Rishabh Wanjari
Aakash Ramesh
Govind Gandhi
Pavith R

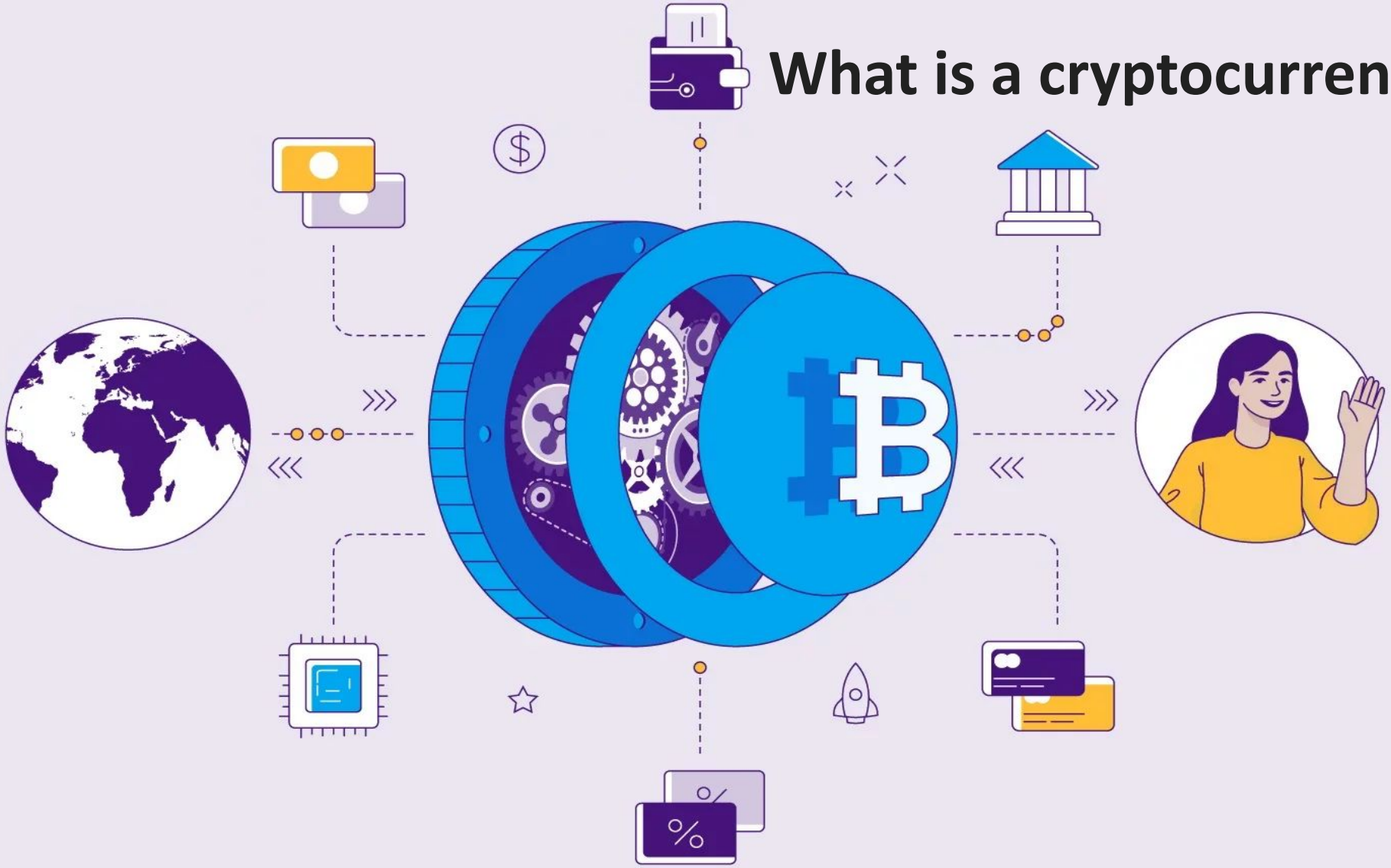
Why are we interested in cryptocurrency?

THE ECONOMIC TIMES | Markets
English Edition | 19 May, 2021, 12:20 AM IST | E-Paper

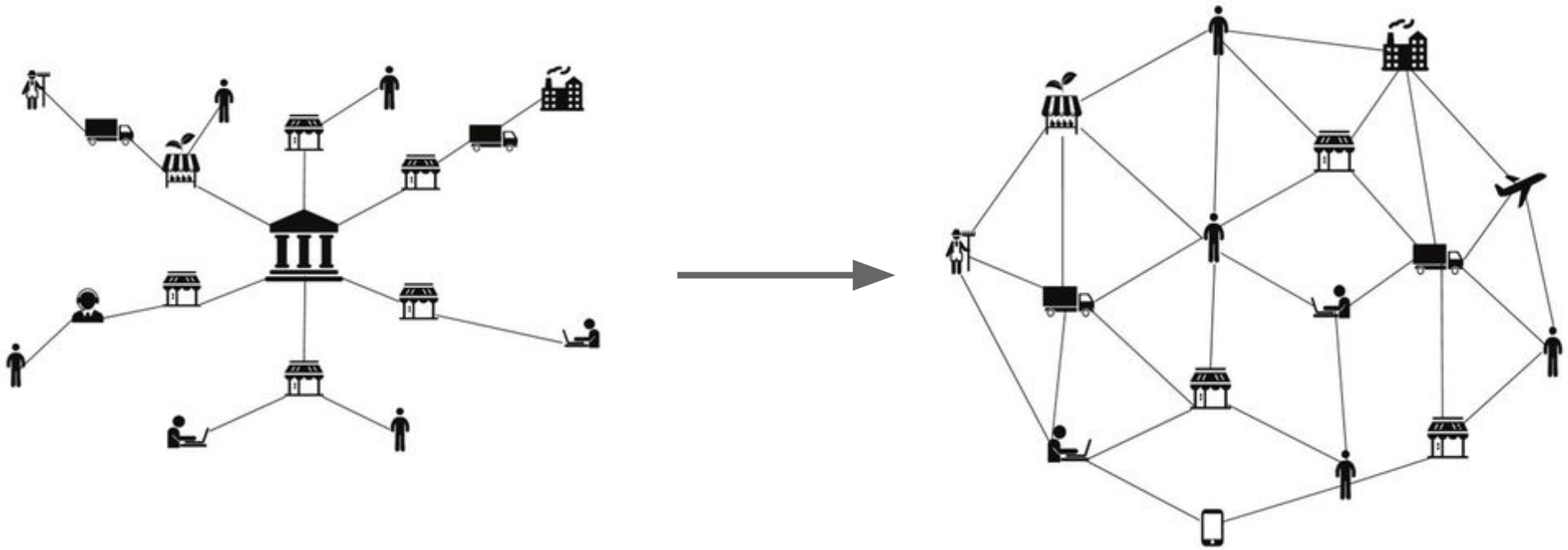
Crypto market value surges to all-time high of $2 trillion, bitcoin at $1.1 trillion

That's more than Canada's GDP in 2019

What is a cryptocurrency?



Decentralization



What is Bitcoin?

Bitcoin is a cryptocurrency whose transactions are made between encrypted addresses. These addresses are secure and are accessible only to the owners.

