Block Chain

A Secure Ledger For High Volume Transactions

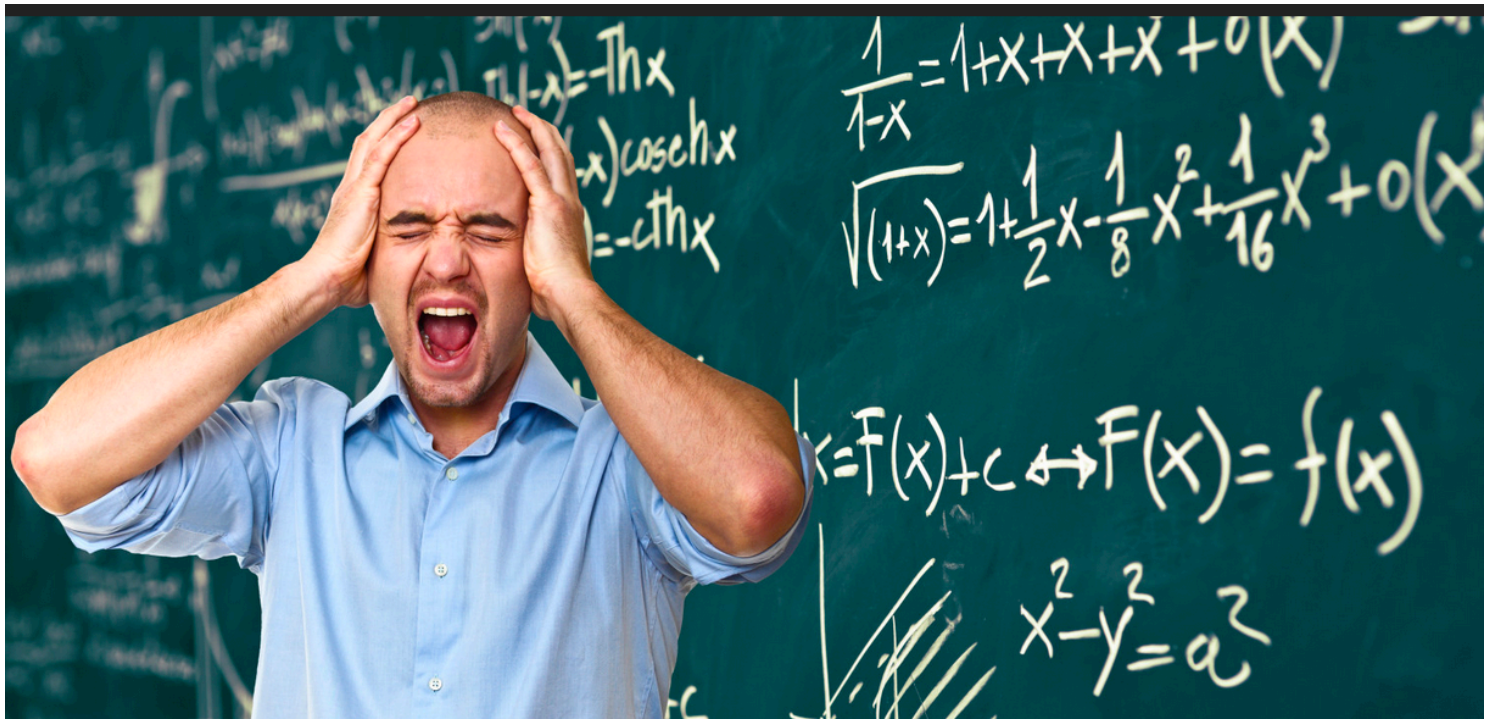
Steve Pittard

Block Chain

How I Hope People Will React

Block Chain

Versus The Usual Reaction



Bit Coin

If You Learn Nothing Else From This….

- ***Bit Coin*** Is a ***(Crypto) Currency*** That Relies Upon….
- ***Block Chain,*** *Which Is* A "Write Once, Read Only" Ledger System
- ***Block Chain*** *Is A Shared Ledger (No Single Owner)*
- A ***Block*** Is Just A Digital Transaction

You may now zone out….. Well, I hope not.

