

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

Asset and Transaction Ledgers

Examples of traditional business ledgers



Are centralized record-keepers indeed trustworthy?

- Cyprus 2013 “haircut” on bank deposits
- Fake academic certificates presented to employers
- Loss of land registry records in Less-Developed Countries (LDCs)
- Insecure storage of patients’ medical records among different medical institutions

And many more…

Asset and Transaction Ledgers

Decentralized Ledgers

A successful decentralized ledger that allowed parties who do 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:

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

Bitcoin:
A practical
use case

While the Nigerian Feminist Coalition was protesting against police brutality in 2020, authorities blocked their bank account. The organisation encouraged their supporters around the world to donate in bitcoin, to pay for supplies, medical support, and legal aid.

Source: https://bitcoinmagazine.com/articles/nigerian-protest-group-finds-sovereign-lifeline-in-bitcoin

Asset and Transaction Ledgers

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, 2014

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

2. The Byzantine Generals’ Problem

The Byzantine Generals' Problem

What is the BGP?

The problem of trust in a **distributed system**, with no central control to enforce rules, is not a new one in computer science. The components may fail to reach consensus due to technical failures or misinformation.

"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

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

The Byzantine Generals’ Problem

The Byzantine Generals’ Problem

The Byzantine Generals' Problem (BGP) was first proposed by Marshall Pease, Robert Shostak and Leslie Lamport in 1982, "expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city."

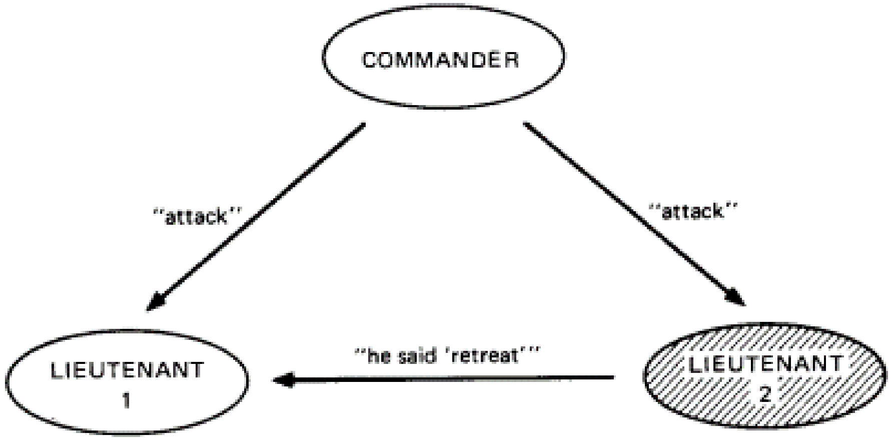


Fig. 1. Lieutenant 2 a traitor.

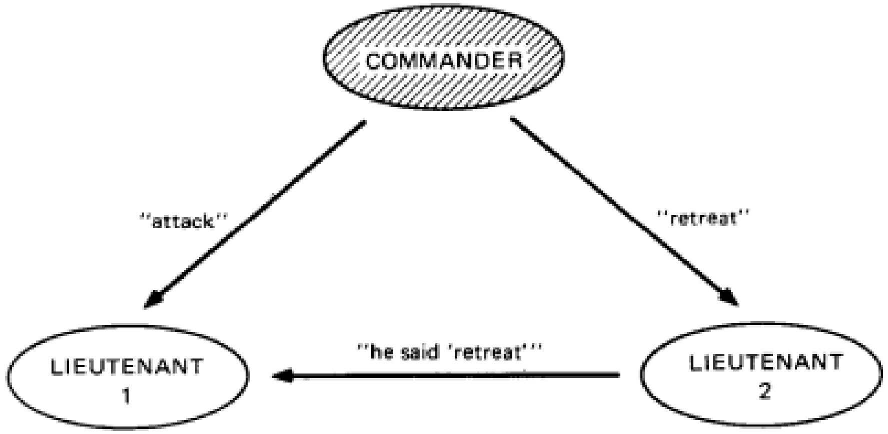


Fig. 2. The commander a traitor.

This is important to understanding why Bitcoin and other open blockchains are designed the way they are!

- In this scenario, a traitor (either the Commander or Lieutenant) prevents the group from reaching consensus. In a financial ledger, think of the traitor as a malicious party that aims to facilitate fraudulent transactions.

Source: https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf The Byzantine Generals’ Problem, Lamport, Shostak, Pease, 1982

The Byzantine Generals' Problem

Problem Formation

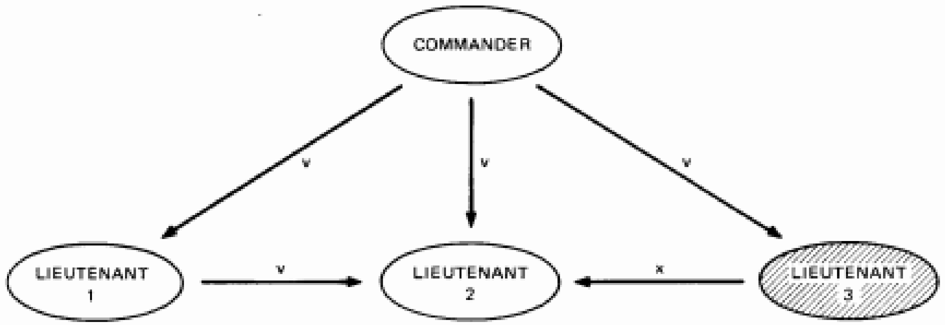


Fig. 3. Algorithm OM(1); Lieutenant 3 a traitor.