Bitcoin is a network of independent computers that generate, propagate, and verify monetary transactions.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Blockchain: Components

There are 4 main components to how a blockchain works:

1. A shared ledger
2. A digital signature
3. A cryptographic hash function
4. Proof of work

The Shared Ledger

Suppose we want to keep track of the money we spend along with a group of friends. We can do this using a shared ledger. It can look something like this:

1. Abhi pays Balaji	ω20
2. Balaji pays Dakshin	ω10
3. Dakshin pays Chetan	ω10
4. Balaji pays Chetan	ω5

Such a ledger is very reliant on the trust between the group of friends.

Debt

Amongst the group of friends, the shared ledger is reliant on the fact that, at the end of some time period (every month or every year), they settle up the differences and pay each other.

6. Chetan pays Dakshin	₿200
7. Balaji pays Dakshin	₿10
8. Chetan pays Abhi	₿100
9. Abhi pays Chetan	₿20

Chetan has racked up ₿280 in debt this way.

Cutting Ties to Real Currency

At the beginning of the ledger, everyone makes a deposit of some amount (say, ₿100).
We impose a new rule that does not allow anyone to spend more money than they have.

Chetan deposits	₿100
Chetan pays Abhi	₿ 20
Chetan pays Balaji	₿ 60
Chetan pays Dakshin	₿30

There’s a problem

This ledger system, however, lets *anyone* add to it.

There is nothing that prevents Chetan from doing this. So, we need a way for both parties involved in the transaction (Dakshin and Chetan) to be able to verify that it is indeed a real transaction.

This is where hash functions and digital signatures come in.

Hash Functions

Typically, hash functions are considered cryptographic if they satisfy the following properties:

- Deterministic: The same input always yields the same hash.
- Intractability: It’s infeasible to find the input for a given hash except by brute force
- Collision-safety: It’s infeasible to find two different inputs which output the same hash.
- Avalanche effect: The smallest change in input should yield a hash so different that the new hash appears uncorrelated with the old hash.
- Speed: It’s computationally fast to generate a hash.

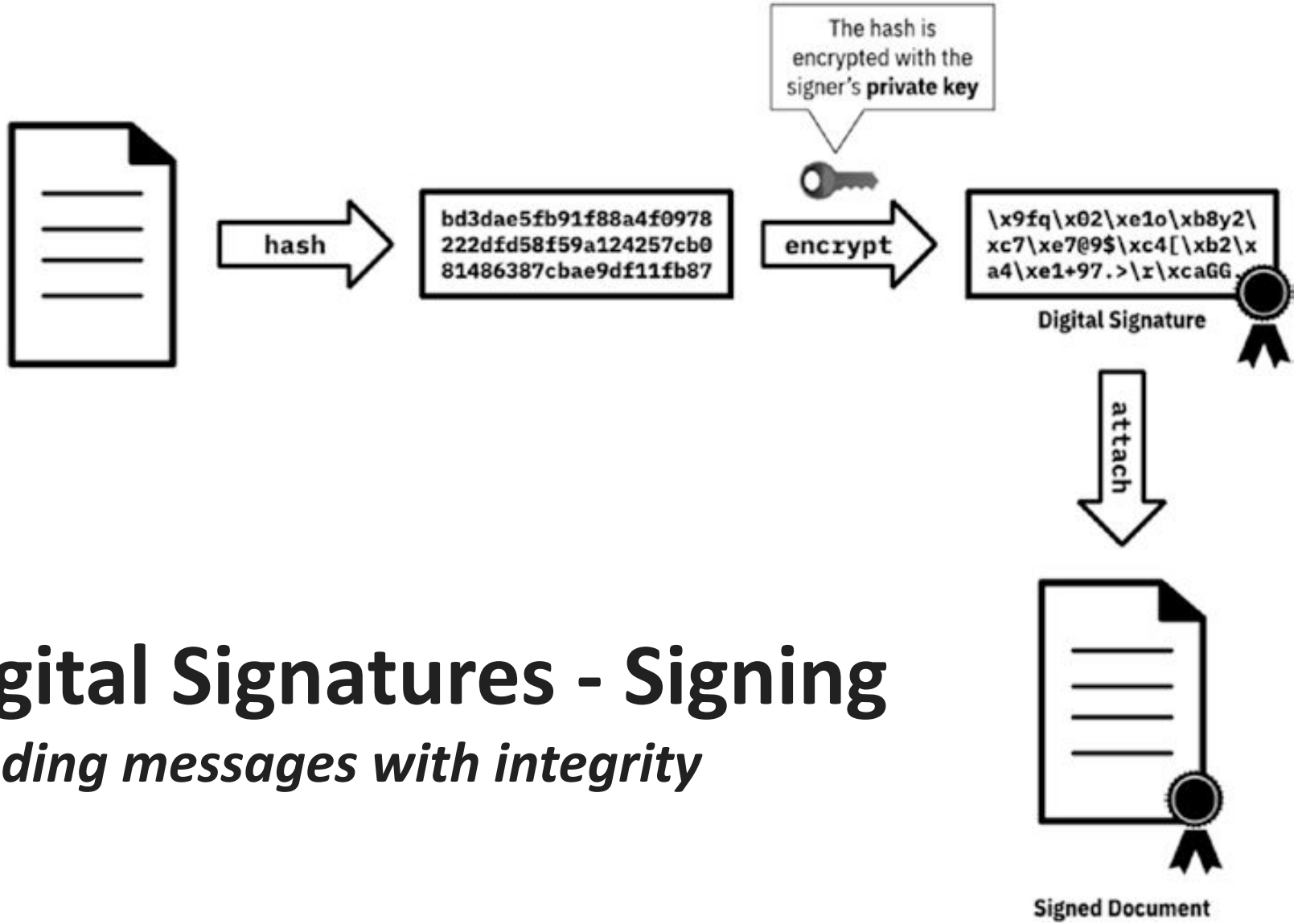
SHA256 - Example

Hash value:

```
8bf6 d93d 32e2 91a9 64a8
ec71 065d 1190 39ae 9ce3
ae45 146c 4469 1431 37de
          ee29
```

Hash value:

