



Haryana Police
(सेवा - सुरक्षा - सहयोग)

हरसमय
Citizen Portal of Haryana Police

9th Batch Gurugram Police Cyber Security Summer Internship 2021 (Online)

Cryptocurrency Technology & **INVESTIGATIONS**

OverView

ATTEMPT ^{To} simply
Understand

Session By

Anupam Tiwari | 05 July 2021 0900 - 1100h

ONSET®

ReQUEST®

Important

POINTS

Just avoid distractions from Social media notifications during the session

&



The capacity to learn is a gift; the ability to learn is a skill; the willingness to learn is a choice.

ALSO

Please Note!

Though I will be **Slow & Deliberate** on major slides,
but still there will be **SLIDES** that **few participants**
may not immediately **ASSIMILATE....but my**
endeavor is to keep it SIMPLE

But take it as part of
LEARNING CURVE.....

Don't worry about it

It Takes
Time

please Note!

I WILL RUSH THROUGH FEW SLIDES & DELIBERATE ON FEW

The slides I rush are **respective take off points** for interested participants to explore and know more

FOR AUDIENCE RETENTION,SLIDES ARE
**GRAPHIC INTENSIVE FROM OPEN DOMAIN IN
GOOGLE SEARCH**

Scribble & think



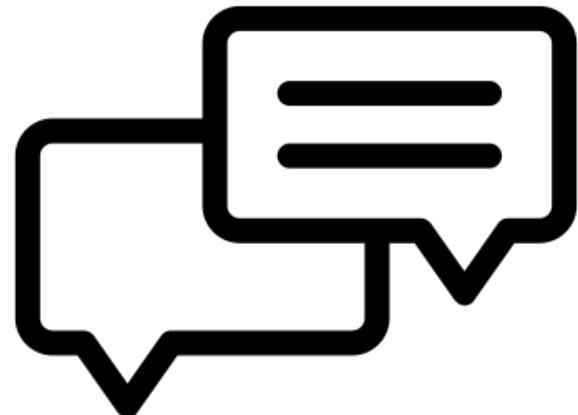
Screenshot

JUSTNOTEIT





**May be posted in CHAT
WINDOW...I will attempt
to answer them all at
the end....**



Or else E-MAIL clarifications: anupam@pm.me

NOT included



INVESTMENT ADVICE

TECHNOLOGY INTERNALS

focus

BLOCK CHAIN
CRYPTOCURRENCY

CRIME+
INVESTI-
GATION

PURPOSE OF TODAY's WEBINAR

Certainly not



with technology &



PURPOSE OF TODAY's WEBINAR

ACQUAINT YOU OF **BLOCKCHAIN & CRYPTOCURRENCY**
TECHNOLOGY

BLOCKCHAIN FOUNDATION BASICS

BRIEF DISCUSSION ON BACKEND WORKINGS & INTERNALS

INVESTIGATIONS & USE CASES



CRYPTOCURRENCY TECHNOLOGY & INVESTIGATIONS

relation ▶between

Bitcoin
vs
Blockchain

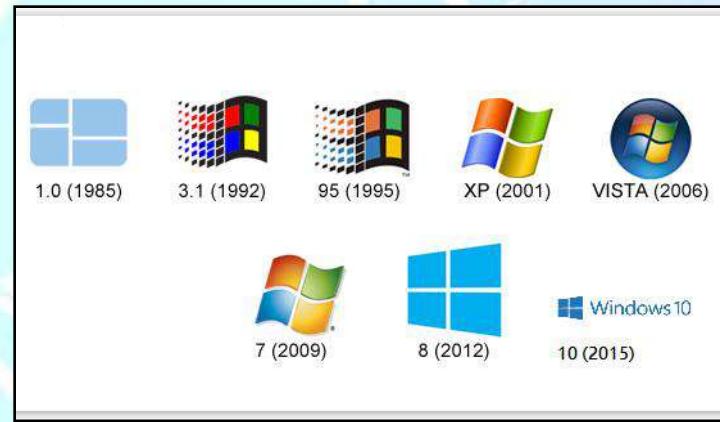


just like



Microsoft Word

**IS AN
APPLICATION OF**



BITCOIN IS AN APPLICATION ON BLOCKCHAIN TECHNOLOGY

**SIMPLE
as that!**

BLOCKCHAIN



**BLOCKCHAIN IS AN ECOSYSTEM OF
MULTIPLE TECHNOLOGIES**



**PLEASE DON'T THINK IT AS A SOFTWARE
WHICH YOU CAN DOWNLOAD, INSTALL
AND IMPLEMENT IN FEW HOURS/DAYS**

In the course of presentation ahead,
Term **BITCOIN** is an application and the
backend technology is **BLOCKCHAIN**

If you understand **BITCOIN** technology,
you will grasp and co-relate other
blockchain applications with much **EASE**



BLOCKCHAIN TECHNOLOGY

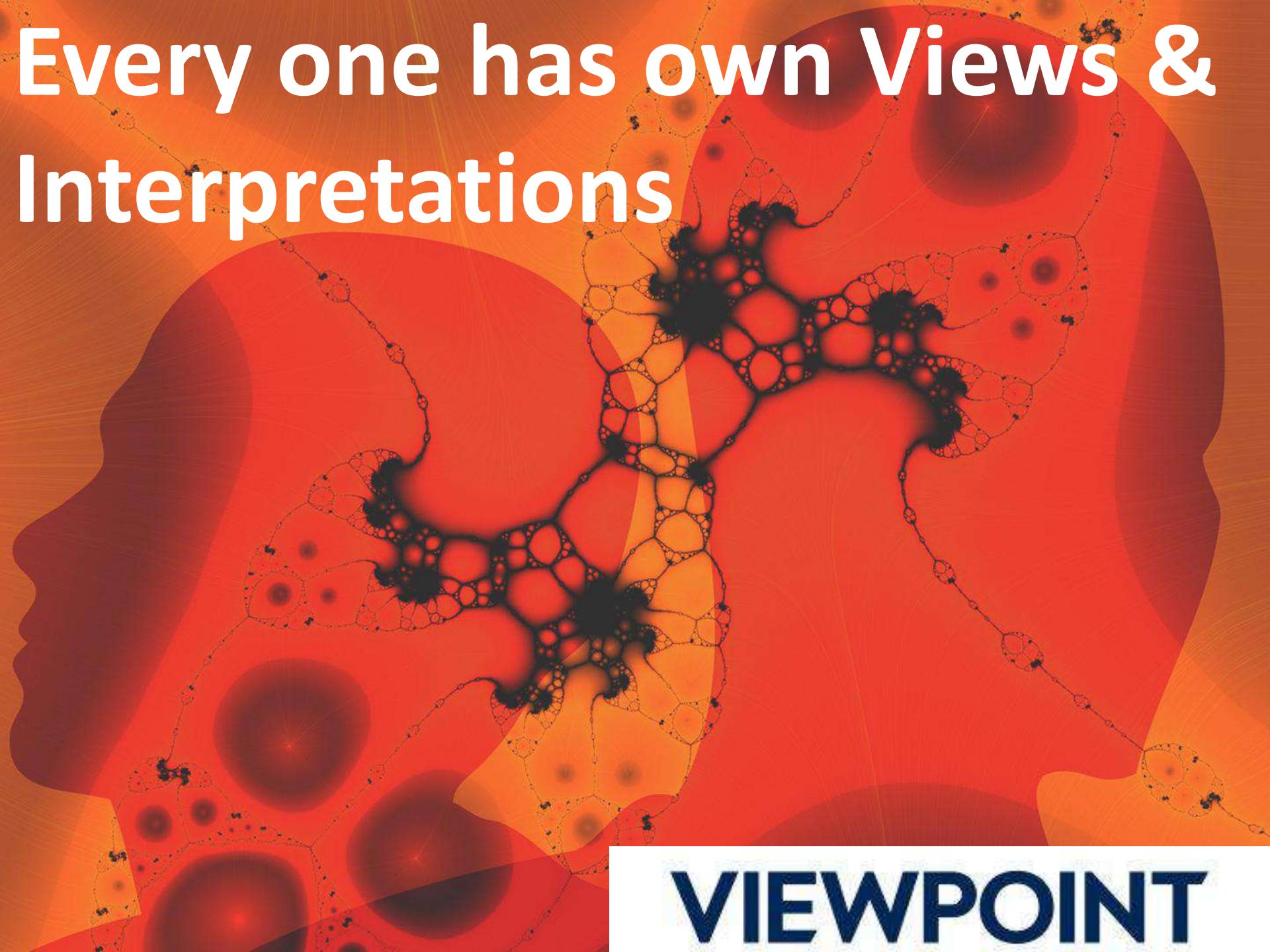
DRIVING BITCOIN SINCE 2009

NONSTOP

P u r p o s e

OF  *bitcoin* ?



A vibrant, abstract fractal pattern serves as the background. It features a complex, branching structure of interconnected circles and lines, primarily in shades of red, orange, and yellow. The pattern is dense in the center and becomes more sparse towards the edges, creating a sense of depth and organic complexity.

Every one has own Views & Interpretations

VIEWPOINT

investor

**HOW TO
BECOME
RICH**

Technologist

$$f(\omega) = \int_{-\infty}^{\infty} f(x) e^{-j2\pi\omega x} dx \quad \frac{dt}{d\omega}$$

$$\mathcal{F} = \oint E_{ext}$$

$$\nabla \cdot E = 0 \quad \nabla \times E = -\frac{1}{c} \frac{\partial H}{\partial t} \quad \nabla \cdot H = 0 \quad \nabla \times H = \frac{1}{c} \frac{\partial E}{\partial t}$$

$$(-i\hbar \frac{\partial}{\partial t}) \Psi = H \Psi$$

$$\rho \left(\frac{\partial v}{\partial t} + v \cdot \nabla v \right) = -\nabla p + \nabla \cdot T + f$$

$$H = -\sum_{i=1}^n p(x_i) \log p(x_i)$$

$$\frac{1}{2} G^2 S^2 \frac{\partial^2 V}{\partial S^2} + r S \frac{\partial V}{\partial S} + \frac{\partial V}{\partial t} - r \cdot V = 0$$

$$+ \sum_{i=1}^n \frac{q_i}{2} M_i^M + C_s \frac{D}{Q} + C_0 D +$$

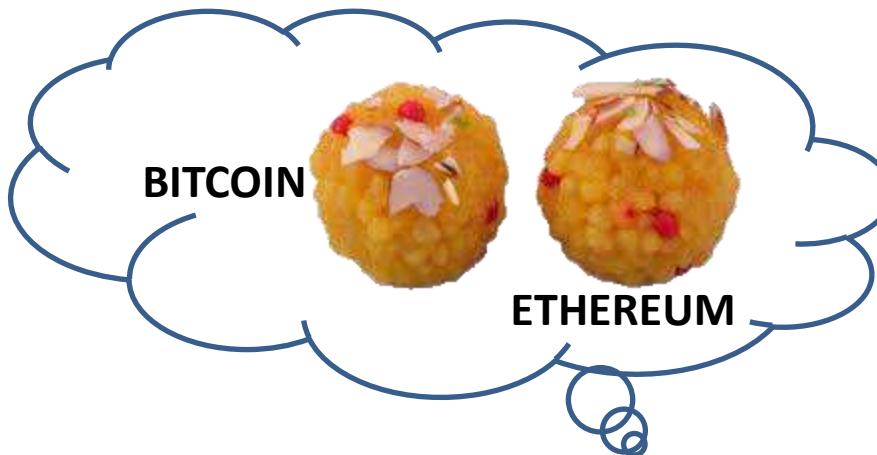
$$+ \frac{Q(p-D)}{2p} M^M + F_0 N +$$

$$+ F_0 N + \sum_{i=1}^n D_i w_i d_i \frac{(1+\omega)}{F_r}$$

$$TC(Q, q_i, m_i) = \sum_{i=1}^n \left[\frac{D_i}{m_i q_i} S_i + C_i D_i + \frac{q_i M_i}{2} \left(m_i \left(1 - \frac{D_i}{P_i} \right) - 1 + 2 \frac{D_i}{P_i} \right) \right] +$$

$$\begin{bmatrix} \frac{d \Delta_P(s, \phi)}{d \phi} \\ \frac{d \Delta_M(s, \phi)}{d \phi} \end{bmatrix} = \begin{bmatrix} J & -L \\ -B & O \end{bmatrix} \begin{bmatrix} \Delta_P(s, \phi) \\ \Delta_M(s, \phi) \end{bmatrix}$$

$$\int_0^{\frac{\pi}{2}} (\log \sin x)^2 dx - \int_0^{\frac{\pi}{2}} (\log \cos x)^2 dx = \frac{\pi}{2} \left\{ \frac{\pi^2}{12} + (\log 2)^2 \right\}$$



Despite RBI warning, 2,500 Indians investing in Bitcoins daily. Here is all you should know about its usage & dangers

In recent cyber attacks, "ransomware" hackers held victims hostage by encrypting their data and demanding them to send bitcoins to regain access to their computers.



Indians invest billions in Bitcoin, Dogecoin, Ether despite RBI's concerns on crypto



3 min read . Updated: 28 Jun 2021, 08:53 AM IST

Bloomberg

- RBI says it has 'major concerns' about the asset class and six months ago the government proposed a ban on trading in digital coins
- In India, where households own more than 25,000 tonnes of gold, investments in crypto grew from about \$200 million to nearly \$40 billion in the past year

<https://www.livemint.com/market/cryptocurrency/indians-invest-billions-in-bitcoin-dogecoin-ether-despite-rbi-s-concerns-on-crypto-11624849781875.html>

Bitcoin craze! Indians invested \$40 bn in crypto last year

Some investors are also concerned about the lack of taxation rules for cryptocurrencies. One investor said that with no income tax rules at present, he is worried about retrospective tax and even raids

Crypto Investments in India Gain Significant Traction Despite Regulatory Uncertainty



Crypto Investments in India Have Risen By 19,900% in a Year

By Connor Sephton Published on: June 28, 2021

<https://news.bitcoin.com/indians-hold-40-billion-in-cryptocurrency-report-suggests/>

<https://coinmarketcap.com/alexandria/article/crypto-investments-in-india-have-risen-by-19-900-in-a-year>

Multinational Corporation

WELCOME
TO THE
FUTURE



सत्यमेव जयते

Government Of India

views





FEW SCREENSHOTS *Ahead....*



Bitcoin is not legal tender in India: finance ministry

The Ministry of Finance G

Last Published: Thu, Jan 04 2018

Virtual currencies are not backed by government fiat

India's Supreme Court Prods Government on Bitcoin Regulation

India: Government to Consider Allowing Crypto Tokens, But Not Cryptocurrencies

Blockchain This Week: TRAI Seeks Blockchain Support, Indian Govt To Power 50 Mn Rural Jobs With



Government lists bill to ban Bitcoin in India, create official digital currency

RBI plans its own cryptocurrency, proposed crypto law may ban Bitcoins and Dogecoins in India

Major concerns about crypto currencies conveyed to govt: RBI governor

...regular earlier this week that clarified banks can no longer cite its circular customers

This co
on cry

BUSINESS

Future of cryptocurrency in India continues to hang in the balance



Blockchain This Week: PM Endorses Blockchain, Calls It An Opportunity & More

Modi govt may set new panel for Cryptocurrency. Will regulation help Bitcoin, Dogecoin and other investors?

Can Modi govt please make up its mind on Bitcoin and cryptocurrencies

Nobody is asking New Delhi to make Bitcoin legal tender or accept tax payments in it. Just a little tolerance of cryptocurrencies will be enough.



India's government wants to kill bitcoin, but it loves blockchain

By Ananya Bhattacharya • February 2, 2018

Blockchain Foundation of India

EDITOR'S PICK | 31,250 views | Mar 5, 2018, 02:13am

This Indian City Is Embracing BlockChain Technology -- Here's Why

INDUSTRY

Hyderabad may house first government blockchain centre

STEPHEN DEMEULENAERE 09 JULY, 2018 10:09 IST

NEW DELHI, JUNE 28, 2018 22:45 IST

UPDATED: JUNE 28, 2018 22:47 IST

BLOCKCHAIN CAN BE USED TO FIGHT CORRUPTION, INCREASE TRANSPARENCY IN GOVT PROJECTS



PM Modi Pitches For Usage Of AI and Blockchain In Agriculture



Dipen Pradhan

Inc42 Staff

21 May '18 • 4 min read

SHARE STORY

243
SHARES



Blockchain Will Check Mischievous Acts Of Middlemen
And Harvest Will Not Go To Waste, Says Modi



Home | Internet | Internet News | PM Modi Says AI, Blockchain Will Change the Nature of Jobs

PM Modi Says AI, Blockchain Will Change the Nature of Jobs

Press Trust of India, 12 October 2018

[Share on Facebook](#)

[Tweet](#)

[Share](#)

[Email](#)

[Reddit](#)

[comment](#)



Prime Minister Narendra Modi Thursday allayed fears of job loss due to technological development, saying artificial intelligence, blockchain, and other technologies will change the nature of employment and provide more opportunities.

Speaking at the launch of the World Economic Forum (WEF) Centre for the Fourth Industrial Revolution, PM



HOME RESOURCE LIST CRYPTO NEWS CRYPTOCURRENCY BITCOIN MINING BLOCKCHAIN ICO EVI

INTERVIEWS

India's Prime Minister Narendra Modi Appraises Blockchain Technology, AI & ML

by Arshmeet Hora | Oct 13, 2018 | Blockchain, Cryptocurrency News

Advertisement



Using blockchain to make land registry more reliable in India

OPINIONS

How Andhra Pradesh Is Emerging As India's Blockchain Hub

Can blockchain solve land record problems?

While blockchain could ensure the integrity and indisputability of future changes, it cannot exist in isolation.

NITI Aayog to recommend use of blockchain in land records, PDS, healthcare

A study by a group of NITI Aayog officials will act as a framework for the central ministries and states for the adoption of the technology.

Maharashtra to roll out blockchain technology for land deals



Part 1
January 2020



सत्यमेव जयते
NITI Aayog

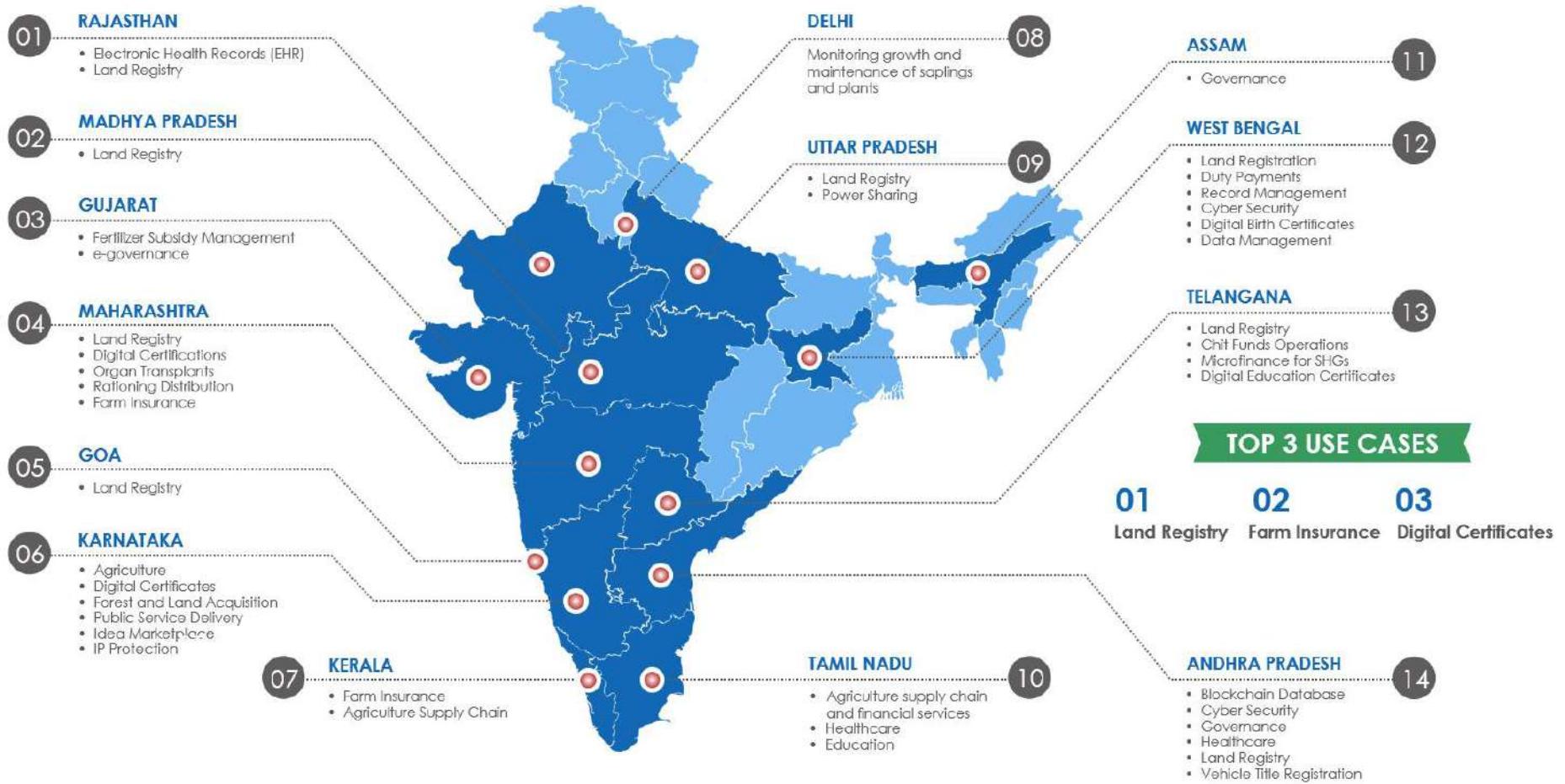
<https://niti.gov.in/node/1056>

BLOCKCHAIN: THE INDIA STRATEGY

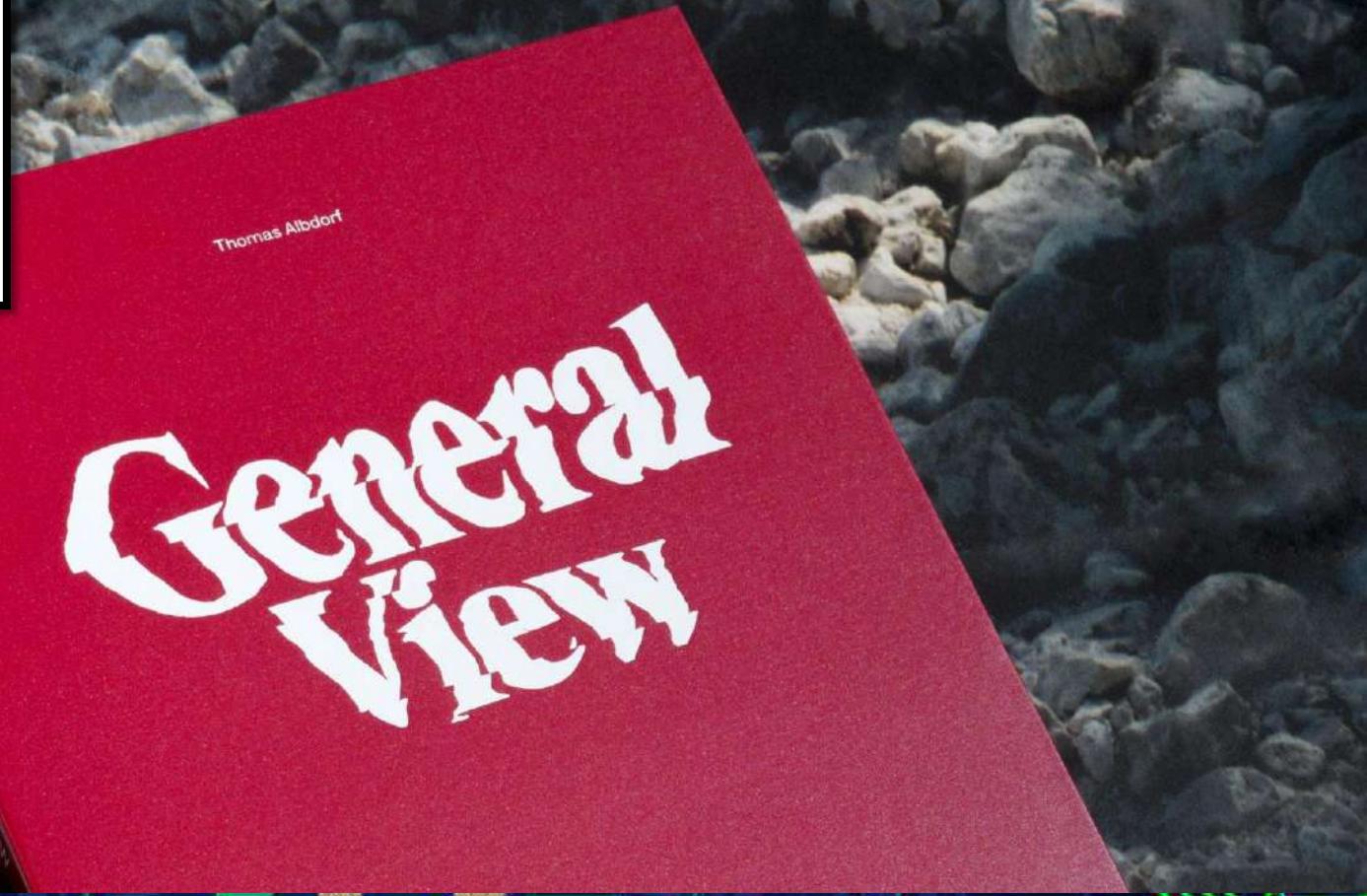
Towards Enabling Ease of Business, Ease of Living, and Ease of Governance



About 50% of the states in India are involved in blockchain related initiatives, driving the public sector blockchain adoption in the country



But!



CRYPTOCURRENCY





CYBERCRIME



... Bitcoin is only used about 10% for crime according to the DEA

Although there's still a lingering misperception that Bitcoin is used primarily for illicit transactions on darknet markets, this myth was recently **dispelled** by a special agent from the US Drug Enforcement Agency (DEA).

According to the Cyber Investigative Task Force, an inter-agency collaboration involving the DEA, FBI, and ATF, 90% or more of Bitcoin volume is entirely unrelated to drug purchases. The peak of Bitcoin's usage for darknet trades occurred between 2011 and 2012.



2021

Jan 19, 2021, 09:37pm EST | 32,097 views

The False Narrative Of Bitcoin's Role In Illicit Activity



Hailey Lennon Contributor

Crypto & Blockchain

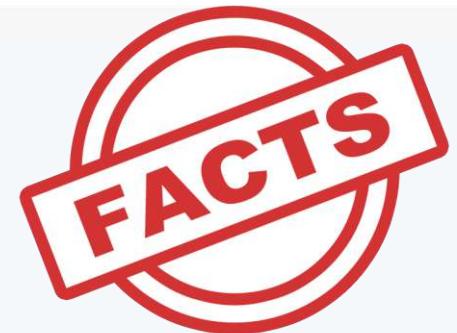
Follow

Crypto-crime & caveats

Paul Marrinan Head of Investigations / Inca Digital

29 Mar 2021

"In 2020, the illicit share of all cryptocurrency activity fell to just 0.34%," reported **Chainalysis** in their second annual crypto-crime report; **CipherTrace** also estimated that figure to be "less than 0.5%." Importantly, Chainalysis and CipherTrace – both industry-



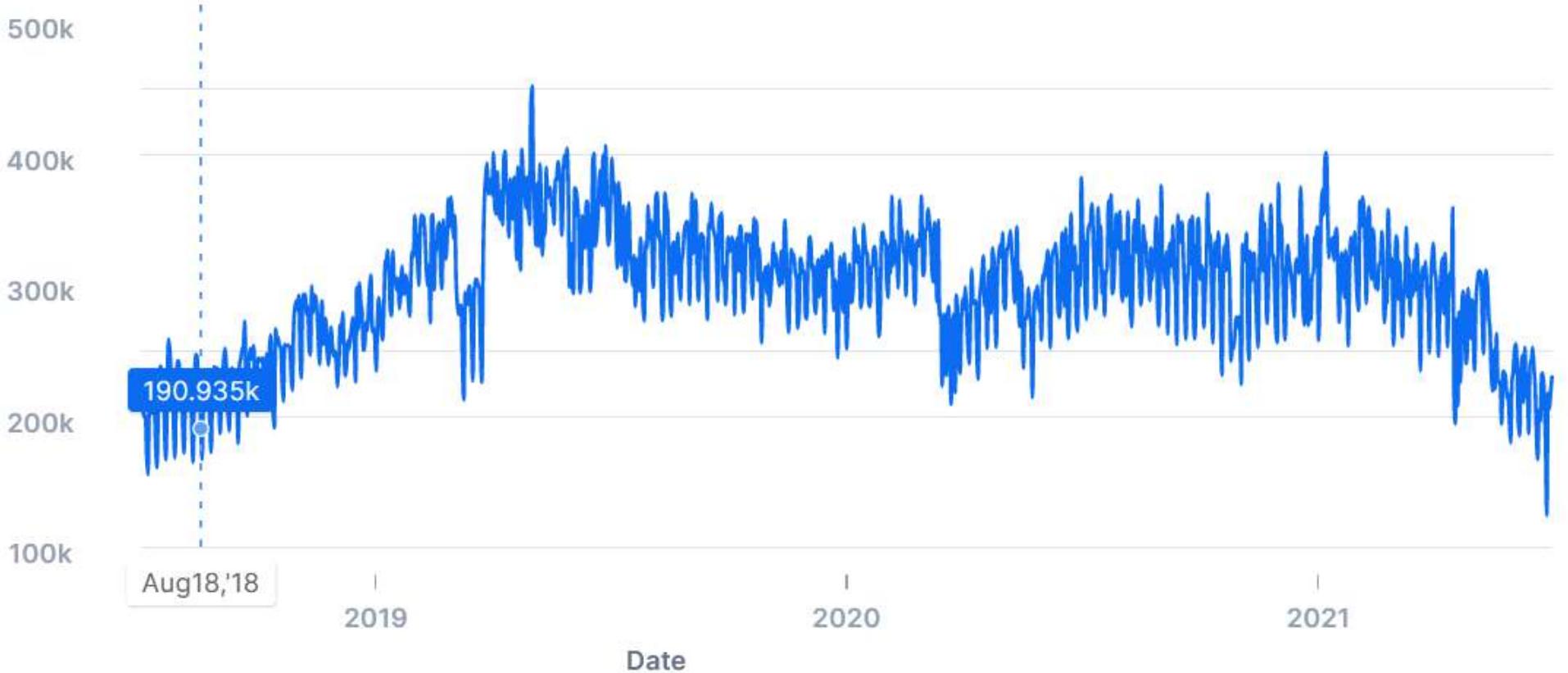
TRANSACTIONS PER DAY

The number of bitcoin transactions in the last 24 hours.