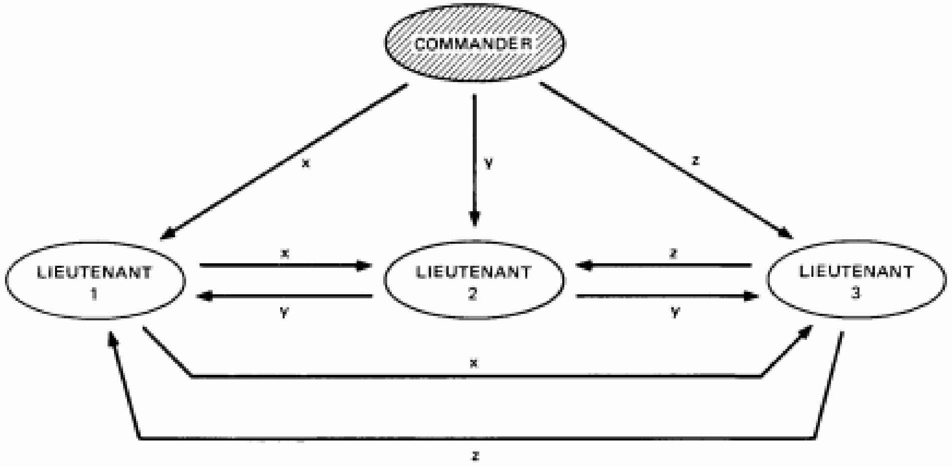


Fig. 4. Algorithm OM(1); the commander a traitor.

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

Imagine the complexity of building consensus with thousands or millions of parties involved.

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

The Byzantine Generals' Problem

The Byzantine Generals' Problem Continued

Past attempts at solving this problem in digital currencies include the following:

- 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 was first proposed on October 31st 2008, by an individual or group under the pseudonym 'Satoshi Nakamoto.' It is the best solution to date and has had – by far – the broadest adoption. October 2018 marked the 10-year anniversary of Bitcoin's whitepaper release. This is a significant milestone for digital currencies.

3. Bitcoin’s Approach to the Byzantine Generals’ Problem

Bitcoin's approach to the Byzantine Generals' Problem

Some Useful Definitions

bitcoin

without capitalization, is used to describe the currency and unit of account for the Bitcoin network.

Bitcoin

with capitalization, is used to describe the concept, network, development project, and enthusiast community.

Bitcoin address

a string of letters and numbers where bitcoin can be sent, similar to how one sends email to an email address.

transaction

A record informing the network of a transfer of bitcoin from one bitcoin address to another.

blockchain*

The complete transaction ledger of the Bitcoin network, showing how bitcoin have been transferred from one address to another over time. The blockchain is a public record of all bitcoin transactions in chronological order.

*Think of a Bitcoin transaction as a single value transfer recorded in a ledger, a block as a page of transactions from the last ten minutes, and a blockchain as the whole ledger book.

Bitcoin’s approach to the Byzantine Generals’ Problem

The Bitcoin Ledger: The Blockchain

- Want to witness and store the Bitcoin blockchain? The starting point:
  - A Bitcoin user downloads a piece of software (the Bitcoin reference client software)
  - This client software will initially download the blockchain, the ledger of all transactions in the history of Bitcoin
  - Each Bitcoin full client stores the complete record of all bitcoin transactions from all time. There is no central record-keeper, just a set of copies distributed among all the clients
- Once the blockchain history is downloaded and validated, the issue of synchronization emerges:
- How are these copies of the blockchain (ledger) kept in sync with each other?
  - In other words, how do they reach distributed consensus without a definitive central party?
  - 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.

Keep in mind that downloading the Bitcoin client software is not mandatory in order to use bitcoin. It is recommended for users wishing to validate their transactions and participate in the consensus process.

Bitcoin’s approach to the Byzantine Generals’ Problem

Synching the Blockchain: Mechanics

1. When a user executes a transaction (sends bitcoin from one address to another), the transaction is eventually broadcast to all network nodes in the system. Within a few seconds, most of the clients in the world see the transaction.

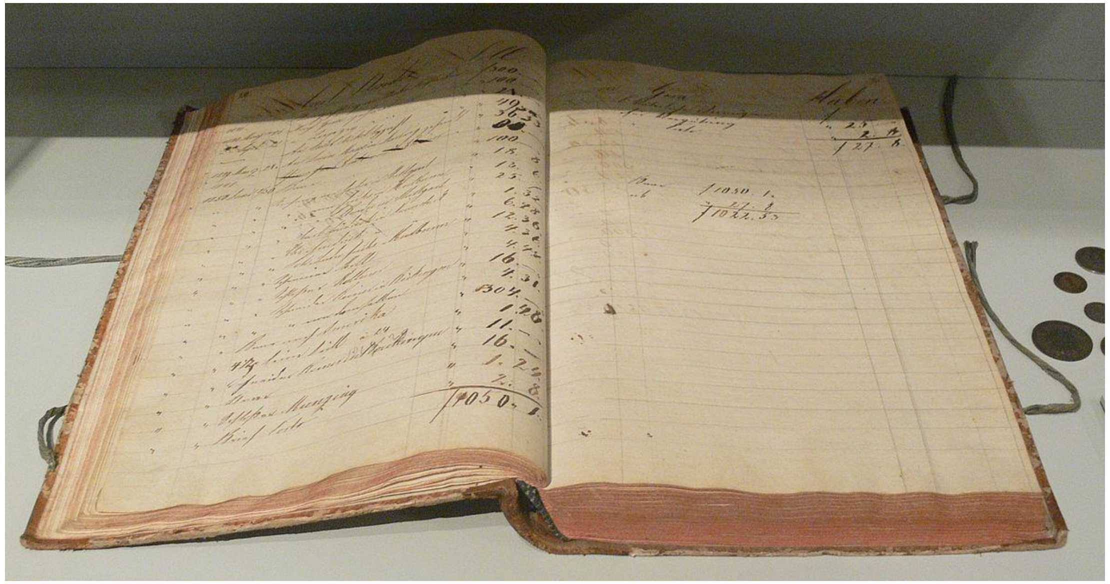
2. At this point, however, the transaction is considered “unconfirmed." Remember the Byzantine Generals’ Problem: what if a dishonest Bitcoin client sent out two transactions moving the same bitcoin to two different addresses? Which one should the clients accept?

3. Bitcoin confirms transactions and resolves the BGP through a process called “mining."

Read more about mining in Chapter 10 of *Mastering Bitcoin* by Andreas M. Antonopoulos

Bitcoin’s approach to the Byzantine Generals’ Problem

Synching the Blockchain: Mining



Looks more like this...

Not this.