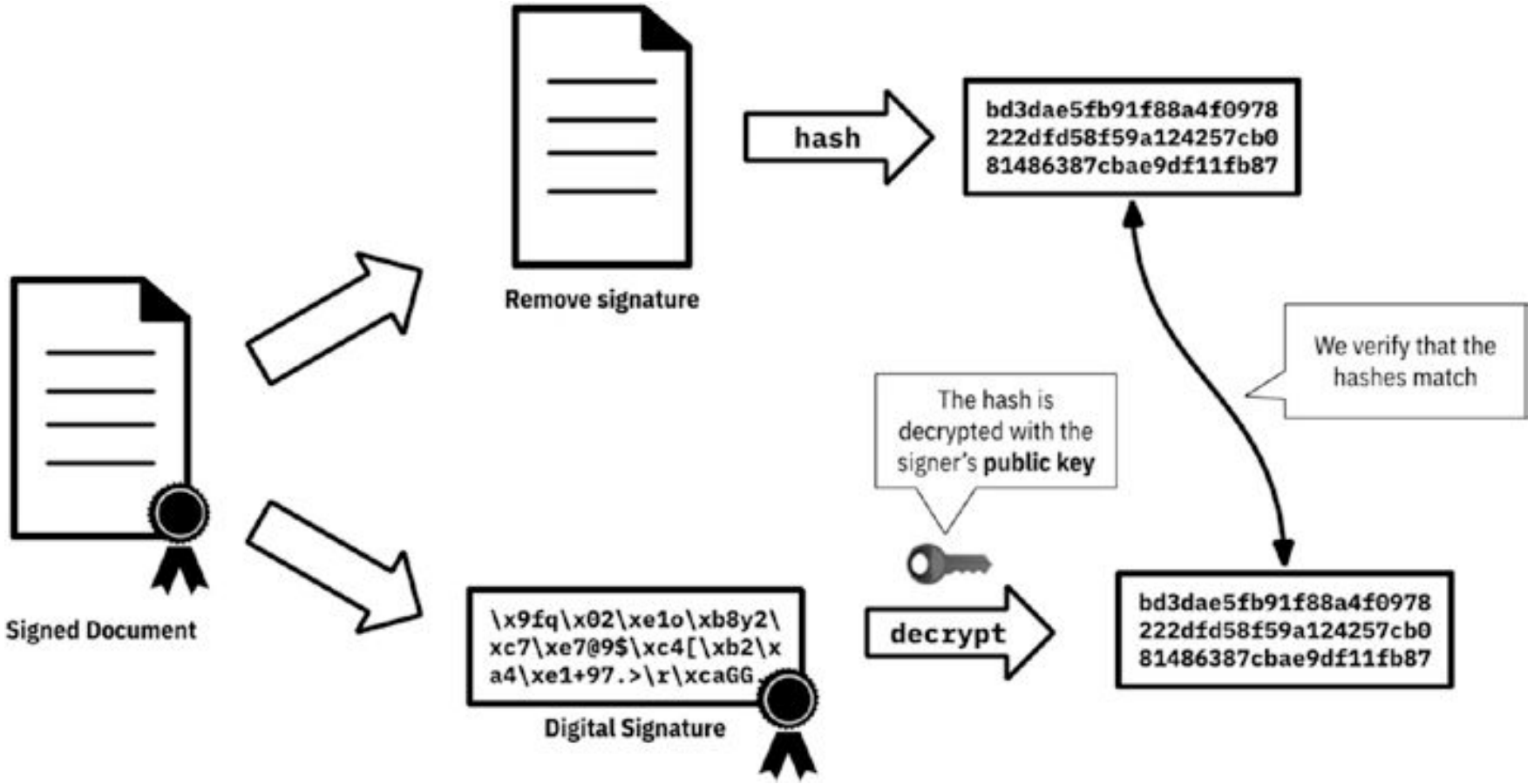
```
8f72 ab8f db92 f071 03f5
70b8 cfe9 2ad6 4f4e fe88
8579 64a8 2e34 f338 8bfe
          96d9
```



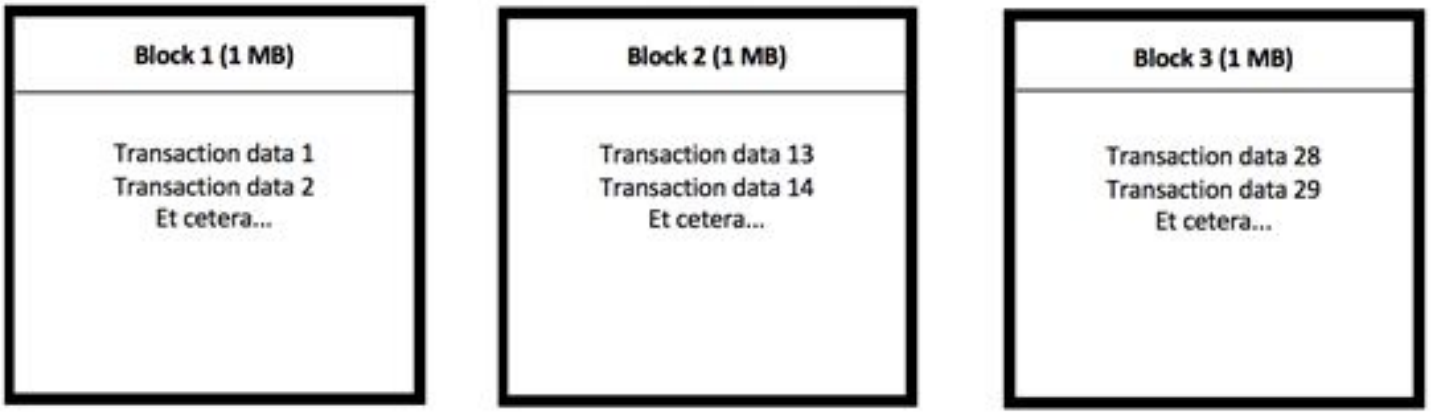
Digital Signatures - Signing

Sending messages with integrity

Digital Signatures - Verification



Organizing the Ledger



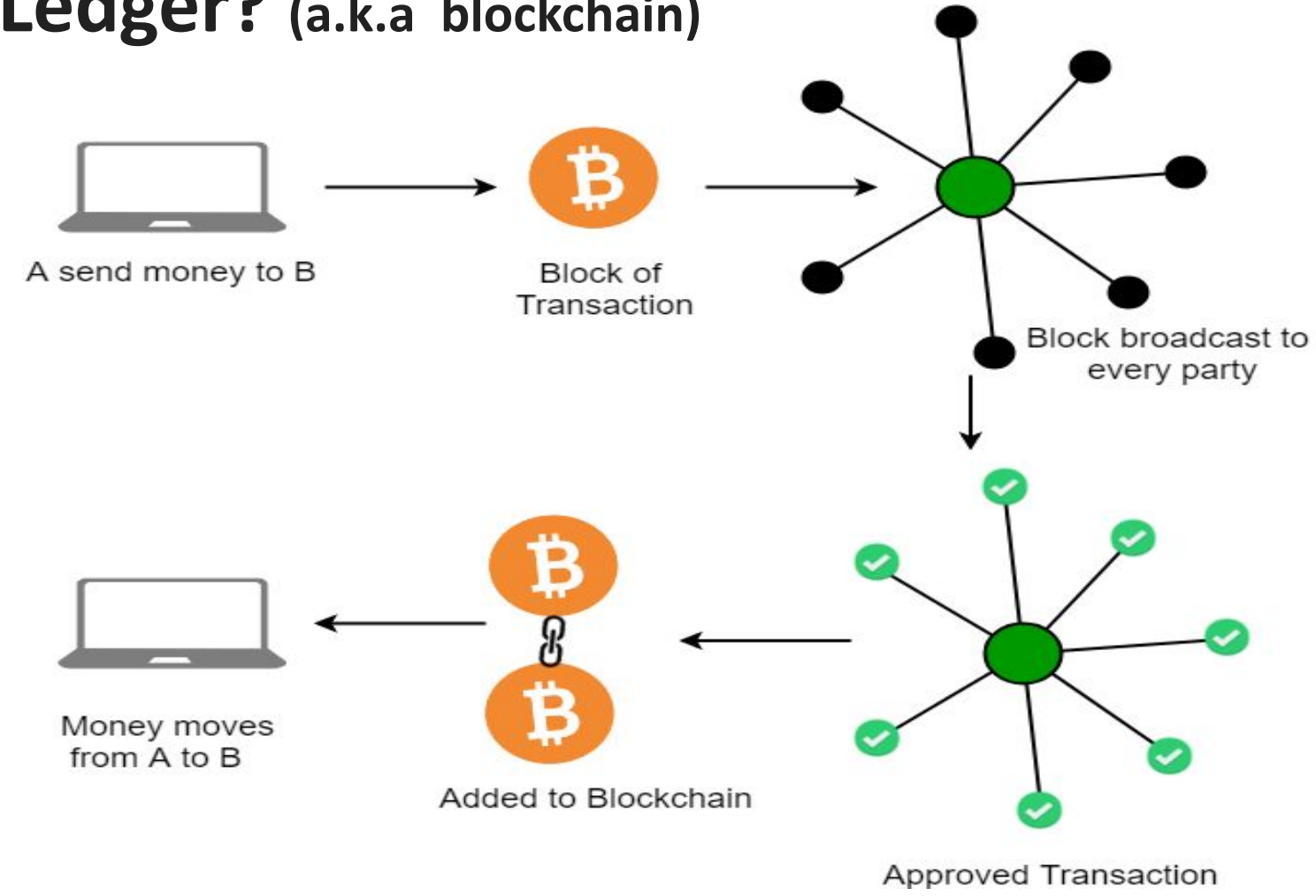
The ledger is split into many blocks that all link to the previous one, forming a chain of blocks.

