Bitcoin!

‘N at*

* Blockchain, consensus algorithms, mad profits, and more!

Eric Ghildyal

ergh.co

@Eric_Ghildyal

- CS Undergrad
- Blockchain Research Project for UNSW
- Not an economist
- Other things

1 BTC ==$11124

1 BTC == ~~$11124~~

1 BTC ==$6447 ish

Table of Contents

What is Bitcoin?

Officially:

> “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.”
>
> https://bitcoin.org

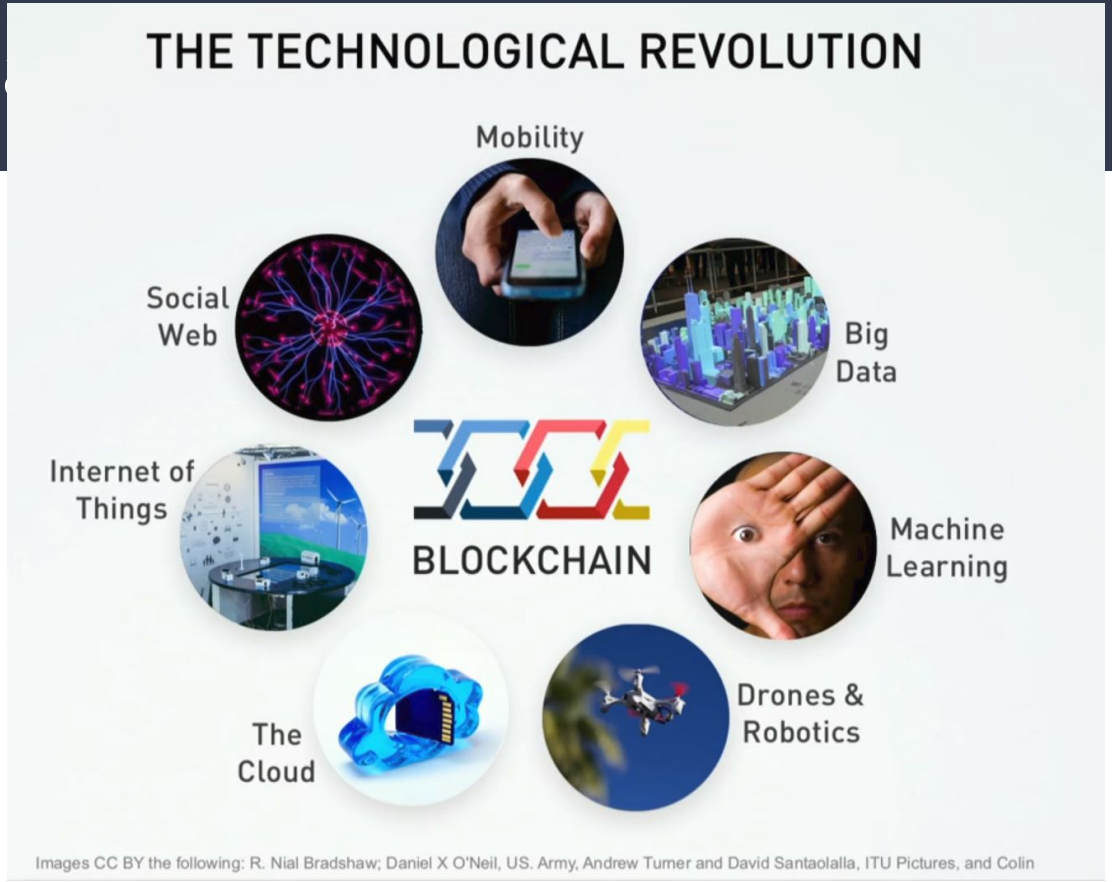
Unofficially:

> An anonymous, decentralized currency that anyone can use simply by downloading a program.

What is a Blockchain?