3 5 1 4 6 7

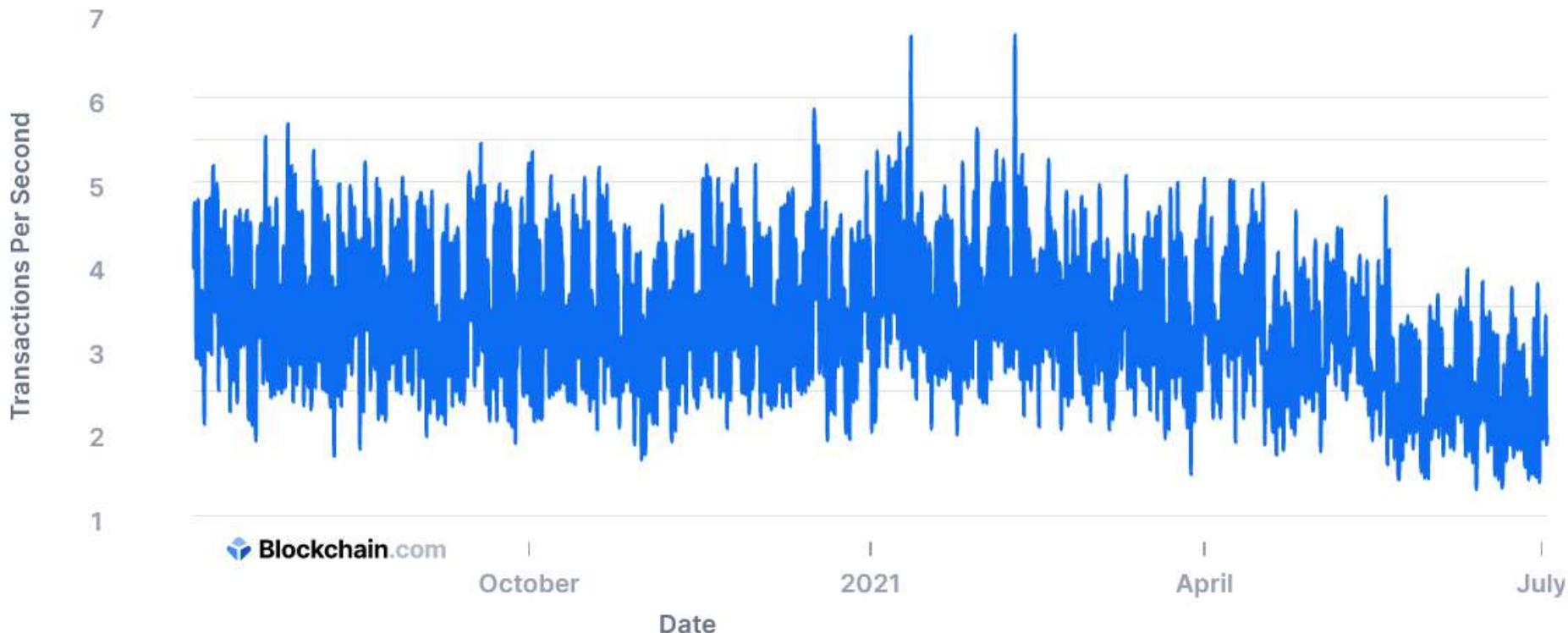
SOURCE : <https://blockchain.info/charts/n-transactions>

TRANSACTIONS PER DAY



Transaction Rate Per Second

The number of transactions added to the mempool per second.



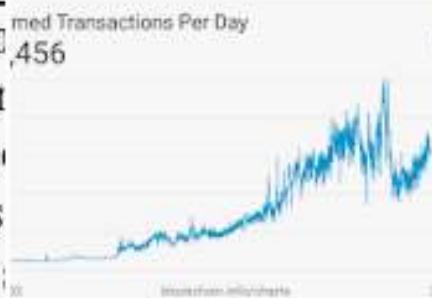
30 Days | 60 Days | 180 Days | **1 Year** | 3 Years | All Time

Raw Values | 7 Day Average | **30 Day Average**

Transactions per second

transaction per second

- 1 to 4 transactions per second
- 10 transactions per second
- 93 transactions per second
- 1,667 transaction per second



around 1,700 transactions per second

Visa does around 1,700 **transactions per second** on average (based on a calculation derived from the official claim of over 150 million **transactions per day**). The potential for adoption is there but is bottlenecked currently by scalability.

<https://towardsdatascience.com/the-blockchain-scalability-problem-and-the-race-for-visa-like-scalability-933e0f3a23>

[The Blockchain Scalability Problem & the Race for Visa-Like ...](#)

READ: “LIGHTNING NETWORK”...explore and know....

Major characteristics of Blockchain



DECENTRALIZATION



TRANSPARENCY



IMMUTABILITY



NEUTRALITY



OPEN-ACCESS



**actual
intent**



bitcoin



**CRYPTOCURRENCY IS AN ATTEMPT
TO BRING BACK A DECENTRALISED
CURRENCY OF PEOPLE, ONE THAT IS NOT
SUBJECT TO INFLATIONARY MOVES BY
A CENTRAL BANK**





CRYPTOCURRENCY IS AN ATTEMPT
TO BRING BACK A DECENTRALISED
CURRENCY OWNED BY PEOPLE ONE THAT IS NOT
SUBJECT TO GOVERNMENTAL MOVES BY
A CENTRAL BANK



इसका मतलब
क्या है सर ?



No
Government
& other

Intervention ➤ **between**



GOVERNMENT



**THIRD
PARTY
VENDORS**

WE ACCEPT

VISA

**VISA
Electron**

Maestro



PayPal

JCB

100% GUARANTEED SECURE SHOPPING



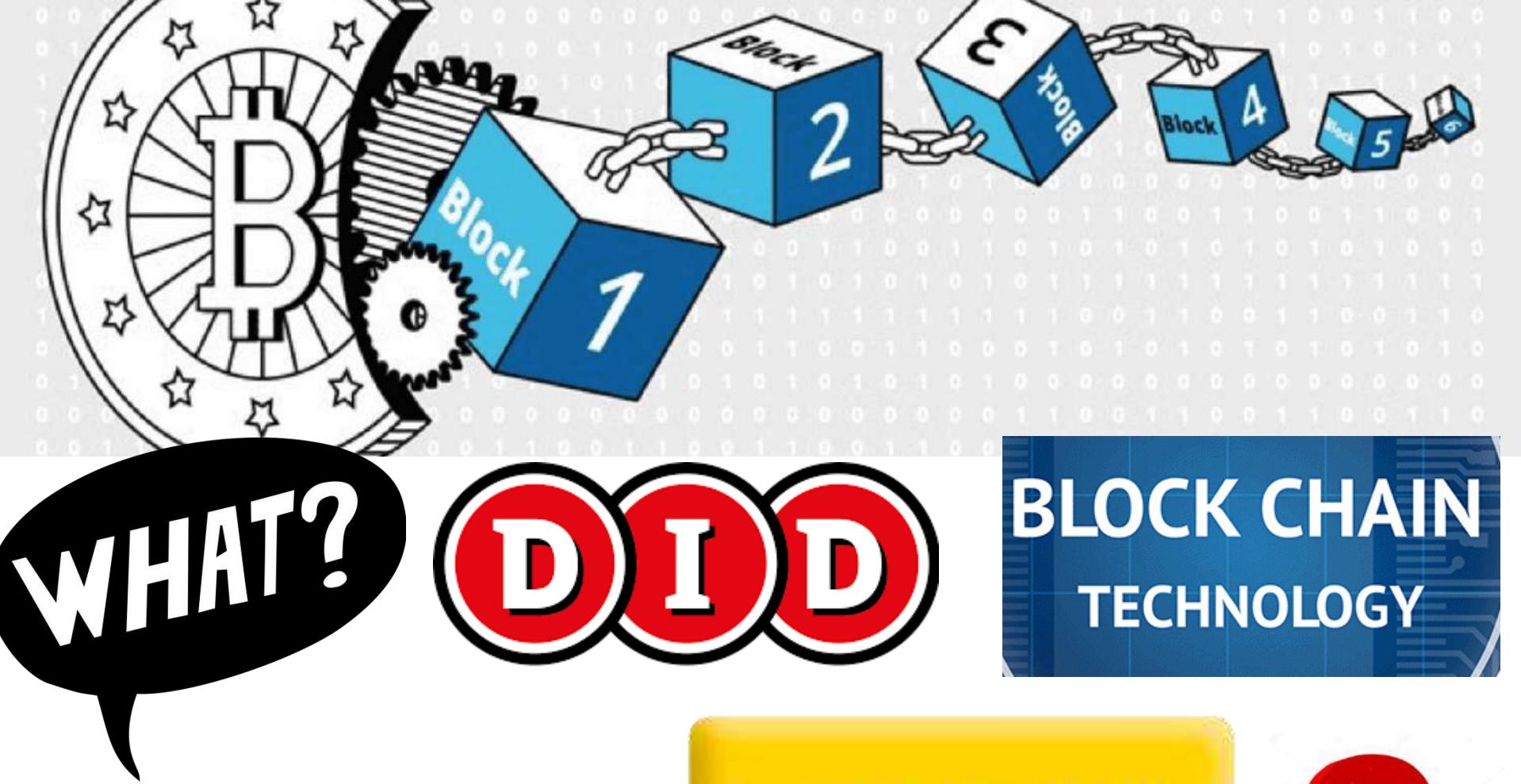
**MasterCard.
SecureCode**

**Verified by
VISA**

**YOU ARE UNDER
SURVEILLANCE**

PRIVACY

**WHO IS
WATCHING?**



ACHIEVE



NEGATION



MIDDLEMEN

WHAT DOES THE MIDDLE MEN DO?



MIDDLE MEN

LET'S TAKE EXAMPLE OF BANKS



PURPOSE OF BANK

Primary functions

Acceptance of Deposits

Providing loans and advances

Credit Creation

Secondary functions

Acts as an Agent

Overdraft facility

Discounting bill of exchange

Provides Locker facility

Issues Traveller cheque

PURPOSE OF BANK

Primary functions

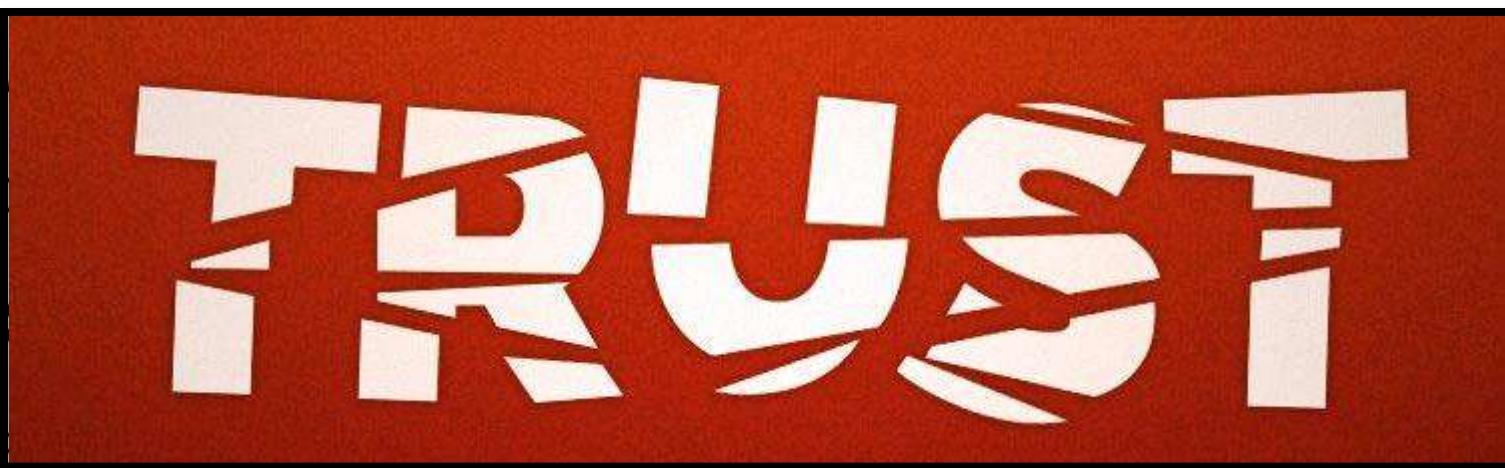
Acceptance of Deposits

Prov

Cred

Sec

Act



Overdraft facility

Discounting bill of exchange

Provides Locker facility

Issues Traveller cheque

**IF THIS TRUST BY “BANK”
IS REPLACED WITH AN
“ALGORITHM”**

IMPORTANT HISTORY

in **BRIEF**

Bitcoin and
The History of Money

1982

In 1982, **David Chaum**, a computer scientist, and cryptographer proposed a scheme that **used blind signatures to build untraceable digital currency**. This research was published in a research paper, Blind Signatures for Untraceable Payments.

<http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF>

The limitation of this scheme was that **the bank had to keep track of all used serial numbers**. This was a central system by design and required to be trusted by the users.

1988



David Chaum and others proposed a refined version named e-cash that not only used a blinded signature, **but also some private identification data to craft a message** that was then sent to the bank.

<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.26.5759>

Allowed the detection of double spending but did not prevent it

1997

Adam Back, a cryptographer introduced hashcash, proposed to thwart email spam. The idea behind hashcash was to solve a computational puzzle that was easy to verify but comparatively difficult to compute. **The idea was that for a single user and a single email, the extra computational effort was negligible, but someone sending a large number of spam emails would be discouraged as the time and resources required to run the spam campaign would increase substantially.**

1998

B-money was proposed by **Wei Dai**, a computer engineer introduced the idea of using Proof of Work (PoW) to create money. It was referred in the paper as solution to a previously unsolved computational problem. This concept is similar to PoW, where money is created by broadcasting a solution to a previously unsolved computational problem.

<http://www.weidai.com/bmoney.txt>

AND THEN IN “2008” THE MAGIC HAPPENED

INFORM
TECH
WWW
SOCIAL MEDIA
SERVICES
BIG DATA
CONTENT
TARGET
CONSUMER
ORGANIZATION
SOCIAL COMPUTER
CONSUMER DEMAND
WEB MARKETING
MULTIMEDIA
NETWORK
PROJECTS
APPS
STATISTICS
BRANDS
SOLUTIONS
BUSINESS
WEB SERVICES
BUZZ
DATA
VISION
ENGINEERING
WEB DEV
SERVICE
BIG
STRATEGY
WORLDWIDE
RESEARCH
COM
PLANNING
ORGANIZATION

DISRUPTIVE TECHNOLOGY



Why huge acceptance to BITCOIN ?

Bitcoin wouldn't be this WIDESPREAD if it didn't solve real problems for real people

Bitcoin solves SEVERAL PROBLEMS inherent to the traditional financial system



Problems with **MONEY** erstwhile to BITCOIN revolution



PROBLEMS WITH MONEY ERSTWHILE TO BITCOIN ARRIVAL

SEGREGATION

People with bank accounts and access to banking services such as online payments or loans are privileged. According to the World Bank, about 28% of the world's population doesn't have a bank account and many people are still stuck in a cash-only environment

Problems with money today

SEGREGATION

Without a bank account and basic banking services, such as online payments, people can't expand their businesses outside their local communities.

A merchant won't be able to offer goods or services on the internet to increase its customer base

Problems with money today

SEGREGATION

Segregation between banked people and unbanked people is driven by several factors

- Banking services **TOO EXPENSIVE** for some people
- One needs **DOCUMENTATION** that many people don't have
- Banking services can be denied to people with certain **political** views or those conducting certain **businesses** or **ethnicity, nationality, sexual preferences, or skin color**

Problems with money today

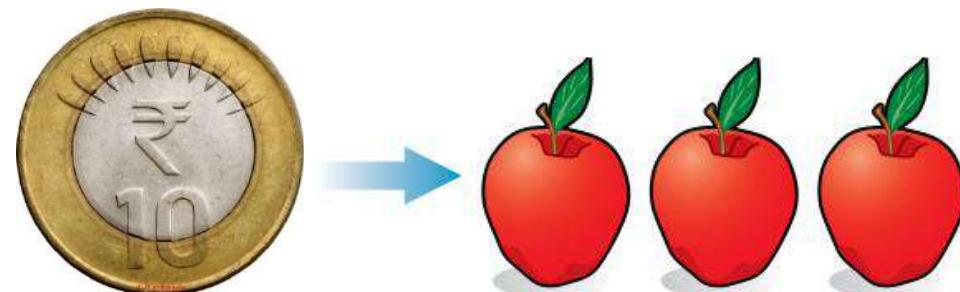
privacy

- Trace payments
- Censor payments
- Freeze funds
- Seize funds

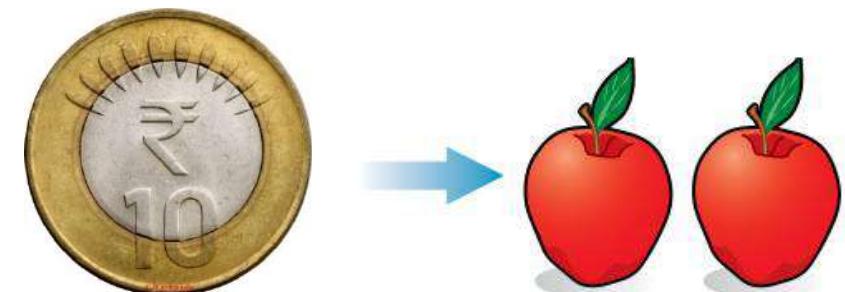
Problems with money today



Today



Tomorrow



Problems with money today



Extreme cases of inflation like this are called HYPERINFLATION

Governments sometimes increase the money supply to EXTRACT VALUE FROM THE POPULATION and pay for expenses such as the NATIONAL DEBT, warfare, or welfare making HYPERINFLATION is apparent

Problems with money today



Most currencies are subject to inflation, some more than others. For example, the Zimbabwean dollar inflated nearly $10^{23}\%$ from 2007–08, peaking at 80 billion percent per month during a few months in 2008. That's an average daily inflation with PRICES DOUBLED EVERY DAY

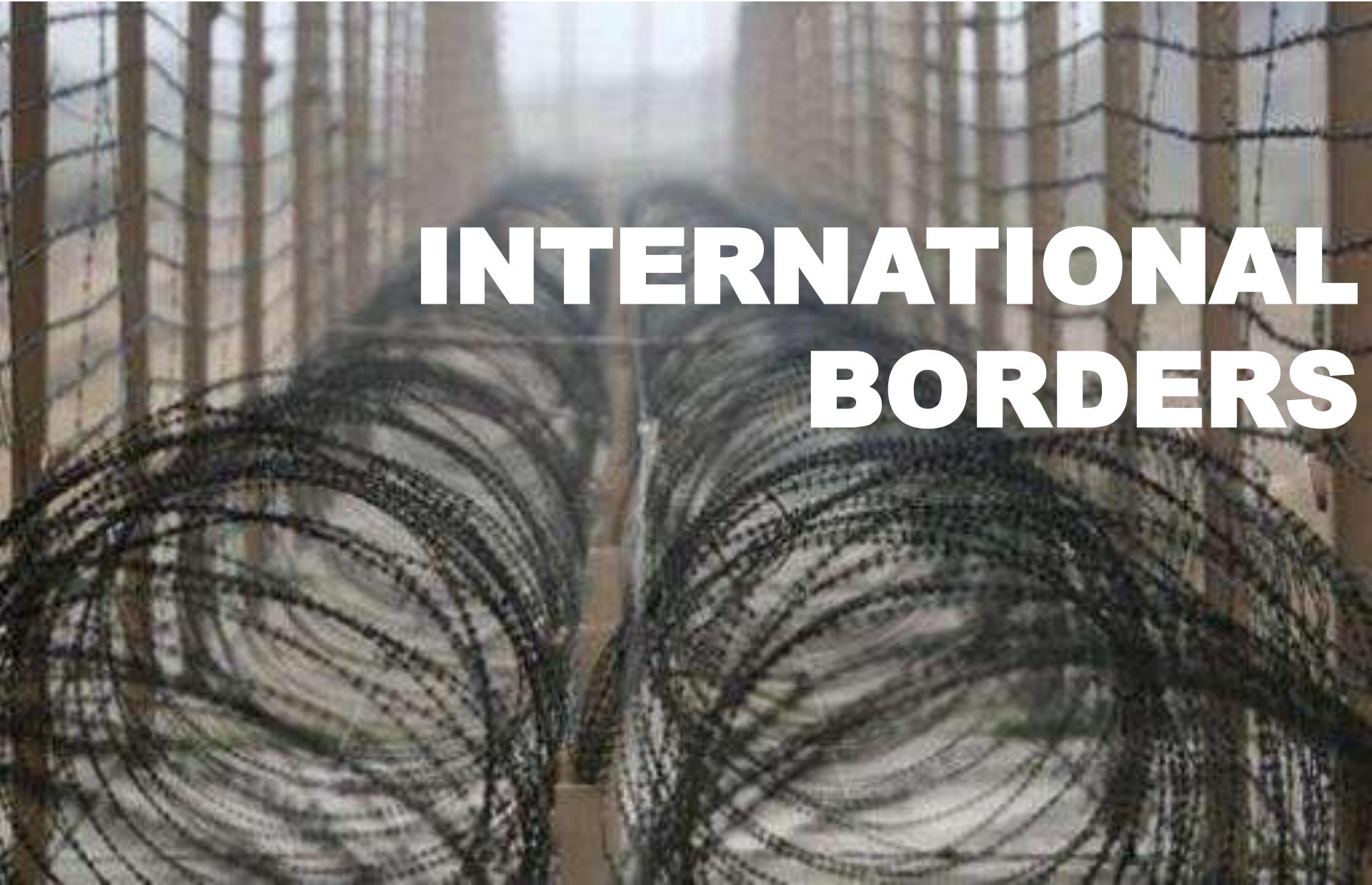
Problems with money today

INFLATION



Country	Year	Worst monthly inflation (%)
Zimbabwe	2007–2008	4.19×10^{16}
Yugoslavia	1992–1994	313×10^6
Peru	1990	397
Ukraine	1992–1994	285
Venezuela	2012–	120

Problems with money today



**INTERNATIONAL
BORDERS**

Problems with money today

INTERNATIONAL BORDERS

“Moving value across national borders using national, or fiat, currency is hard, expensive, and sometimes even forbidden. If you want to send **1,000 Swedish crowns (SEK) from Sweden to a person in the Philippines, you can use a service like Western Union for the transfer”**



A typical remittance recipient will be able to receive only cash, which doubles or triples the cost to 10.5% or 16.3%, depending on how quickly or conveniently they want it

FEES TABLE: EURO Example

THIS IS THE FEE TABLE

Track your transfer in **WU.COM**

RUMANIA, MOLDAVIA

Principal amount (€)	Money in Minutes ³ Transfer fee (€) ²
0.01 — 25.00	3.90
25.01 — 50.00	4.50
50.01 — 100.00	5.50
100.01 — 200.00	6.50
200.01 — 250.00	9.50
250.01 — 300.00	12.50
300.01 — 400.00	15.50
400.01 — 600.00	19.50
600.01 — 750.00	34.50
750.01 — 1 000.00	39.50
>1 000	49.50

BULGARIA

Principal amount (€)	Money in Minutes ³ Transfer fee (€) ²
0.01 — 25.00	3.90
25.01 — 50.00	4.90
50.01 — 100.00	5.90
100.01 — 200.00	6.90
200.01 — 250.00	9.90
250.01 — 300.00	12.90
300.01 — 400.00	16.00
400.01 — 500.00	20.00
500.01 — 600.00	35.00
600.01 — 700.00	38.00
700.01 — 800.00	43.00
800.01 — 900.00	45.00
900.01 — 1 000.00	49.00
1 000.01 — 1 100.00	52.00

MOROCCO

Principal amount (€)	Money in Minutes ³ Transfer fee (€) ²
0.01 — 500.00	3.90
500.01 — 1 000.00	7.90
1 000.01 — 2 000.00	10.90
2 000.01 — 3 000.00	18.90

MALI, SENEGAL

Principal amount (€)	Money in Minutes ³ Transfer fee (€) ²
0.01 — 50.00	3.90
50.01 — 100.00	5.90
100.01 — 250.00	6.90
250.01 — 500.00	11.90
500.01 — 1 000.00	18.90
1 000.01 — 2 000.00	35.90
2 000.01 — 3 000.00	43.90

PHILIPPINES

Principal amount (€)	Money in Minutes ³ Transfer fee (€) ²	Servicio 12 horas ³ Transfer fee (€) ²
0.01 — 25.00	4.90	3.90
25.01 — 50.00	5.90	3.90
50.01 — 500.00	6.90	4.90
500.01 — 1 000.00	8.90	5.90
1 000.01 — 1 500.00	10.90	6.90
1 500.01 — 2 000.00	11.90	8.90
2 000.01 — 3 000.00	13.90	10.90

CHINA

Principal amount (€)	Money in Minutes ³
0.01 — 50.00	3.90

ARGENTINA, BOLIVIA, BRASIL, COLOMBIA, ECUADOR, HONDURAS, NICARAGUA, PARAGUAY, PERU, DOMINICAN REPUBLIC

Principal amount (€)	Money in Minutes ³ Transfer fee (€) ²
0.01 — 3 000.00	4.90

CUBA

Principal amount (€)	Money in Minutes ³ Transfer fee (€) ²
0.01 — 500.00	4.90
500.01 — 1 000.00	6.90
1 000.01 — 2 000.00	9.90

CHILE, URUGUAY, REST LATIN AMERICA

Principal amount (€)	Money in Minutes ³ Transfer fee (€) ²
0.01 — 500.00	14.90
500.01 — 850.00	20.90
850.01 — 1 000.00	24.90
1 000.01 — 1 500.00	14.90
1 500.01 — 2 500.00	20.90
2 500.01 — 3 000.00	24.90

REST OF THE EUROPEAN ECONOMIC AREA¹

Principal amount (€)	Money in Minutes ³ Transfer fee (€) ²
0.01 — 85.00	11.90
85.01 — 165.00	16.90
165.01 — 300.00	19.90
300.01 — 325.00	23.90
325.01 — 400.00	28.90
400.01 — 610.00	31.90

RUSSIA

Principal amount (€)	Money in Minutes ³ Transfer fee (€) ²
0.01 — 100.00	8.75
100.01 — 200.00	13.90
200.01 — 300.00	15.90
300.01 — 500.00	22.90
500.01 — 850.00	28.90
850.01 — 1 000.00	39.90
1 000.01 — 1 500.00	49.90
1 500.01 — 2 500.00	59.90
300.01 — 325.00	23.90
325.01 — 400.00	28.90
400.01 — 610.00	31.90
610.01 — 815.00	35.90
815.01 — 1 000.00	42.90
1 000.01 — 1 220.00	46.90
1 220.01 — 1 435.00	59.90
1 435.01 — 1 625.00	65.90
1 625.01 — 2 030.00	70.90
2 030.01 — 2 530.00	84.90
2 530.01 — 3 000.00	99.90

**NO NEED TO ZOOM
IN AND SEE....IT'S A
REFERENCE TABLE**

FEES TABLE: EURO Example

Track your transfer in **WU.COM**

RUSSIA

Principal amount (€)	Money in Minutes*	Transfer fee (€)†
----------------------	-------------------	-------------------

0.01 — 100.00	8.75
100.01 — 200.00	13.90
200.01 — 300.00	15.90
300.01 — 500.00	22.90
500.01 — 850.00	28.90
850.01 — 1 000.00	39.90
1 000.01 — 1 500.00	49.90
1 500.01 — 2 500.00	59.90
2 500.01 — 3 000.00	70.00



FEES ON INTERNATIONAL MONEY TRANSFER

“In addition to being able to book a transfer 24/7, **you’ll pay a small standard fee of \$15 for transfers under \$10,000 at OFX** “

“In addition to the international transfer fee, a margin on the daily exchange rate is also tacked on to most foreign transfers. This rate is typically around **5% at most major banks**, so if you’re sending **\$10,000, you may have to pay up to \$500**”

“Your recipient may also be charged to receive foreign payments”

“ Whenever you send money internationally, You could pay up **to \$50 to transfer the money**, but the fee will depend upon the bank that you’re using, as well as how much money you’re sending”

<https://www.ofx.com/en-gb/faqs/how-much-does-it-cost-to-send-money-internationally/#:~:text=In%20addition%20to%20the%20international,to%20pay%20up%20to%20%24500.>

RESOLVING PROBLEMS

TRADITIONAL

Problems

- Segregation
- Privacy issues
- Inflation
- Borders

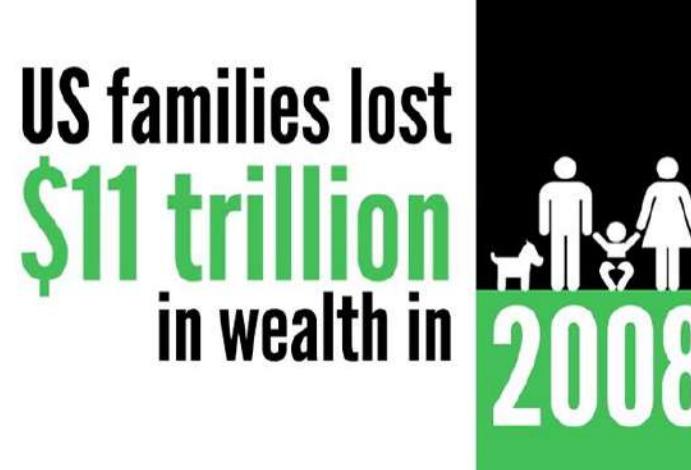
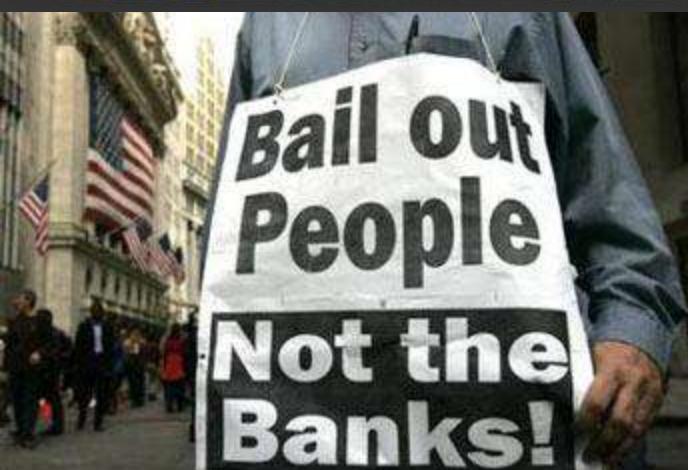
HOW BITCOIN SOLVES THESE ISSUES GLOBALLY?