For Bitcoin, each block has a size of 2,400 transactions.

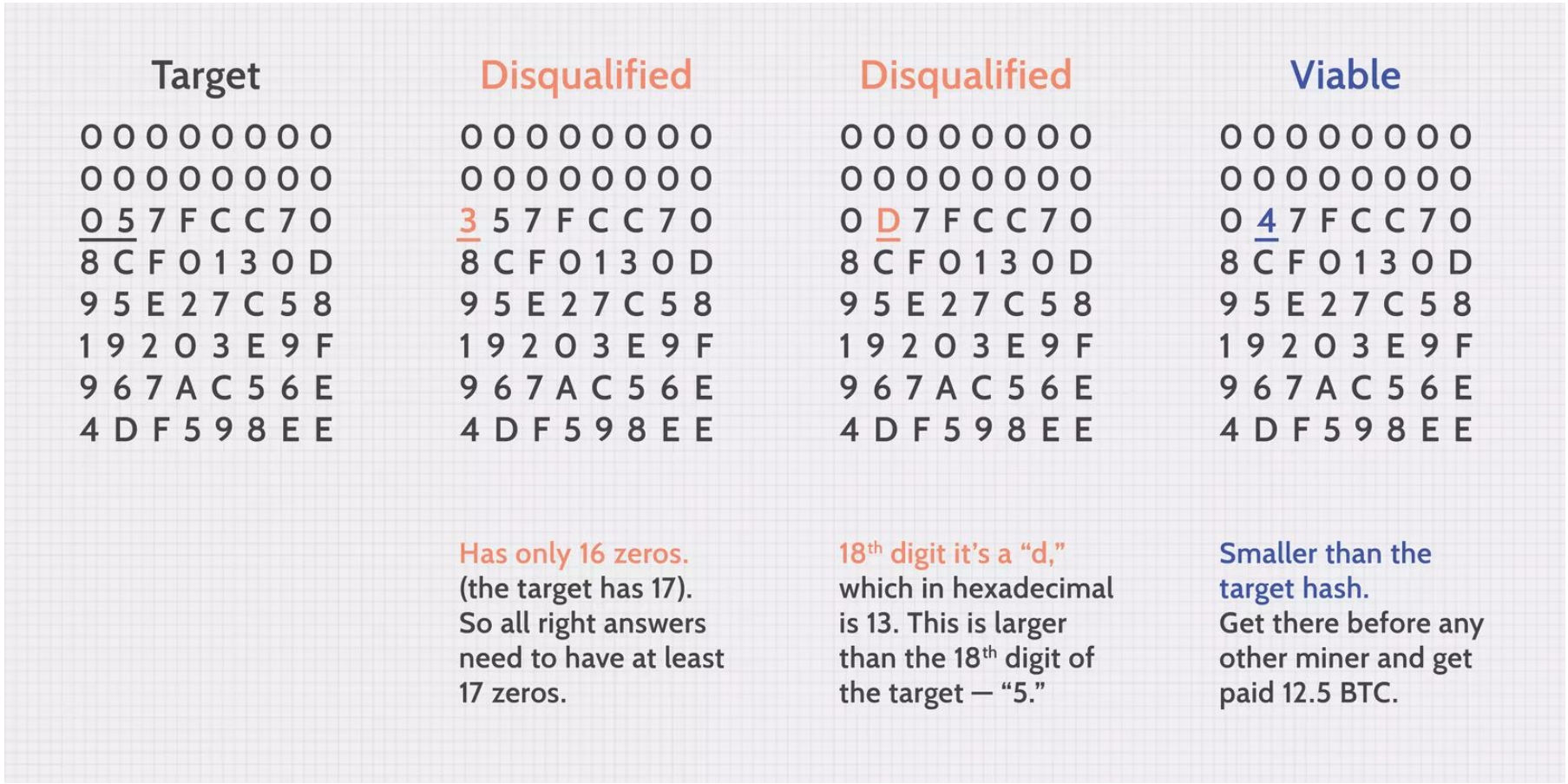
Where is the Ledger? (a.k.a blockchain)

Having a single location of the ledger also requires trust.

Instead, everyone has their own copy of it. They can broadcast the changes they make to everyone else.



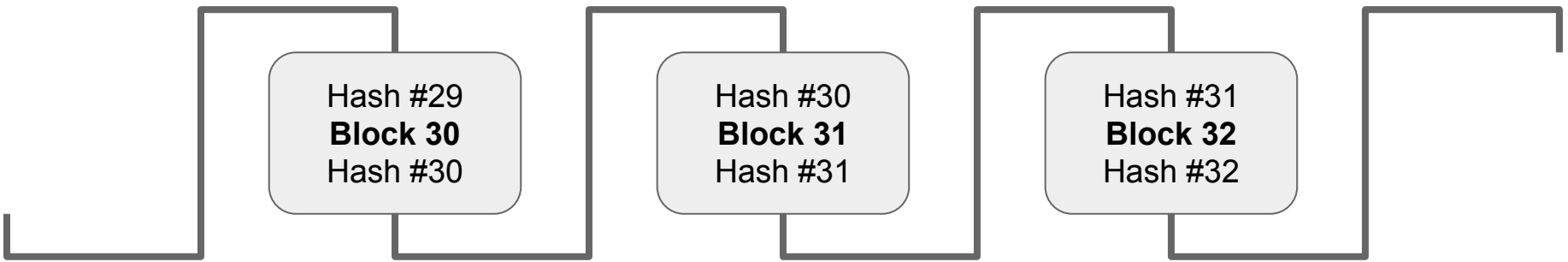
Proof of Work Consensus



The difficulty of this problem keeps increasing such that, in the Bitcoin network