Block Chain

Block Chain Can Be Used For Documenting:

- Global Shipments Of Food, Medicine, Supplies
- Transportation of Organs In Emergent Donor Situations
- Medical Compliance and Attendance
- Course Completion And Academic Transcripts
- Copyrights (e.g. musical works, manuscripts)

Bit Coin

Most People Hear About Block Chain Because ***Bit Coin Uses Block Chain*** – And That's About All They Know

- People Generally Like Things That Can Make You Rich
- Bit Coin Is Useful For Teaching People About Block Chain
- Warning: Owning Bit Coin Leads To Obsessive Behavior

24 Sep 2014 00:00 UTC - 23 Sep 2019 19:44 UTC **XBT/USD** close:**9814.85262** low:**170.87549** high:**19447.68573**

https://www.xe.com/currencycharts/?from=XBT&to=USD&view=1Y


BEFORE CRYPTO
AFTER CRYPTO

Time Line

1990 – “Linked Time Stamps” introduced by Haber and Stormetta (like a Digital Notary Public)

1996 – “Smart Contracts” introduced Nick Szabo

2009 – “Block Chain” introduced by Satoshi Nakamoto

Time Line

Weird Plot Twist !

Time Line

Turns Out That Satoshi Nakamoto….

Could be an anonymous person or group of people
Maybe one or more of the following ?

Dorian Nakamoto

Nick Szabo

Craig Wright

“Old School” Money Transfer & Exchange Scenarios

Entity A Uses Their Bank to Send Money To Entity B's Bank

Both Banks Take A Fee For the Exchange

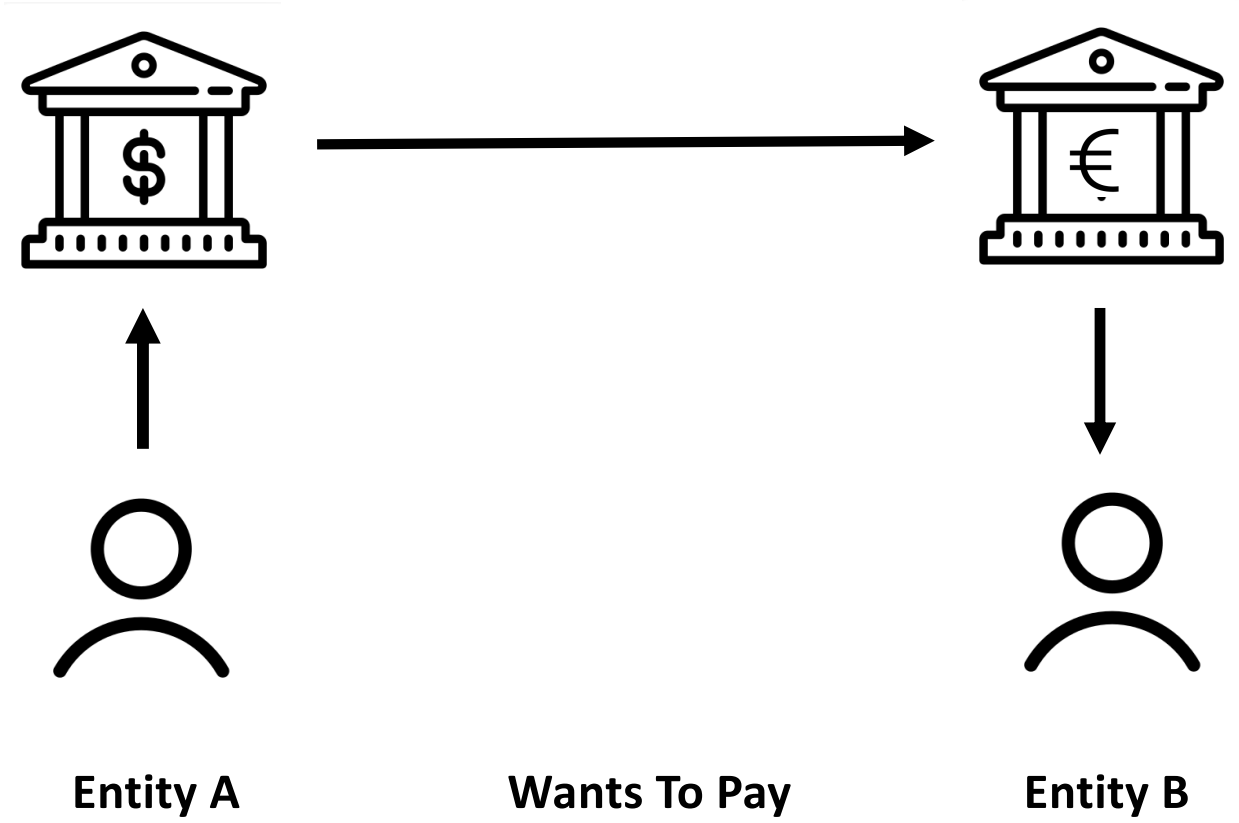
Both Banks Have Their Own Private Ledgers

