Welcome to

Blockchain technology and application

-WhatsApp Group

My number: 6362 221296

-Assignments & Quizzes

-Basic programming skills

What If……..


Registration Number:
KA 01 5555
Make: Mahindra
Model: Scorpio
Engine Number:
s3bfngh999
Chassis number:
Y77772010
Year of mfg: 2012
Color: Black
Mileage: 36000 kms
Transaction date:
15/6/2017
Seller: Mr. …..
Buyer: Ms……
Insurance claims: 2

Blockchain Internals

Ms. Shiny Abraham sold her Silver color Maruti Ritz to Mr. Vijay Amritraj for 5 lacs on 1/1/2015. The odometer reading at the time was 22000 kms. The amount was transferred to her account at 6 pm and had a transaction ID TX5010.

:

:

Mr. Vijay Amritraj sold to

:

:

Mr. xxyy sold to….

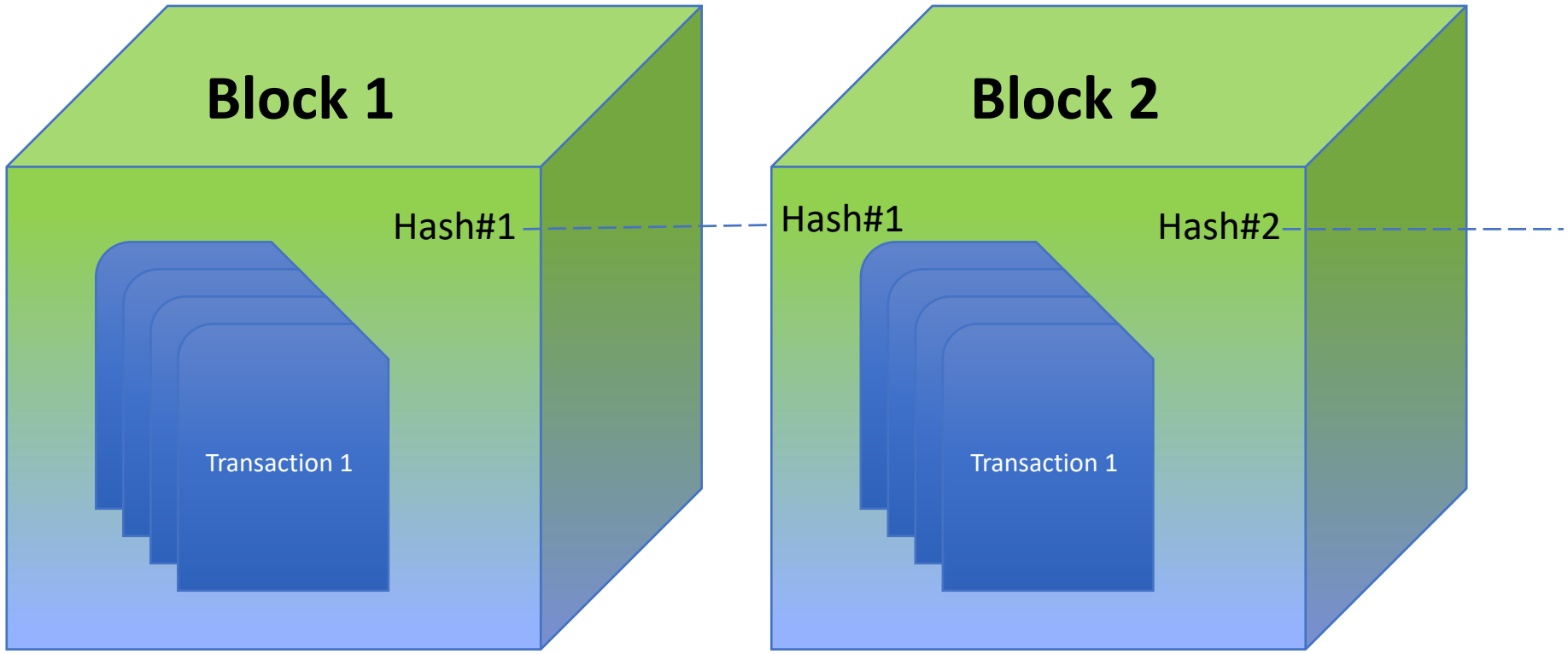
Blockchain internals

Ms. Shiny Abraham sold her Silver color Maruti Ritz to Mr. Vijay Amritraj for 5 lacs on 1/1/2015. The odometer reading at the time was 22000 kms. The amount was transferred to her account at 6 pm and had a transaction ID TX5010.