- The Blockchain is a concept
- Bitcoin is a Blockchain implementation
- Bitcoin uses it as a distributed, immutable ledger

What is

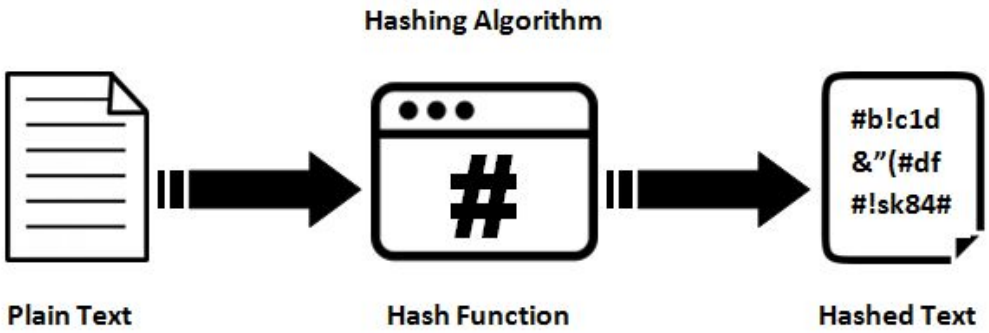

THE TECHNOLOGICAL REVOLUTION
Mobility
Social Web
Big Data
Internet of Things
BLOCKCHAIN
Machine Learning
The Cloud
Drones & Robotics
Images CC BY the following: R. Nial Bradshaw; Daniel X O'Neil, US. Army, Andrew Turner and David Santaolalla, ITU Pictures, and Colin

Blockchain Terms

- Block
  - Holds data and metadata
  - Base “unit” of a **block**chain
- Node
  - Program that stores the chain in local memory and can publish to the chain
- Consensus algorithm
  - An Algorithm that the blockchain uses when determining which block to use as the next one
- Hash
  - soon...

Hashing

Hashing takes a larger set of data and maps it onto a fixed size set of data.
Usually goes one direction.
Ie: you can't "un-hash" something



https://stackoverflow.com

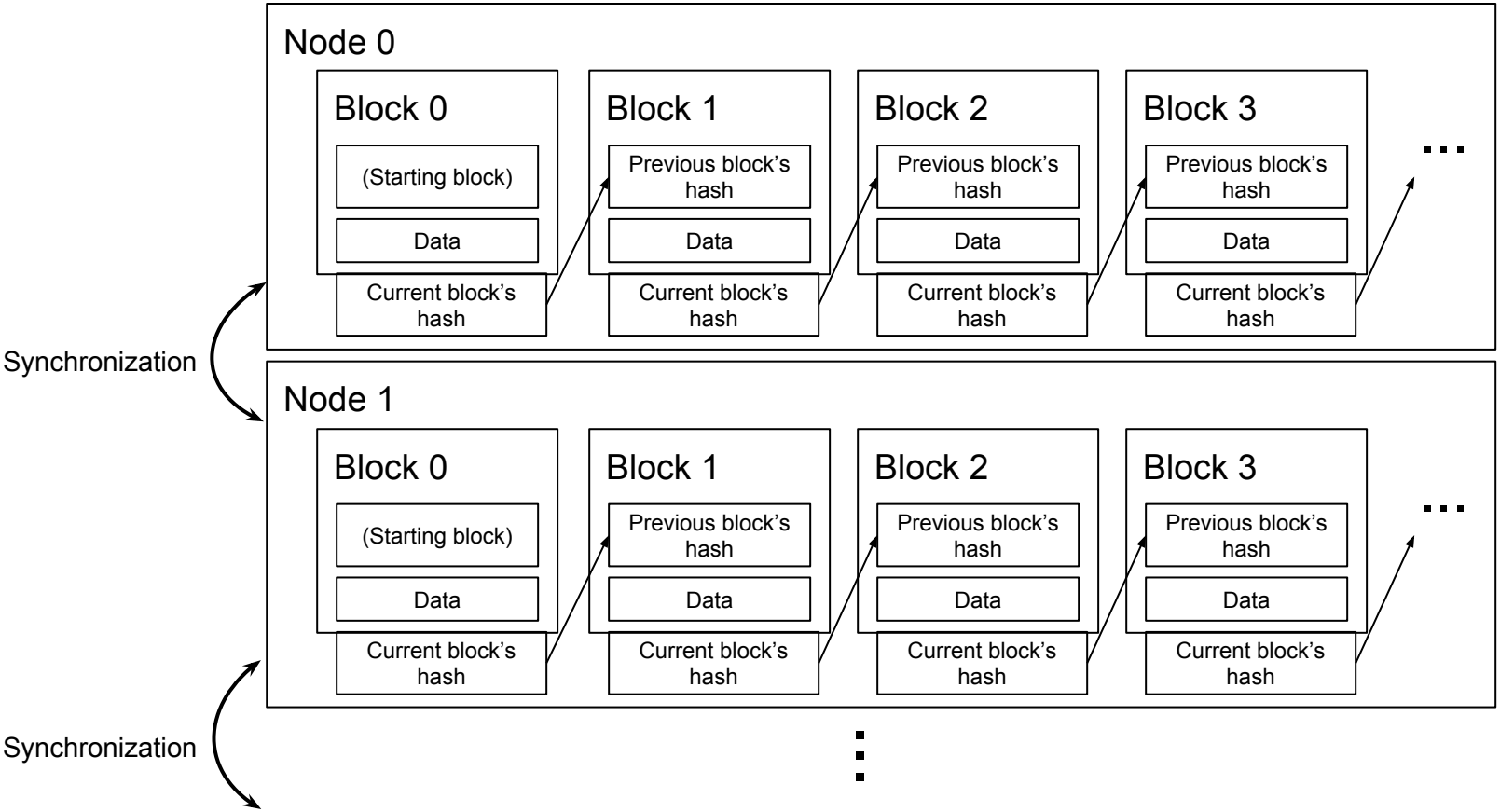
Ex (sha1):