Mining is a rather misleading analogy for what ‘miners’ do.

Think of the miners as 'bookkeepers' and it will make much more sense.

Image Source: Wikimedia Commons. Ledger and Coal Strip Mine

Bitcoin's approach to the Byzantine Generals' Problem

Mining and Proof-of-Work

Mining:

- The process by which new blocks are appended to the blockchain, and new units of bitcoin are "minted" according to a deterministic issuance schedule. The total supply is finite, limited to approximately 21 million bitcoin.
- The integrity of transactions and blocks is ensured through a contribution of computational power, e.g. proof-of-work. The candidate block data is repeatedly hashed until it is less than the value of a desired pattern according to the current difficulty rate. (Note: A hash's value is 'less' if it has more leading zeroes.)
- If the process seems complicated, do not worry! It is automated. The setup and maintenance of mining machines is often the only manual work involved.

1st Step: Collect unconfirmed transactions from the mempool to include in the candidate block

2nd Step: Construct candidate block with a reference to the previous block and a nonce (random number)

3rd Step: Solve proof-of-work and broadcast the candidate block to be verified by other network nodes

4th Step: If block is valid and part of greatest cumulative difficulty chain, miner receives the block reward

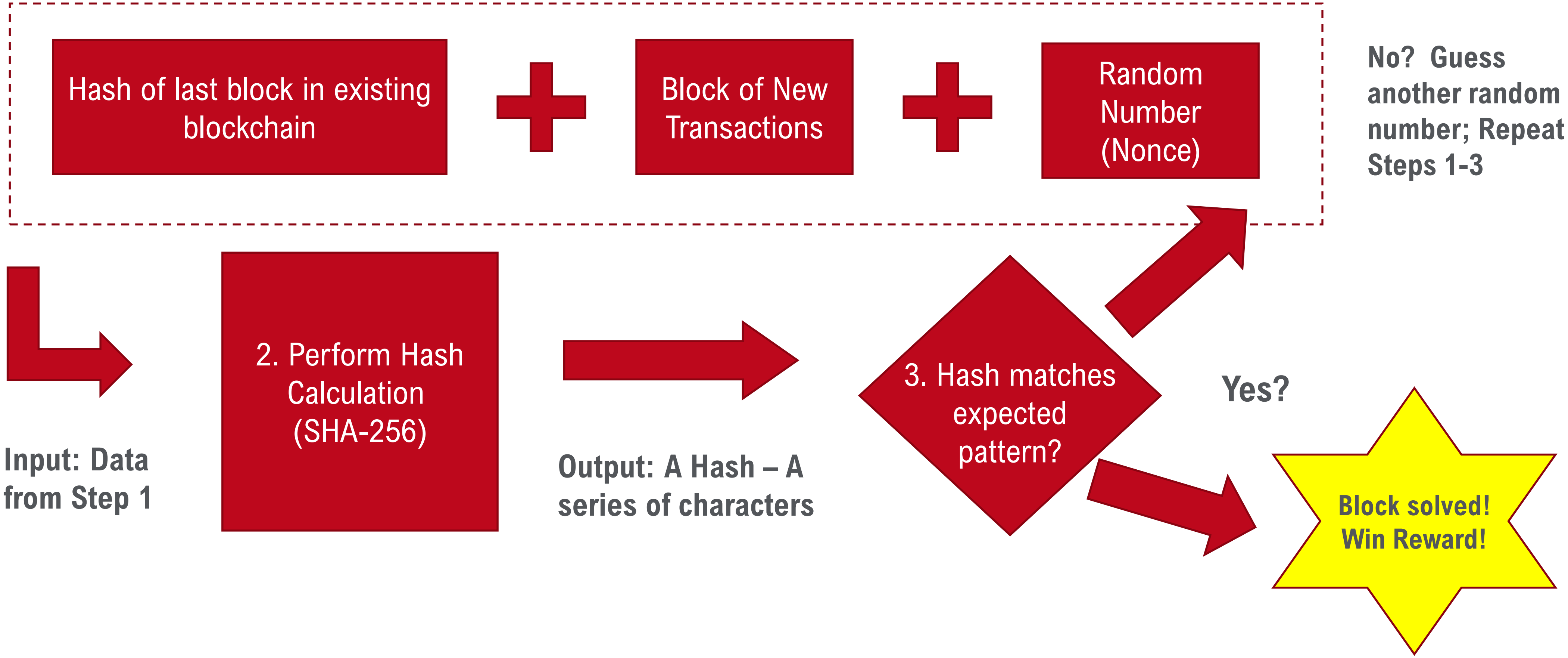
https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch10.asciidoc

https://www.coindesk.com/information/how-to-set-up-a-miner/

Bitcoin’s approach to the Byzantine Generals’ Problem

Mining in 3 Steps (again)

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


Hash of last block in existing blockchain
Block of New Transactions
Random Number (Nonce)
No? Guess another random number; Repeat Steps 1-3
Input: Data from Step 1
2. Perform Hash Calculation (SHA-256)
Output: A Hash – A series of characters
3. Hash matches expected pattern?
Yes?
Block solved! Win Reward!

Bitcoin's approach to the Byzantine Generals' Problem

Mining: Winning a Prize?

Once a miner has a winning block, it broadcasts it to the other clients:

- The client nodes verify that the hash matches the expected pattern and accept the new block, adding it to their own copy of the blockchain. Note: Blockchain = a chain of blocks (!)
- After that, all miners start working on finding the next block, incorporating the new previous block hash as their starting point in Step 1

The miner is allowed to collect as part of having a winning block:

The current block subsidy (6.25 bitcoin per block), which increases the circulating supply of bitcoin