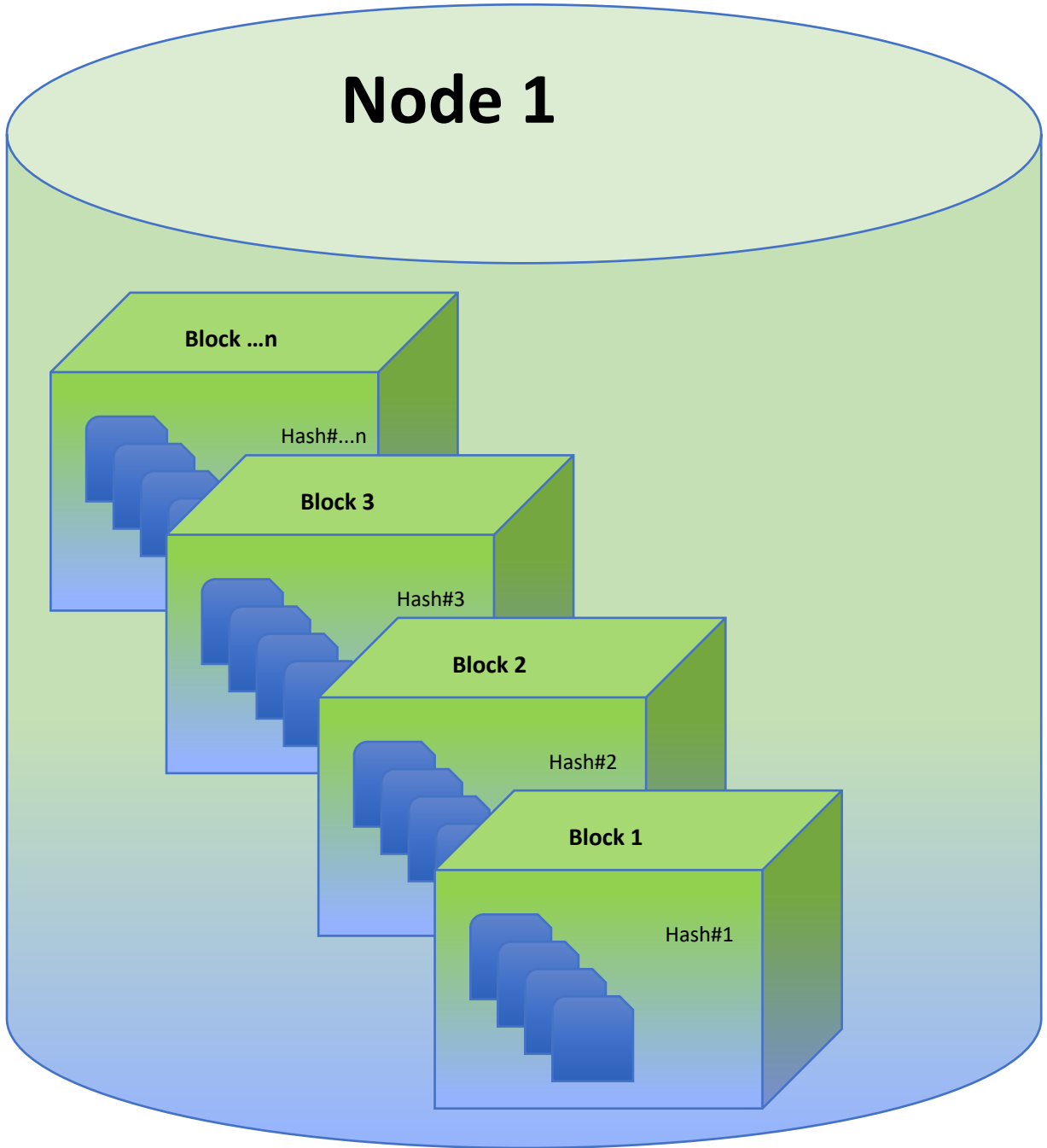
Code: 52200065010

- ✓ **5 Transactions** like the above, per envelope
- ✓ Add all transaction codes and write the **sum** on the envelopes
- ✓ Link the envelopes by including an extra sheet of the **previous envelope's sum**