It's story
TIME

HOW IT ALL STARTED

Once upon a time





Causes of the 2008 Global Financial Crisis



•HOW IT ALL STARTED.



Bitcoin: A Peer-to-Peer Electronic Cash System



2008

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

14:10
Hours Minutes

Eastern Daylight Time

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

RESOLVING PROBLEMS

TRADITIONAL

Problems

- Segregation
- Privacy issues
- Inflation
- Borders

BITCOIN

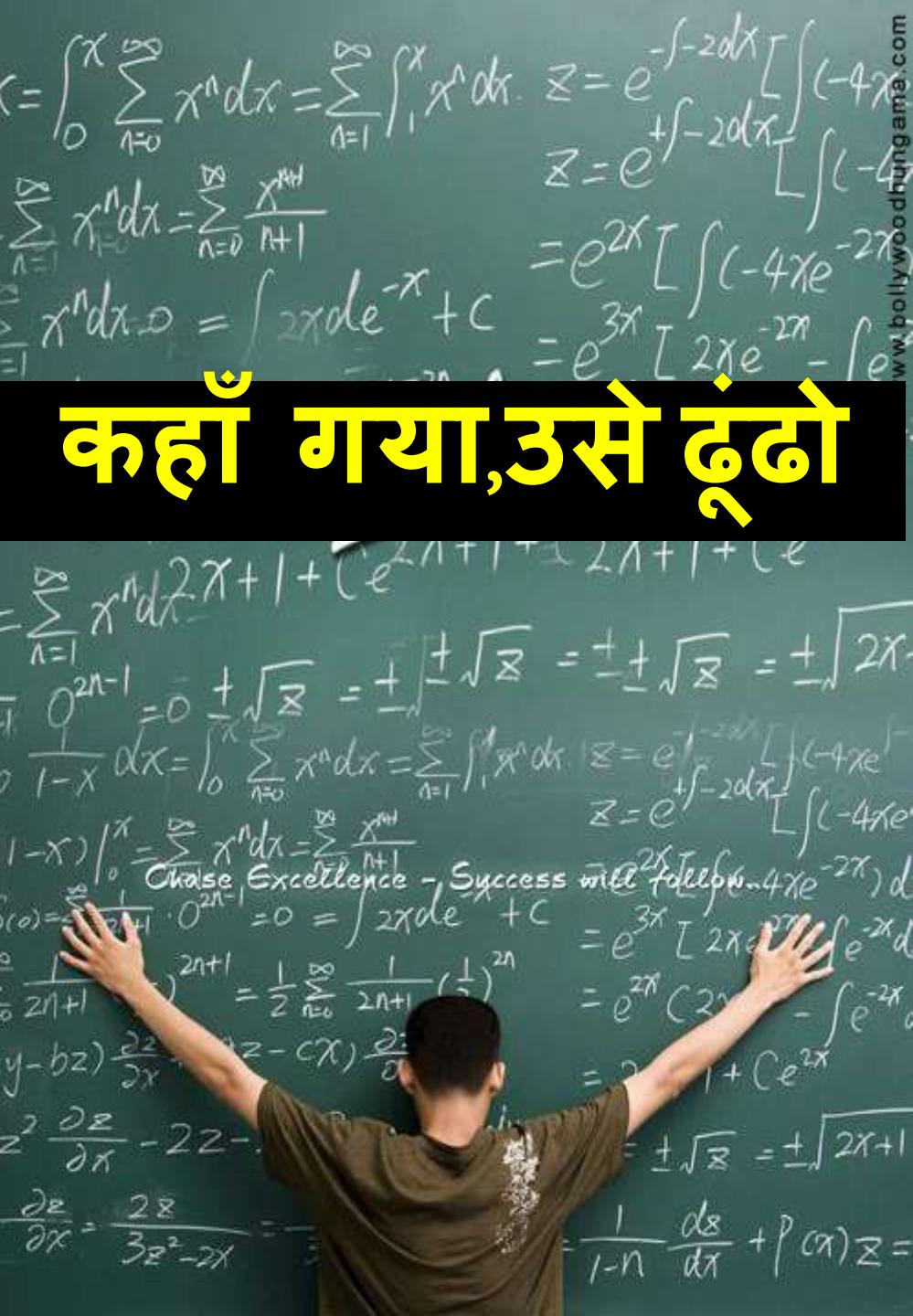
Problems fixed

- Segregation
- Privacy issues
- Inflation
- Borders

WHO IS SATOSHI NAKAMOTO

Name used by the
unknown person who
designed BITCOIN
and **created its**
original reference
implementation

Financial crisis
dollar weakens
STOCK MARKET



"Bitcoin's Creator Unmasked!!!"

Who Is The Real Satoshi Nakamoto?

Bitcoin's Mysterious Creator



Bitcoin Creator Satoshi Nakamoto is A Group of Indians: John McAfee



By **Ashish Bhatnagar** - April 25, 2019 14:15

NEWS

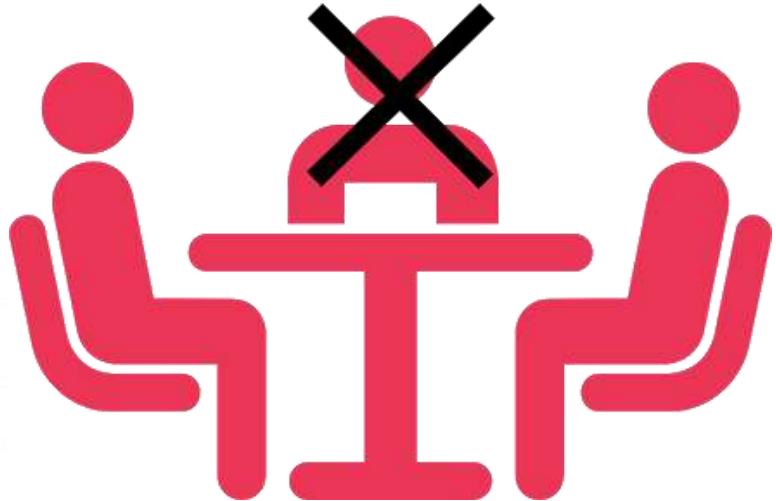
BITCOIN



**Satoshi Nakamoto released
the Version 0.1 of Bitcoin
software on Sourceforge on 9
January 2009.**

2009





Nakamoto created domain name [bitcoin.org](https://www.bitcoin.org) and continued to collaborate with other developers on the [Bitcoin software](https://github.com/bitcoin/bitcoin)

2009

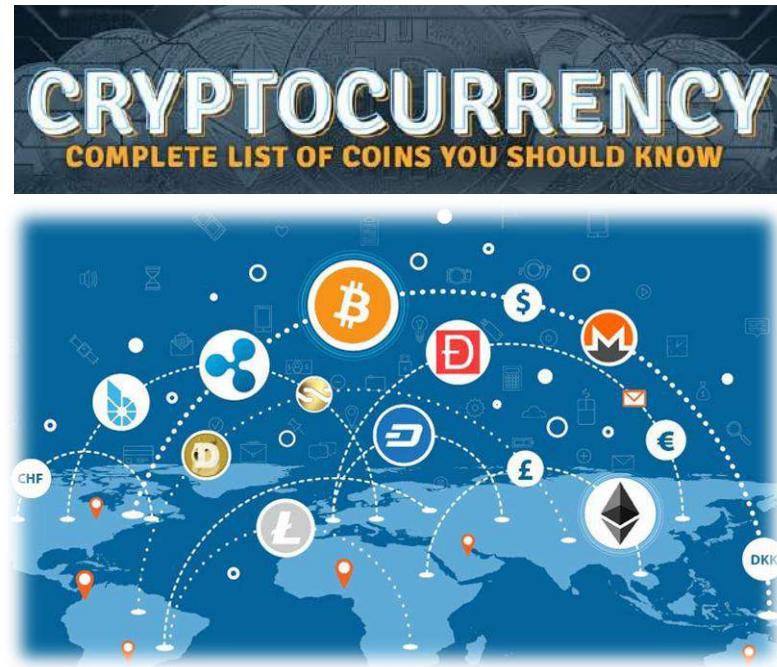


Around mid 2010, he handed over control of the source code repository to Gavin Andresen and transferred several related domains to various prominent members of the Bitcoin community, and stopped his involvement in the project



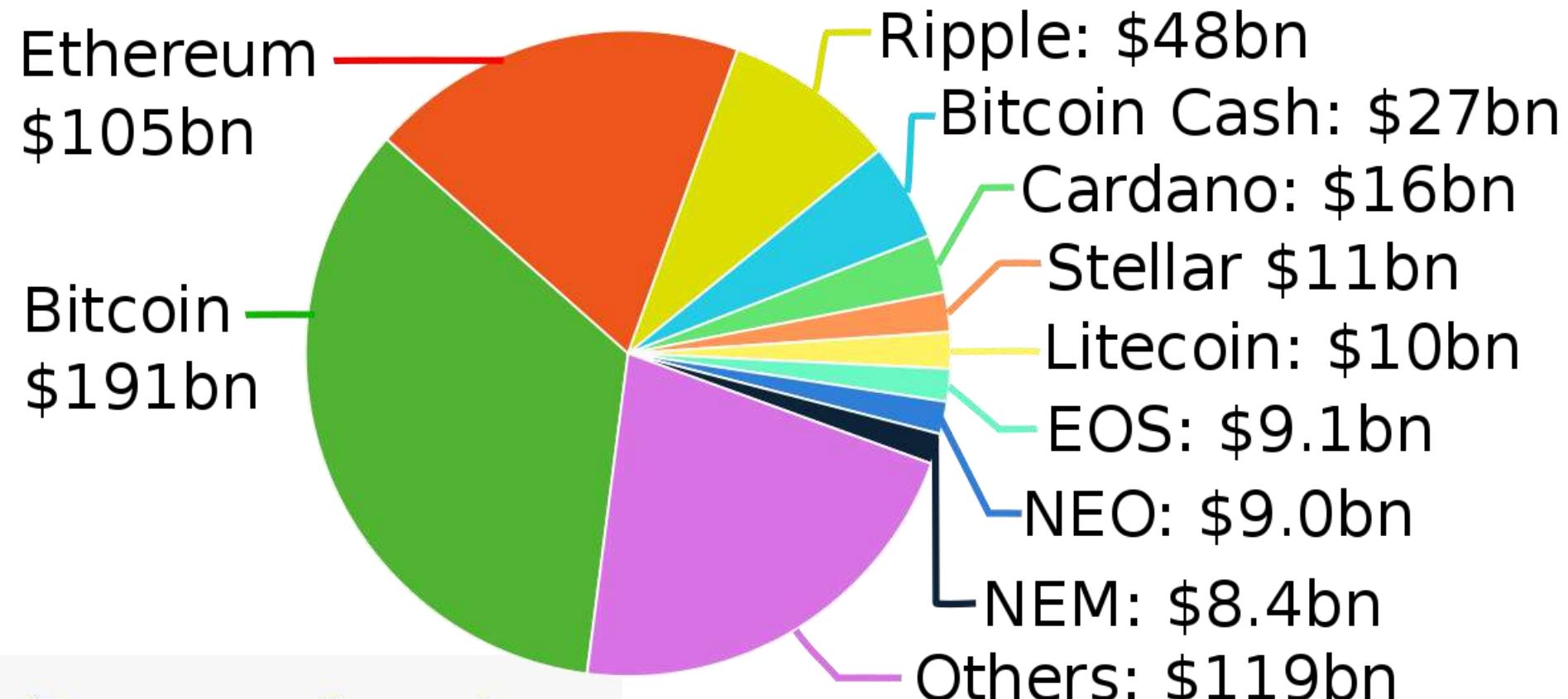
AS ON DATE

5000+



**Known number of
CRYPTOCURRENCIES that
exist in the world today**

STATISTICS



Approximates



MOST*



OF THEM



Differently Do Things

ELECTRONIC CURRENCIES BUY SERVICES
ORGANIZATION ONLINE MARKET
TRADING MONEY
BIT BANKING CRYPTO CURRENCY
TRANSACTION DIGITAL COIN
WWW TRADE
CASH COIN
MINING SECURITY
EXPERTISE PROFITABILITY
PEER COIN TRADE BUSINESS
LITE COINS EXCHANGE
TRANSACTIONS MARKET
UNIT & MONEY
NET COIN
MONEY

Total Market Cap

~Rs 172 Trillion

Rs 17,25,82,39,99,99,975

AS OF 02 Jul 2021
1 BITCOIN IS WORTH

Approximately

~32,976\$

ie ₹ 24,99,890/-

Is it worth it?

SOURCE : <https://blockchain.info/charts/n-transactions>

 **bitcoin**
LOOKS

LOOK



1454A2geTxajwF8eqry7oLECdomgDSj6Zx

WHAT'S
THIS?

What Do Bitcoins “Look” Like?

1454A2geTxaJwF8eqry7oLECdomgDSj6Zx



Public Key (“Address”)

34 characters starting with **I** or **3**

Represents a possible destination for payment

5JHkYd4mYkTsCsF5axnFj573PG6tqpeJ39Rz2M33vwBka4S1hu6



Private Key

51 characters starting with **5**

Required to transfer value from the address

BITCOIN is often **ADVERTISED**
as **ANONYMOUS** Digital Currency
that offers a high level of user
PRIVACY



Bitcoin is not anonymous

PEOPLE can **HIDE** their
IDENTITIES behind a
WALLET ADDRESS, and
generate **ADDITIONAL**
ADDRESSES if needed

ANONYMITY

VS

PSEUDONYMITY

Public key addresses similar in function to an email address, are used to send and receive BITCOINS and record transactions, as opposed to personally identifying information.



**DESIGNED
FOR ANONYMOUS**



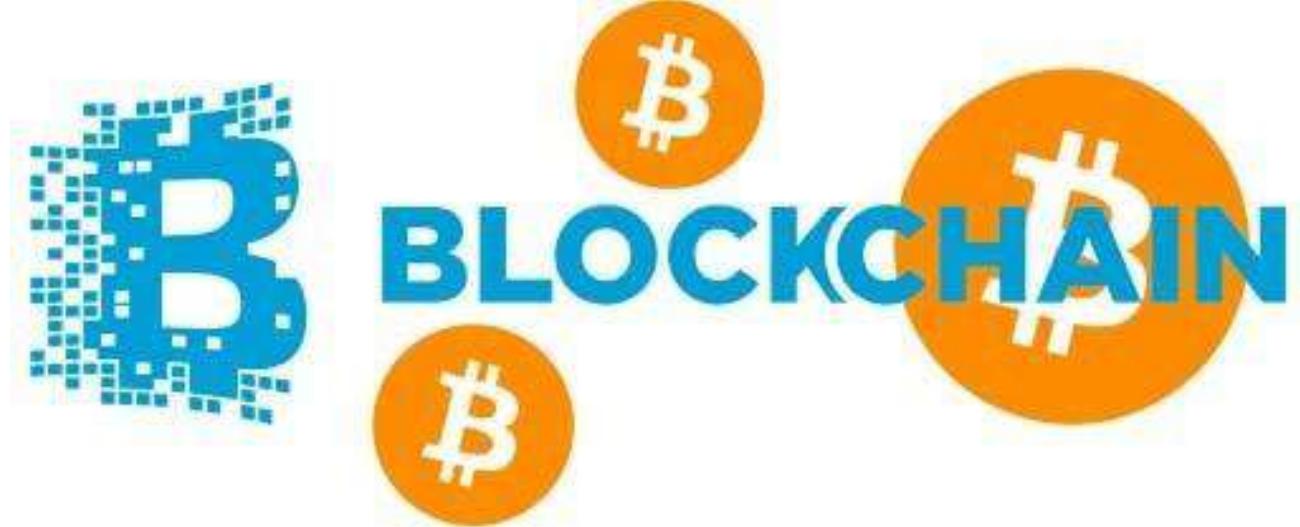
the devil's in the details

More **DETAILS** an Investigator
KNOWS about the **TECH**
ARCHITECTURE, the **CLOSER**
he gets to **CLOSE** the **CASE**

BEHIND THE
SCENES

परदे के
पीछे

FIRST
THINGS
FIRST



Blockchain and Bitcoin



WHAT
IS
THIS?

**BLOCKCHAIN
IS A COMBINATION OF
VARIOUS
TECHNOLOGIES**

Amalgamation

**TWO
WORDS.**

FirstWord



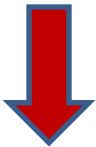
Second Word.



ONE GOOD ANALOGY

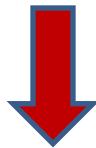
Imagine ...

GENESIS BLOCK i.e. BLOCK 0

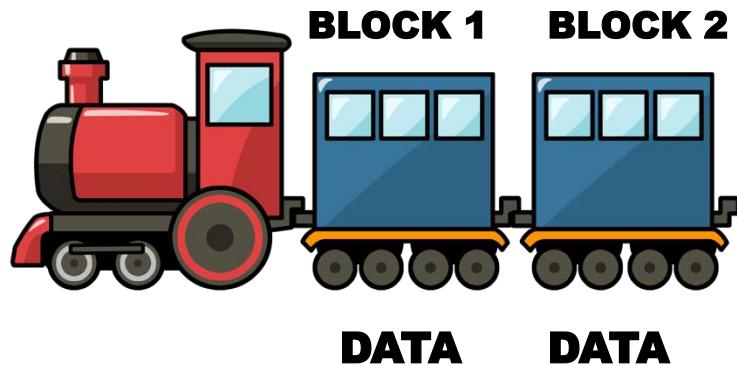


ONE GOOD ANALOGY

GENESIS BLOCK i.e. BLOCK 0



We add **DATA TRANSACTIONS** as material in train bogies



**Before we dwell into
DETAILS, we will LEARN
and REFRESH some basic
TECHNICAL terms**



LOTS



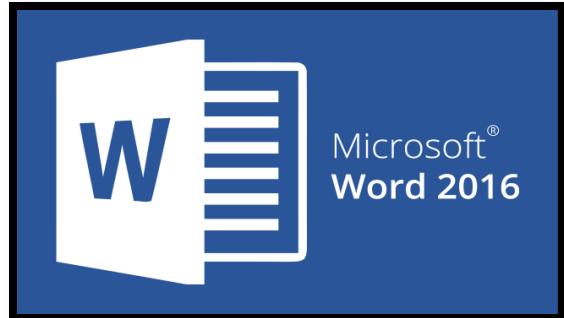
CRYPTOGRAPHY

1



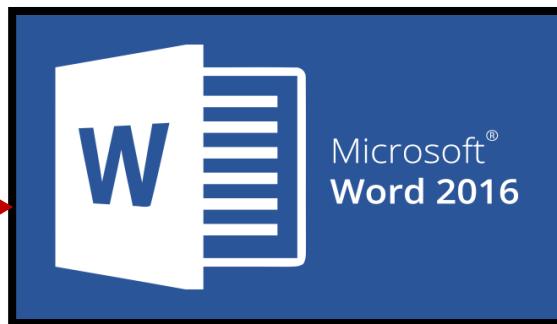
CONCEPT

FIRST



PERSON-TO-PERSON

TRADITIONAL WAY OF SHARING DOCUMENTS



TRADITIONAL WAY OF SHARING DOCUMENTS

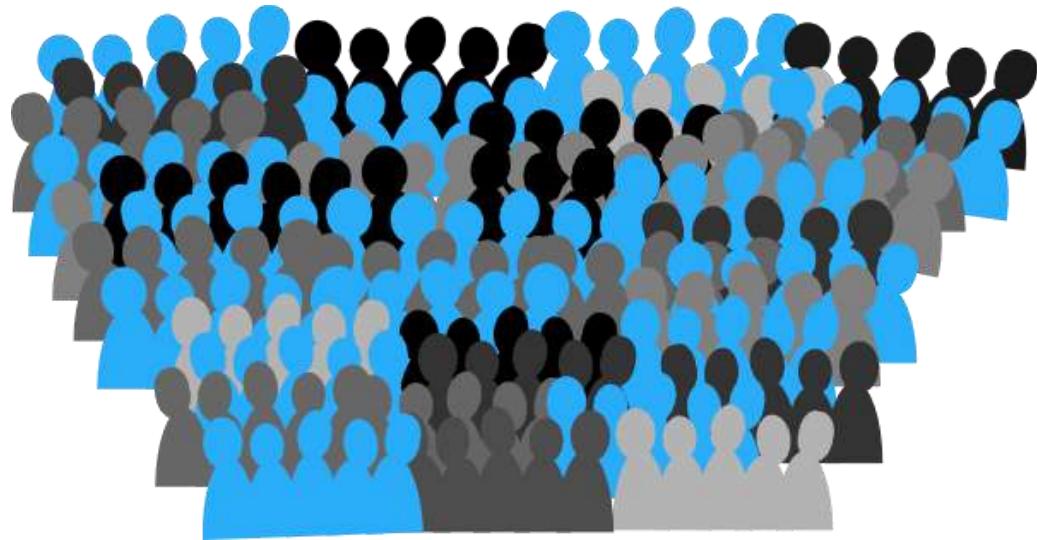


Google docs

**IF SUFFICIENT
BANDWIDTH NOT
AVAILABLE, SERVER
CRASHES**



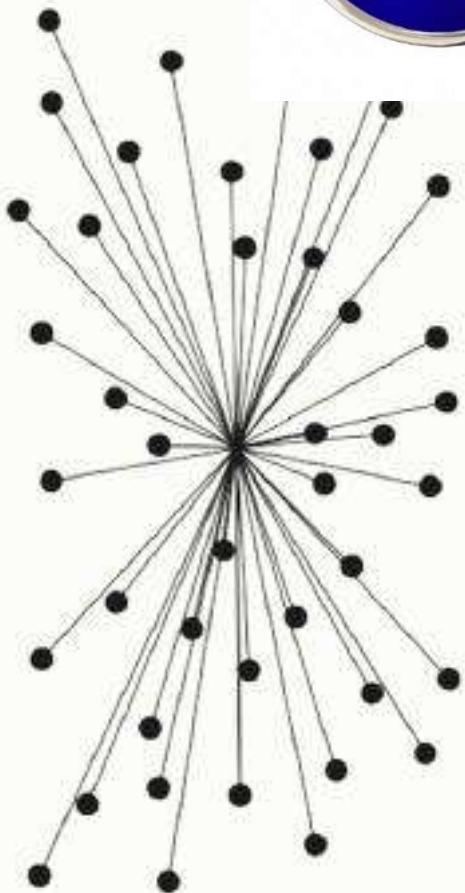
Google docs



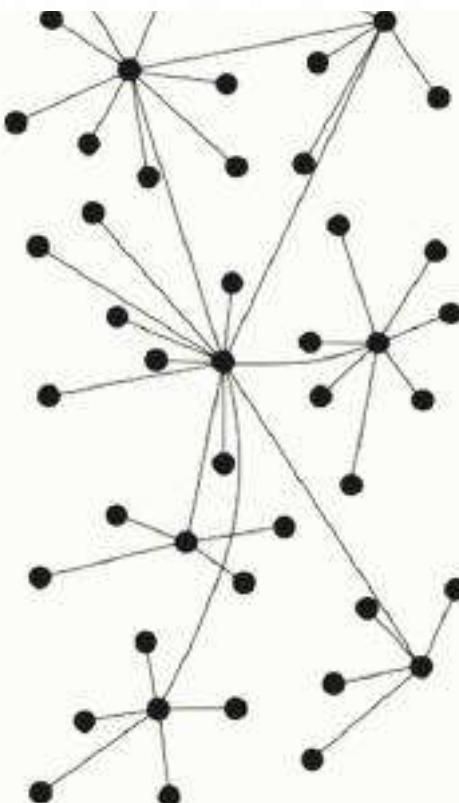
**OPTION
1**

**OPTION
2**

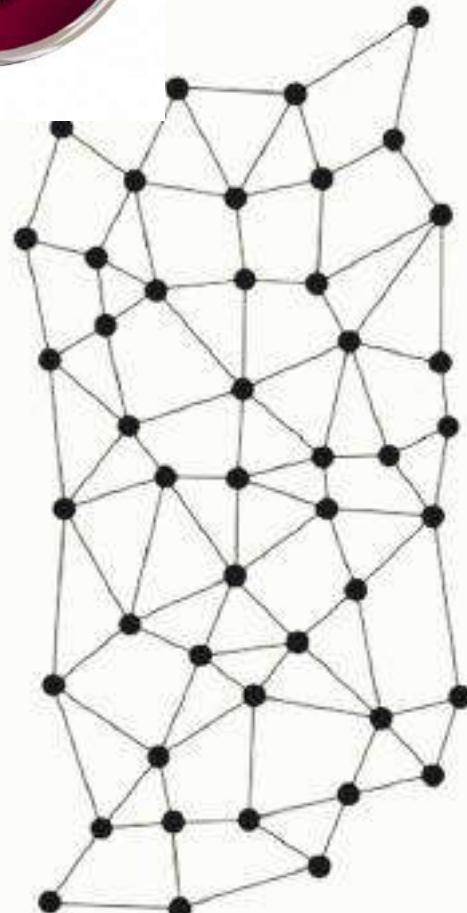
**OPTION
3**



Centralised (A)



Decentralised (B)



Distributed (C)



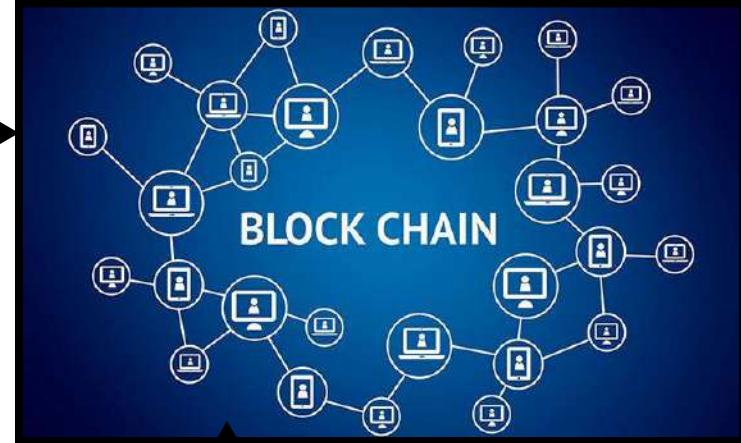
**Everyone edits on their local copy of the document –
the Internet takes care of ensuring consistency**

EXPECTATIONS



Microsoft®
Word 2016

**EVERY NODE
MAINTAINS A LOCAL
COPY**



**ALL THE COPIES ARE
IDENTICAL**



**ALL THESE COPIES ARE
UPDATED BASED ON GLOBAL
INFORMATION**



Microsoft®
Word 2016



A

PUBLIC
LEDGER

DR ABC

Rs 1000/-



B

PUBLIC
LEDGER

BUSINESS MAN

Rs 1000/-



C

PUBLIC
LEDGER

CABLE WALA

Rs 1000/-



D

PUBLIC
LEDGER

DRIVER

Rs 1000/-

Note : 'Rs' here is just a denoting currency, in Bitcoin network it is JUST a tokens



A

PUBLIC
LEDGER

DR ABC

Rs 1000/-



Rs 200/-



B

PUBLIC
LEDGER

BUSINESS MAN

Rs 1000/-



C

PUBLIC
LEDGER

CABLE WALA

Rs 1000/-



D

PUBLIC
LEDGER

DRIVER

Rs 1000/-



A

PUBLIC
LEDGER

DR ABC

Rs 1000/-

A>B Rs 200



B

PUBLIC
LEDGER

BUSINESS MAN

Rs 1000/-

A>B Rs 200



C

PUBLIC
LEDGER

CABLE WALA

Rs 1000/-

A>B Rs 200



D

PUBLIC
LEDGER

DRIVER

Rs 1000/-

A>B Rs 200



A

PUBLIC
LEDGER

DR ABC

Rs 1000/-

A>B Rs 200



B

PUBLIC
LEDGER

BUSINESS MAN

Rs 1000/-

A>B Rs 200



C

PUBLIC
LEDGER

CABLE WALA

Rs 1000/-

A>B Rs 200



D

PUBLIC
LEDGER

DRIVER

Rs 1000/-

A>B Rs 200



A

PUBLIC
LEDGER

DR ABC
Rs 1000/-
A>B Rs 200
B>D Rs 600



B

PUBLIC
LEDGER

BUSINESS MAN
Rs 1000/-
A>B Rs 200
B>D Rs 600



C

PUBLIC
LEDGER

CABLE WALA
Rs 1000/-
A>B Rs 200
B>D Rs 600



D

PUBLIC
LEDGER

DRIVER
Rs 1000/-
A>B Rs 200
B>D Rs 600



A

PUBLIC
LEDGER

DR ABC
Rs 1000/-
A>B Rs 200
B>D Rs 600



B

PUBLIC
LEDGER

BUSINESS MAN
Rs 1000/-
A>B Rs 200
B>D Rs 600



C

PUBLIC
LEDGER

CABLE WALA
Rs 1000/-
A>B Rs 200
B>D Rs 600



D

PUBLIC
LEDGER

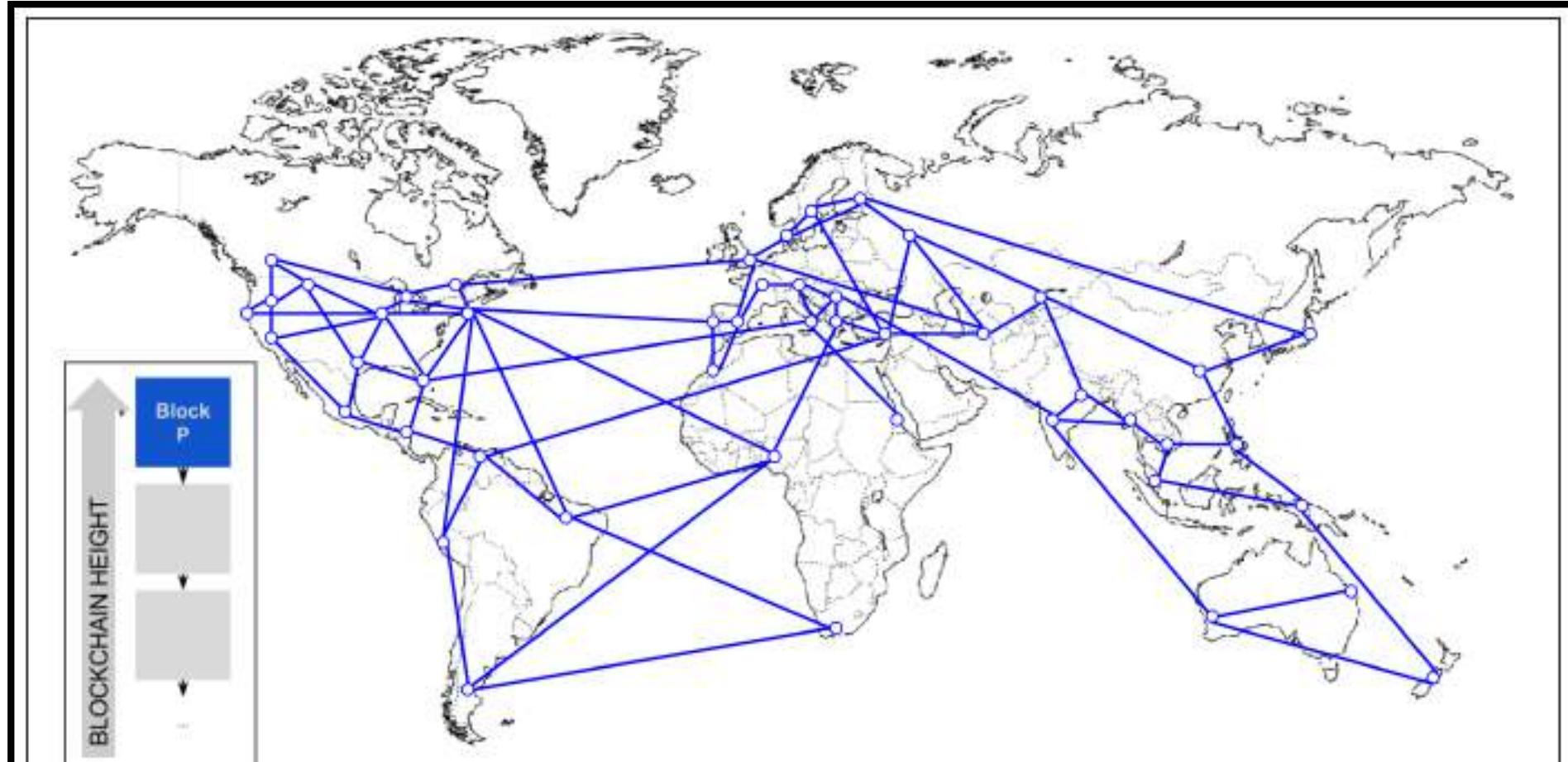
DRIVER
Rs 1000/-
A>B Rs 200
B>D Rs 600



A network diagram consisting of numerous dark blue human icons connected by a web of thin blue lines on a light blue background. The icons are distributed across the frame, with some forming larger clusters and others being more isolated.