"Hello World" → `0a4d55a8d778e5022fab701977c5d840bbc486d0`
"Hello World1" → `cd1144e1b687f6d586c215f09ddd1a67a8f1c0f3`

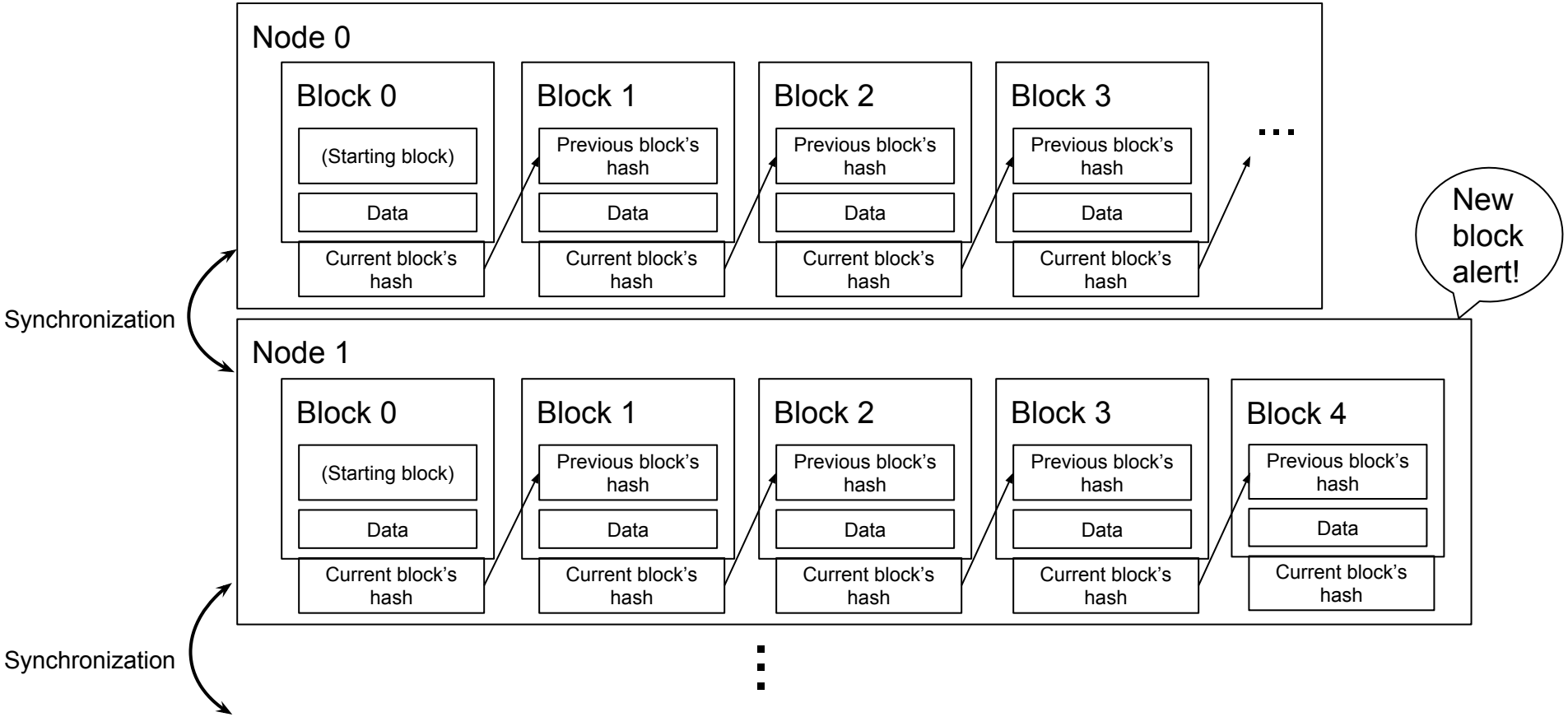
How does Bitcoin use the Blockchain?