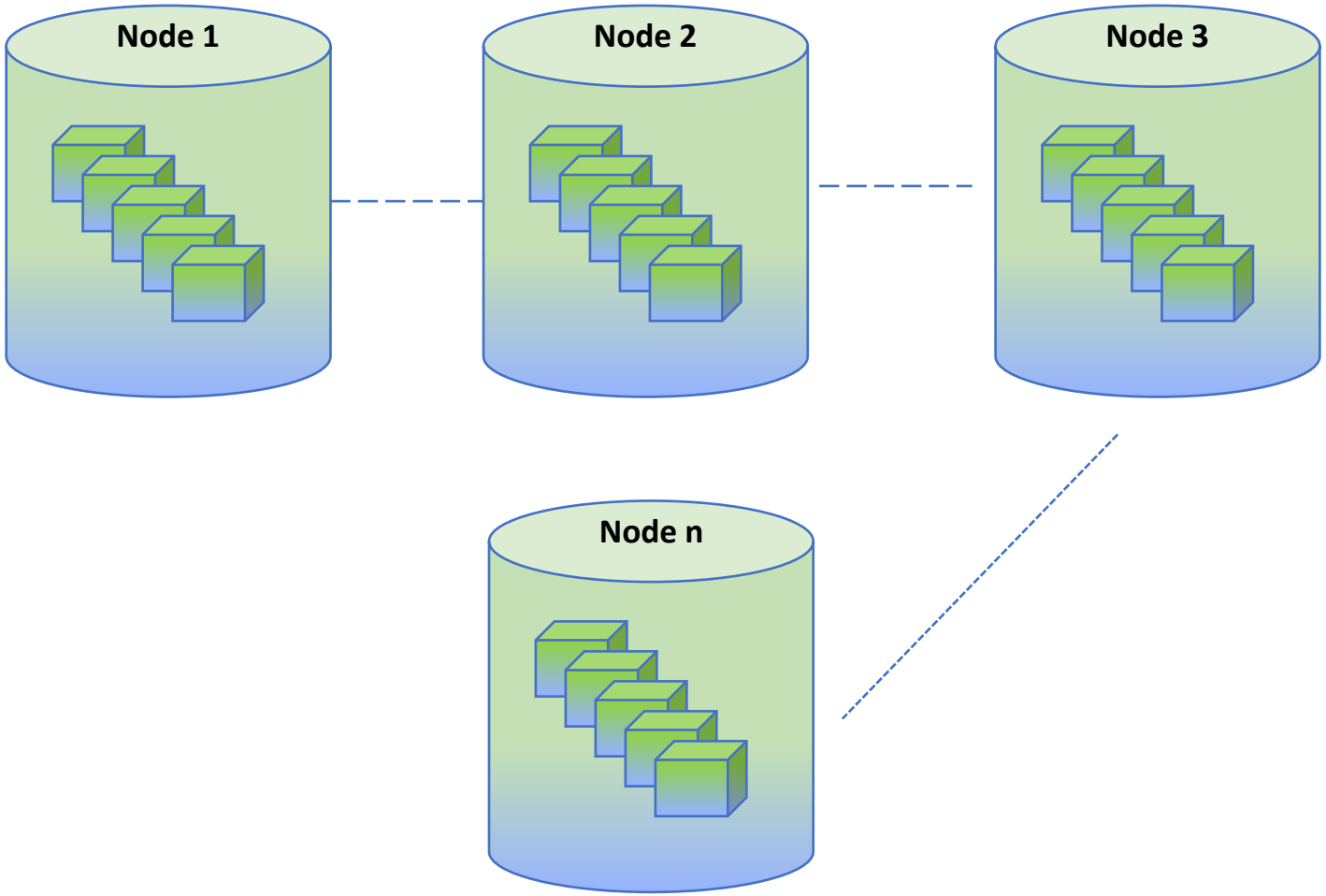
Blockchain


Block 1
Hash#1
Transaction 1
Block 2
Hash#1
Hash#2
Transaction 1

Blockchain



Blockchain



blockchain.info

Exercise

You will be split into breakout-rooms of 5 members each

Each team prepares a presentation for the following topic

Explain the internals of blockchain

Ground rules:

- divide the topic into modules per team member
- after time is up, return to the main session and present
- every team member has to speak (time limit of 1 min per speaker)

Byzantine Generals problem

- Two or more armies have surrounded a fort
- Each army is led by a different general
- If all the armies become allies and attack precisely at the same time, they can win the fort
- If there is a difference in time of attack, they will lose

Byzantine Generals problem

How to communicate the exact time?