imagine

All the participants are GEOGRAPHICALLY LOCATED APART in a boundary less CYBER WORLD



PUBLIC LEDGER

Rs 1000/-
A>B Rs 200
B>D Rs 600
C>B Rs 100
B>C Rs 200
A>B Rs 100
C>D Rs 250
B>C Rs 170
D>C Rs 189



MILLIONS OF
TRANSACTIONS

A>B Rs 100
C>D Rs 250
B>C Rs 170
D>C Rs 189



GLOBAL EXCEL SHEET

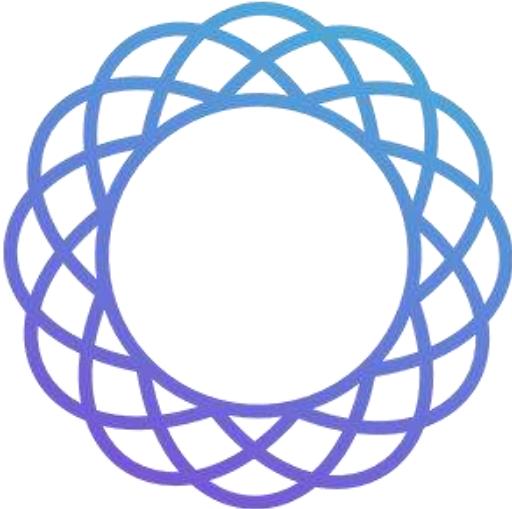
3
4
5
6
7
8
9
10
11
12
13

Sheet1



100%

Ready



THE DISTRIBUTED LEDGER

Distributed Ledger is a **Consensus** of
Replicated, Shared & Synchronized
digital data **geographically** spread across
multiple sites & countries



~**380 GB**

**CURRENT BITCOIN BLOCKCHAIN
APPROX SIZE AS IN Jul 2021**

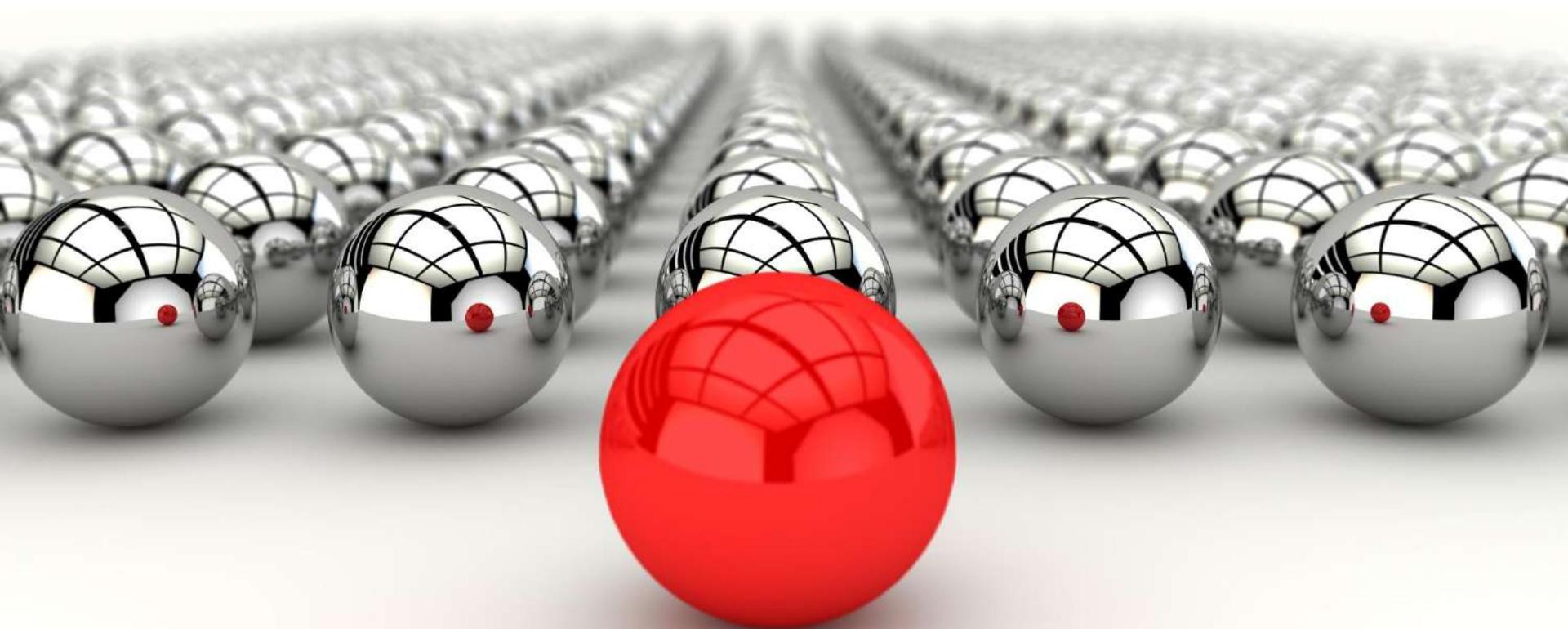
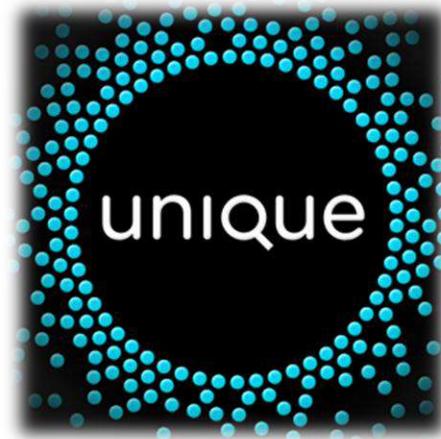
2



CONCEPT

SECOND

#ash



#ash

**Algorithms are cardinal
to complete
ecosystem network of
any Blockchain**

hQIOAOuHn1ue4n32EAf/UEF6JLrap10BMdKMvb+Dz9GvoijUiixH+gh
vC3ktMwo7OWqPyJseVRSPB0v6d0wy65KrzsHwhOHO/CKEk205STAw:
6E+Gc4iumM1725JNahJzcL5ED33LFdZ6uoEjgqggxG1dFwvwksRHA:
T9aRVbkXNxXkQn2FWhWuhPQFNWLwIVrDd9TPtDvpRT16YiB1AM9ks:
Hk9yfy1nGXdh106EDvvTvd/Lq1xsFjKh6y/pG6NxABGdT6VoeWGVt:
xoSYkWm8MmAkqYZLraSEzyxxu4cQzvzz3vrpN3AgAhObP2eUFU:

Hash function takes an input
and returns a fixed-size
alphanumeric string

hQIOAOuHn1ue4n32EAf/UEF6JLrap10BMdKMvb+Dz9GvoijUiixH+gh
vC3ktMwo7OWqPyJseVRSPB0v6d0wy65KrzsHwhOHO/CKEk205STAw:
6E+Gc4iumM1725JNahJzcL5ED33LFdZ6uoEjgqggxG1dFwvwksRHA:
T9aRVbkXNxXkQn2FWhWuhPQFNWLwIVrDd9TPtDvpRT16YiB1AM9ks:
Hk9yfy1nGXdh106EDvvTvd/Lq1xsFjKh6y/pG6NxABGdT6VoeWGVt:
xoSYkWm8MmAkqYZLraSEzyxxu4cQzvzz3vrpN3AgAhObP2eUFU:

hQIOAOuHn1ue4n32EAf/UEF6JLrap10BMdKMvb+Dz9GvoijUiixH+gh
vC3ktMwo7OWqPyJseVRSPB0v6d0wy65KrzsHwhOHO/CKEk205STAw:
6E+Gc4iumM1725JNahJzcL5ED33LFdZ6uoEjgqggxG1dFwvwksRHA:
T9aRVbkXNxXkQn2FWhWuhPQFNWLwIVrDd9TPtDvpRT16YiB1AM9ks:
Hk9yfy1nGXdh106EDvvTvd/Lq1xsFjKh6y/pG6NxABGdT6VoeWGVt:
xoSYkWm8MmAkqYZLraSEzyxxu4cQzvzz3vrpN3AgAhObP2eUFU:

**This input can be text, image,
document or any message or
any file in the cyber ecosystem**

hQIOAOuHn1ue4n32EAf/UEF6JLrap10BMdKMvb+Dz9GvoijUiixH+gh
vC3ktMwo7OWqPyJseVRSPB0v6d0wy65KrzsHwhOHO/CKEk205STAw:
6E+Gc4iumM1725JNahJzcL5ED33LFdZ6uoEjgqggxG1dFwvwksRHA:
T9aRVbkXNxXkQn2FWhWuhPQFNWLwIVrDd9TPtDvpRT16YiB1AM9ks:
Hk9yfy1nGXdh106EDvvTvd/Lq1xsFjKh6y/pG6NxABGdT6VoeWGVt:
xoSYkWm8MmAkqYZLraSEzyxxu4cQzvzz3vrpN3AgAhObP2eUFU:

To achieve

WE NEED

HASH ALGORITHMS

97ECB7E

97ECB7E

hQIOAOuHn1ue4n32EAf/UEF6JLrap10BMdKMvb+Dz9GvoijUiixH+gh
vC3ktMwo7OWqPyJseVRSPBOv6d0wy65KrzsHwhOH/CKEk205STAw:
6E+Gc4iumM1725JNahJzcL5ED33LFdZ6uoEjgqggxG1dFwvwksRHA:
T9aRVbkXNxXkQn2FWhWuhPQFNWLwIVrDd9TPtDvpRT16YiB1AM9ks:
Hk9yfy1nGXdhio6EDvvTvd/Lq1xsFjKh6y/pG6NxABGdT6VoeWGVt:
xoSYkWm8MmAkqYXZLraSEzyxxxu4cQzvzz3vrpN3AgAhObP2eUFU:

Types

Algorithm and variant	Name
MD5 (as reference)	BLAKE-256
SHA-0	BLAKE-512
SHA-1	BLAKE2s
SHA-2	BLAKE2b
SHA-224	BLAKE2X
SHA-256	BLAKE3
SHA-384	ECOH
SHA-512	FSB
SHA-512/224	GOST
SHA-512/256	Grøstl
SHA-3	HAS-160
SHA3-224	HAVAL
SHA3-256	JH
SHA3-384	LSH ^[17]
SHA3-512	MD2
SHAKE128	MD4
SHAKE256	MD5
	MD6
	RadioGatún
	RIPEMD
	RIPEMD-128
	RIPEMD-160
	RIPEMD-320

Types

Algorithm and variant

MD5 (as reference)

SHA-0

SHA-1

SHA-2 SHA-224
SHA-256
SHA-384
SHA-512
SHA-224
SHA-512/256

SHA-3 SHA3-224
SHA3-256
SHA3-384
SHA3-512
SHAKE128
SHAKE256

There are many others
too....

Name
BLAKE2
BLAKE3
HMAC
MD6
One-key MAC (OMAC; CMAC)
PMAC (cryptography)
Poly1305-AES
SipHash
HighwayHash ^[14]
UMAC
VMAC
BSD checksum (Unix)
SYSV checksum (Unix)
sum8
sum16
sum32
fletcher-4
fletcher-8
fletcher-16
fletcher-32
Adler-32
xor8
Luhn algorithm
Verhoeff algorithm
Damm algorithm

Name
BLAKE-256
BLAKE-512
BLAKE2s
BLAKE2b
BLAKE2X
BLAKE3
ECOH
FSB
ST
Grøstl
HAS-160
HAVAL
JH
LSH ^[17]
MD2
MD4
MD5
MD6
RadioGatún
RIPEMD
RIPEMD-128
RIPEMD-160
RIPEMD-320

HASHES WELL KNOWN

Name	Bits	Secure so far?	Used in Bitcoin?
SHA256	256	Yes	Yes
SHA512	512	Yes	Yes, in some wallets
RIPEMD160	160	Yes	Yes
SHA-1	160	No. A collision has been found.	No
MD5	128	No. Collisions can be trivially created. The algorithm is also vulnerable to pre-image attacks, but not trivially.	No

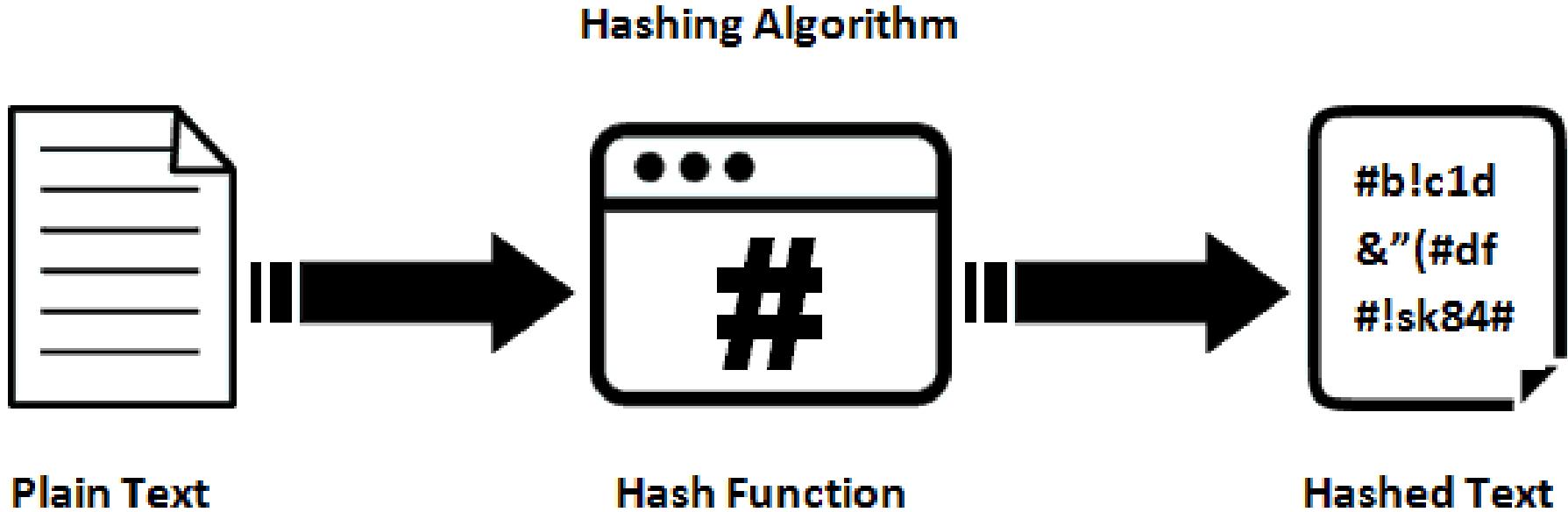
Even if a single collision has been found in a cryptographic hash function, most cryptographers will consider the function insecure



SECURE HASHING
ALGORITHM

RIPEMD-160

RACE Integrity Primitives Evaluation Message Digest



Cryptographic Hash Functions

Find the hash of **JAMMU**

MD5 (128-bit)

SHA1 (160-bit)

RIPEMD-160

SHA224

SHA256

Use any online site to compute the hash. I have used <https://anyhash.com/>

Cryptographic Hash Functions

Find the hash of **JAMMU**

MD5 (128-bit)

7e88dcd475a1aa0135d4fc2b06251ccb

SHA1 (160-bit)

46885096ccaae22977c46a9e61ac4d6e9627f4d3

RIPEMD-160

51663f408506f13e756367f7f921c680df806d3d

SHA224

c10a6d1d717c012b19809bb1df549723196231a138b4aa7c12cbbf19

SHA256

d4d3f74c27251a48231e7a55c160dd41f0b13cce4a300872dc407d068ff60a27

Use any online site to compute the hash. I have used <https://anyhash.com/>

Cryptographic Hash Functions

Find the hash of **JAMMU**

MD5 (128-bit)

7e88dcd475a1aa0135d4fc2b06251ccb

SHA1 (160-bit)

46885096ccaae22977c46a9e61ac4d6e9627f4d3

RIPEMD-160

51663f408506f13e756367f7f921c680df806d3d

SHA224

c10a6d1d717c012b19809bb1df549723196231a138b4aa7c12cbbf19

SHA256

d4d3f74c27251a48231e7a55c160dd41f0b13cce4a300872dc407d068ff60a27

Find the hash of **JAMmU**

MD5 (128-bit)

b506f585c9d25bbd7e45d9af9fee3b4e

SHA1 (160-bit)

72e5168b6d7b2c21605e443f5263176b80618efb

RIPEMD-160

1d0fe6732faf9d1647548bae70bb24ac33ccf1b6

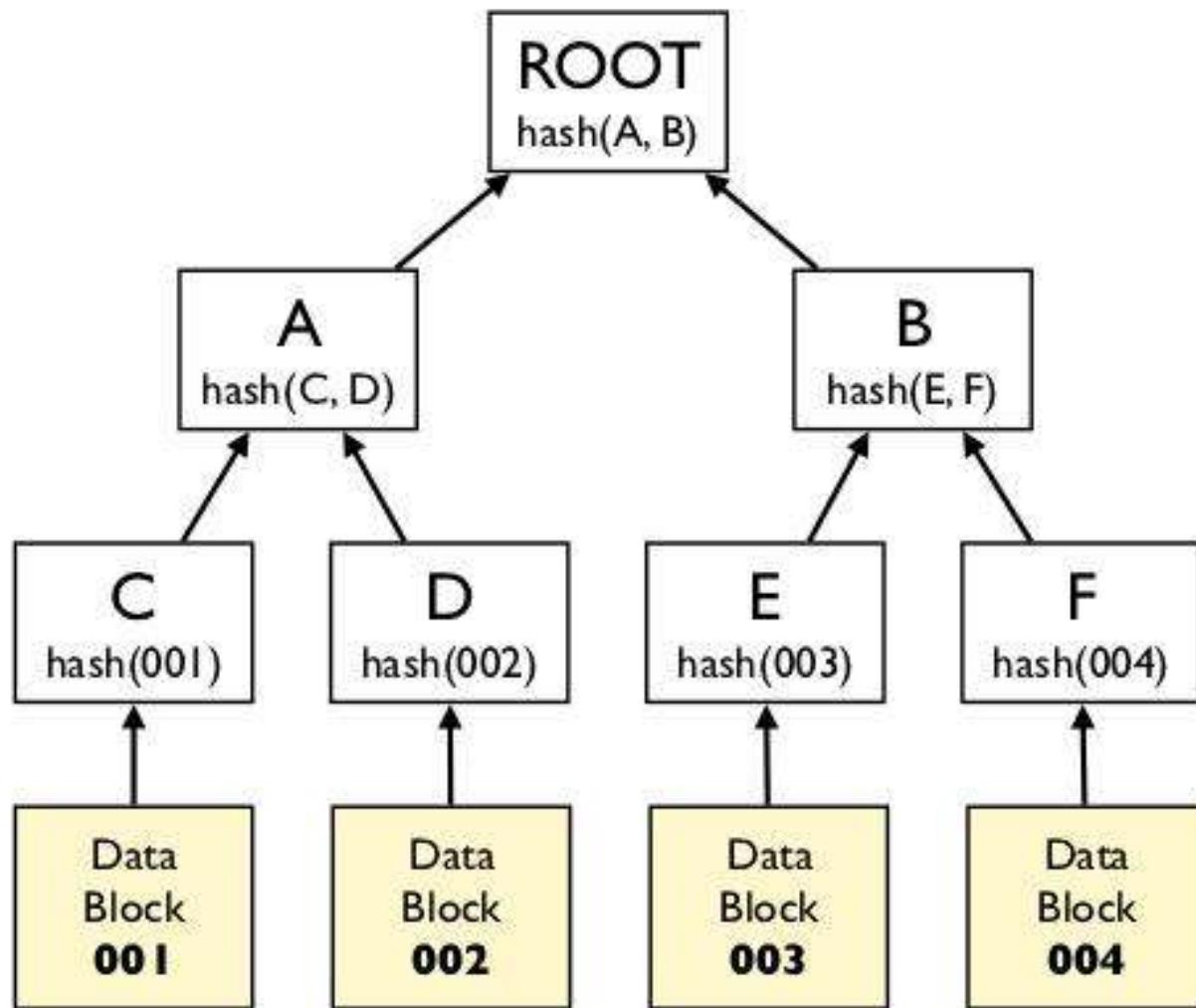
SHA224

73eae3bc59a512c37b764238e7914234fa74320fc344d7e32035a9d8

SHA256

20710c81b7277cea413f6bc1c00587b25fcd1169522f49dd5121fc28c1331709

MERKLE TREE

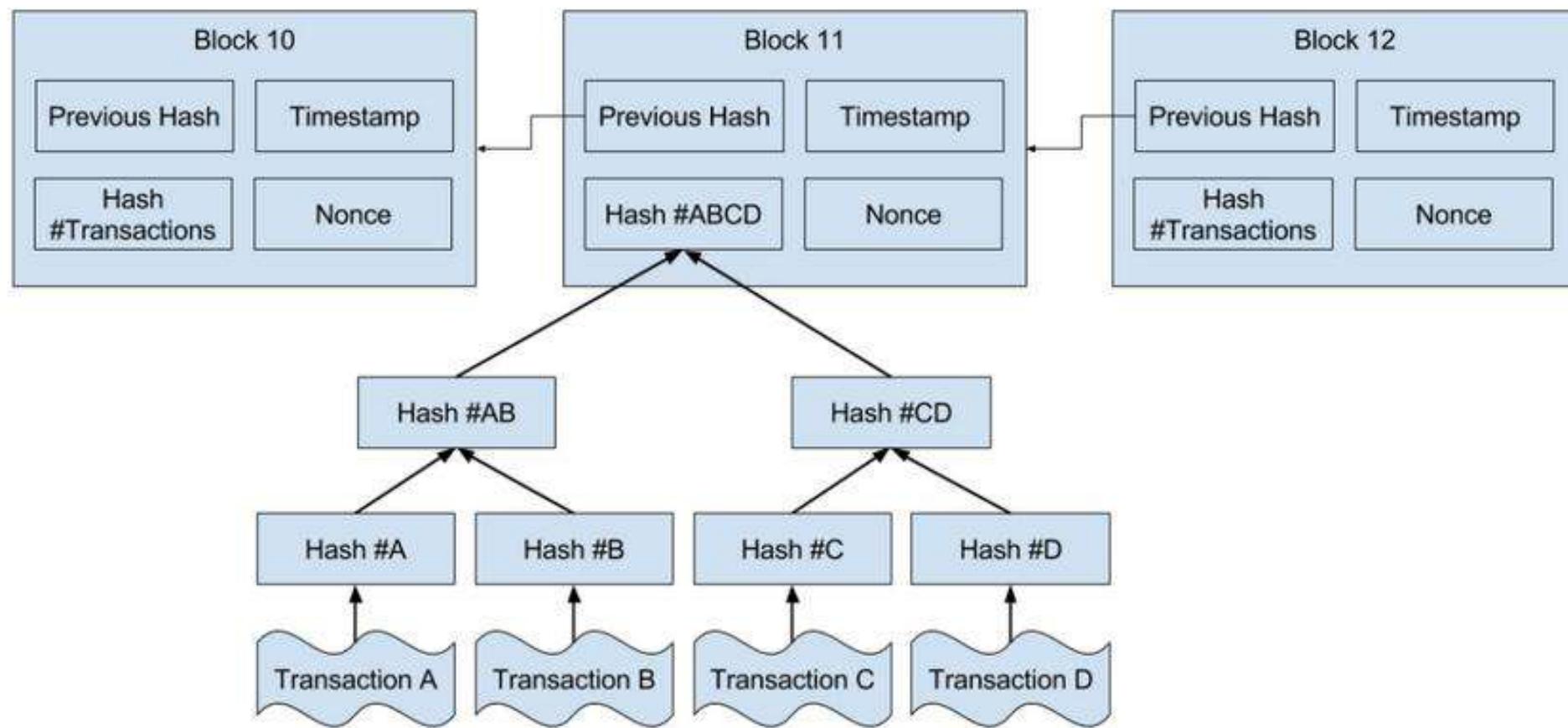


Leaves: hashes of data blocks.

Nodes: hashes of their children.

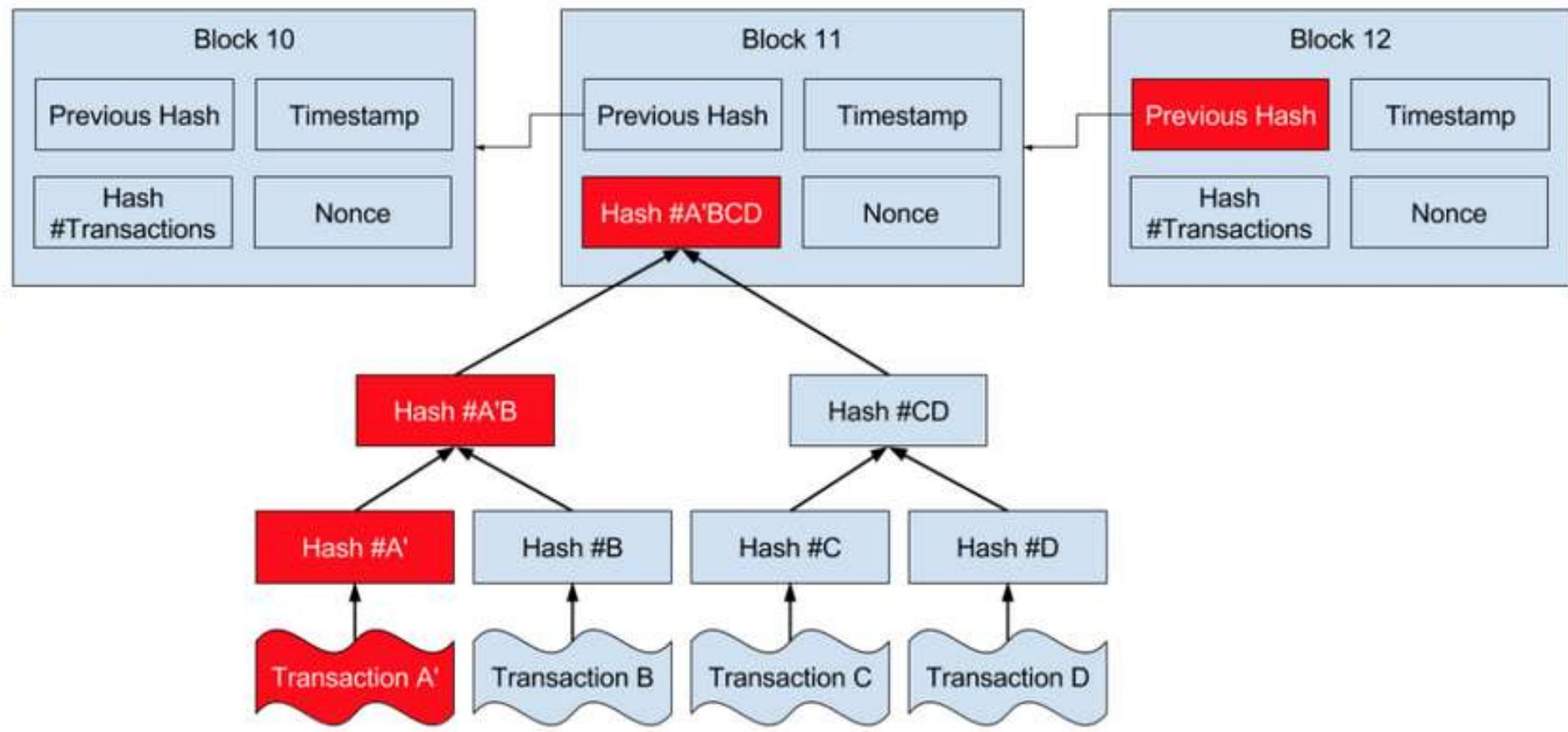
Used to detect inconsistencies between replicas (anti-entropy) and to minimise the amount of transferred data

MERKLE TREE



hash-based data structure that is a generalization of the *hash* list

MERKLE TREE



hash-based data structure that is a generalization of the hash list

TRIE

A **trie** is a special tree that can compactly store strings

TRIE that stores
"David",
"Maria",
and "Mario"

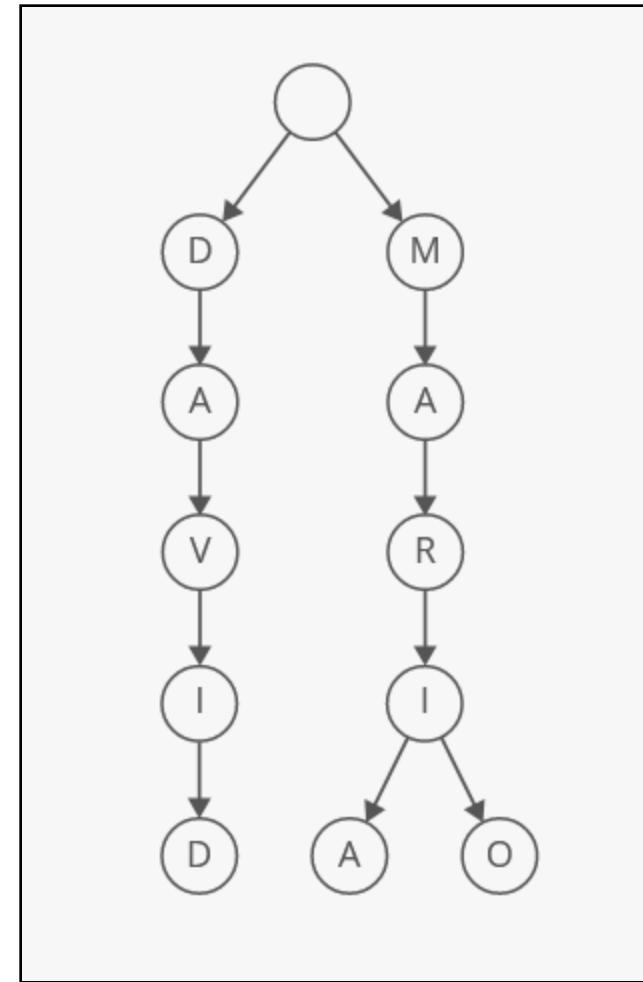
ethereum

Space-Efficient.
Efficient Prefix Queries.