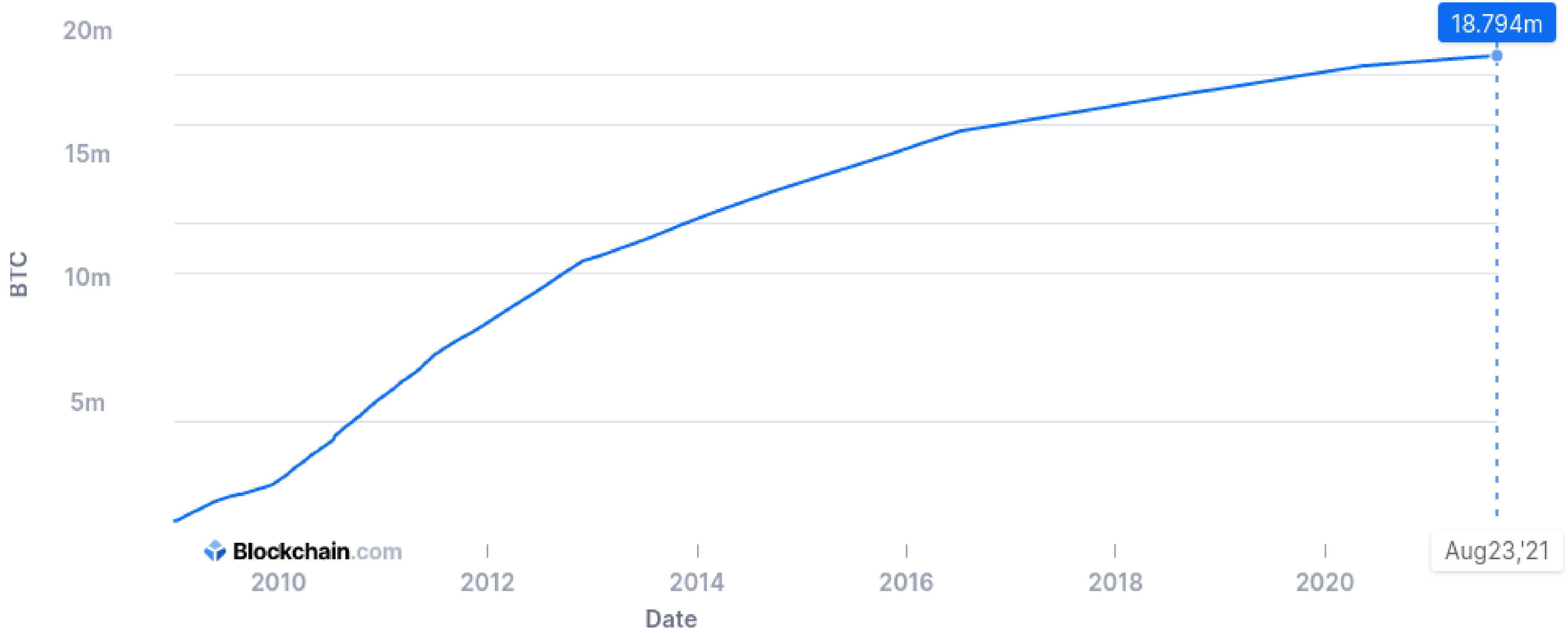
The fees from all the transactions that were included in the block

The block reward started at 50 bitcoin per block and halves every 210,000 blocks, about every 4 years.

In September 2020, the block reward is 6.25 bitcoin. This amount far outweighs transaction fees. The next halving will take place in 2024. New block rewards, except transaction fees, will stop once the network reaches Block 6,930,000 (sometime around the year 2140). The total number of bitcoin issued by then will be about 21 million - https://en.bitcoin.it/wiki/Controlled_supply

Bitcoin's approach to the Byzantine Generals' Problem

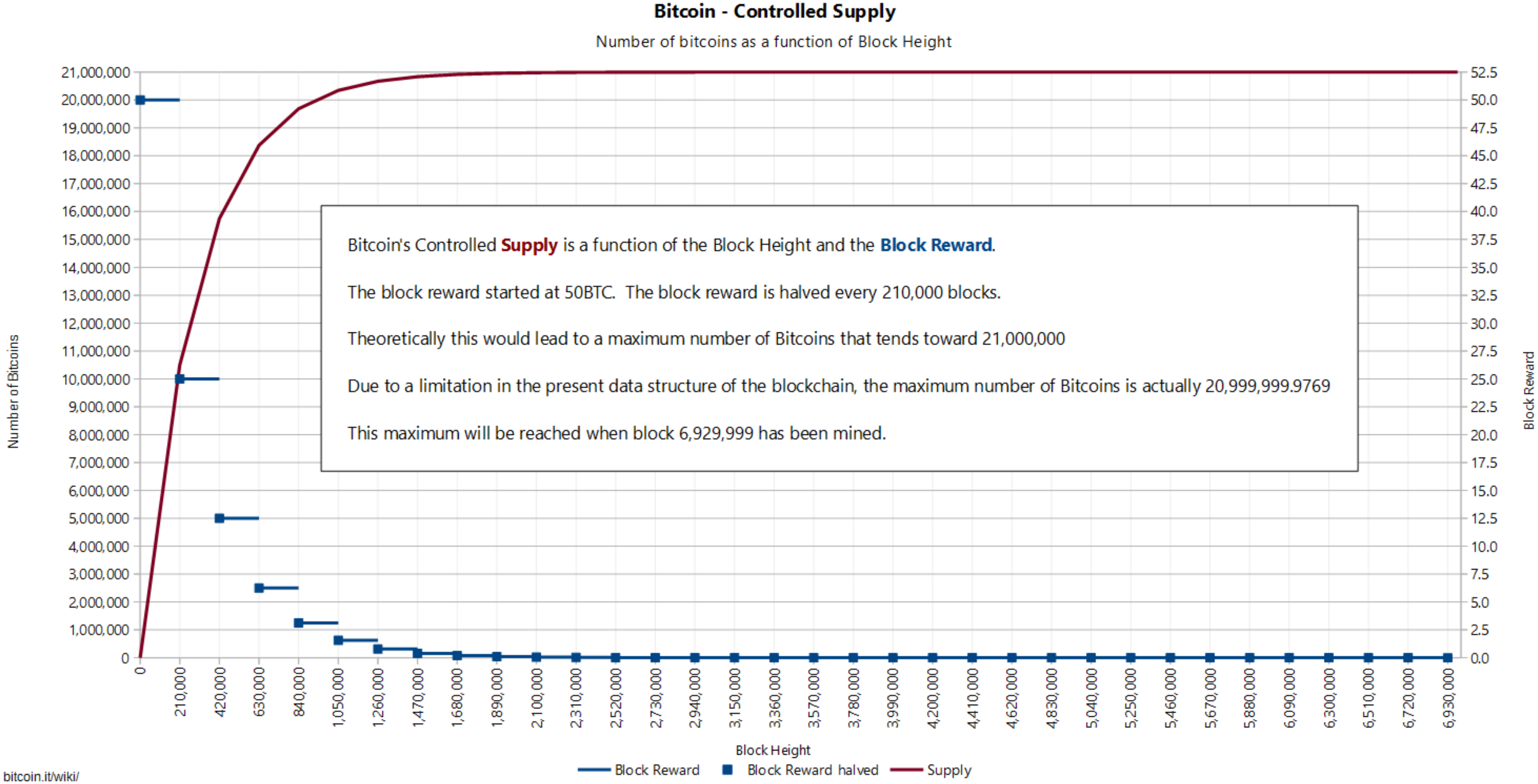
Mining: Winning a Prize?