- fire signals or trumpet signals can be heard or seen by the enemy
- messengers can be intercepted
- one of the generals or lieutenants can be a traitor

How did Bitcoin solve this problem?

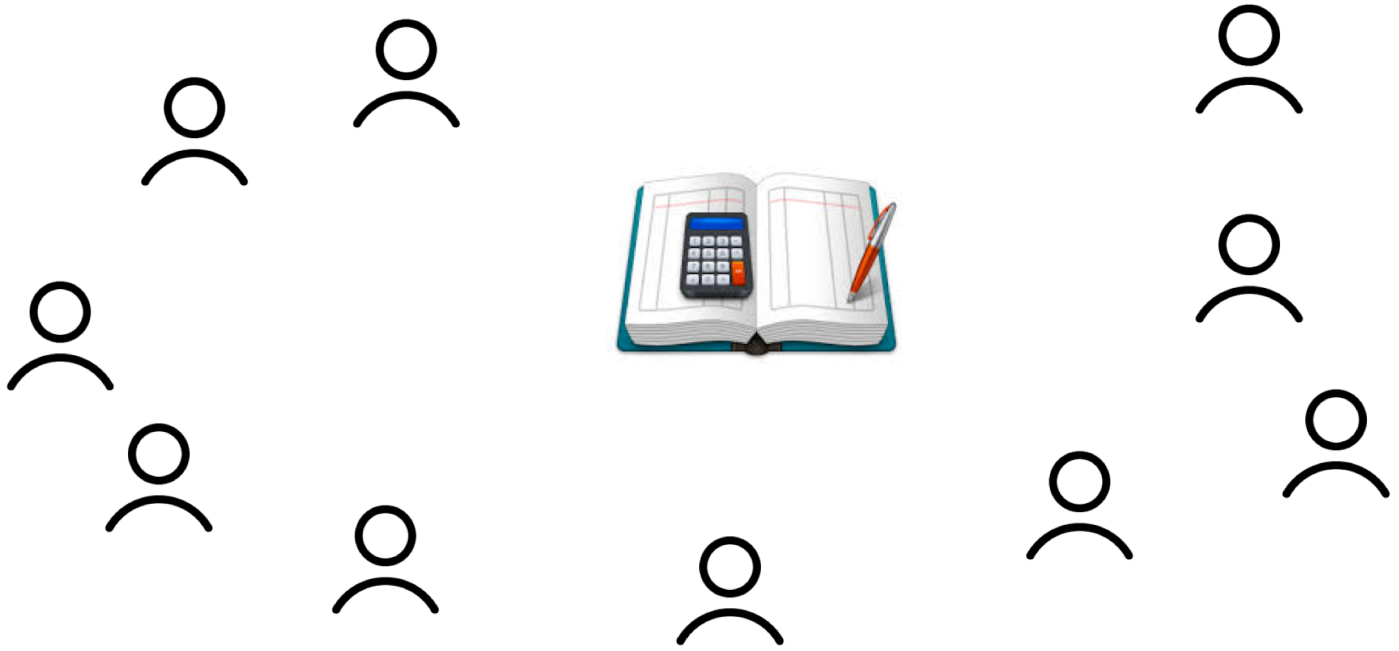
Consensus

How did they achieve that?

- distributed ledger
- digital signatures
- proof of work
- chain of blocks

The community ledger

All of you decide to create a community ledger for all money spent / owed.