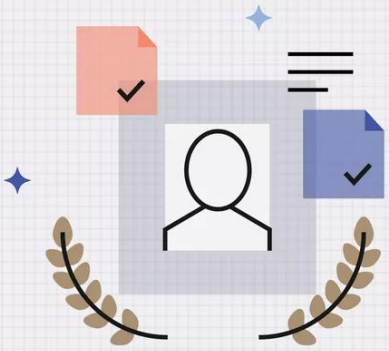
```
******* Mining *********

Found a new block with starting with 00 in: 0.021504640579223633 seconds
With the hash being =  00ff2dcd0ff5951178a4c28f82bd28002999c3520851c49e681e6193f71b0ce6


******* Mining *********

Found a new block with starting with 000 in: 0.1748180389404297 seconds
With the hash being =  000e03e7e2a980fa7f20382890d1a4ade6a46ebf9a4adf0b020c25db199c367e


******* Mining *********

Found a new block with starting with 0000 in: 2.346092700958252 seconds
With the hash being =  000086e6818142c4caf84ae9db45ab7fbb8687076416c301204d6d288ec929f4


******* Mining *********

Found a new block with starting with 00000 in: 18.0671603679657 seconds
With the hash being =  0000017c14333b9d75e3c7665fae4385e384c0ab330e57e4d53973478ba5da74


******* Mining *********

Found a new block with starting with 000000 in: 336.44659876823425 seconds
With the hash being =  000000080018e4701d3449692cab9219c41c5ba9f760fb285e1760ce2c689422


******* Mining *********

Found a new block with starting with 0000000 in: 8780.913450241089 seconds
With the hash being =  000000021fb64f77f9e4812346a51c8cede35045eab6a7647efadc658b27b207
```

Computational work and Blockchain



Bitcoin Rewards

2 conditions for “winning” a block



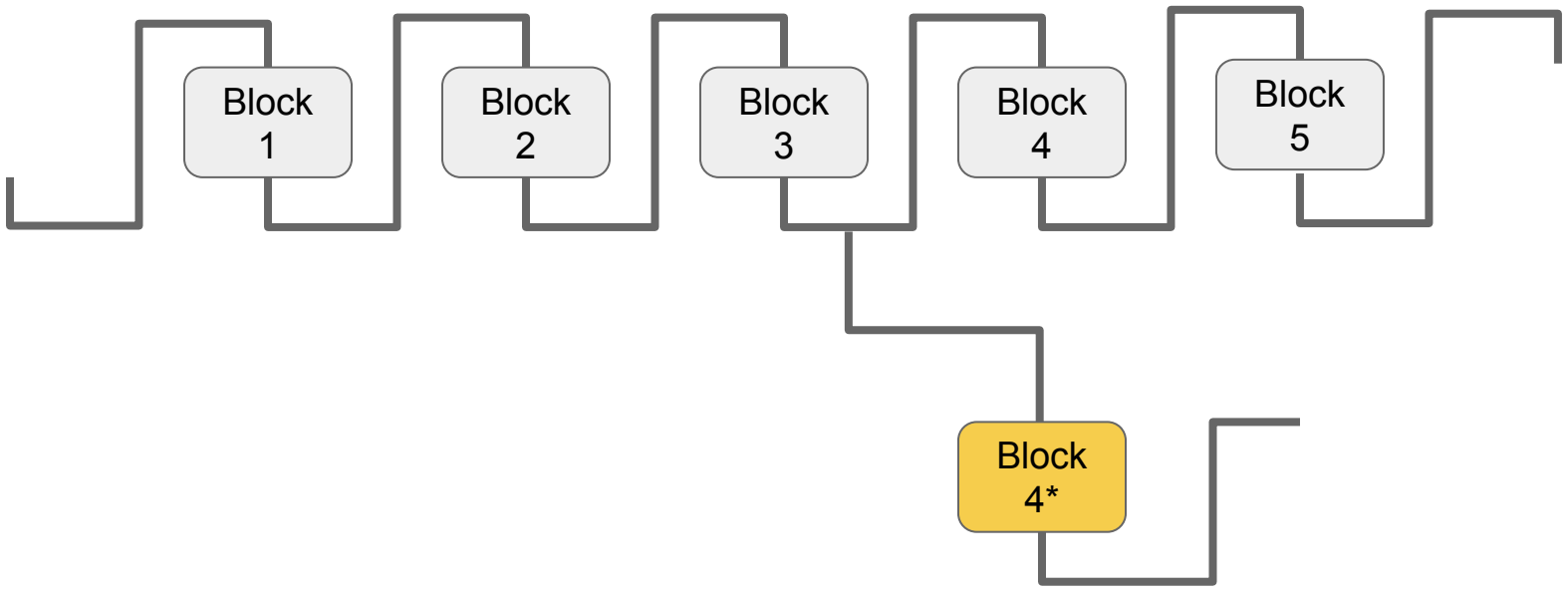
Effort

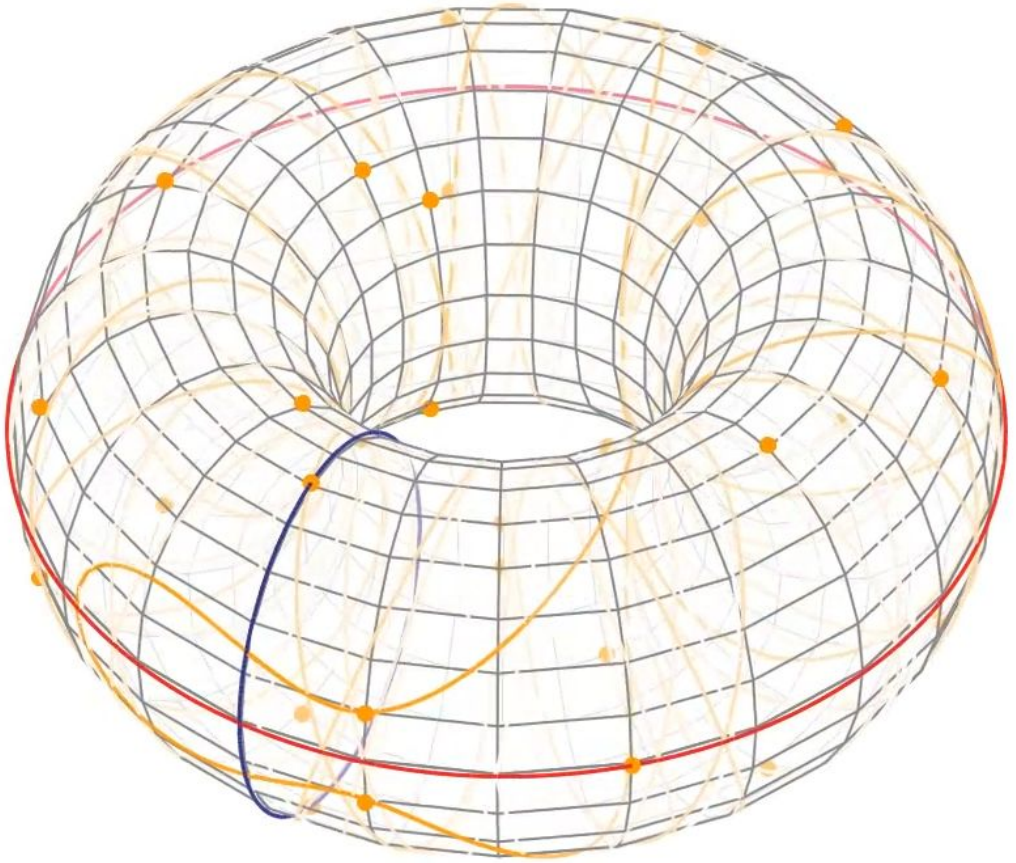
Verify ~ 1MB worth of transactions.