Tries can quickly answer queries about words with shared prefixes, like:

How many words start with "**aict**"?

What's the most likely next letter in a word that starts with "**educati**"?



TRIE

Also called digital tree or prefix tree, is a type of search tree, a tree data structure used for locating specific keys from within a set.

These keys are most often strings, with links between nodes defined not by the entire key, but by individual characters

PATRICIA TREES

**Practical Algorithm To Retrieve
Information Coded In Alphanumeric**

PATRICIA TREES

A tree-based data structure that stores (key, value) bindings in which a key represents a path so the nodes in tree that share the same prefix can also share the same path



ethereum

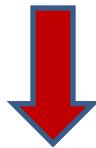
LET'S GO



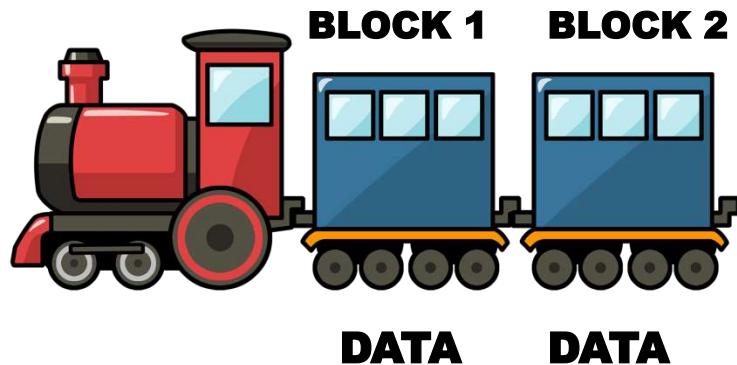
- ANYHASH
- MERKLE
- MD5 SUM LINUX

ONE GOOD ANALOGY

GENESIS BLOCK i.e. BLOCK 0

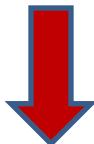


We add **DATA TRANSACTIONS** as material in train bogies

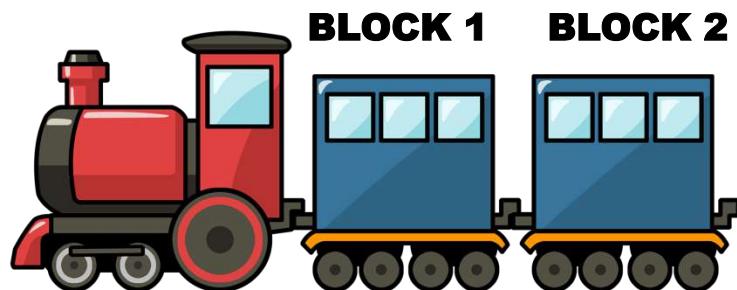


ONE GOOD ANALOGY

GENESIS BLOCK i.e. BLOCK 0



Now, with concepts of **HASH** and
MERKLE TREES

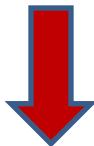


In Block 1, we add hash of Block 0

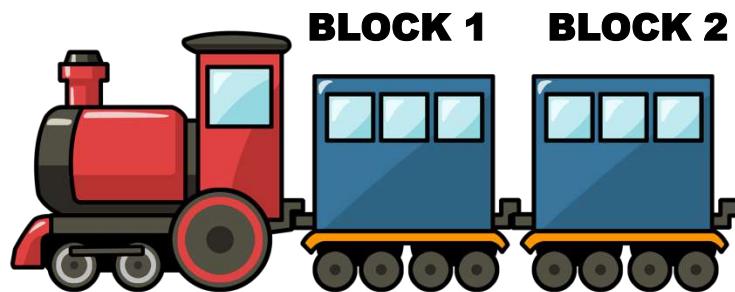
In Block 2, we add hash of Block 1

ONE GOOD ANALOGY

GENESIS BLOCK i.e. BLOCK 0



Now, with concepts of **HASH** and
MERKLE TREES



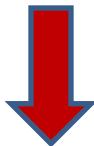
In Block 1, we add hash of Block 0

In Block 2, we add hash of Block 1

WE LINK THE BOGIES MATHEMATICALLY

ONE GOOD ANALOGY

GENESIS BLOCK i.e. BLOCK 0

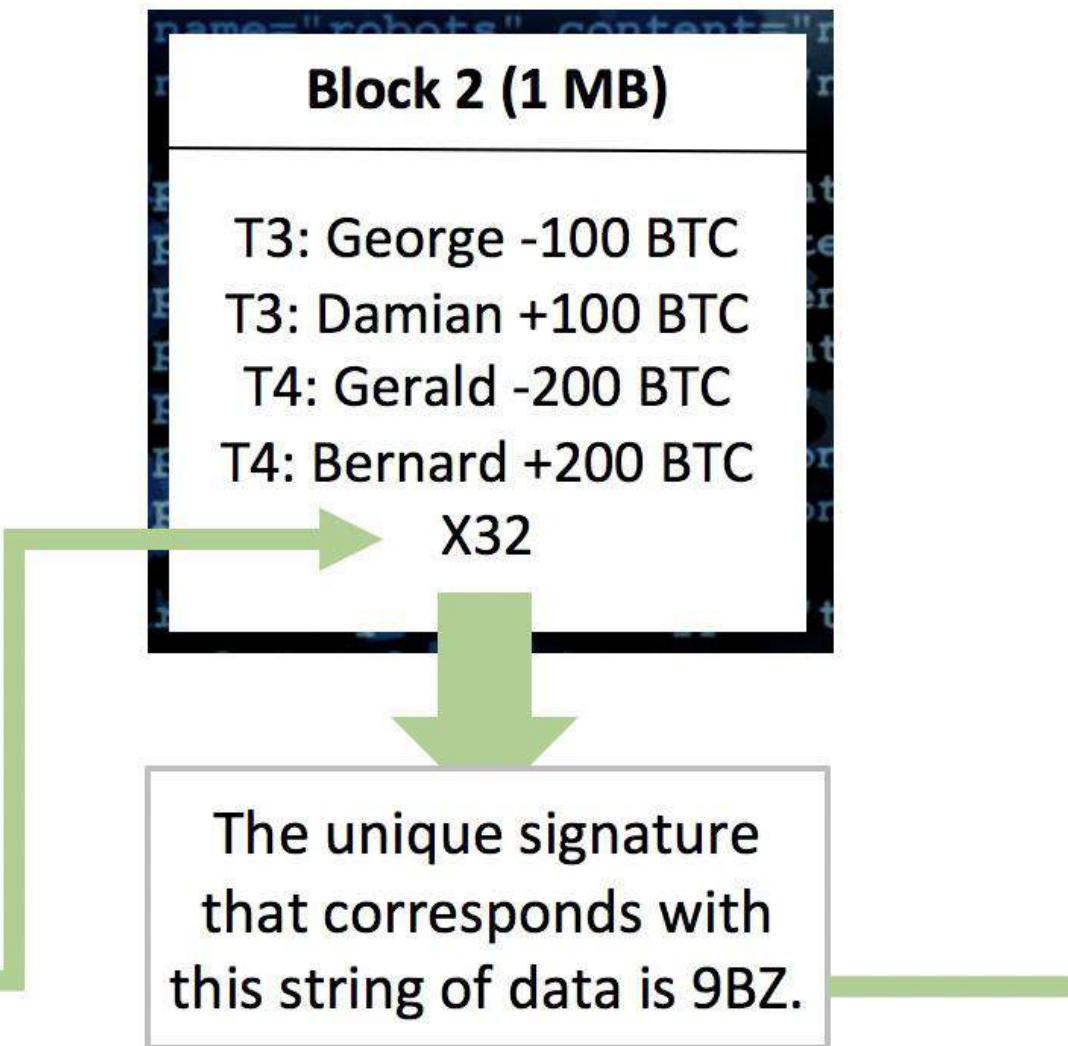


BLOCK 1 BLOCK 2 BLOCK 3 BLOCK 4 BLOCK 5 BLOCK 6 BLOCK 7



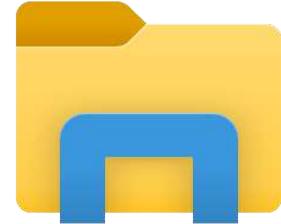
MATHEMATICALLY LINKED BOGIES

**Each of
these
BLOCKS
follows
some
rules**



we know

WINDOWS EXPLORER



Similarly

there is

BLOCKCHAIN EXPLORER

LET'S GO



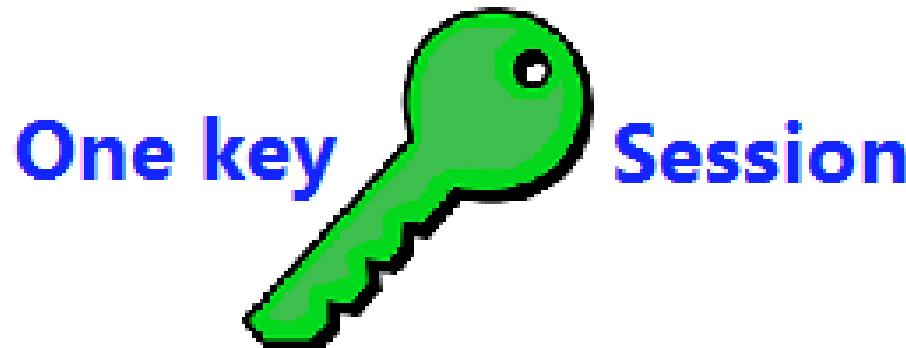
3



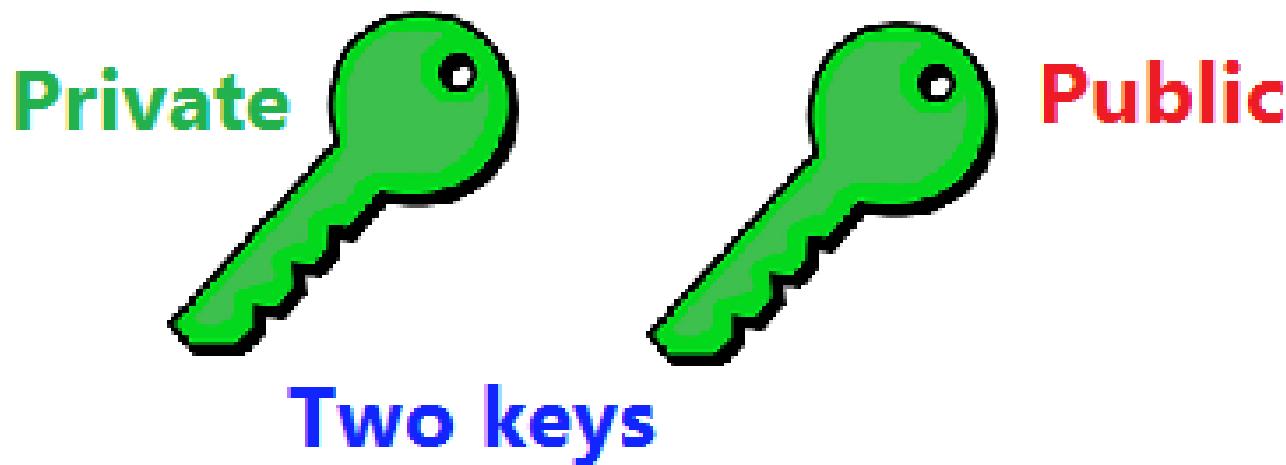
CONCEPT

THIRD

Symmetric Encryption



Asymmetric Encryption



A KEY PAIR

what one key does



the other will validate

⌚ ➡ PUBLIC encrypts



⌚ ➡ PRIVATE decrypts

⌚ ➡ PRIVATE digitally signs



⌚ ➡ PUBLIC verifies the signature

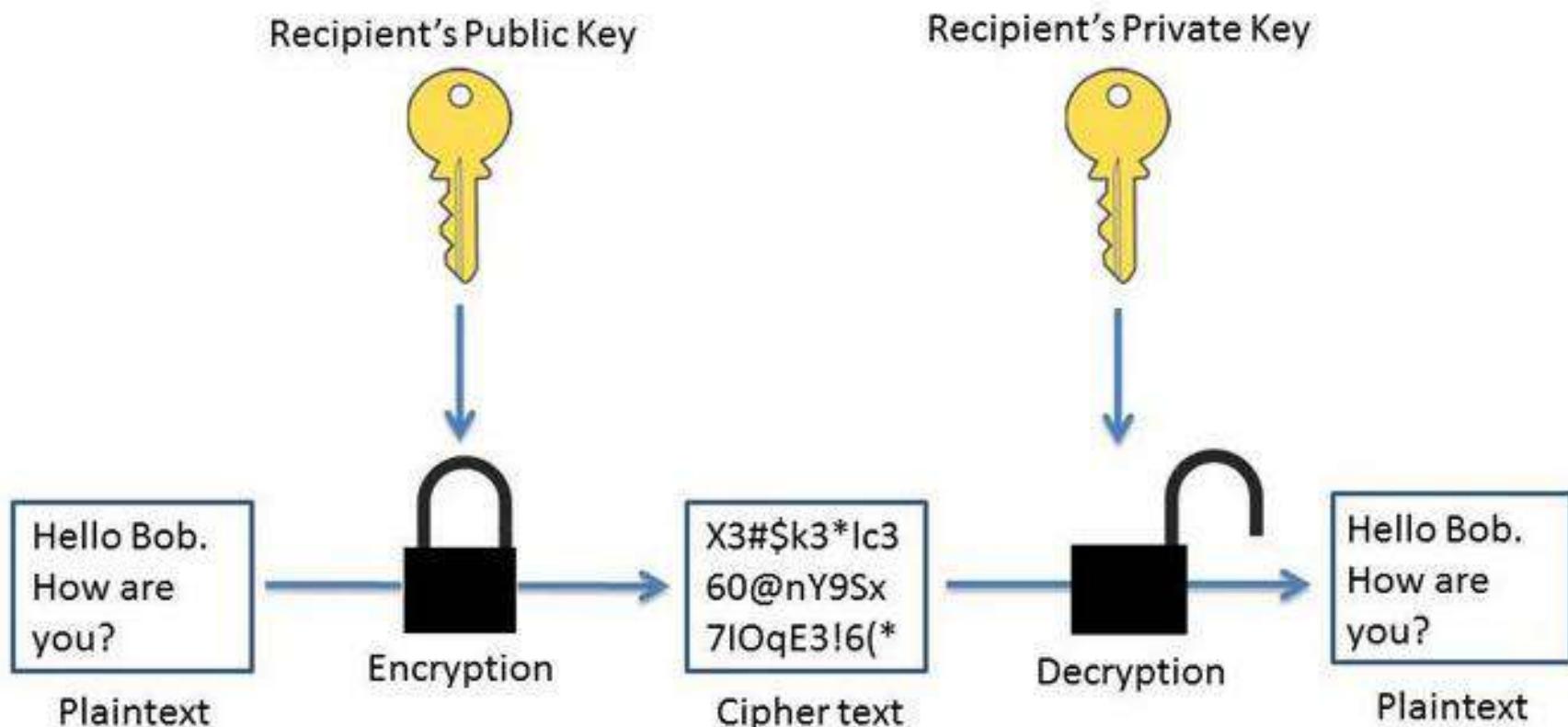
⌚ ➡ PRIVATE authenticates



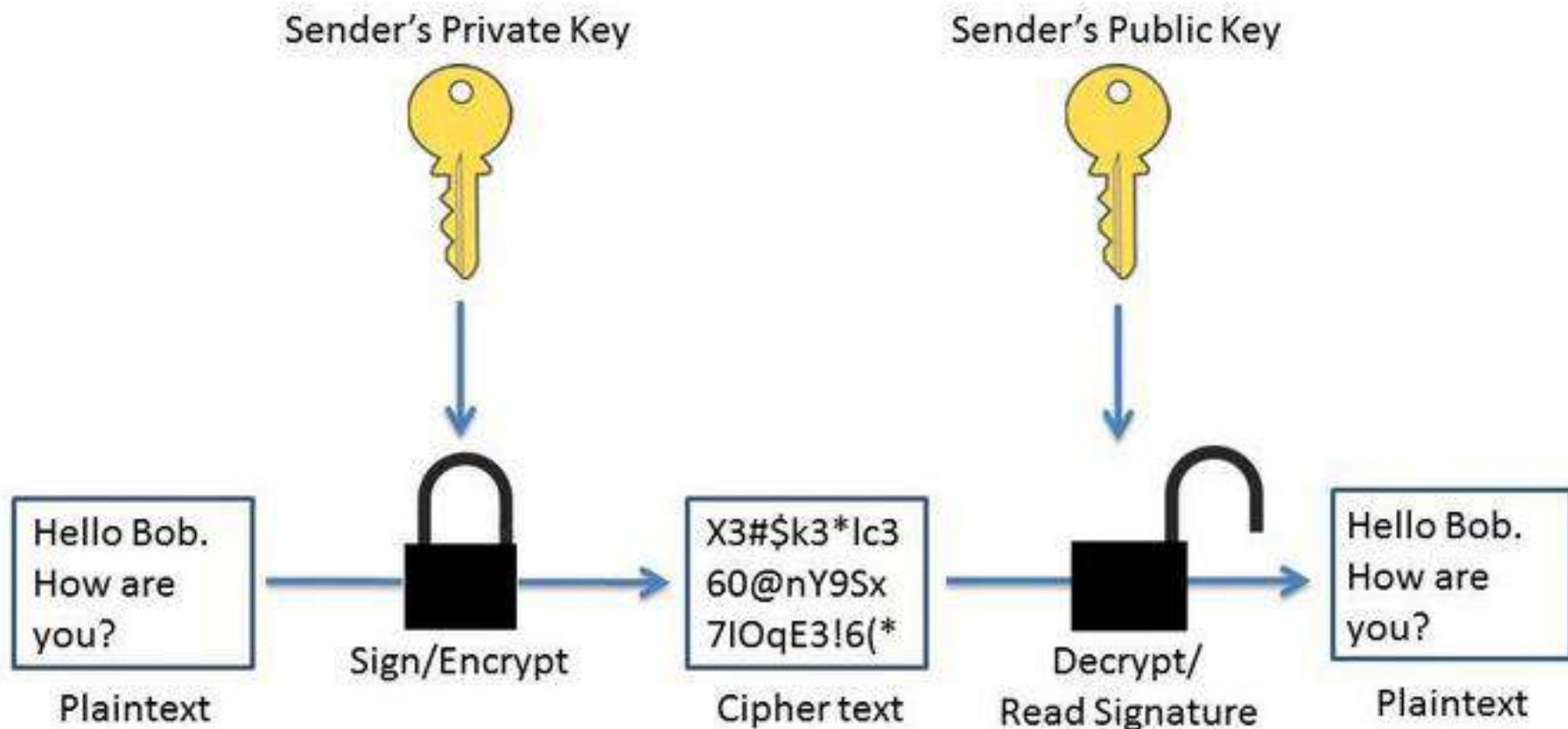
⌚ ➡ PUBLIC verifies the authentication



Public Key Encryption



Digitally Signing a Message



NONREPUDIATION

Sender encrypts message using
sender's Private key at source.

Message is decrypted at destination
using **sender's Public key**

Sender (S)

Recipient (R)

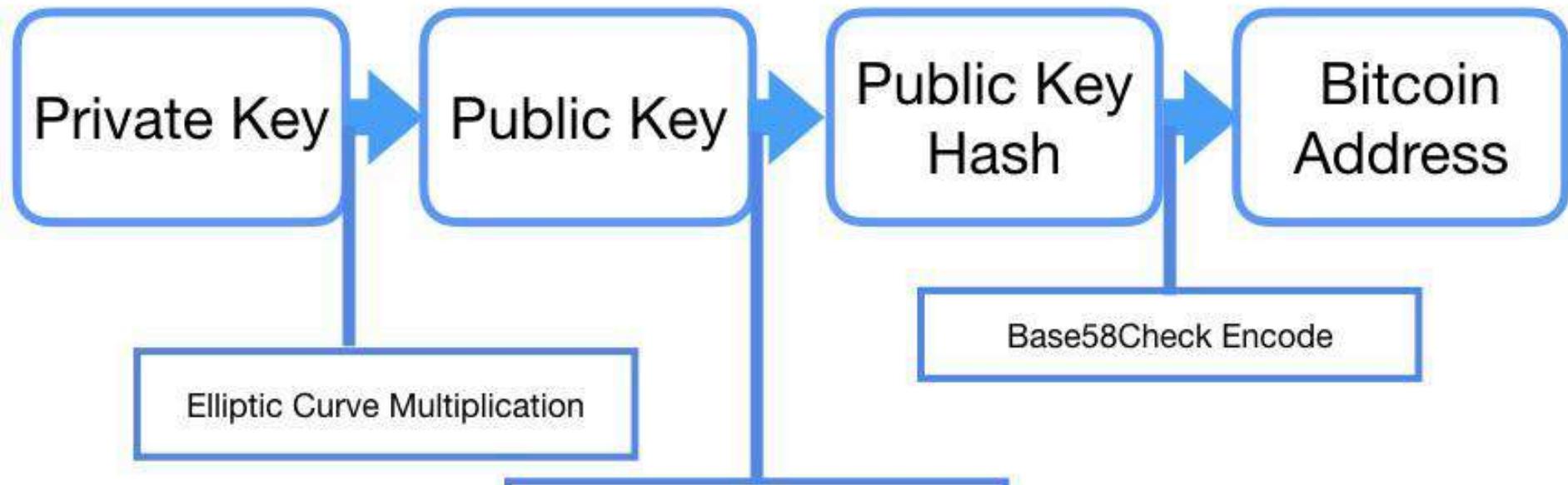
LET'S GO

Linux Terminal

ADDRESSING SCHEME IN BLOCKCHAIN

BITCOIN INTERNALS

Behind a simple address



Your sample private key :

18E14A7B6A307F426A94F8114701E7C8E774E7F9A47E2C2035DB29A206321725

Public key derived is

0450863AD64A87AE8A2FE83C1AF1A8403CB53F53E486D8511DAD8A04887E5B2
3522CD470243453A299FA9E77237716103ABC11A1DF38855ED6F2EE187E9C582
BA6

Hex of

The SHA-256 output received is

600ffe422b4e00731a59557a5cca46cc183944191006324a447bdb2d98d4b408

Now we take RIPEMD-160 Hash of the above output and get this as follows as seen vide the screenshot :

010966776006953d5567439e5e39f86a0d273bee

Now add Add version byte in front of RIPEMD-160 hash (0x00 for Main Network).so that the above output becomes :

00010966776006953D5567439E5E39F86A0D273BEE

Further to above,Perform SHA-256 hash on the extended RIPEMD-160 result ie so we get

445c7a8007a93d8733188288bb320a8fe2debd2ae1b47f0f50bc10bae845c094

and now we perform SHA-256 hash on the result of the this recent SHA-256 hash as seen below in the screenshot...and we get this as

d61967f63c7dd183914a4ae452c9f6ad5d462ce3d277798075b107615c1a8a30

Now take the first 4 bytes of the second SHA-256 hash and this is the address checksum ie D61967F6

and then add the 4 checksum bytes at the end of extended RIPEMD-160 hash as hashed above and we get the 25-byte binary Bitcoin Address.

00010966776006953D5567439E5E39F86A0D273BEED61967F6

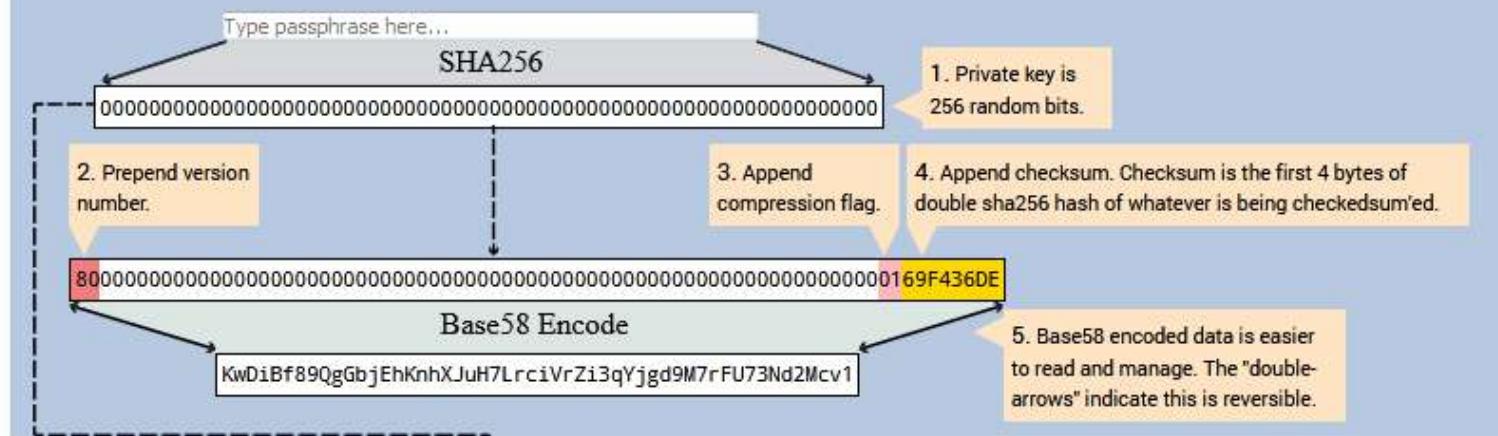
Now the last step...we Convert the result from a byte string into a base58 string using Base58Check encoding at <https://incoherency.co.uk/base58/>

Bitcoin Address :

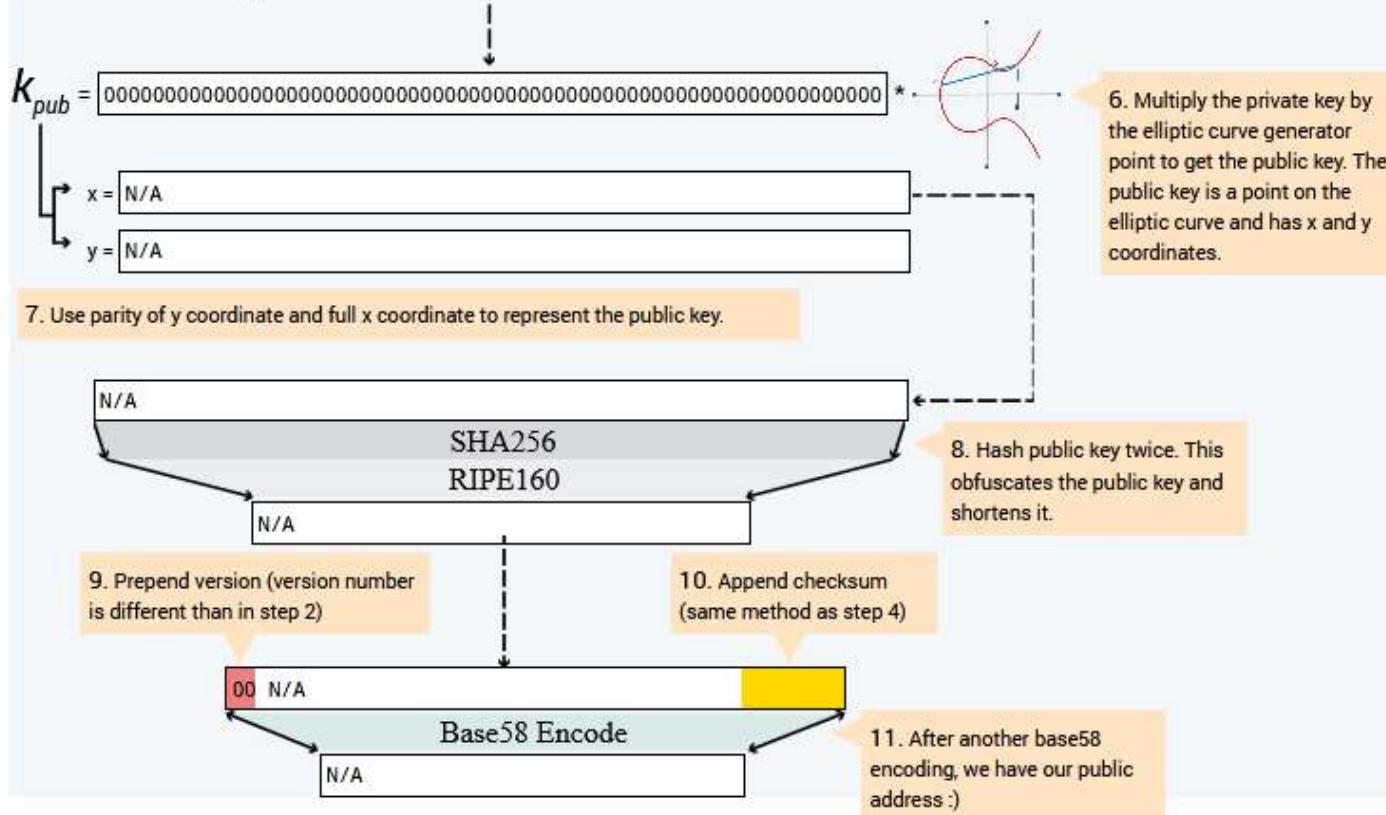
16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM

CHECK YOUR SELF AT <https://gobittest.appspot.com/Address>

Generate Private Key



Generate Public Key



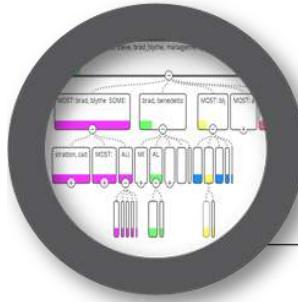
**1.46×10^{48} possible
Bitcoin Addresses**



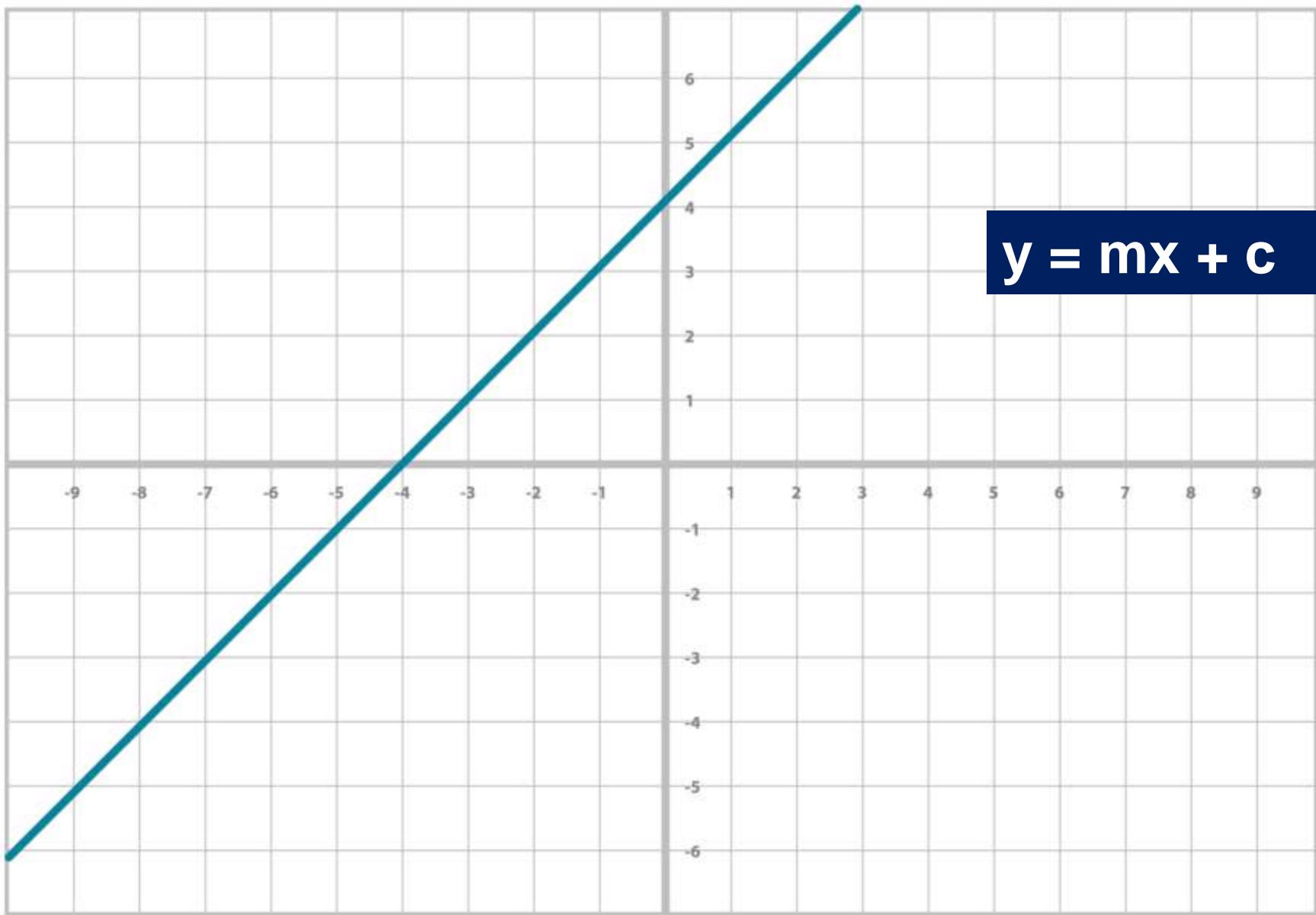
**That gives every
person on Earth
 2.05×10^{38} Different
Addresses**

Let's just revise ECC

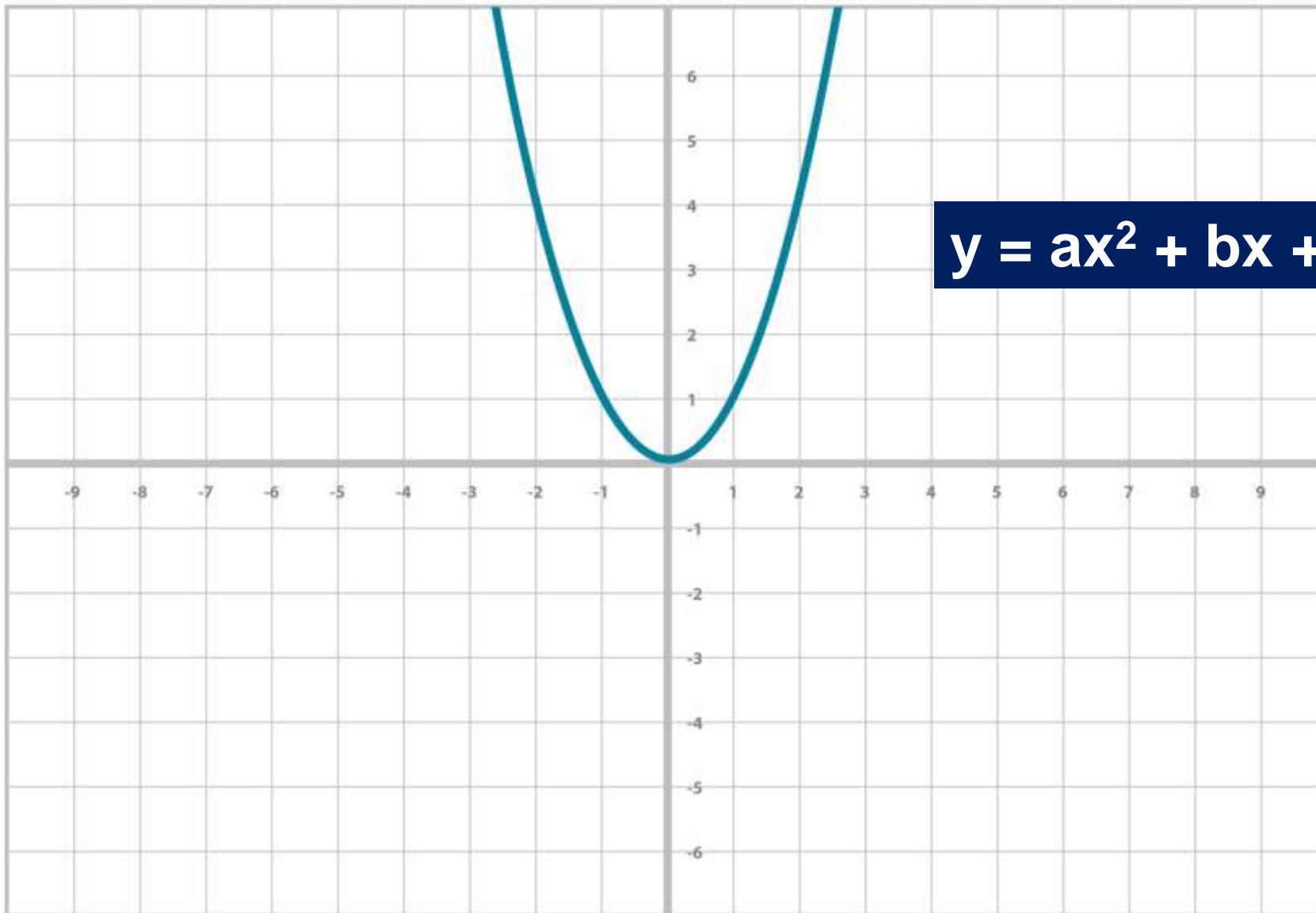
overview



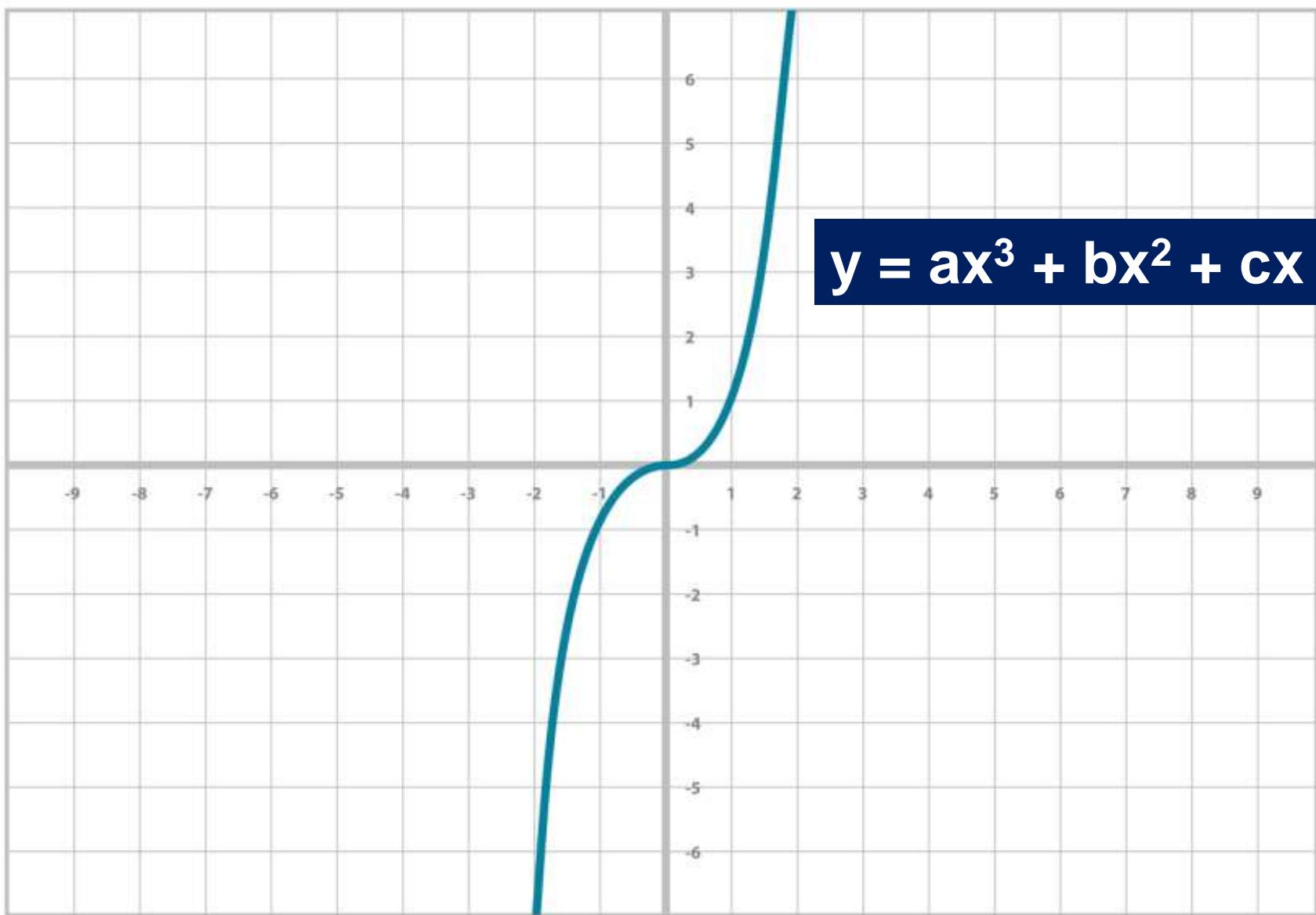
LINEAR EQUATION



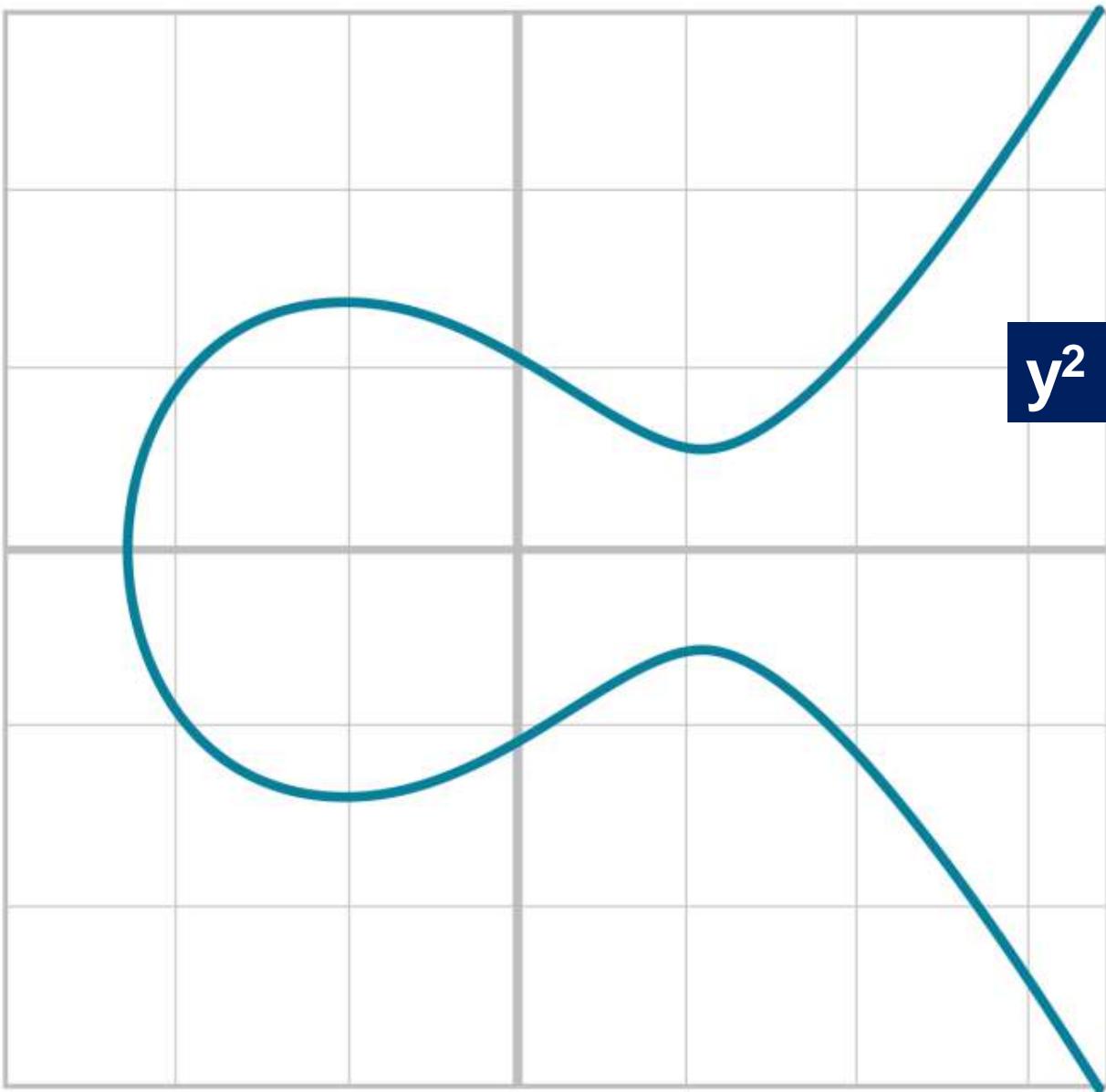
QUADRATIC EQUATION



CUBIC EQUATION

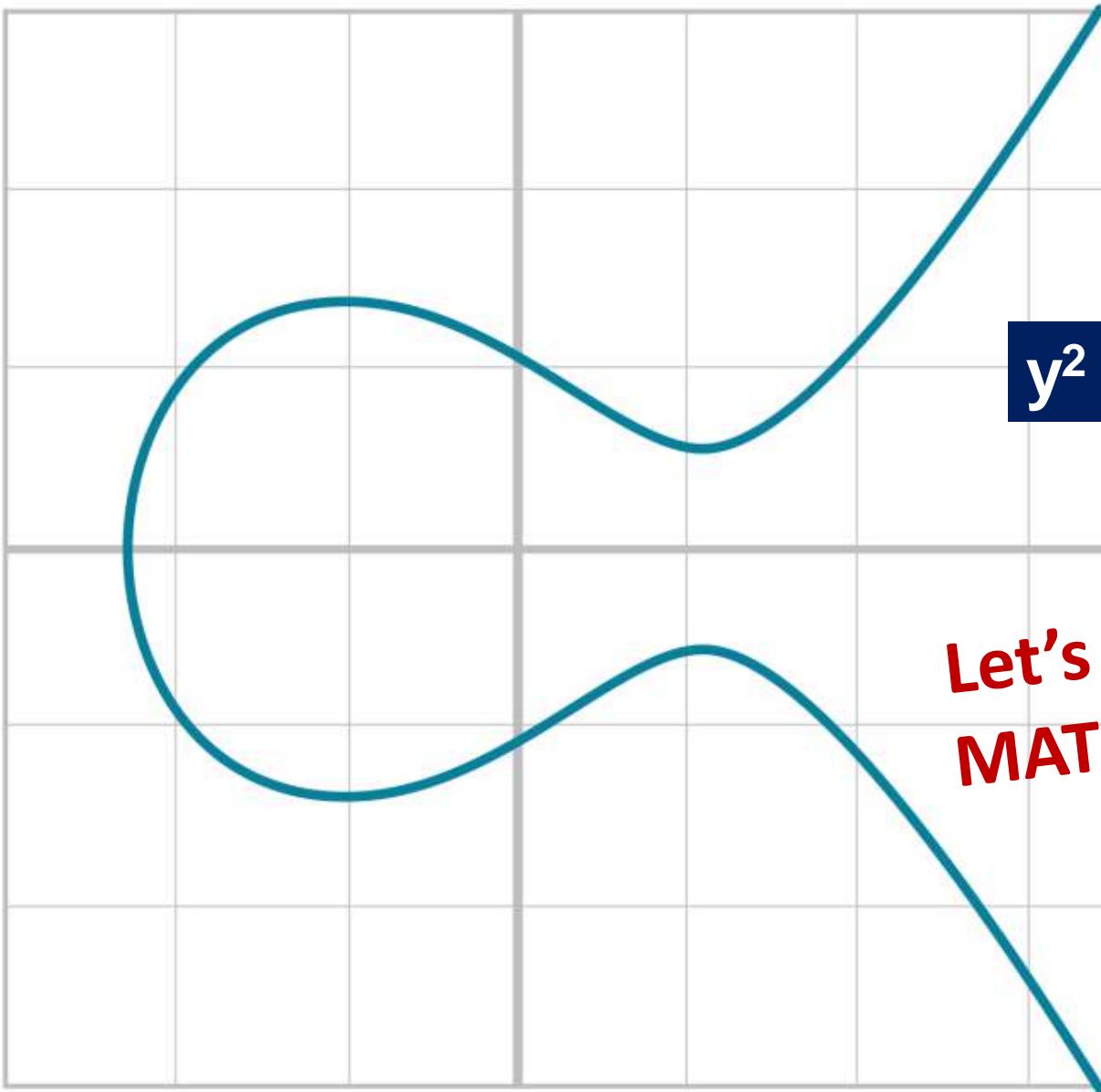


ELLIPTIC CURVE EQUATION



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

ELLIPTIC CURVE EQUATION



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

Let's see FINITE FIELD
MATHEMATICS in brief

FINITE FIELD

Also known as Galois Fields

Finite set which is a field; this means that multiplication, addition, subtraction and division (excluding division by zero) are defined and satisfy the rules of arithmetic.

The number of elements of a finite field is called its order or, sometimes, its size

FINITE FIELD PROPERTIES

- If a and b are in the set, $a + b$ and $a \cdot b$ are in the set.

PROPERTY CLOSED

- 0 exists and has the property $a + 0 = a$.

ADDITIVE IDENTITY

- 1 exists and has the property $a \cdot 1 = a$.

MULTIPLICATIVE IDENTITY

- If a is in the set, $-a$ is in the set, which is defined as the value that makes $a + (-a) = 0$.

ADDITIVE INVERSE

- If a is in the set and is not 0, a^{-1} is in the set, which is defined as the value that makes $a \cdot a^{-1} = 1$.

MULTIPLICATIVE INVERSE

FINITE FIELD PROPERTIES

- If a and b are in the set, $a + b$ and $a \cdot b$ are in the set.

PROPERTY CLOSED

- 0 exists and has the property $a + 0 = a$.

ADDITIVE IDENTITY

- 1 exists and has the property $a \cdot 1 = a$.

MULTIPLICATIVE IDENTITY

- If a is in the set, $-a$ is in the set, which is defined to make $a + (-a) = 0$.

ADDITIONAL

Sir ji,

- If a is in the set, what is the value of $a + a$?

MULTIPLICATIVE



BITCOIN & BLOCKCHAIN कहाँ है ?

NORMAL MATHS

ADDITION / SUBTRACTION

$11 + 6 =$

$17 - 6 =$

$8 + 14 =$

$4 - 12 =$

NORMAL MATHS

ADDITION / SUBTRACTION

$$11 + 6 = 17$$

$$17 - 6 = 11$$

$$8 + 14 = 22$$

$$4 - 12 = -8$$

FINITE FIELD with F 19

ADDITION - SUBTRACTION

$$11 + 6 =$$

$$17 - 6 =$$

$$8 + 14 =$$

$$4 - 12 =$$

FINITE FIELD with F 19

ADDITION - SUBTRACTION

$$11 + 6 = 17 \% 19 = \textcolor{red}{17}$$

$$17 - 6 =$$

$$8 + 14 =$$

$$4 - 12 =$$

FINITE FIELD with F 19

ADDITION - SUBTRACTION

$$11 + 6 = 17 \% 19 = \textcolor{red}{17}$$

$$17 - 6 = 11 \% 19 = \textcolor{red}{11}$$

$$8 + 14 =$$

$$4 - 12 =$$

FINITE FIELD with F 19

ADDITION - SUBTRACTION

$$11 + 6 = 17 \% 19 = \textcolor{red}{17}$$

$$17 - 6 = 11 \% 19 = \textcolor{red}{11}$$

$$8 + 14 = 22 \% 19 = \textcolor{red}{3}$$

$$4 - 12 =$$

FINITE FIELD with F 19

ADDITION - SUBTRACTION

$$11 + 6 = 17 \% 19 = \textcolor{red}{17}$$

$$17 - 6 = 11 \% 19 = \textcolor{red}{11}$$

$$8 + 14 = 22 \% 19 = \textcolor{red}{3}$$

$$4 - 12 = -8 \% 19 = \textcolor{red}{11}$$

FINITE FIELD with F 19

MULTIPLICATION

$$2 \times 4 =$$

$$7 \times 3 =$$

$$15 \times 4 =$$

$$11 \times 11 =$$

FINITE FIELD with F 19

MULTIPLICATION

$$2 \times 4 = 8 \% 19 = \mathbf{8}$$

$$7 \times 3 = 21 \% 19 = \mathbf{2}$$

$$15 \times 4 = 60 \% 19 = \mathbf{3}$$

$$11 \times 11 = 121 \% 19 = \mathbf{7}$$

FINITE FIELD with F 19

DIVISION

$$2/3 =$$

$$3/15 =$$

Fermat's Little Theorem

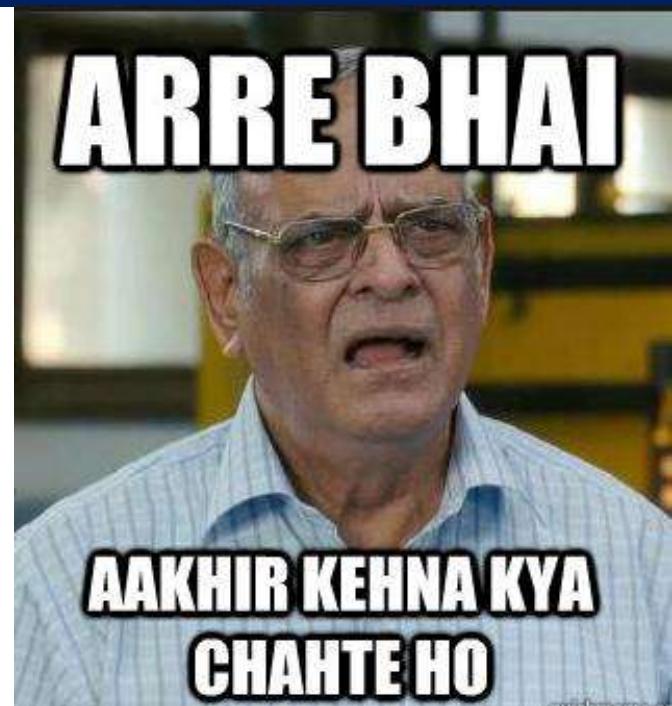
$$a^{p-1} \equiv 1 \pmod{p}$$

FINITE FIELD with F 19

DIVISION

$$2/3 = 2 \times 3^{(19-2)\%19} = 7$$

$$3/15 = 3 \times 15^{(19-2)\%19} = 4$$



Fermat's Little Theorem

$$a^{p-1} \equiv 1 \pmod{p}$$



WHY THIS KOLAVERI DI

**Y not simply use common
Maths?**



WHY THIS KOLAVERIDI

**If anyone has got a python terminal
access around on mobile or pc just add
two numbers**

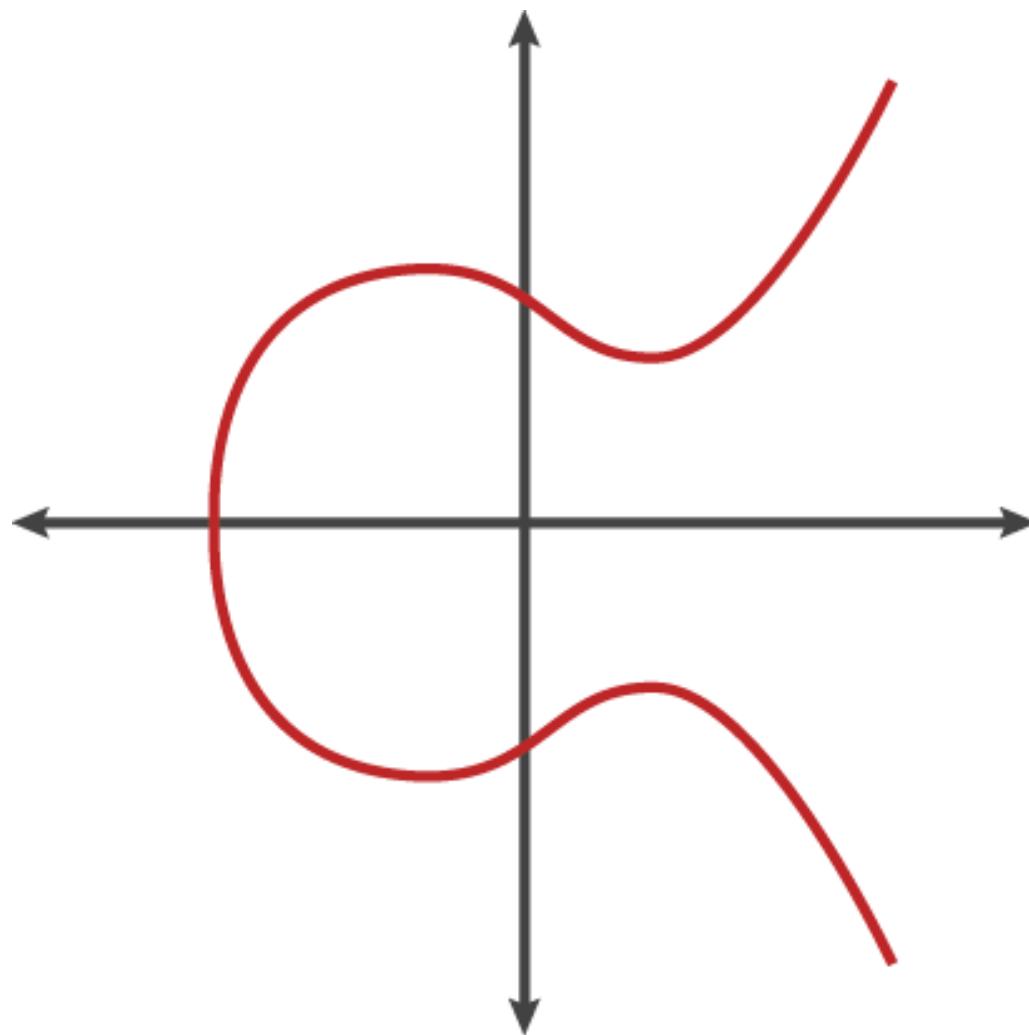
0.1 + 0.2 :

LET'S GO

Linux Terminal

ECDSA

ECDSA ('Elliptical Curve Digital Signature Algorithm') is the cryptography behind private and public keys used in Bitcoin.