Exercise

- Divided into break-up rooms
- Discuss and come up with 2-3 ways you can cheat in this ledger system

Problems with this approach

- Who hosts the ledger?
  - make it distributed
- P1 can add a transaction stating P2 owes him money
  - P2 should add a digital signature using Public and Private keys
- P2 can copy a transaction repeatedly along with digital signature
  - Unique transaction ID
  - Hash instead of digital sig

Public & Private Keys

Bob wants to send Alice an encrypted email. To do this, Bob takes Alice's public key and encrypts his message to her. Then, when Alice receives the message, she takes the private key that is known only to her in order to decrypt the message from Bob.

Although the companies owning the server might try to read the message, they will be unable to because they lack the private key to decrypt the message. Only Alice will be able to decrypt the message as she is the only one with the private key. And, when Alice wants to reply, she simply repeats the process, encrypting her message to Bob using Bob's public key.

Problems with this approach..

- How to trust broadcasted blocks?
  - Proof of work

    - Set a target that the hash should meet, like first 60 digits should be 0.

    - This ensures that there has been a lot of computing done to arrive at the block.

➢Is that good enough?

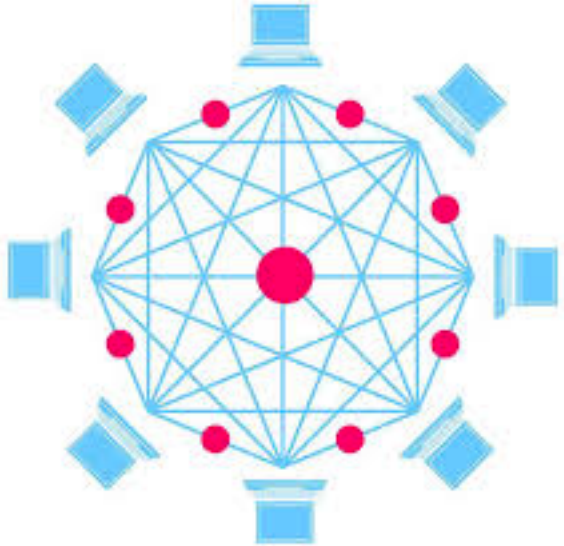
    - Also link blocks with previous hash and include that in the current hash

Blockchain

def·i·ni·tion
\dĕ-fə′-nĭ-shən\

meaning of a word;
can be subjective

Blockchain *is a distributed ledger for maintaining a permanent and secure ledger that is managed by computers in a peer-to-peer network*.