The Transaction Might Not Happen Due to Regulations

Banks Can Be Hacked

The Transaction Might Be Reported To Respective Government(s)

Interstate Or International Banking Regulations



In This Case, Both Entities Use The Same Third Party Service

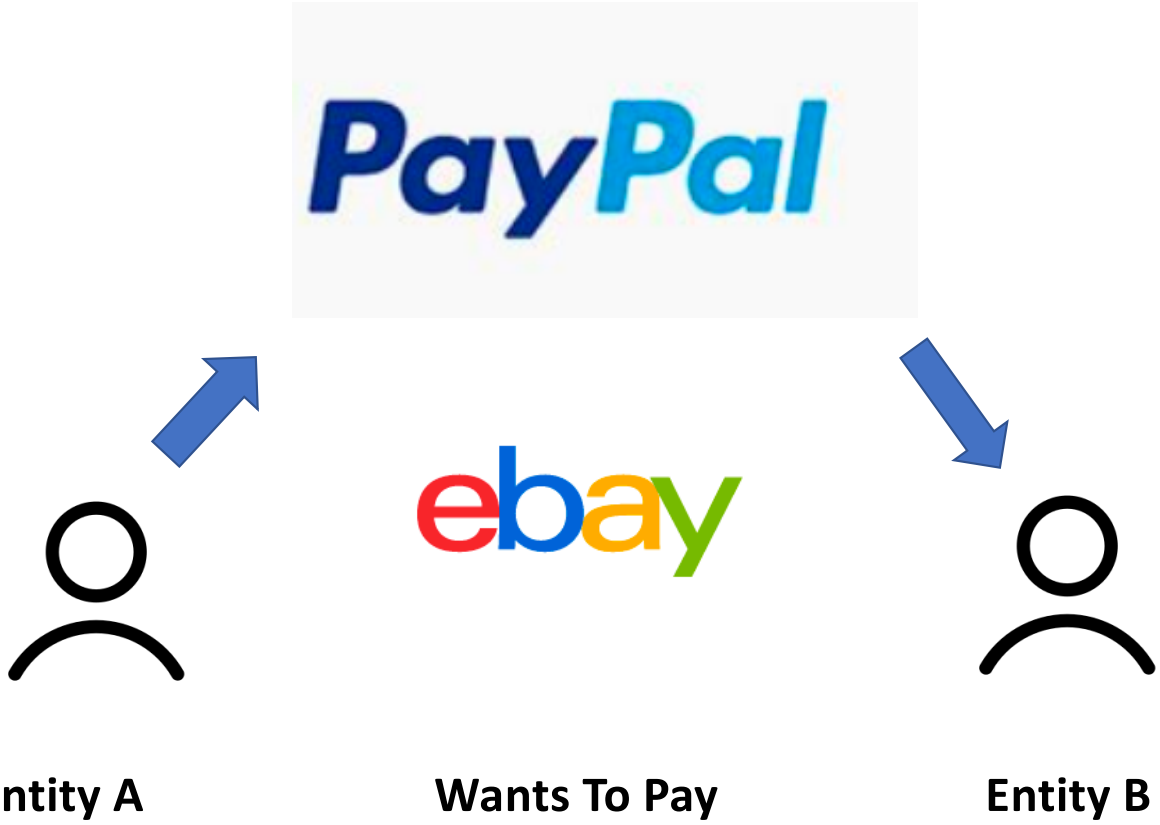
Pay Pal Takes A Fee And
Can Raise It

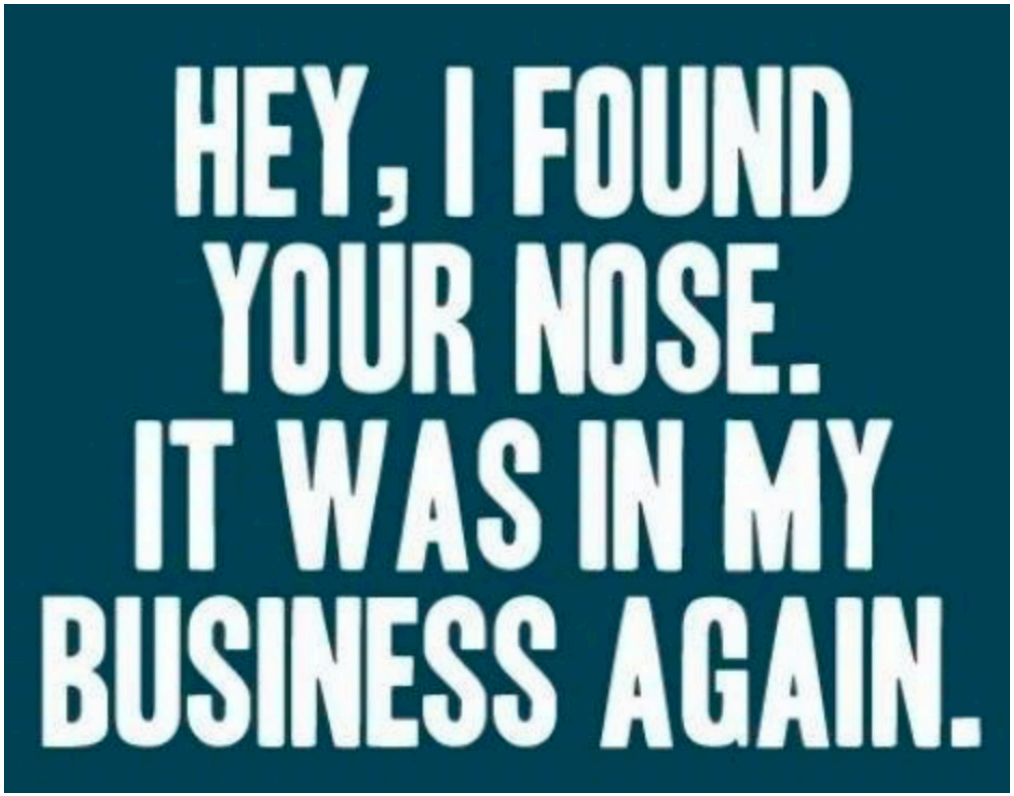
Pay Pal Maintains A
Private Ledger

Ledger Could Be Hacked

The Transaction Might Be
Reported To the Government

Pay Pal, (like a bank), Knows
A lot About You




HEY, I FOUND
YOUR NOSE.
IT WAS IN MY
BUSINESS AGAIN.

Bit Coin

- No Need To Pay Intermediaries
- User Retains Control Of Information And Actions
- No Central Authority
- Anonymous (if desired)
- Transactions Are Publicly Verifiable

But, Is This Secure ?

Use of Hashes

“Proof Of Work”

“Distributed Ledger”

Block Chain

- Transactions are stored in blocks that form a public ledger referred to as a **Block Chain**
- Each **block** contains a **“hash”** (unique id) as well as the **hash** of the previous block all the way up to first block of the chain.