- Over 18 million bitcoin (more than 80% of the total bitcoin supply) have been issued so far through block rewards. The rate will keep decreasing until the final issuance takes place in 2140.

Bitcoin’s approach to the Byzantine Generals’ Problem

Controlled Supply



Bitcoin - Controlled Supply

Number of bitcoins as a function of Block Height

Bitcoin's Controlled **Supply** is a function of the Block Height and the **Block Reward**.

The block reward started at 50BTC. The block reward is halved every 210,000 blocks.

Theoretically this would lead to a maximum number of Bitcoins that tends toward 21,000,000

Due to a limitation in the present data structure of the blockchain, the maximum number of Bitcoins is actually 20,999,999.9769

This maximum will be reached when block 6,929,999 has been mined.

bitcoin.it/wiki/

Bitcoin's approach to the Byzantine Generals' Problem

Mining: Auto-Adjusting Puzzles

This winning of prizes sounds very tempting. Why hasn't a powerful computer mined all the bitcoin yet?

Fortunately, the difficulty auto-adjusts to account for how much computing power is being contributed to mining in the Bitcoin network, so that new blocks are not mined too quickly or too slowly.

- Difficulty adjustments happen every 2,016 blocks or approximately two weeks.
- If the average block time in that period was greater than ten minutes ('too hard'), difficulty is decreased.
- If the average block time in that period was less than ten minutes ('too easy'), difficulty is increased.

Whether miners on the Bitcoin network consist of old laptop CPUs or super-computers, in the long term blocks will still be created approximately every 10 minutes.

Anyone can set up a mining node. Profitability will vary depending on factors such as the type and quality of hardware chips, electricity prices, energy sources, labor / maintenance costs, and taxes. If it becomes too unprofitable for some miners, they may leave the network and rejoin when the difficulty drops.

For a recent exploration of the viability of individual at-home mining (U.S.-focused), see:
https://bitcoinmagazine.com/business/how-to-mine-bitcoin-at-home

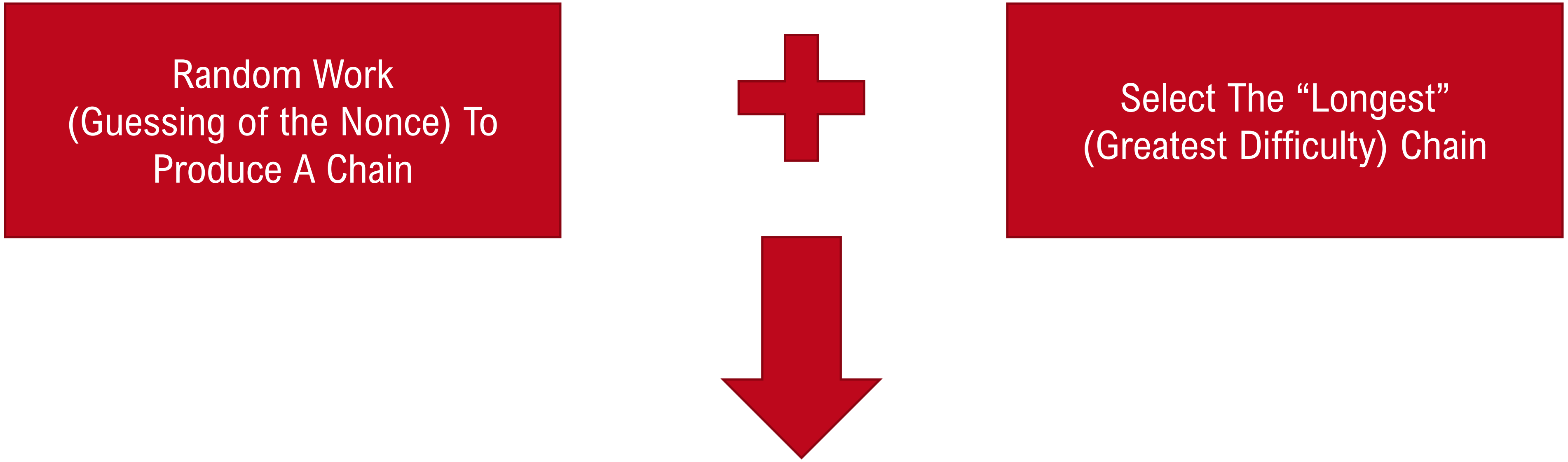
Bitcoin’s approach to the Byzantine Generals’ Problem

Back to the Byzantine Generals’ Problem

- “But, you have not yet solved the BGP, just moved it to the miners. What if two miners send out blocks with different information (i.e. different transactions within the block)? How do the clients choose which one to include?”
- The answer is that when a client is trying to decide which block history to accept, it must choose the one that is not only the “longest” (in the number of blocks), but the one that has the “greatest cumulative difficulty” (total proof-of-work used to create it). In other words, the chain that took the most computation power to build.
- Blocks that are invalid, or a version of the chain that has less cumulative proof-of-work, will become "orphaned," and those transactions will need to be reprocessed.
- Given this system, a traitor / dishonest node cannot keep broadcasting bad signals into the Bitcoin network, such as attempting to double-spend by including a transaction in one block and then erasing it in the next. Unless he or she controls a significant majority of the hashing power and can sustain that control, which would be very hard to do. More on this on the next slides.
- One useful mental model of the block reward scheme is a **lottery**. The miner who 'wins,' is a matter of probabilities. This prevents any one party from taking control.