#blockchain

IBM
@IBM

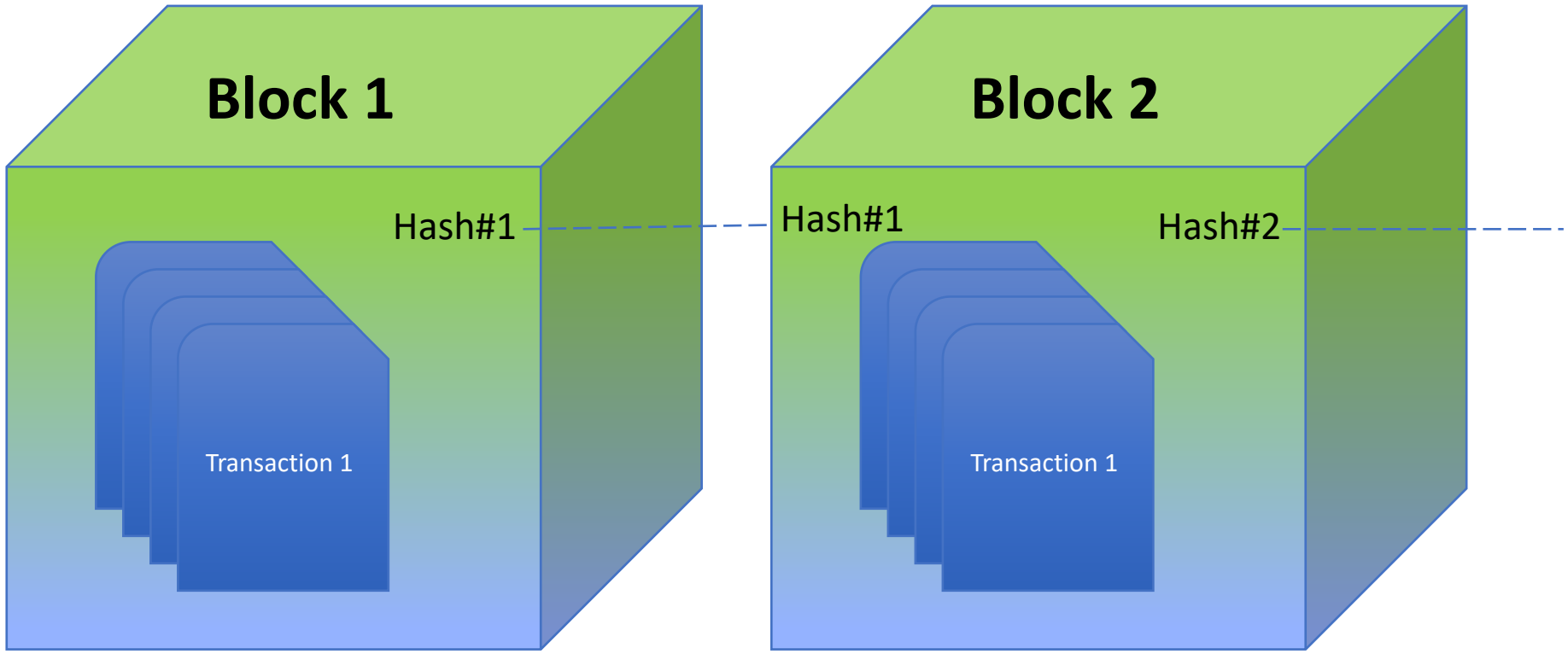
Follow

Ginni Rometty: "What the internet did for communications, I think #blockchain will do for trusted transactions." bit.ly/2tOyc56