- Transactions are verified by Peer to Peer network participants “miners”

A Block Contains Transaction Info

Data: Transfer 100 BTC From Person A To Person B

Hash: A Unique Numeric Identifier

```
a37938270ba6fafb4c27273cc93bfa598f361000
```

The Hash is a function of the Block's Content. So if the Block Content changes then so does the Hash.

Hash Of The Previous Block:

A Unique Numeric Identifier of the Previous Block In The Chain

A Chain Of Three Blocks

The “Genesis” Block

Hash: 4F2B

Previous Hash: 0000

Data: Transfer 100 BTC From Person A To Person B

Hash: 7CD4

Previous Hash 4F2B

Data: Debit Person A 100 BTC

Hash: N5V7

Previous Hash 7CD4

Data: Credit Person B 100 BTC

A Hacker Changes Block #2 To “Debit Person A 10 BTC” - **Block 3 Is Now Invalid**

The “Genesis” Block

Was Hash: 7CD4

Hash: 4F2B

Previous Hash: 0000

Data: Transfer 100 BTC
From Person A To Person B

Hash 8CF4

Previous Hash 4F2B

Data: Debit Person A
10 BTC

Hash: N5V7

Previous Hash: 7CD4

Data: Credit Person B
100 BTC

Block Chain

Use of Hash IDs Helps Prevent Fraud, But….