- The Blockchain is what allows Bitcoin to exist and work
- It provides the decentralized and anonymous aspects to the currency
- Blocks hold transactions
    - Ex: Block 485282 holds 2246 transactions

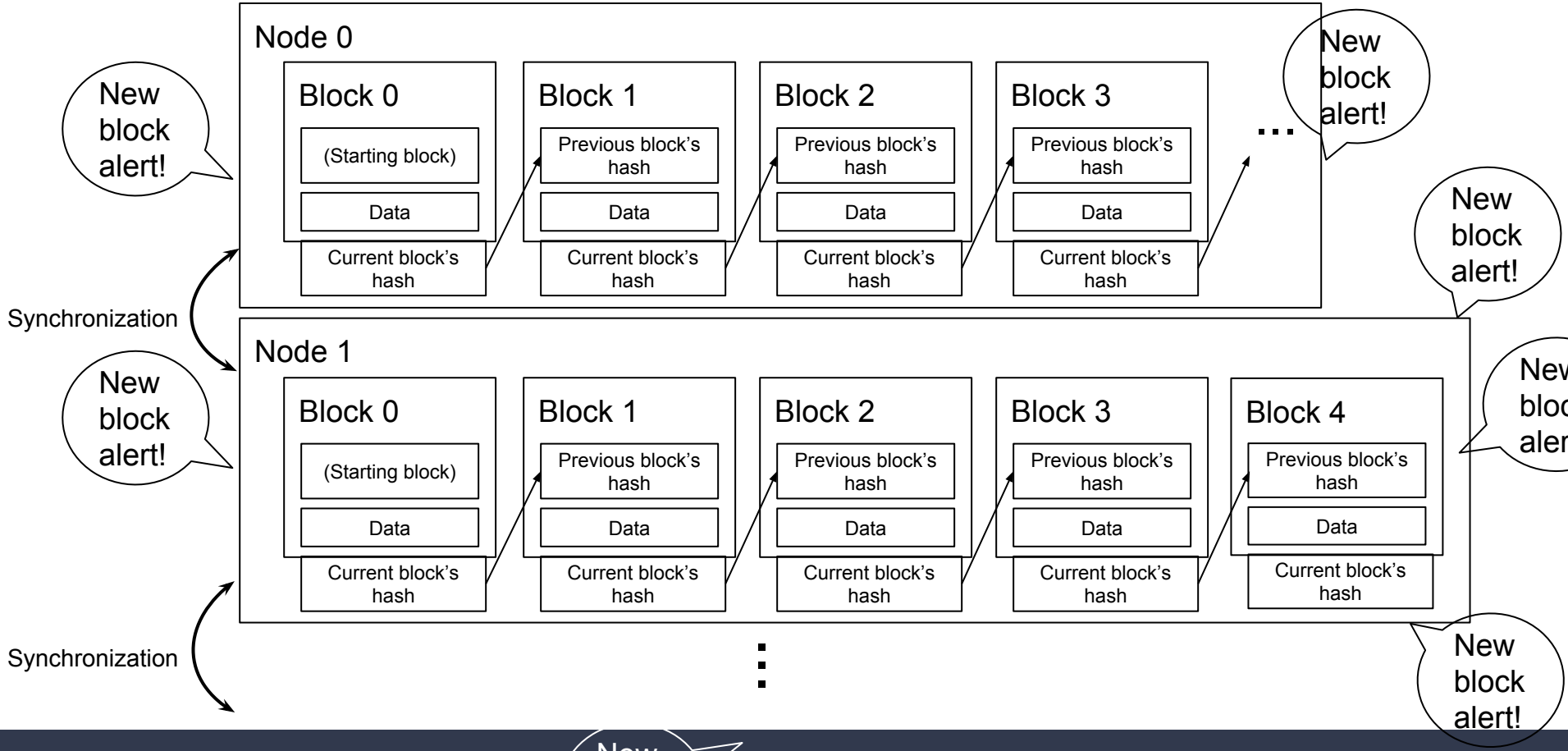
https://blockchain.info/



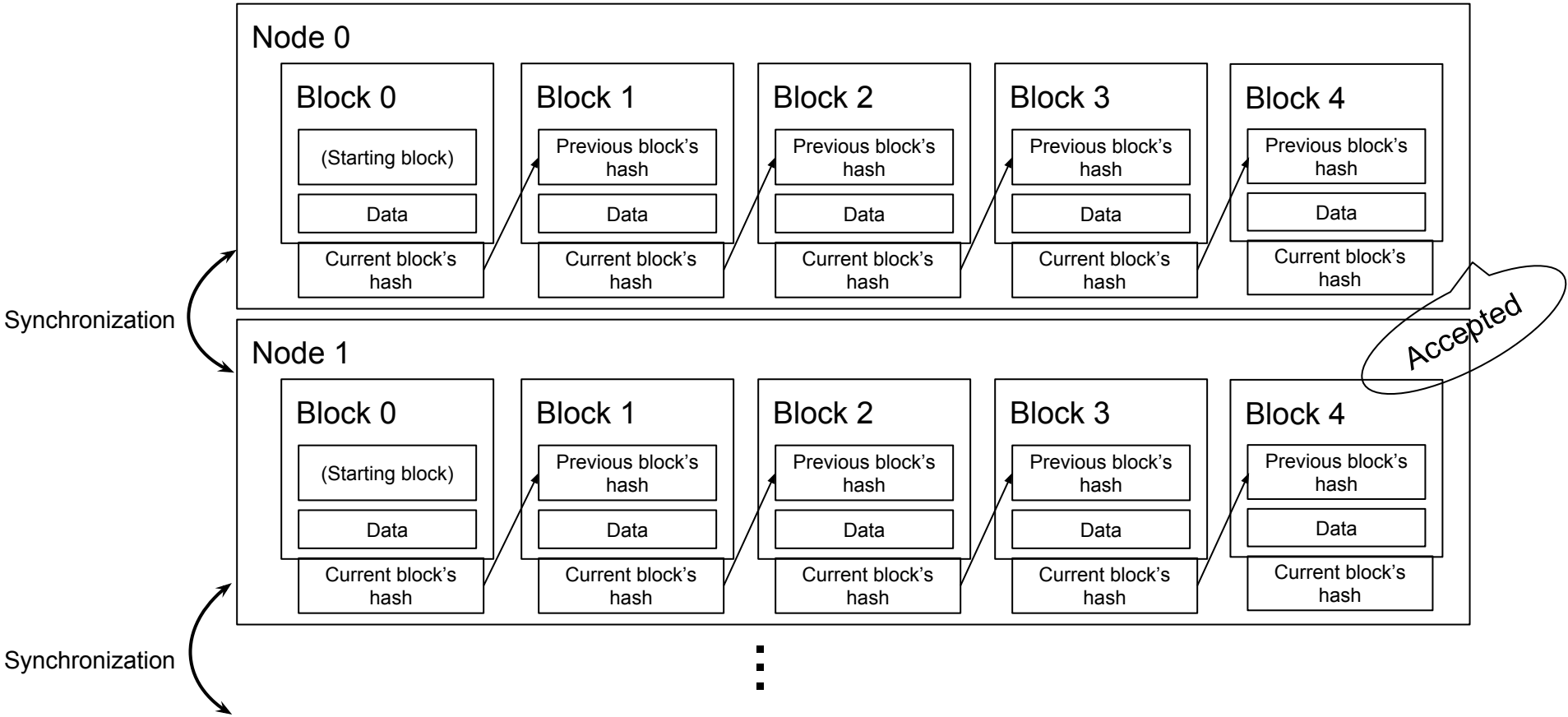
Blockchain Example



Blockchain Example



Blockchain Example



Blockchain Example

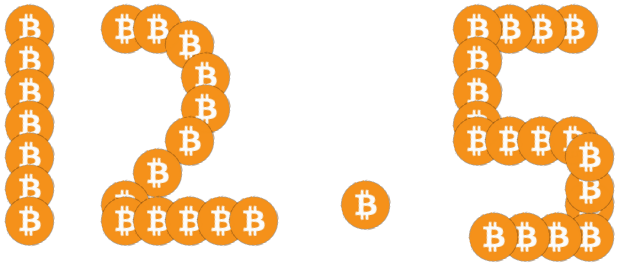
Bitcoin Terms

- Wallet
  - The place you store your bitcoins
- Wallet Address
  - The unique address your wallet gets assigned so that people can send you money
  - Ex: 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2
- Mining
  - What runs the chain!

Mining

- Mining nodes validate transactions and adds them to the block they are building