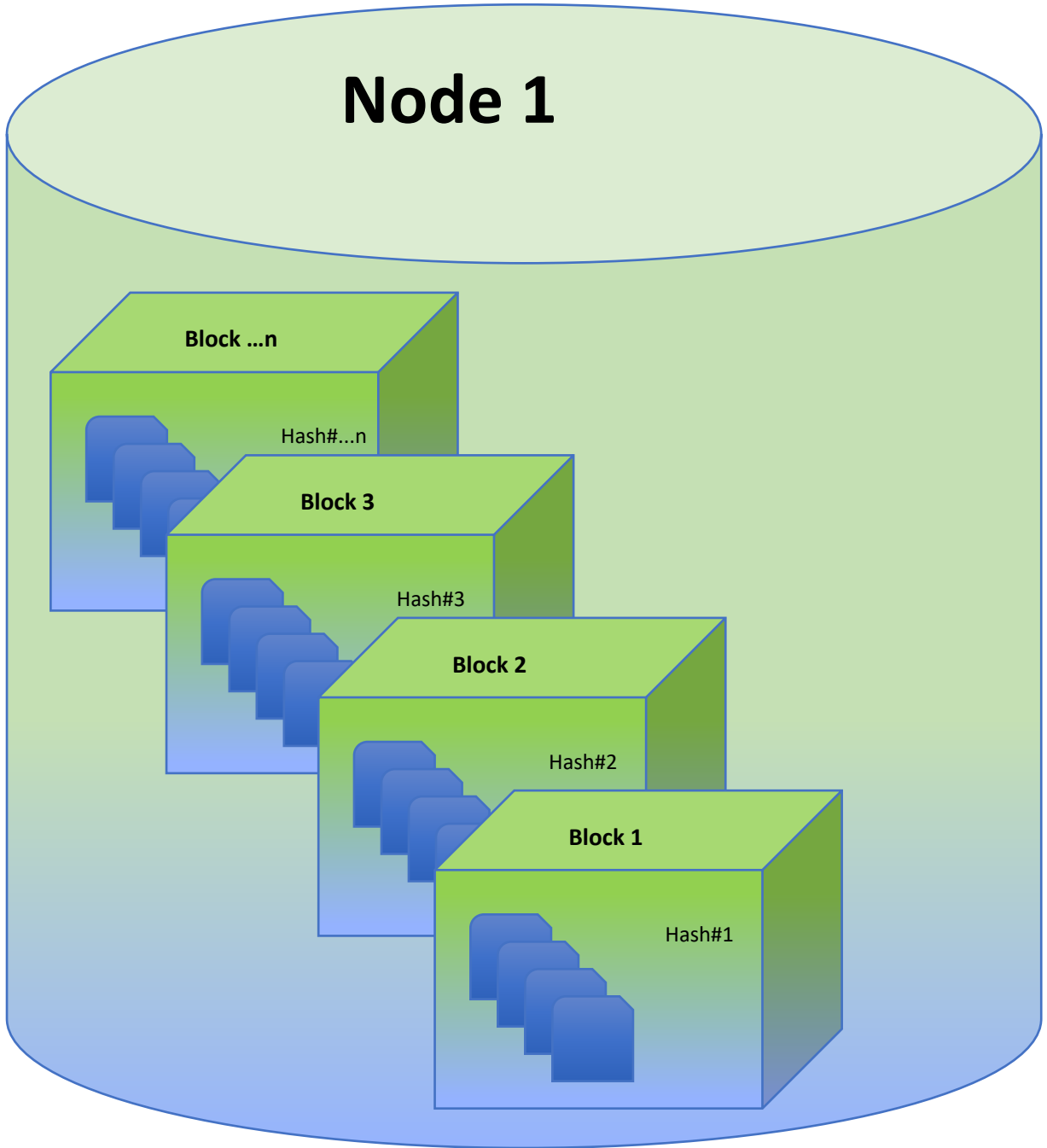
11:49 AM - 21 Jun 2017

"As a tamper-proof public ledger, blockchain is ideal for proof of work"-John Halamka
CIO of Beth Israel Deaconess Medical Center, Boston