Luck

Arrive at the right answer to a numeric problem first.

An Attempt at Attacking a Blockchain





Elliptic Curve Digital Signature Algorithm

(ECDSA)

Elliptic Curve:

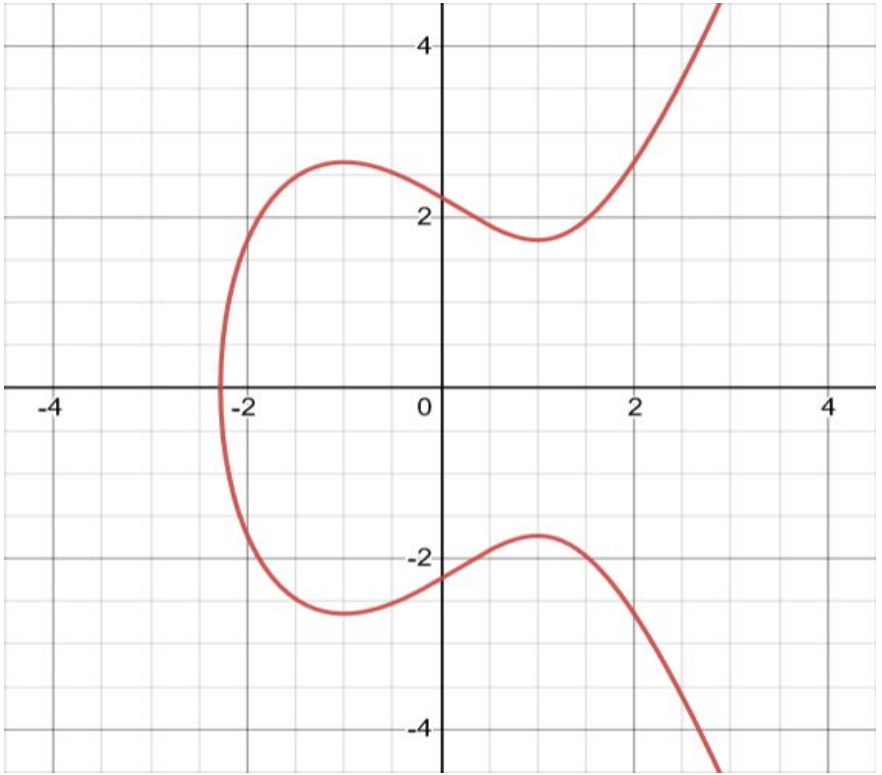
- It is a **smooth**, **projective**, **algebraic curve** of **genus one**, along with a **distinguished point at infinity**, defined over a field $\mathbb{K}$.

- For a field of characteristic ≠ 2 or 3, it is of the form:

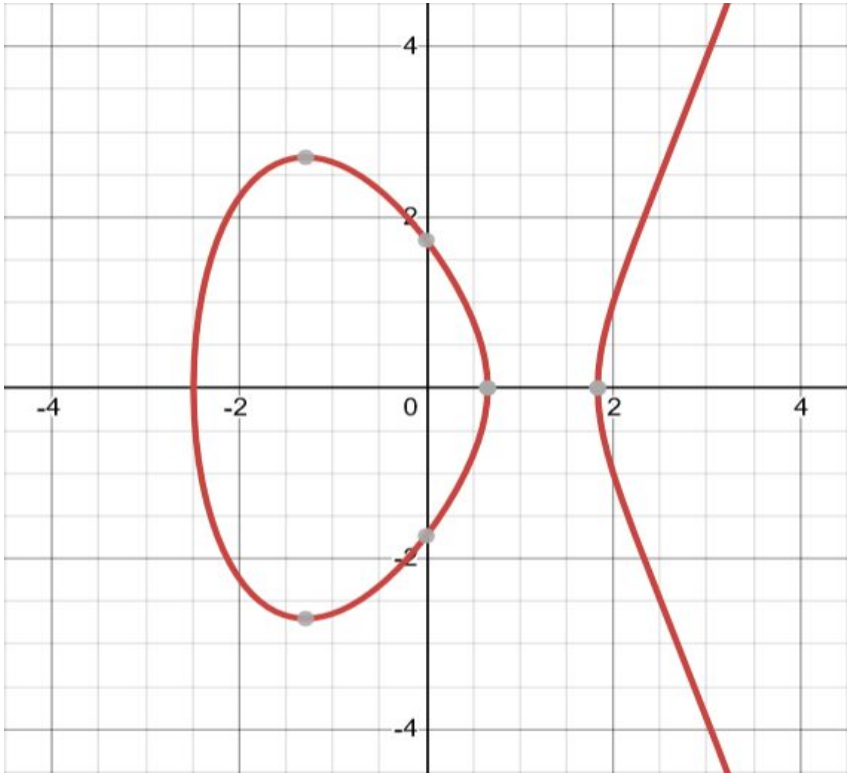
$$y^2 = x^3 + ax + b$$

Example curves:

Field = **R** (characteristic zero)