Bitcoin’s approach to the Byzantine Generals’ Problem

Back to the Byzantine Generals’ Problem



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

Select The “Longest”
(Greatest Difficulty) Chain

Solution to the Byzantine Generals' Problem

Bitcoin’s approach to the Byzantine Generals’ Problem

Mining: Proof-of-Work and the Energy Debate

This random number creation (“proof-of-work”) is the subject of confusion:

- Some people consider it (a) wasted effort or (b) an indication of poor system design (“why do they need to do so much work to record a transaction when my database can do it instantly?”).
- In fact, it is the **key element** to the ledger's security, requiring investment in and expenditure of specialised equipment and energy, thus preventing any one party from hijacking the system.

For more information on electricity sources and consumption in Bitcoin mining, see:

- "The Bitcoin Mining Network - Trends, Composition, Average Creation Cost, Electricity Consumption & Sources" report and key takeaways by CoinShares Research (December 2019)
- "Cryptocurrency Proof-of-Work Mining Energy Consumption" by Tyler Bain at the CryptoCurrency Certification Consortium (C4)'s Blockchain Training Conference (August 2019)

Bitcoin’s approach to the Byzantine Generals’ Problem

Mining: 51% Attack

- Bitcoin solves the Byzantine Generals’ Problem so long as honest miners consist of at least 50% of the hashing power. (This research puts the practical threshold closer to 66.67%.)
- **51% Attack:** If one miner controls more than 50% of the hash power, they can produce a “longer” chain than all other miners combined. They could reverse their own past transactions. They can’t spend other people's coins, but they can prevent transactions from being confirmed.

Fun facts:

- 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 pool members backed off voluntarily in order to preserve confidence in the system.
- The largest mining pool currently controls more hashing power than Bitcoin’s entire global hashrate in November 2017!

Bitcoin's approach to the Byzantine Generals' Problem

Implications

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

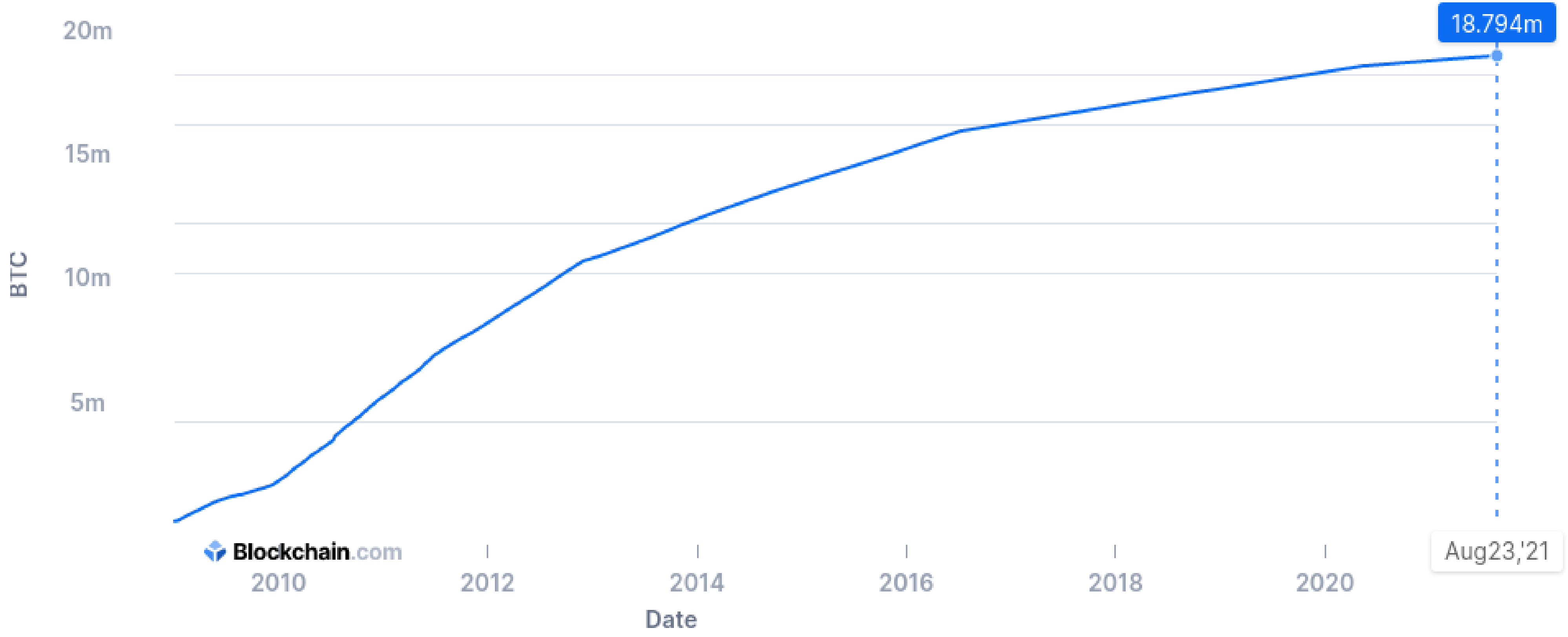
- In future sessions, we will discuss:
  - How to transact with bitcoin in practice
  - Strengths and weaknesses of Bitcoin specifically, relative to other technologies
  - Implications in the area of currency and beyond