- Large Compute Clusters Can Recompute Hashes To Cover Up Hacks
- In Effect, Rewrite Ledger Entries
- If There Is Only One Ledger Copy, Then Evidence Is Erased

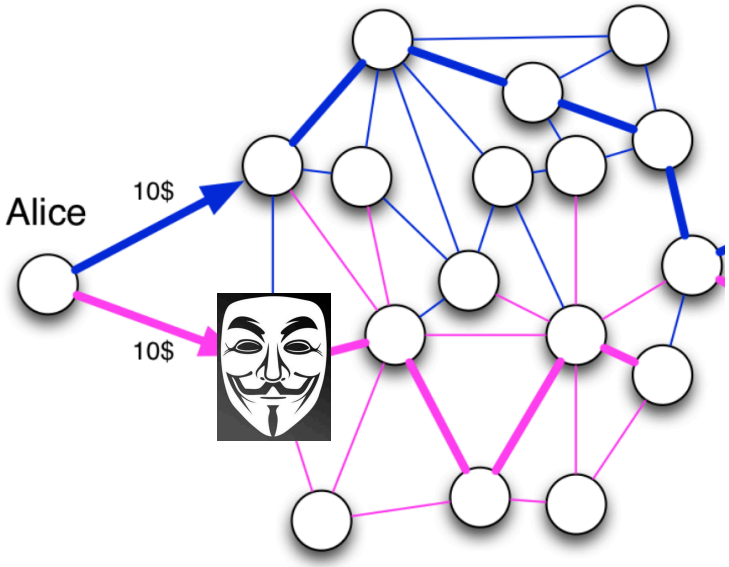
Block Chain

“Proof Of Work” - PoW

- A method to intentionally delay the creation of new blocks – For BitCoin it’s about 10 minutes / block
- Tampering With One Block Requires PoW Recalculation for all impacted Blocks
- Very Slow To Do With a Large De-Centralized Ledger

10 Minutes

10 Minutes



Recompute Hash For 16 nodes at 10 minutes Each, Serially: 160 minutes.

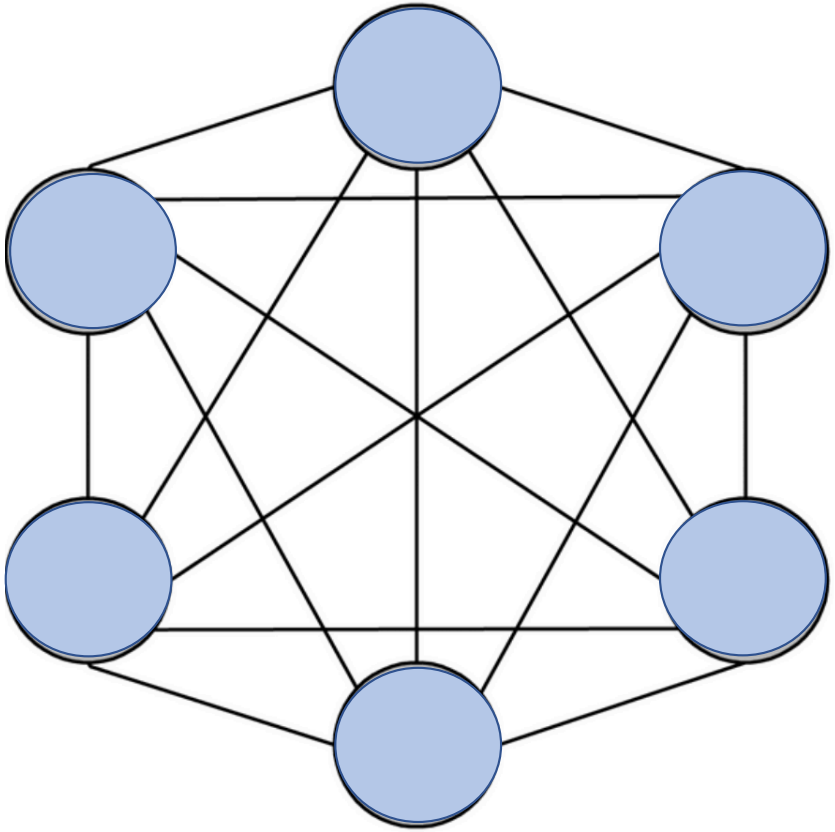
Block Chain

“Distributed Ledger – Peer to Peer Network

- Block Chains Use A Peer To Peer Network
- No One Entity “Owns” The Ledger Or Network
- Any One Can Join The Network
- Every One Gets A Copy of The Ledger
- Must Be A Consensus On The Ledger State