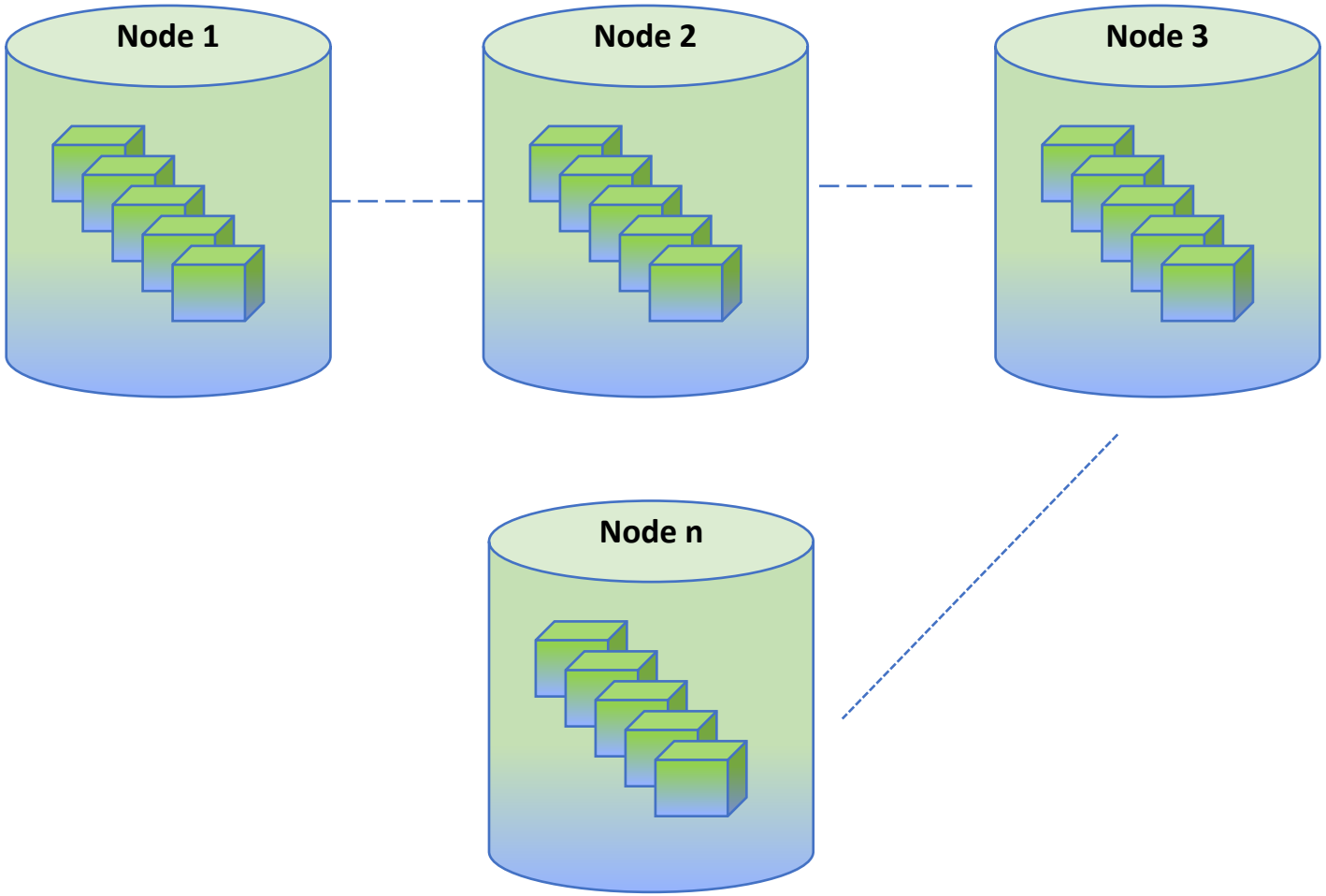
Blockchain


Block 1
Hash#1
Transaction 1
Block 2
Hash#1
Hash#2
Transaction 1

Blockchain



Blockchain



blockchain.info

Blockchain internals

What is a MINER Node?

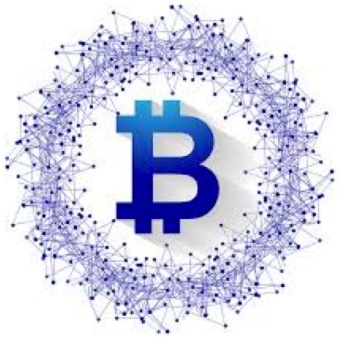
A node with extremely powerful hardware that can take a pool of transactions and create a hash that meets the blockchain’s difficulty level.
Typically, these nodes pick transactions that pay for the mining.

Once such a block is accepted into the blockchain, the miner’s account is credited with the fees.

Link: https://shop.bitmain.com/

Public and Private Blockchain

Public Blockchain:
Any one can choose to be a node in this public world-wide network and submit transactions.
Digital currencies like Bitcoin and Ethereum are good examples.



Private Blockchain:
A private blockchain is more private in scope and participants are limited by defined criteria. For instance, a factory and all its suppliers/vendors.
Such a private network can be implemented using frameworks such as IBM Hyperledger, Ethereum or others.

Permissioned & permissionless Blockchain

Permissionless Blockchain:
Any one can process transactions.

ethereum

Permissioned Blockchain:
Only approved or predefined users/nodes can process transactions.

Finance & Trade

Mizuho Bank & Blockchain (4:23)

- https://www.youtube.com/watch?v=FmhB83dCYzg

Banks & Blockchain (2:44)

- https://www.youtube.com/watch?v=_v439vNdsC4

Retail

Food Safety – Walmart & IBM (3 mins)

- https://www.youtube.com/watch?v=SV0KXBxSoio

Supply-chain management

Port of Antwerp & Blockchain (4:15 mins)

- https://www.youtube.com/watch?v=JTbUQYINNEU

Energy management

Bosch & Blockchain (2:46 mins)

- https://www.youtube.com/watch?v=W6CsnH57E6g

IoT Security

SmartAxiom – IoT security ledgers (3:45 mins)

- https://www.youtube.com/watch?v=9Z72pchFO1Q

Manufacturing

Aviation & Blockchain (2:30 mins)

https://www.youtube.com/watch?v=ToMhSKpM_7A

Mercdes Benz & Blockchain

- https://www.youtube.com/watch?v=4sSDZAdlZHY (2:10)

Government

https://www.youtube.com/watch?v=0xrMyDauK78
(3:10)
https://www.youtube.com/watch?v=ZsedI2slhUw
(4:33)

Pharma Industry

Pharma:
https://www.youtube.com/watch?v=rSpIkuvTLh0
(2:30 mins)

Enterprise Ethereum

…customer success stories

Explore the different customer stories here:

https://ethereum.org/en/enterprise/

ethereum

Assignment

- Install Geth client