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

4. Bitcoin: Some Key Metrics

Bitcoin: Some Key Metrics

Bitcoin Metrics: Number of Bitcoin in Circulation

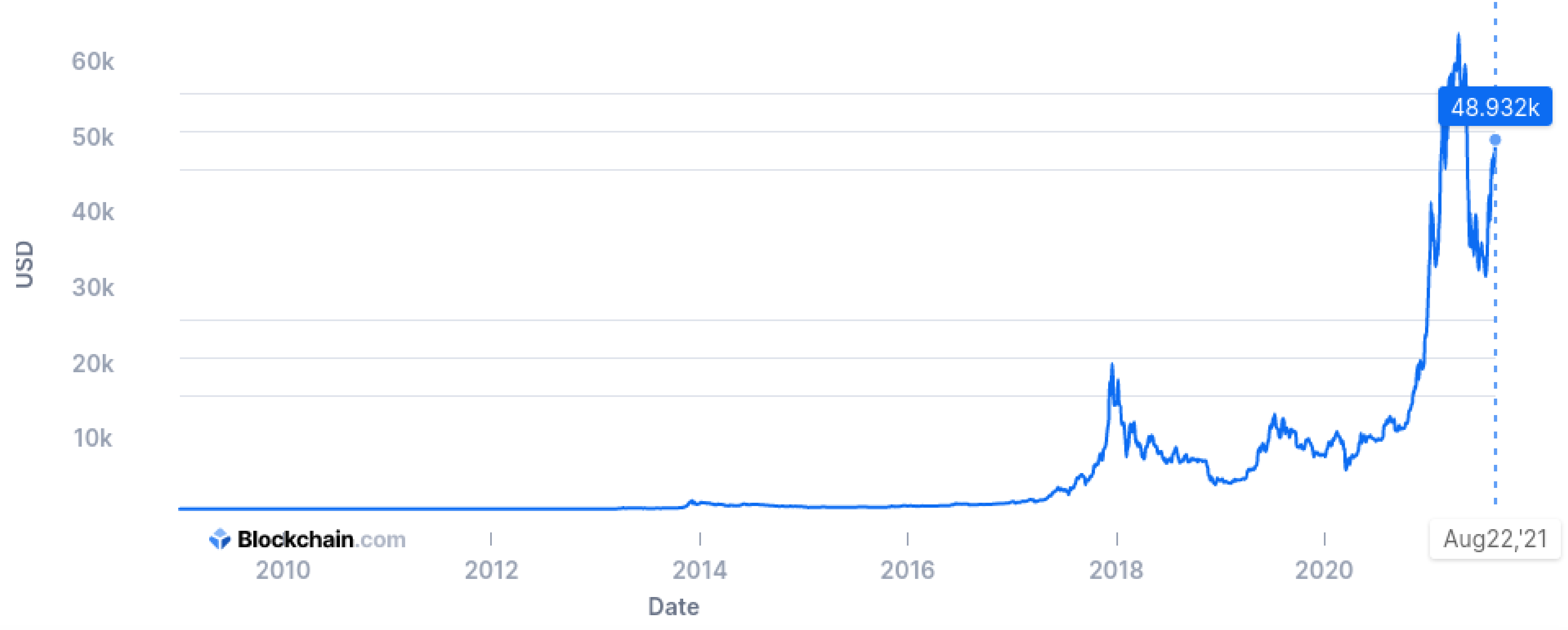


Over 18,794,000 bitcoin in circulation as of August 23rd, 2021.