1 2 3

1 2 3

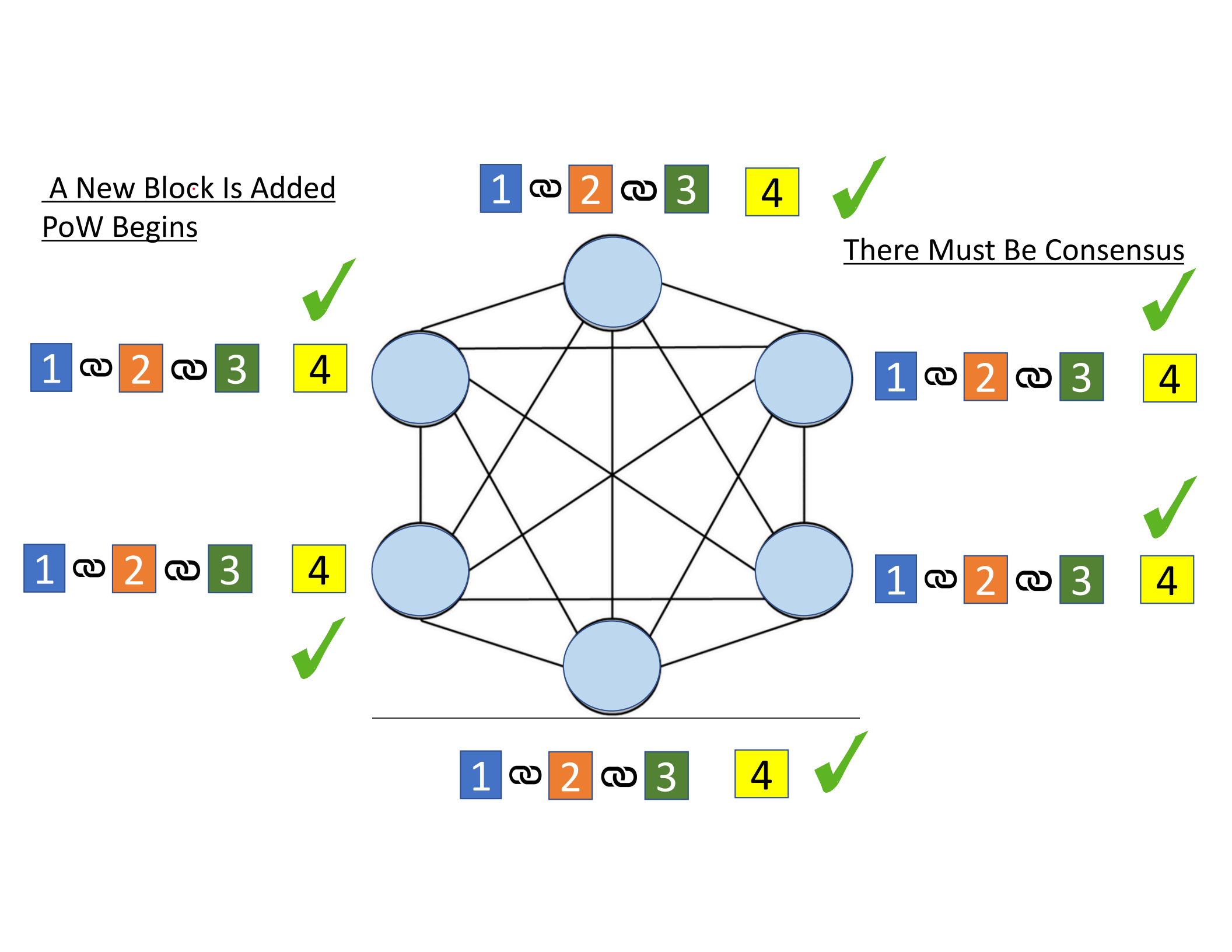


1 2 3

1 2 3

1 2 3

A New Block Is Added
PoW Begins



Block Chain

"***Smart Contracts"*** help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman."

https://blockgeeks.com/guides/smart-contracts/

Brainstorm Ideas

Longitudinal Patient Records

Patient X Got Drug Y At Time Z

Identification

People Who