- Mining is a bunch of hashing
- People mine in order to get a reward (in bitcoin)
  -

Mining

- Mining nodes validate transactions and adds them to the block they are building
- Mining is a bunch of hashing
- People mine in order to get a reward (in bitcoin)
  - 

≈ $80,000

Bitcoin Mining Example

- Difficulty is currently(ish)
  - 2,603,077,300,219
- Mining
  - test → a94a8fe5ccb19ba61c4c0873d391e987982fbbd3
  - test0 → 9b4bf5cdb7381fe38284a05d44d0631cf253c095
  - …
  - test5 → 911ddc3b8f9a13b5499b6bc4638a2b4f3f68bf23
  - …
  - test17 → 08a25c0f270b29aeba650e6b2d1a9947a778c5da

Mining For DH-coin

- Rules:
  - Everybody can play
  - Whoever finds the answer first (according to me) wins
- Steps:
  - Take out your phone and open the calculator app
  - I will put numbers on the screen and you will have to solve the problem with the correct answer
  - Ex: 109 + 572 + 2967 + 4583 - 957 = ? (7274)

$$2 + 432 + 568 + 543 - 613 - 97$$

GO!

835

$$1 + 666 + 24 + 58008 - 34 - 299$$

GO!

58366

$$6739 - 9375 + 2398 + 9357 + 2957$$

GO!

12076

$$111 + 222 + 333 + 444 - 555$$

GO!

555

Mining For DH-coin results

- Outcomes
- “Difficult work”
- Reward
- Mining Pools

Alt-Coins?

- Alternative Coins
- Ripple (XRP), Litecoin, Ether
- Proof Of Work, Proof of Stake, Proof of Burn

Getting Started

- Coinbase (https://www.coinbase.com/)
- Bitcoin “Official” Website (https://bitcoin.org/)
  - Whitepaper (https://bitcoin.org/bitcoin.pdf)
- Blockchain Demo (https://anders.com/blockchain/)

The Future?

- Yes

The Future?

- Yes
- But watch out

Thanks! Questions?

Eric Ghildyal - ergh.co - ericghildyal@gmail.com