ECDSA ADVANTAGE

Parameters	Elliptic Curve Key Length	RSA Key Length
secp192k1	192	1536
secp192r1	192	1536
secp224k1	224	2048
secp224r1	224	2048
secp256k1	256	3072
secp256r1	256	3072
secp384r1	384	7680
secp512r1	512	15360

**TRY
FIND
OUT
HOW
&
WHY?**

sextuple $T = (p, a, b, G, n, h)$ over a finite field F_p

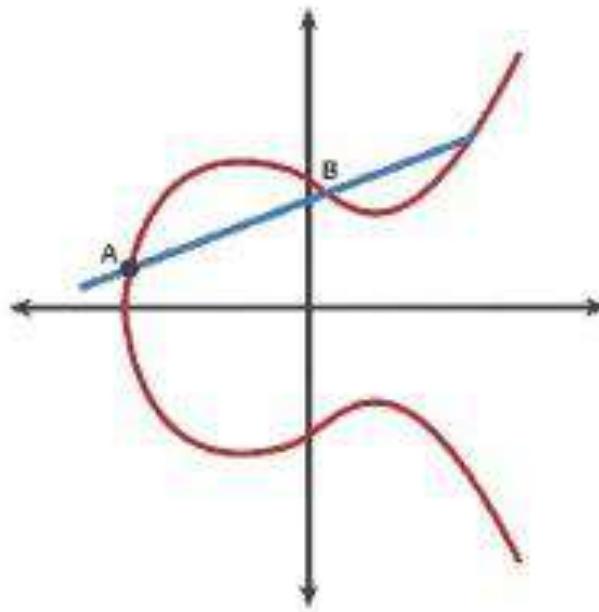
ECDSA

secp256k1 refers to the parameters of the elliptic curve used in **Bitcoin's public-key cryptography**, and is defined in *Standards for Efficient Cryptography (SEC)*



ECDSA

It consists of combining the math behind finite fields and elliptic curves to create **one way equations**, meaning you can choose your private key (some number) and easily calculate your public key (some other number).



A line passing through two points on an elliptic curve will pass through a third point

ECDSA

- **Bitcoin or Ethereum** uses Elliptic Curves (EC) to **generate private and public key pairs**
- **Small size – High security**
- **Standards for Efficient Cryptography Group (SECG) for efficient and interoperable cryptography**
- **The SECG has published a document** with a recommended set of elliptic curve domain parameters, referred by the **letters p, a, b, G, n, h**, referred to as the Elliptic Curve Domain Parameters.

2.4.1 Recommended Parameters secp256k1

The elliptic curve domain parameters over \mathbb{F}_p associated with a Koblitz curve `secp256k1` are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field \mathbb{F}_p is defined by:

$$\begin{aligned} p &= \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE} \\ &\quad \text{FFFFFC2F} \\ &= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 \end{aligned}$$

The curve $E: y^2 = x^3 + ax + b$ over \mathbb{F}_p is defined by:

$$\begin{aligned} a &= 00000000 00000000 00000000 00000000 00000000 00000000 00000000 \\ &\quad 00000000 \\ b &= 00000000 00000000 00000000 00000000 00000000 00000000 00000000 \\ &\quad 00000007 \end{aligned}$$

The base point G in compressed form is:

$$\begin{aligned} G &= 02 \text{ } 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 \\ &\quad 59F2815B 16F81798 \end{aligned}$$

and in uncompressed form is:

$$\begin{aligned} G &= 04 \text{ } 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 \\ &\quad 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 \\ &\quad A6855419 9C47D08F FB10D4B8 \end{aligned}$$

Finally the order n of G and the cofactor are:

$$\begin{aligned} n &= \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C} \\ &\quad D0364141 \\ h &= 01 \end{aligned}$$

2.4.1 Recommended Parameters secp256k1

The elliptic curve domain parameters over \mathbb{F}_p associated with a Koblitz curve secp256k1 are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field \mathbb{F}_p is defined by:

$$\begin{aligned} p &= \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE} \\ &\quad \text{FFFFFFC2F} \\ &= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 \end{aligned}$$

The curve E : $y^2 = x^3 + ax + b$ over \mathbb{F}_p is defined by:

$$\begin{aligned} a &= 00000000 00000000 00000000 00000000 00000000 00000000 00000000 \\ &\quad 00000000 \\ b &= 00000000 00000000 00000000 00000000 00000000 00000000 00000000 \\ &\quad 00000007 \end{aligned}$$

The base point G in compressed form is:

$$G = \text{02 } 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9$$
$$\quad \text{59E238C9B } 16F81798$$

and in uncompressed form is:

$$G = \text{04 } 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9$$
$$\quad \text{F2815B } 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448$$
$$\quad \text{A6855419 9C47D08F FB10D4B8}$$

Finally the order n of G and the cofactor are:

$$n = \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C}$$
$$\quad \text{D0364141}$$

$$h = 01$$

2.4.1 Recommended Parameters secp256k1

The elliptic curve domain parameters over \mathbb{F}_p associated with a Koblitz curve secp256k1 are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field \mathbb{F}_p is defined by:

$$\begin{aligned} p &= \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF}\\ &\quad \text{FFFFFFC2F}\\ &= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 \end{aligned}$$

The curve $E: y^2 = x^3 + ax + b$ over \mathbb{F}_p is defined by:

$$\begin{aligned} a &= 00000000 00000000 00000000 00000000 00000000 00000000 00000000\\ &\quad 00000000\\ b &= 00000000 00000000 00000000 00000000 00000000 00000000 00000000\\ &\quad 00000007 \end{aligned}$$

The base point G in compressed form is:

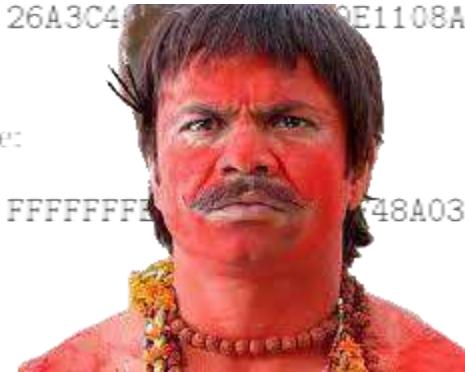
$$G = \text{02 } 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9
59F2815B 16F81798$$

and in uncompressed form is:

$$G = \text{04 } 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9
F2815B 16F81798 483ADA77 26A3C4A2 E0A986E9 C4B9E1108A8 FD17B448
A6855419 9C47D08F FB10D4B8$$

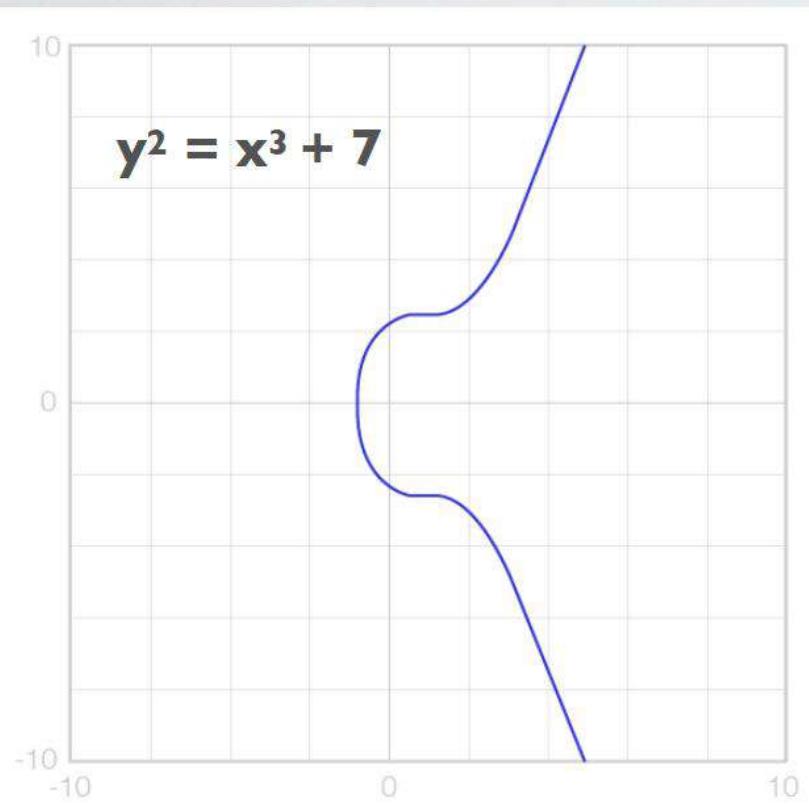
Finally the order n of G and the cofactor are:

$$\begin{aligned} n &= \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF}\\ &\quad \text{D0364141}\\ h &= 01 \end{aligned}$$



ECDSA: BITCOIN EQUATION

SECP256k1



- Bitcoin and Ethereum both uses the same secp256k1 elliptic curve domain parameters.
- secp256k1 uses the following elliptic curve equation: $y^2 = x^3 + ax + b$
- In the following slides we will go thru each parameter p, a, b, G, n, h
 - Parameter a = 0
 - Parameter b = 7

<https://www.secg.org/sec2-v2.pdf>

ECDSA: BITCOIN EQUATION

SECP256K1: PARAMETER P

- A finite field is a field with a finite number of elements, defined by parameter p, which is a prime number. Thus the finite field $F_p = \{0, \dots, p - 1\}$
- This means that modulo p should be used in the equation:
 - The EC equation: $y^2 = x^3 + ax + b$
 - The EC equation with modulo operation: $y^2 = x^3 + ax + b \pmod{p}$
- $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 = 2^{256} - 2^{32} - 977$
- $p = \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F}$

ECDSA: BITCOIN EQUATION

SECP256K1: PARAMETER G

- The basepoint G , also known as the generator or primitive element, is a predetermined point (X_G, Y_G) on the elliptic curve that everyone uses to compute other points on the curve.

ECDSA: BITCOIN EQUATION

DOT OPERATIONS

- There are two operations often called dot operations which can be applied to a base point (aka generator G) (x_G, y_G) on the elliptic curve:
 - Point addition
 - Point doubling
- The elliptic curve ($y^2 = x^3 + 7$) has the following properties:
 - If a line intersects two points P and Q, it intersects a third point on the curve -R.
 - If a line is tangent to the curve, it intersects another point on the curve.
 - All vertical lines intersect the curve at infinity.

ECDSA: BITCOIN EQUATION

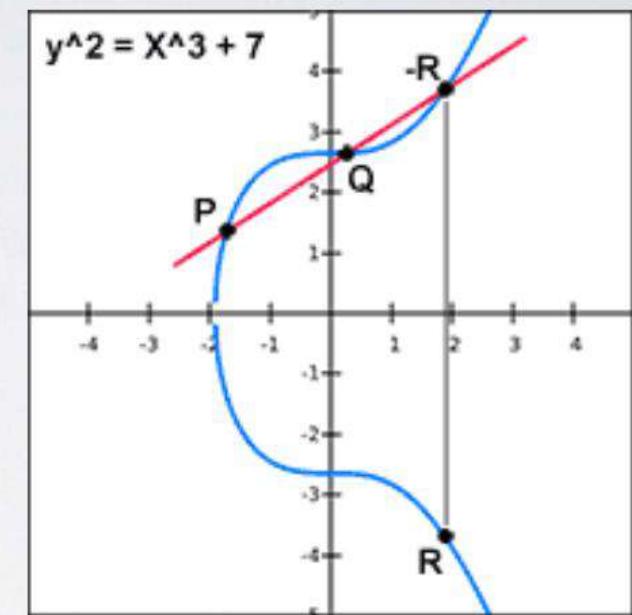
POINT ADDITION

- Adding two points P and Q on a elliptic curve ($P \neq Q$).
- Geometry approach:
 - Draw a straight line between $P (x_1, y_1)$ and $Q (x_2, y_2)$.
 - The line will intersect the elliptic curve at exactly one more point $-R$.
 - The reflection of the point $-R$ with respect to x-axis gives the point $R (x_3, y_3)$, which is the results of addition of points P and Q.
- *Point addition* does not mean addition of the x or y coordinates of P and Q. It is just a name given for this approach.

ECDSA: BITCOIN EQUATION

POINT ADDITION

- Mathematical approach (ECAdd):
 - $\lambda = (y_G - y) \text{ modinv}(x_G - x) \pmod{p}$
 - $x_R = \lambda^2 - x - x_G \pmod{p}$
 - $y_R = \lambda(x - x_R) - y \pmod{p}$
- λ is the slope of the line
- x and y are the coordinates of P
- Point Q is the base point G (x_G, y_G)



ECDSA: BITCOIN EQUATION

The canonical form is

$$y^2 = (x^3 + ax + b) \bmod p$$

so the curve is defined by the constants

$$a = 0$$

$$b = 7$$

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$$

ECDSA: BITCOIN EQUATION

Thus putting the *a* and *b* values

$$y^2 = (x^3 + 7) \bmod p$$

ECDSA: Deriving public key

Public key = Private key * Generator point

G is a point (g_x, g_y) on the secp256k1 curve

$g_x =$

5506626302227734366957871889516853432625060
3453777594175500187360389116729240

$g_y =$

3267051002075881697808308513050704318447127
3380659243275938904335757337482424

ECDSA: Deriving public key

Public key = Private key * Generator point

G is a point (g_x, g_y) on the secp256k1 curve

$\text{g}_x =$

5506626302227734366957871880853432625060
345377759417550018736038911240

$\text{g}_y =$

3267051002075881697808
338065924327593890433



Kaun hain ye log
kahan se aate hain ye log

Public.py ECC

Private to Bitcoin Address

LET'S GO





Private Key



Public Key



**BASICALLY CHUNKS OF INFO
THAT CAN BE USED TO
MATHEMATICAL
GUARANTEE ABOUT MESSAGES**

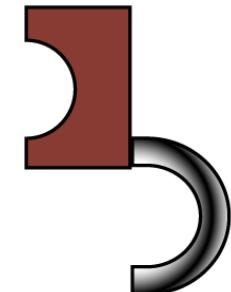


THATS
ME

Private key



Public key



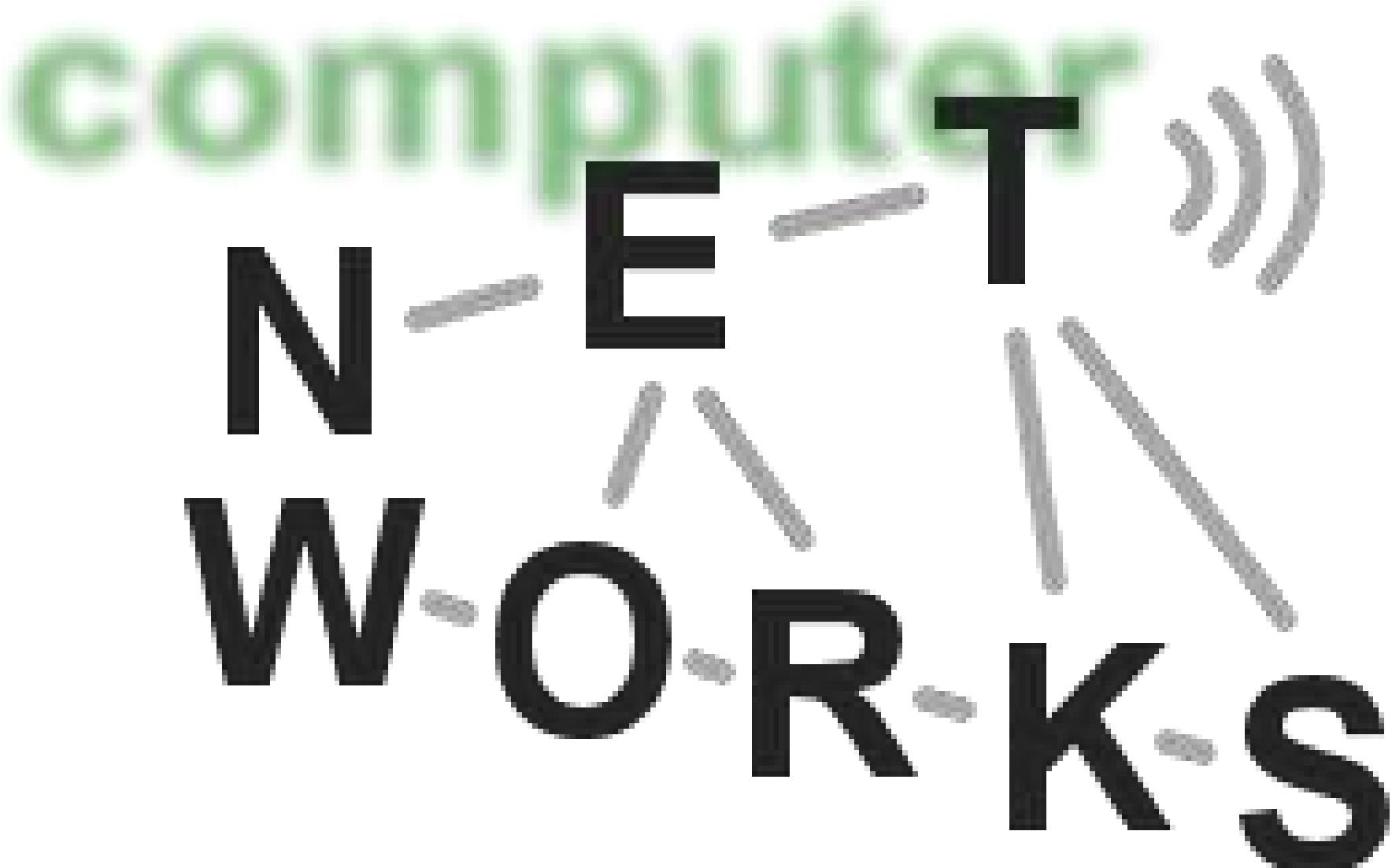
4

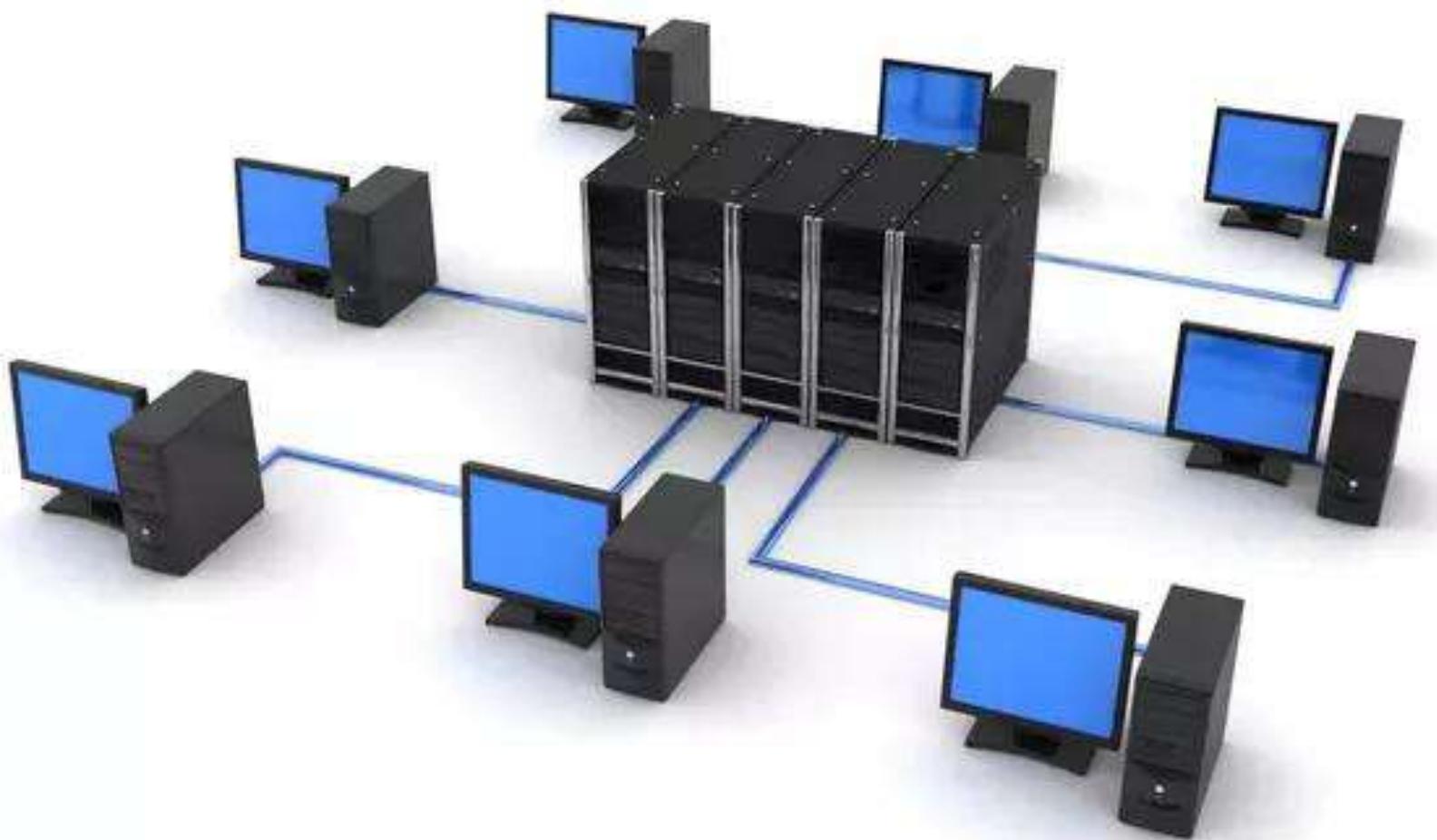
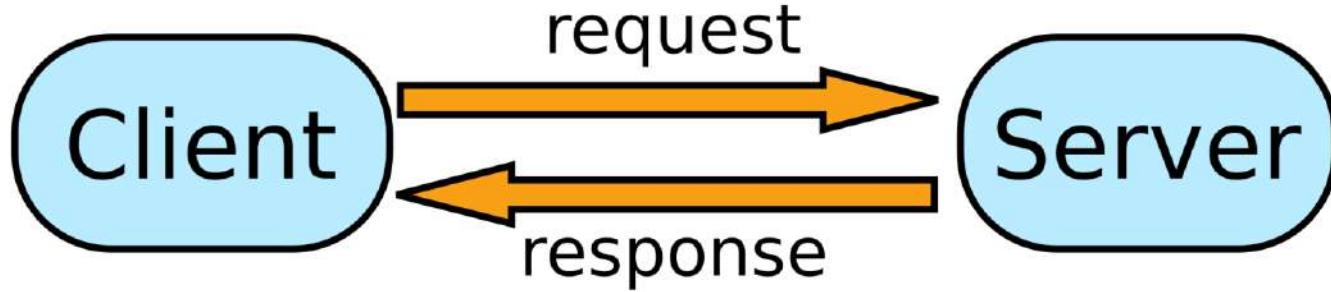


CONCRETE

FOURTH

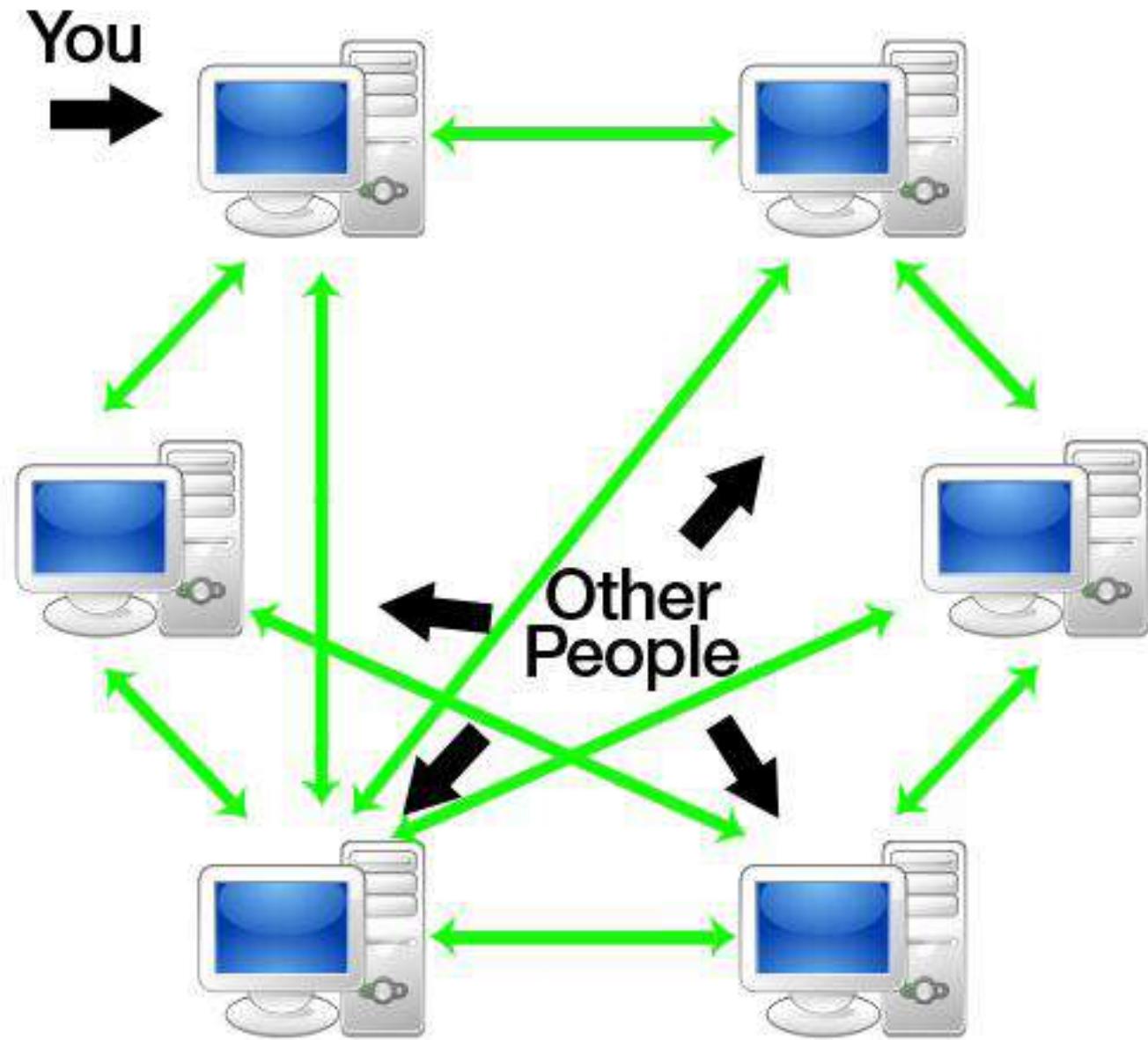
Computer
N-E-T
W-O-R-K-S





Peer-to-Peer (P2P) network is created when **two or more** PCs are connected & share resources **without** going through a separate **server** computer

Peer-to-Peer Model



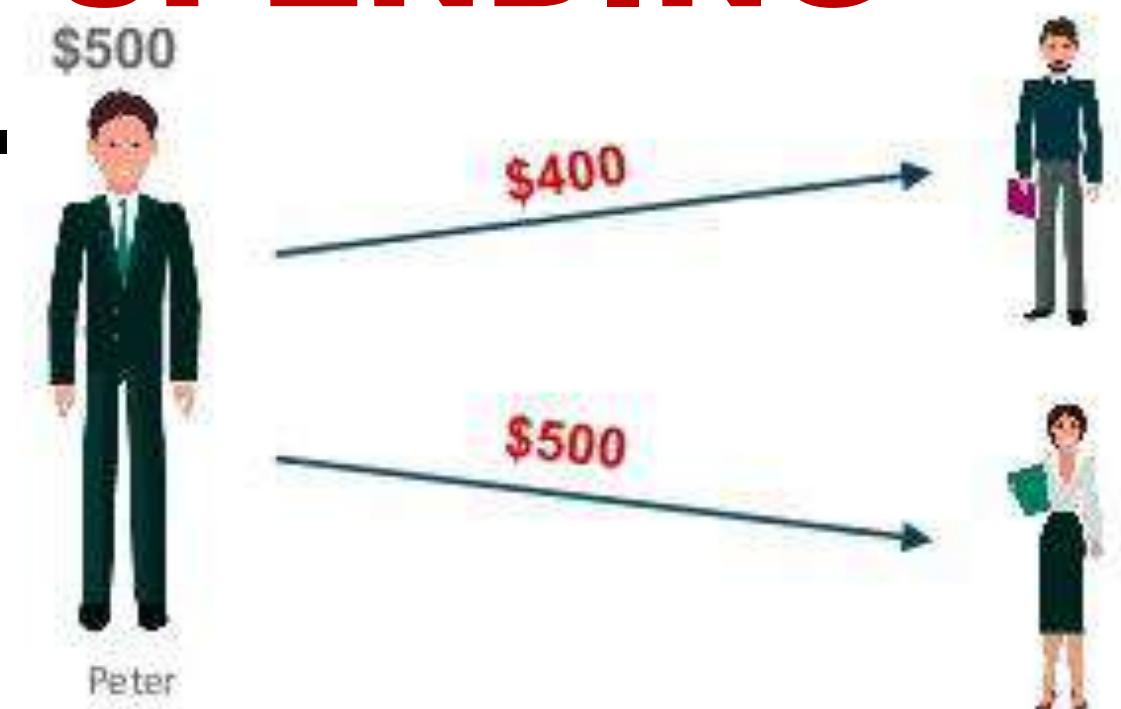
5

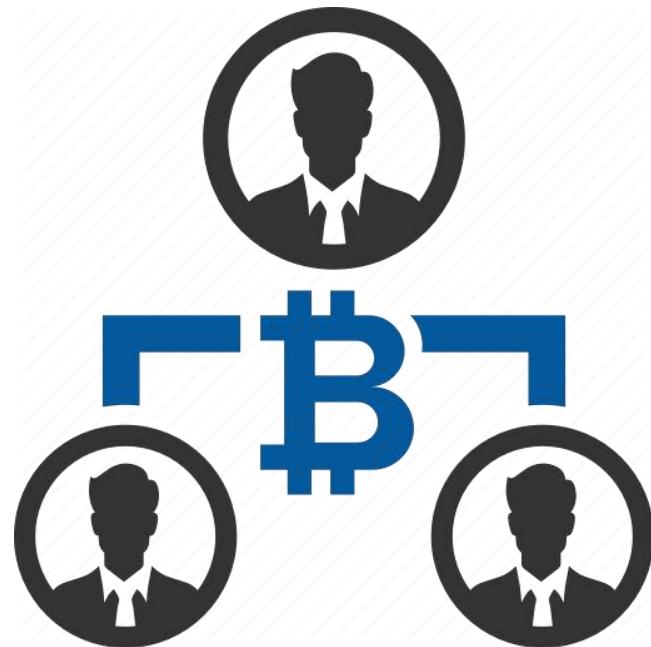


CONCEPT

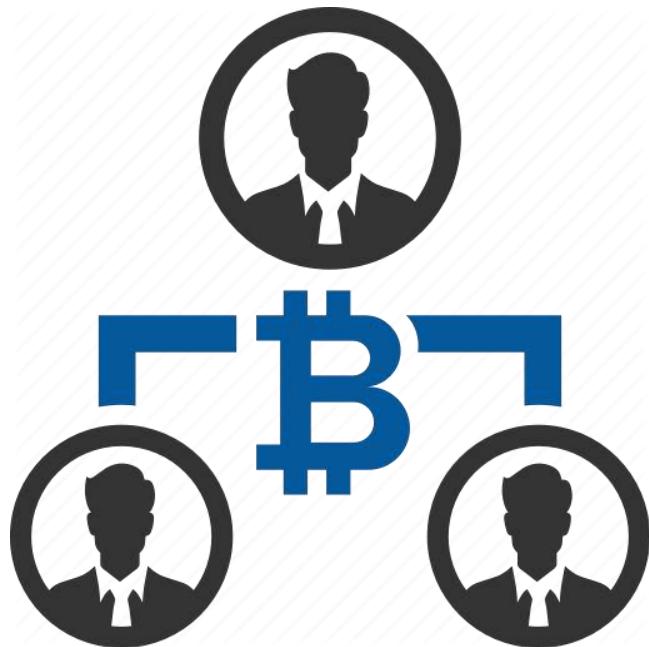
FIFTH

**E-CURRENCY HAS BEEN
ATTEMPTED IN PAST
BUT FAILED OWING TO
BEYOND CONTROL
DOUBLE SPENDING
PROBLEM.**





Double-spending is a potential flaw in a digital cash scheme in which the same **single digital token can be spent more than once**. Unlike physical cash, a digital token consists of a digital file that can be duplicated or falsified.