Source: https://www.blockchain.com/charts/total-bitcoins

Bitcoin: Some Key Metrics

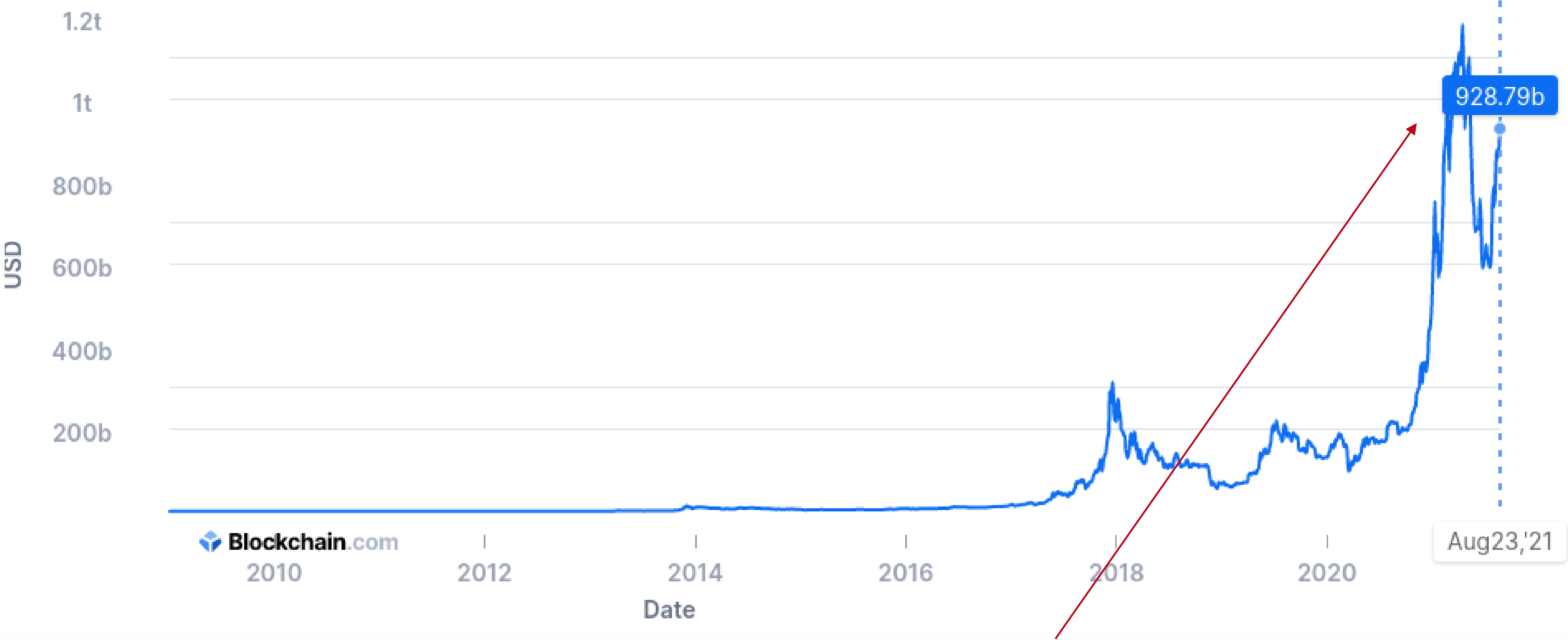
Bitcoin Metrics: Market Price



Source: https://www.blockchain.com/charts/market-price

Bitcoin: Some Key Metrics

Bitcoin Metrics: Market Capitalization

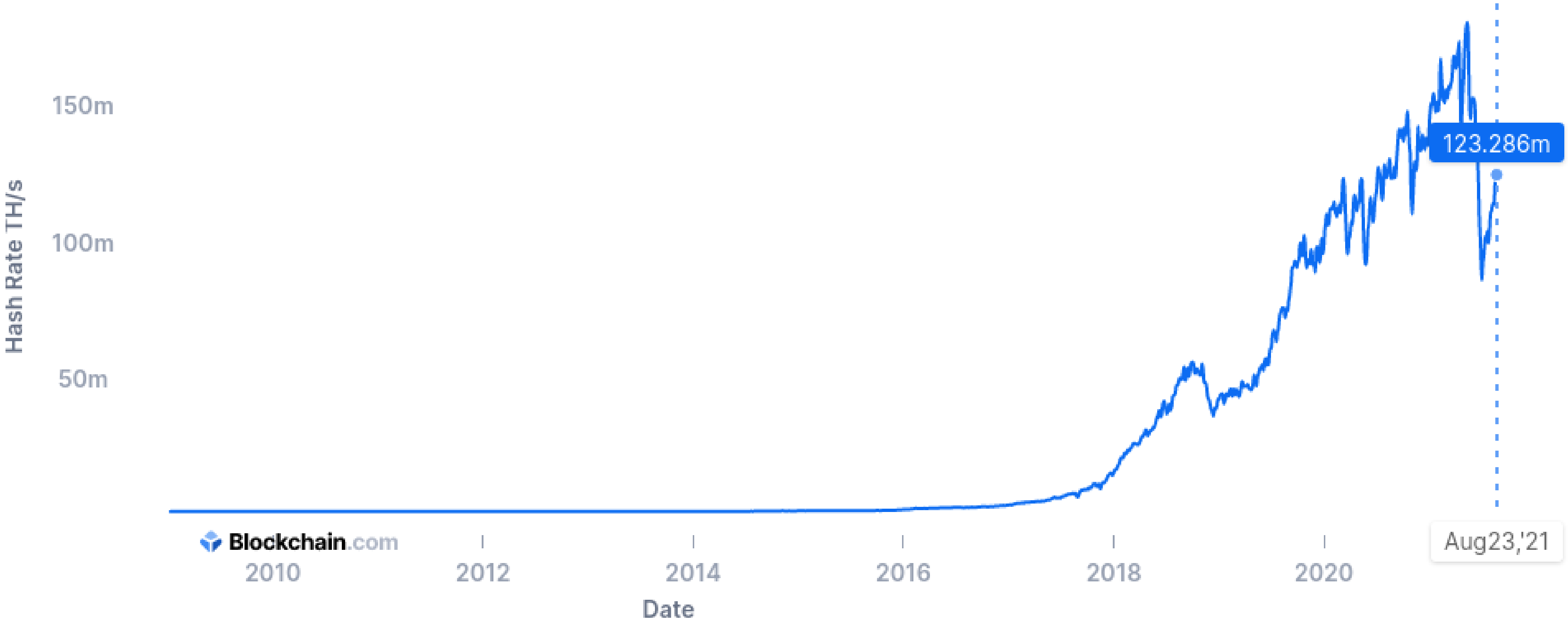


Total BTC market value = number of bitcoin issued (x) market price

Source: https://www.blockchain.com/charts/market-cap

Bitcoin: Some Key Metrics

Bitcoin Metrics: Total Network Hash Rate



Think of the total network hash rate as the total computing power dedicated to the network, by miners all around the world.

Session 2: The Byzantine Generals’ Problem

Conclusions

- Historically, all ledgers of importance have been centralized. While giving a measure of control, central record-keepers have weaknesses in the areas of:
    - Corruption
    - Inclusion
    - Technical failures
- The Byzantine Generals’ Problem, a matter of study for computer scientists 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 has popularised decentralized asset systems.
- Leading technologists believe that the implications of this technical breakthrough will be far-reaching, extending beyond digital currency.

Session 2: The Byzantine Generals' Problem

Further Reading

Bitcoin: A Peer-to-Peer Electronic Cash System (Satoshi Nakamoto)

https://bitcoin.org/bitcoin.pdf

How the Byzantine General Sacked the Castle: A Look Into Blockchain

https://medium.com/@DebrajG/how-the-byzantine-general-sacked-the-castle-a-look-into-blockchain-370fe637502c

Bitcoin Mining

https://www.buybitcoinworldwide.com/mining/

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

Session 2: The Byzantine Generals' Problem

Further Reading

The Economics of Cryptocurrencies – Bitcoin and Beyond

https://www.chapman.edu/research/institutes-and-centers/economic-science-institute/_files/ifree-papers-and-photos/koeppel-april2017.pdf

Banking Is Only The Beginning: 36 Big Industries Blockchain Could Transform

https://www.cbinsights.com/research/industries-disrupted-blockchain/?utm_source=CB+Insights+Newsletter&utm_campaign=fa48df10a8-ThursNL_02_01_2018&utm_medium=email&utm_term=0_9dc0513989-fa48df10a8-90141994

How Bitcoin Mining Works, CoinDesk

https://www.coindesk.com/information/how-bitcoin-mining-works/

Hash Rate all-time high

https://news.bitcoin.com/rapid-profits-bitcoin-hashrate-accelerates-difficulty-all-time-high/

Bitmain Mining

https://www.investopedia.com/news/crypto-mining-giant-bitmain-going-public-4050-billion-valuation/

https://www.prnewswire.co.uk/news-releases/bitmain-announces-specs-for-next-gen-antminer-s19-and-s19-pro-coming-soon-861798654.html

UNIVERSITY *of* NICOSIA

Questions?

Contact Us:

Twitter: **@mscdigital**
Course Support: **digitalcurrency@unic.ac.cy**
IT & Live Session Support: **dl.it@unic.ac.cy**