$y^2 = x^3 - 3x + 5$

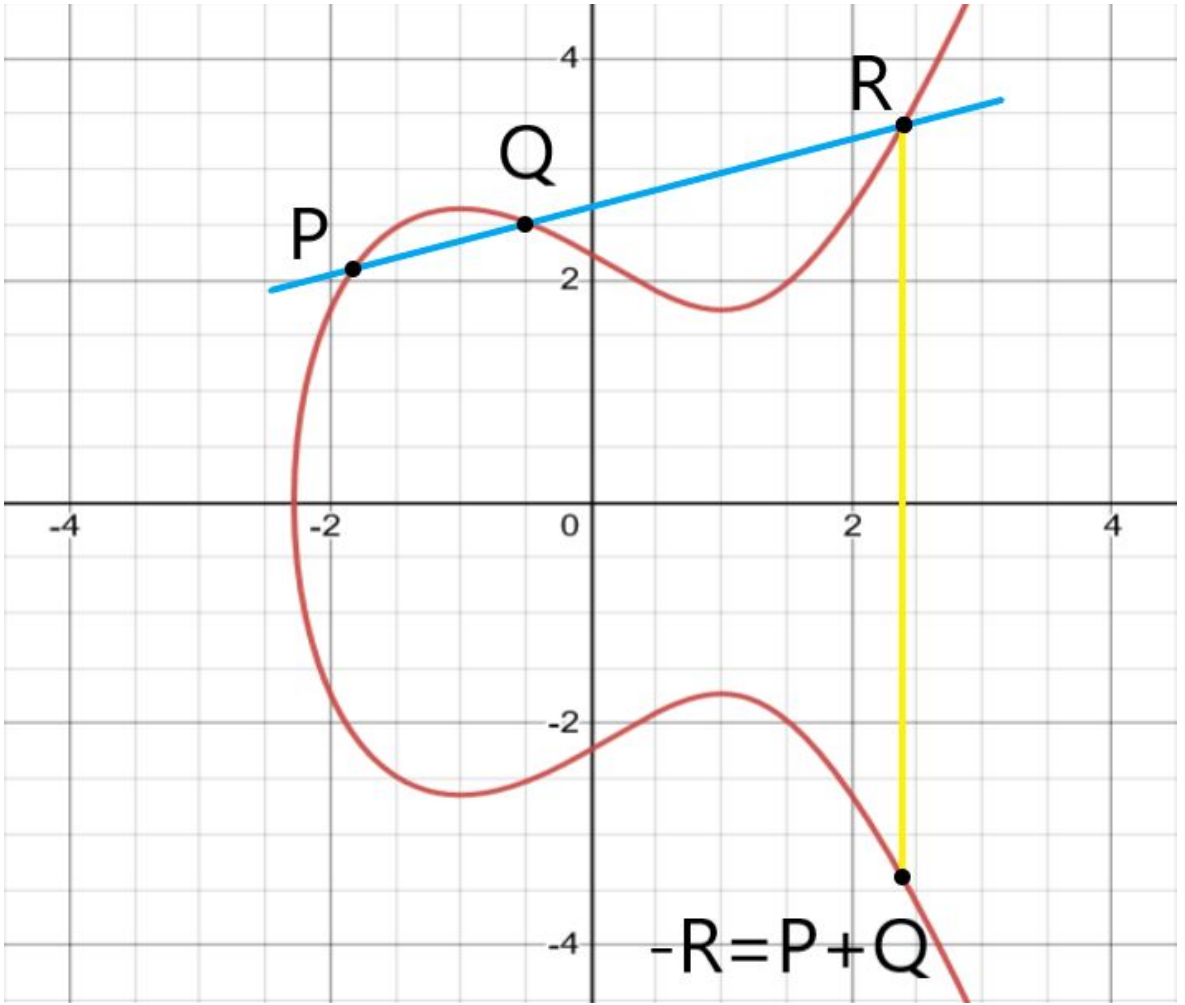


$y^2 = x^3 - 5x + 3$

Operations:

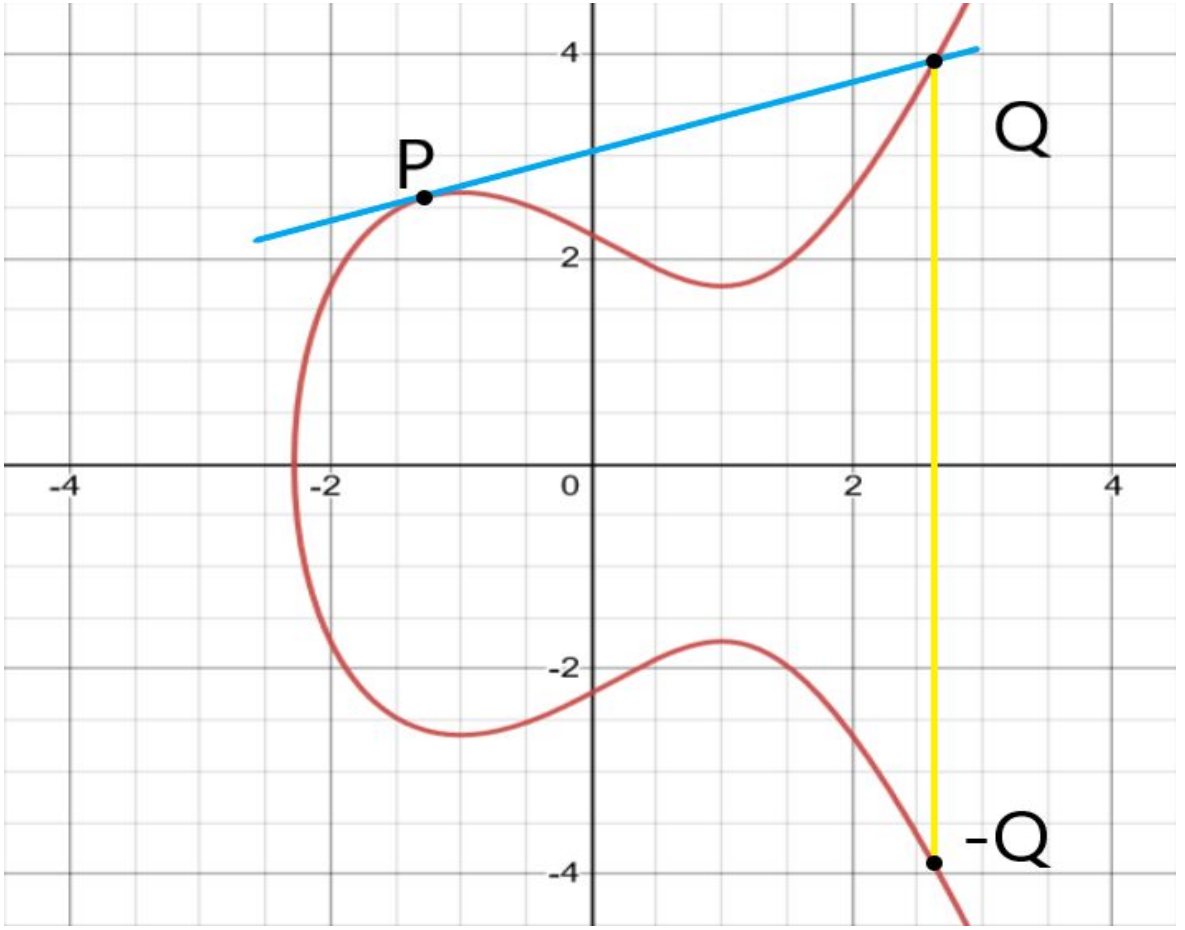
Adding 2 Points:

When the points are distinct



Adding 2 Points:

When the points are the same



We can calculate the coordinates of the sum using the following.

$$P + Q = R$$
$$(x_p, y_p) + (x_q, y_q) = (x_r, y_r)$$
$$\lambda = \frac{y_q - y_p}{x_q - x_p}$$
$$x_r = \lambda^2 - x_p - x_q$$
$$y_r = \lambda(x_p - x_r) - y_p$$

Also we define the point at infinity as identity.

$$\mathcal{O} + \mathcal{O} = \mathcal{O}$$
$$\mathcal{O} + P = P$$

Point Multiplication

- We define multiplication of a point by scalar as follows.

$$n \times P = P + P + \ldots\ldots + P \text{ (n times)}$$

- The set of points in the field K satisfying a given elliptic curve along with the point at infinity, together with the operation of point addition forms a group.

Security

- It is analogous to the asymmetry in calculating the product of two large primes p *x* q = n vs factorizing n into p *x* q.
- Given a scalar n we can find the point multiplication n x P of a point P, relatively easily using methods such as ‘Double and Add’
- Whereas given two points P and Q = n x P, it is nearly impossible to find n with anything better than brute force.

The usage in cryptography

Parameters

- The curve and the field it's defined on.
- A base point G from the curve

n = Order of G (n x G = O), n must be a large prime number.

The private key S_k is a number between 1 and n-1.

The public key is $P_k = S_k \times G$

To sign a message *m*

- Calculate e = HASH(m).
- Select a cryptographically secure k between *1* and *n-1*.
- Calculate $(x_1, y_1) = k \times G$.
- $r = x_1 \bmod n$. If $r = 0$, choose a different k.
- $s = k^{-1}(e + r S_k) \bmod n$. If $s = 0$, choose a different k.
- The pair (r , s) is the signature.

To Verify Signature

- Check, $P_k \neq O$, P_k lies in the curve and $n \times P_k = O$.
- Calculate e as previously done.
- Calculate $u_1 = es^{-1}$ mod n, and $u_2 = rs^{-1}$ mod n.
- Calculate C = $(x_2, y_2) = u_1 \times G + u_2 \times P_k$.
- Signature is valid if $x_2 \equiv r \bmod n$, invalid otherwise

Correctness of the algorithm

We have

$$C = u_1 \, x \, G + u_2 \, x \, P_k$$

$$= u_1 \, x \, G + u_2 S_k \text{ x G}$$

$$= (u_1 + u_2 S_k) \text{ x G}$$

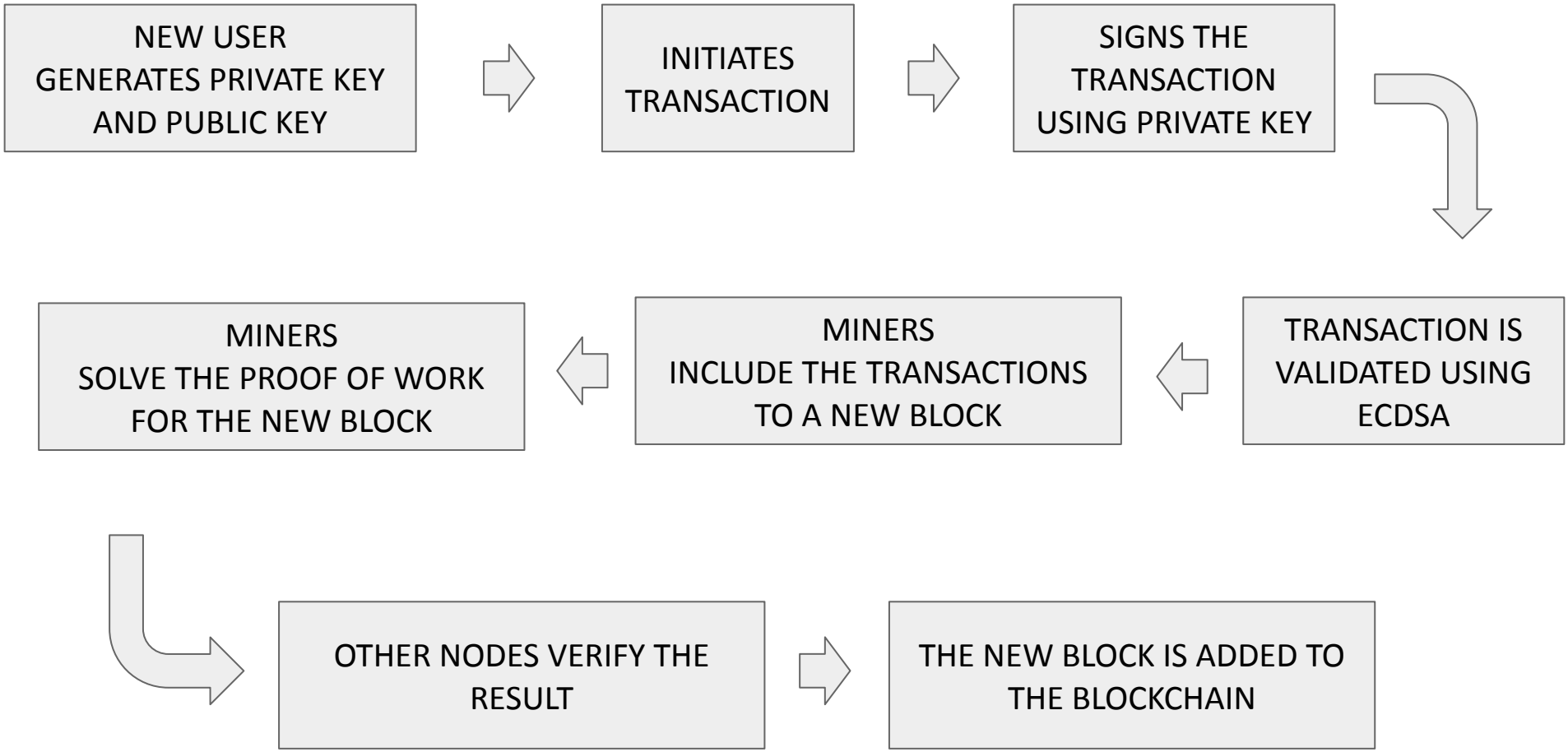
$$= (e s^{-1} + r s^{-1} \, S_k) \text{ x G}$$

$$= (e + r S_k) s^{-1} \text{x G}$$

$$= (e + r S_k)(e + r S_k)^{-1} k \text{ x G}$$

$$= k \text{ x G}$$

Quick Reference
$P_k = S_k$ x G
$(x_1, y_1) = k \, x \, G$
$r = x_1 \bmod n$
$s = k^{-1}(e + r \, S_k) \bmod n$
$u_1 = e s^{-1}$
$u_2 = r s^{-1}$


NEW USER
GENERATES PRIVATE KEY
AND PUBLIC KEY
INITIATES
TRANSACTION
SIGNS THE
TRANSACTION
USING PRIVATE KEY
TRANSACTION IS
VALIDATED USING
ECDSA
MINERS
INCLUDE THE TRANSACTIONS
TO A NEW BLOCK
MINERS
SOLVE THE PROOF OF WORK
FOR THE NEW BLOCK
OTHER NODES VERIFY THE
RESULT
THE NEW BLOCK IS ADDED TO
THE BLOCKCHAIN

References and Further Reading

You can play around with our implementation at: https://github.com/aakash-ramesh/crypto_redux
Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
Van Flymen, D. (2017). Learn blockchains by building one. The fastest way to learn how Blockchains work is to build one.
https://fangpenlin.com/posts/2019/10/07/elliptic-curve-cryptography-explained/
Daley, S. (2020, March 25). 25 blockchain applications & real-world use cases disrupting the status quo. Built In.
https://builtin.com/blockchain/blockchain-applications
3Blue1Brown. (2017, July 7). But how does bitcoin actually work? https://www.youtube.com/watch?v=bBC-nXj3Ng4
WIRED. (2017, November 28). Blockchain Expert Explains One Concept in 5 Levels of Difficulty | WIRED.
https://www.youtube.com/watch?v=bBC-nXj3Ng4
https://economictimes.indiatimes.com/markets/forex/crypto-dogecoin-soaring-crashes-robinhood-token-trading/articleshow/82391415.cms
https://gadgets.ndtv.com/finance/dogecoin-price-in-india-today-inr
https://fangpenlin.com/posts/2019/10/07/elliptic-curve-cryptography-explained/
https://www.investopedia.com/tech/how-does-bitcoin-mining-work/
https://blog.goodaudience.com/blockchain-for-beginners-what-is-blockchain-519db8c6677a
https://www.geeksforgeeks.org/blockchain-technology-introduction