To resolve **Double-spending** issue,
CONSENSUS mechanism is used

A close-up photograph showing a group of people's hands stacked together in a circular pattern. The hands belong to individuals with various skin tones and clothing styles, including a green plaid shirt, a blue denim jacket, and a red and white plaid shirt. The hands are positioned with fingers interlaced, creating a sense of unity and teamwork.

CONSENSUS



**Consensus is defined as a
GENERAL AGREEMENT
of a state**



That MEANS, if ANUPAM sends Rs 100 worth of Bitcoin to RAHUL, ANUPAM will lose Rs 100 worth of Bitcoin, and RAHUL will gain Rs 100 worth of Bitcoin



**Every CLEAN TRANSACTION
has to be recorded on the Bitcoin
public ledger, and a
CONSENSUS ALGORITHM
ensures no malicious
transactions nor changes can be
made on the Blockchain itself**

Proof of Elapsed Time (PoET)

Proof of Authority (PoA)

Proof of Capacity

Proof of Burn

Proof of Activity

CONSENSUS TYPES

F·E·W

Delegated Proof of Stake (DPoS)

Byzantine Fault Tolerance

Proof of Importance

Direct Acyclic Graphs (DAGs)

6

CONCRETE

SIXTH

VERY IMPORTANT

ATTENTION!

```
355 #access {  
356   display: inline-block;  
357   height: 69px;  
358   float: right;  
359   margin: 11px 28px 0px 0px;  
360   max-width: 800px;  
361 }  
362  
363 #access ul {  
364   font-size: 13px;  
365   list-style: none;  
366   margin: 0 0 0 -0.8125em;  
367   padding-left: 0;  
368   padding-top: 10px;  
369 }  
370  
371 #access ul li {  
372   background-color: #f0f0f0;  
373   border: 1px solid #e0e0e0;  
374   border-radius: 10px;  
375   color: #333333;  
376   display: inline-block;  
377   height: 28px;  
378   line-height: 28px;  
379   margin-right: 10px;  
380   padding: 0 10px;  
381 }
```



What is Proof-of-Work?

PROOF OF WORK

***Proof Of Work* Is A Piece Of Data
Which Is Difficult To Produce But
Easy For Others To Verify And Which
Satisfies Certain Requirements**

Proof of Work

**Bitcoin Uses
The Hashcash Proof
Of Work System.**



Byzantine General Problem

REACHING A CONSENSUS.... & BLOCKCHAIN



Proof of Work

BYZANTINE GENERALS

& WHY IS IT IMPORTANT FROM A

BLOCKCHAIN PERSPECTIVE?



**ATTEMPTING
TO EXPLAIN THE SAME IN A**



FORM

**FOR EASY
ASSIMILATION**

**Ahead explanation
demands your**

**EARS ATTENTION
& FOCUS**

(FOUNDATION OF BITCOIN MINING CONCEPTS)

BYZANTINE GENERAL CONSENSUS



ARMY 1



ENEMY FORT TO BE
ATTACKED



ARMY 2

IN THE BACK OLD DAYS, THERE WERE TWO ARMY'S 1 & 2, DESIRING TO ATTACK A ENEMY FORT

BYZANTINE GENERAL CONSENSUS



ARMY 1



ENEMY FORT TO BE
ATTACKED



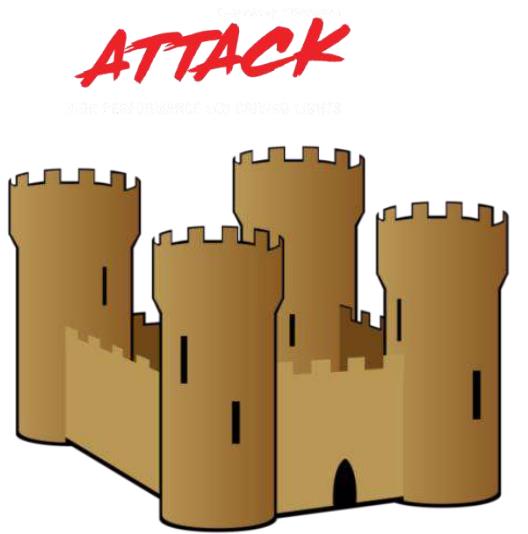
ARMY 2

**CONDITION IS THAT BOTH HAVE TO
ATTACK AT THE SAME TIME, ELSE THEY
LOSE**

BYZANTINE GENERAL CONSENSUS



ARMY 1



ARMY 2

**SO A CONSENSUS IS REQUIRED
(WHAT DAY/TIME TO ATTACK)**

BYZANTINE GENERAL CONSENSUS

Ideal
Conditions



ARMY 1



ARMY 2



MESSENGER SENT FROM 1 TO 2

BYZANTINE GENERAL CONSENSUS

Ideal
Conditions



ARMY 1



ENEMY FORT TO BE
ATTACKED



ARMY 2

MESSENGER SENT FROM 1 TO 2

BYZANTINE GENERAL CONSENSUS

Ideal
Conditions



ARMY 1



ENEMY FORT TO BE
ATTACKED



ARMY 2



MESSENGER SENT FROM 1 TO 2

BYZANTINE GENERAL CONSENSUS

Ideal
Conditions



ARMY 1



ENEMY FORT TO BE
ATTACKED

ARMY 2



MESSENGER SENT FROM 1 TO 2

BYZANTINE GENERAL CONSENSUS

Ideal
Conditions



ARMY 1



ARMY 2



MESSENGER SENT FROM 2 TO 1

BYZANTINE GENERAL CONSENSUS

Ideal
Conditions



ARMY 1



ENEMY FORT TO BE
ATTACKED



ARMY 2



MESSENGER SENT FROM 2 TO 1

BYZANTINE GENERAL CONSENSUS

Ideal
Conditions



ARMY 1



ENEMY FORT TO BE
ATTACKED



ARMY 2

MESSENGER SENT FROM 2 TO 1

BYZANTINE GENERAL CONSENSUS

Ideal
Conditions



ARMY 1



ENEMY FORT TO BE
ATTACKED

ARMY 2



MESSENGER SENT FROM 2 TO 1

BYZANTINE GENERAL CONSENSUS

Ideal
Conditions



ARMY 1



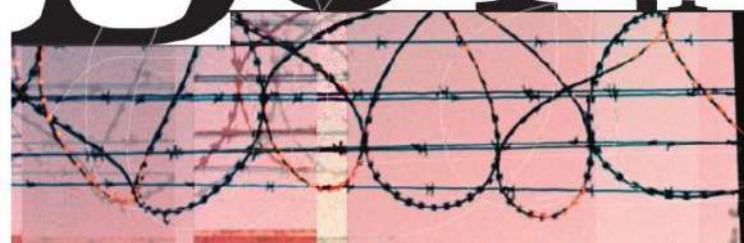
ARMY 2



**BOTH GENERALS AGREE AS PER
EXCHANGE OF MESSAGE**

BYZANTINE GENERAL CONSENSUS

BUT F



MESSINGER is

COMPROMISED

Intercepted



BRIBED

BYZANTINE GENERAL CONSENSUS



thus

**MESSAGE HAS CHANCES OF
BEING COMPROMISED**

BYZANTINE GENERAL CONSENSUS



ARMY 1



ENEMY FORT TO BE
ATTACKED



ARMY 2

thus SECURE COMMUNICATION
REQUIRED

BYZANTINE GENERAL CONSENSUS



ARMY 1



ARMY 2

HOW TO ENSURE GUARANTEED
UNALTERED MESSAGE EXCHANGE?

BYZANTINE GENERAL CONSENSUS

“In fact it was proved **indisputably**—that the problem has **no true solution**. That’s **not to say** computers cannot **communicate** with each other **reliably**, but **100% certainty is not possible**. Best efforts simply make communication **very very reliable but never foolproof**.”

BYZANTINE GENERAL CONSENSUS

PROOF OF WORK IS THE ANSWER



BYZANTINE GENERAL CONSENSUS

ATTACK MONDAY HASH

8cd65c330ce4d0c58a45e676c2d08f0ddca6
c61f3b0a927ade10368d2d5aae6e

BYZANTINE GENERAL CONSENSUS

NOW WE place



CONDITION

BYZANTINE GENERAL CONSENSUS

NOW WE place

CONDITION

PREfix

BYZANTINE GENERAL CONSENSUS

THE **CONDITION** IS THAT
THE **PREFIX** OF THE
OUTPUT HASH SHOULD
BE SUCH THAT THE **HASH** IS
PREFIXED BY 7 '0's

BYZANTINE GENERAL CONSENSUS

ATTACK MONDAY HASH

DESIRED

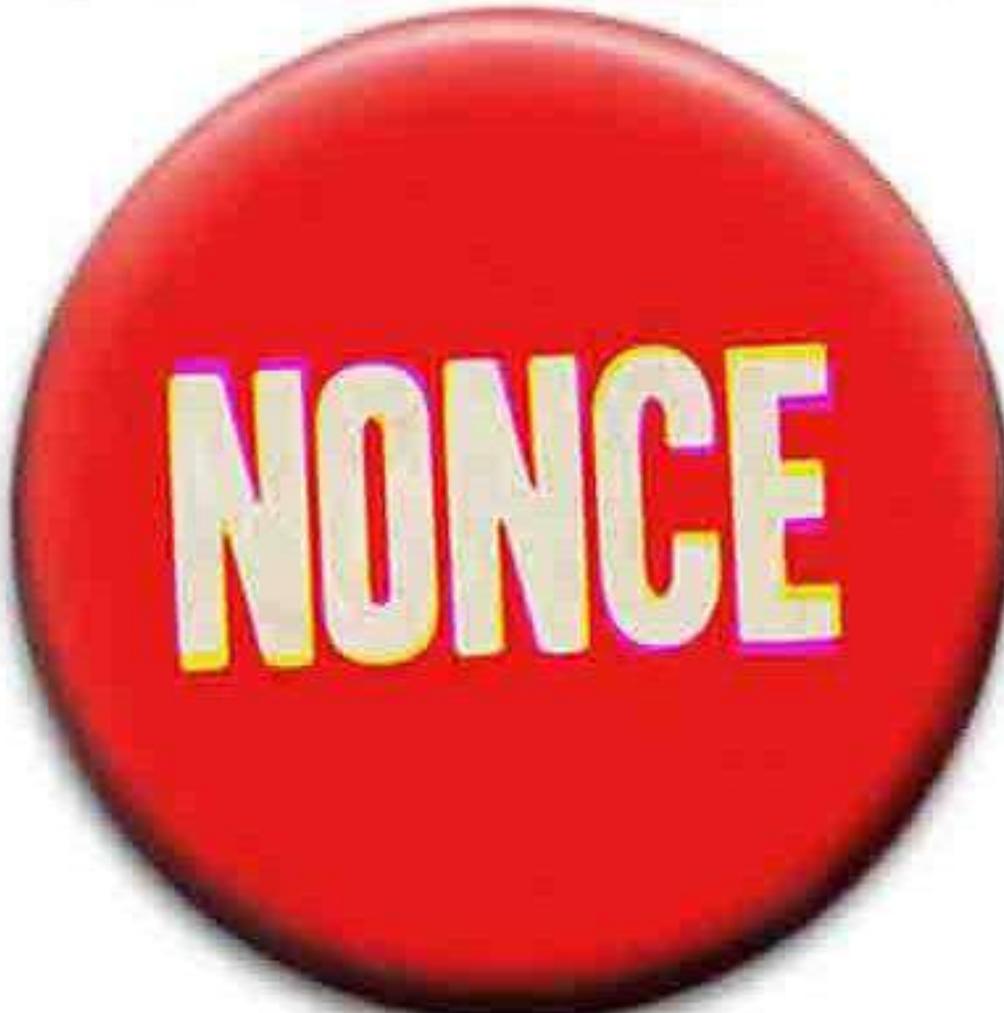
Output

0000000d1a2ea819ed13742fe7
386a34c25bb48e99b1ba8327c3
9551f6da5c01f98

BYZANTINE GENERAL CONSENSUS

How Do You Do That?

BYZANTINE GENERAL CONSENSUS



NONCE

BYZANTINE GENERAL CONSENSUS

ATTACK MONDAY HASH

8cd65c330ce4d0c58a45e676c2d08f0d
dca6c61f3b0a927ade10368d2d5aae6e

NONCE : 61584

0000000d1a2ea819ed13742fe7386a34c25
bb48e99b1ba8327c39551f6da5c01f98

BYZANTINE GENERAL CONSENSUS

**NONCE CANNOT BE
CALCULATED BY A
FORMULA,**

IT CAN ONLY BE GUESSED

BYZANTINE GENERAL CONSENSUS

**DIFFICULT TO CALCULATE
EASY TO VERIFY**

BYZANTINE GENERAL CONSENSUS



ARMY 1



ARMY 2

MESSAGE GOES WITH NONCE

BYZANTINE GENERAL CONSENSUS



ARMY 1



ARMY 2



MESSAGE GOES WITH NONCE

BYZANTINE GENERAL CONSENSUS



ARMY 1



ARMY 2

MESSAGE VERIFIED WITH NONCE

BYZANTINE GENERAL CONSENSUS



ARMY 1



ARMY 2

MESSENGER RETURNS & CONFIRMS

BYZANTINE GENERAL CONSENSUS



ARMY 1



ENEMY FORT TO BE
ATTACKED



ARMY 2

MESSENGER RETURNS & CONFIRMS

BYZANTINE GENERAL CONSENSUS



**CONSENSUS REACHED TO ATTACK AT
A COMMON TIME**

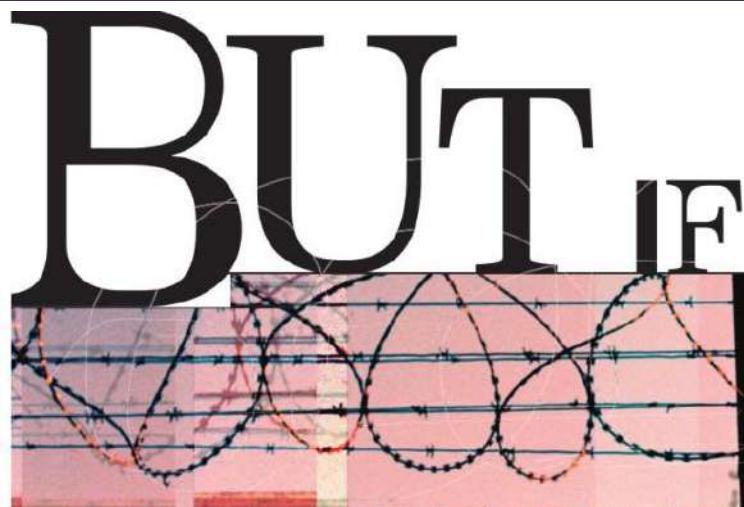
BYZANTINE GENERAL CONSENSUS

But our **STORY** doesn't end here.

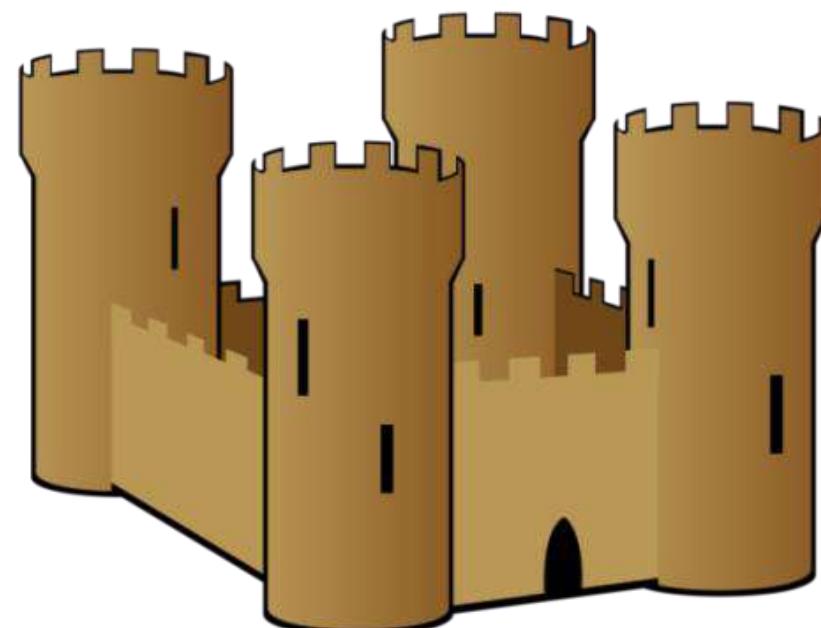
BYZANTINE GENERAL CONSENSUS

The town is now well aware of the tricks that these generals are using, so they simply purchase a giant supercomputer and when they catch a messenger they now have the computing resources to modify the nonce so that the seven '0' s property is satisfied.

BYZANTINE GENERAL CONSENSUS



FORT READY ^{WITH}
THAT MUCH COMPUTING
POWER



EQuIP



COMPUTER
HARDWARE

BYZANTINE GENERAL CONSENSUS

solution

**WE ADD MORE COMPUTING
REQUIREMENTS & MAKE IT
PRACTICALLY IMPOSSIBLE
FOR THE FORT TO SOLVE THE
NONCE**

BYZANTINE GENERAL CONSENSUS

**What's the connect with
BITCOIN CONSENSUS?**

**here&
Now**

BYZANTINE GENERAL CONSENSUS

Let's now say that there is not just two generals and one city, but lots of generals and lots of cities. Idea works best when we have many, many cities

BYZANTINE GENERAL CONSENSUS



https://www.reddit.com/r/Buttcoin/comments/4qa12v/byzantine_generals_proofofwork_for_dummies/ SOURCE

BYZANTINE GENERAL CONSENSUS

SATOSHI'S IDEA IN A NUTSHELL

The generals all combine their many messages into a **SINGLE GIANT MESSAGE** (a “block”) which gets but a **SINGLE NONCE** at the end of it

GENERAL G¹ : WE ATTACK AT NOON!

GENERAL G² : WE ATTACK AT DAWN!

GENERAL G³ : WE ATTACK AT DUSK!

...

GENERAL G¹⁷⁴: WE ATTACK AT MIDNIGHT!

h9Klemoa3DheeMqz9x77ebaomEqz12f3Ba3e08e

BYZANTINE GENERAL CONSENSUS

All Generals Take The Combined Message-block and set all of their computers to go on the great nonce hunt. Perhaps there are a thousand armies, and each army has many computers. Their combined efforts may find a working nonce in a reasonable amount of time.

And it only takes *one* of them finds the nonce that satisfies the requirements: once one finds it, they immediately share it with all the others.

BYZANTINE GENERAL CONSENSUS

**IS THERE A QUESTION
WORRYING YOU?**

BYZANTINE GENERAL CONSENSUS

IS THERE A QUESTION WORRYING YOU?

What if *all* of the cities bought supercomputers and did the same thing the generals did, team-up to find a nonce?

BYZANTINE GENERAL CONSENSUS

Yes, they could do that, at considerable expense. (Akin to the “51% attack” — it works if the cities have as much or more computing power as all the armies combined.)

It's Not Impossible to Defeat this scheme, but the generals have made things very hard on attempts of the cities by teaming up.

BYZANTINE GENERAL CONSENSUS

While in Bitcoin we can see the PRE-FIXED ZERO's in Bitcoin explorer...in Ethereum we don't see in the Ethereum explorer as it is seen in encoded form..the command line to check the zero's in ETHEREUM blockchain is

ethminer --check-pow <headerHash><seedHash><difficulty><nonce>

MINING

Mining is the process by which new Bitcoin is added to the money supply



Mining serves to secure the Bitcoin system against fraudulent transactions or double-spend



Miners provide processing power to the Bitcoin network in exchange for the opportunity to be rewarded Bitcoin.

MINING

Miners validate **new transactions** and record them on the global ledger



A new block, containing transactions that occurred since the last block, is “mined” every 10 minutes



Transactions that become part of a block and added to the blockchain are considered “**CONFIRMED**”

MINING

The process of new coin generation is called **MINING**, because the reward is designed to simulate diminishing returns, just like mining for precious metals



Bitcoin's money supply is created through mining, similar to how a central bank issues new money by printing bank notes.

MINING

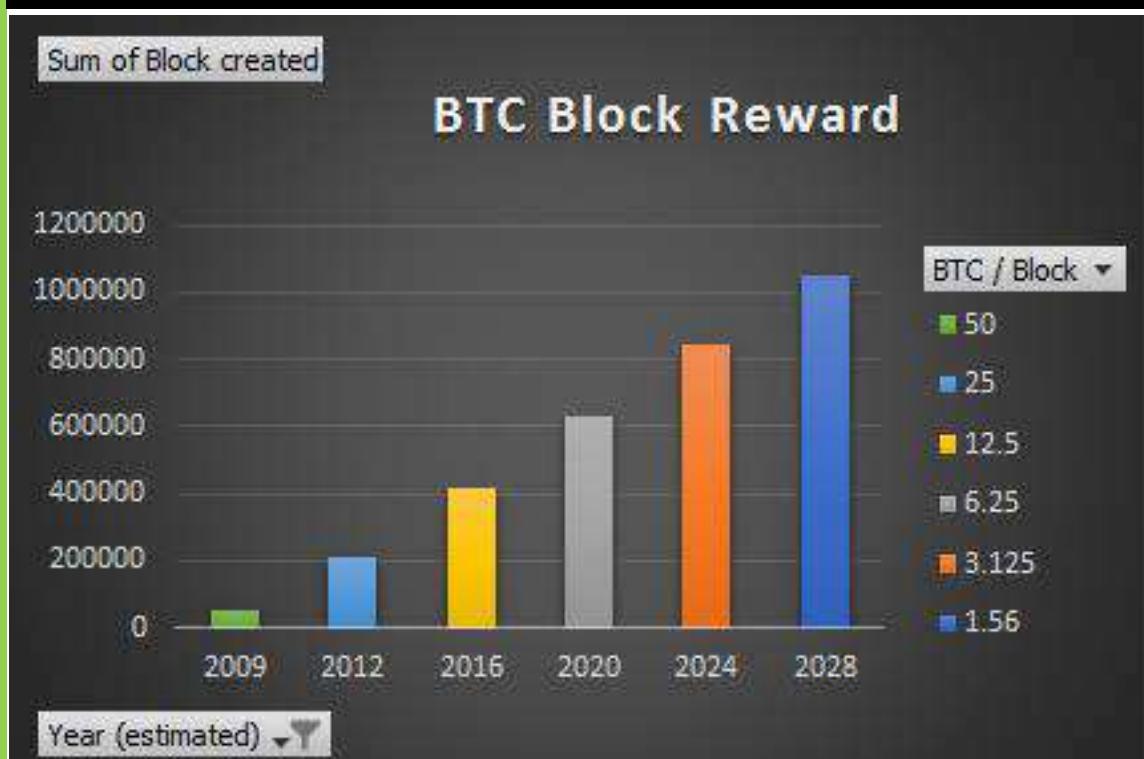
The amount of newly created bitcoin a miner can add to a block decreases approximately every four years (or precisely every 210,000 blocks).



It started at 50 bitcoin per block in January of 2009 and halved to 25 bitcoin per block in November of 2012. It will halve again to 12.5 bitcoin per block sometime in 2016.

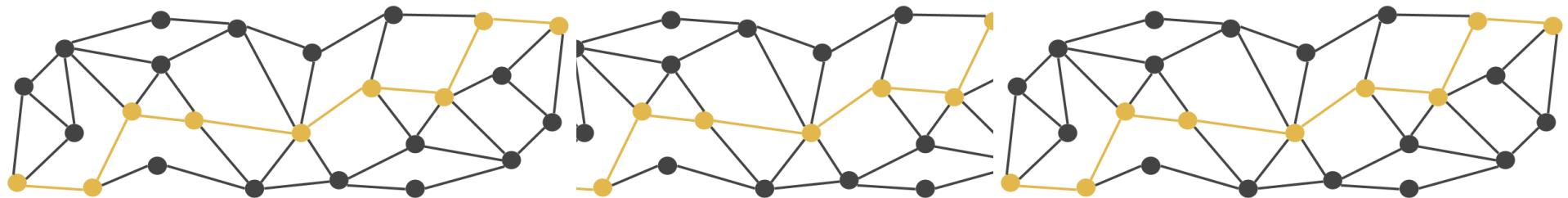
MINING REWARDS

Year (estimate)	Block created	BTC / Block
2009	52560	50
2010	105120	50
2011	157680	50
2012	210240	25
2013	262800	25
2014	315360	25
2015	367920	25
2016	420480	12.5
2017	473040	12.5
2018	525600	12.5
2019	578160	12.5
2020	630720	6.25
2021	683280	6.25
2022	735840	6.25
2023	788400	6.25
2024	840960	3.125
2025	893520	3.125
2026	946080	3.125
2027	998640	3.125
2028	1051200	1.56
2029	1103760	1.56
2030	1156320	1.56



MINING DIFFICULTY

Satoshi Nakamoto's main invention is the decentralized mechanism for *emergent consensus*



Emergent, because **consensus is not achieved explicitly — there is no election or fixed moment when consensus occurs**. Instead, **consensus is an emergent artifact of the asynchronous interaction of thousands of independent nodes, all following simple rules**

HASH RATE

Measure of MINER's performance

**Speed at which a MINER SOLVES the
Bitcoin code**

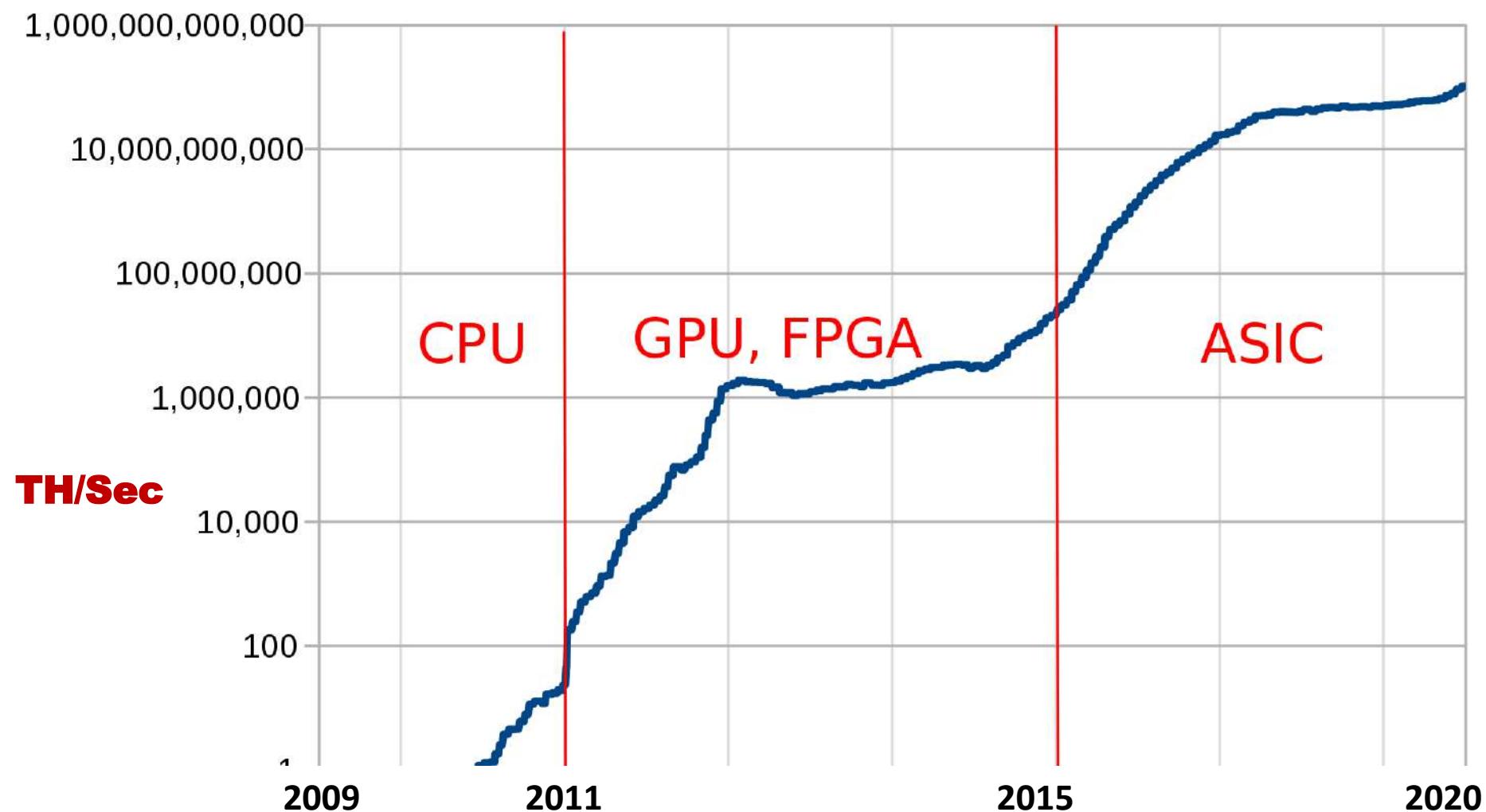


**Higher hash rate INCREASES opportunity for
mining & receiving reward.**

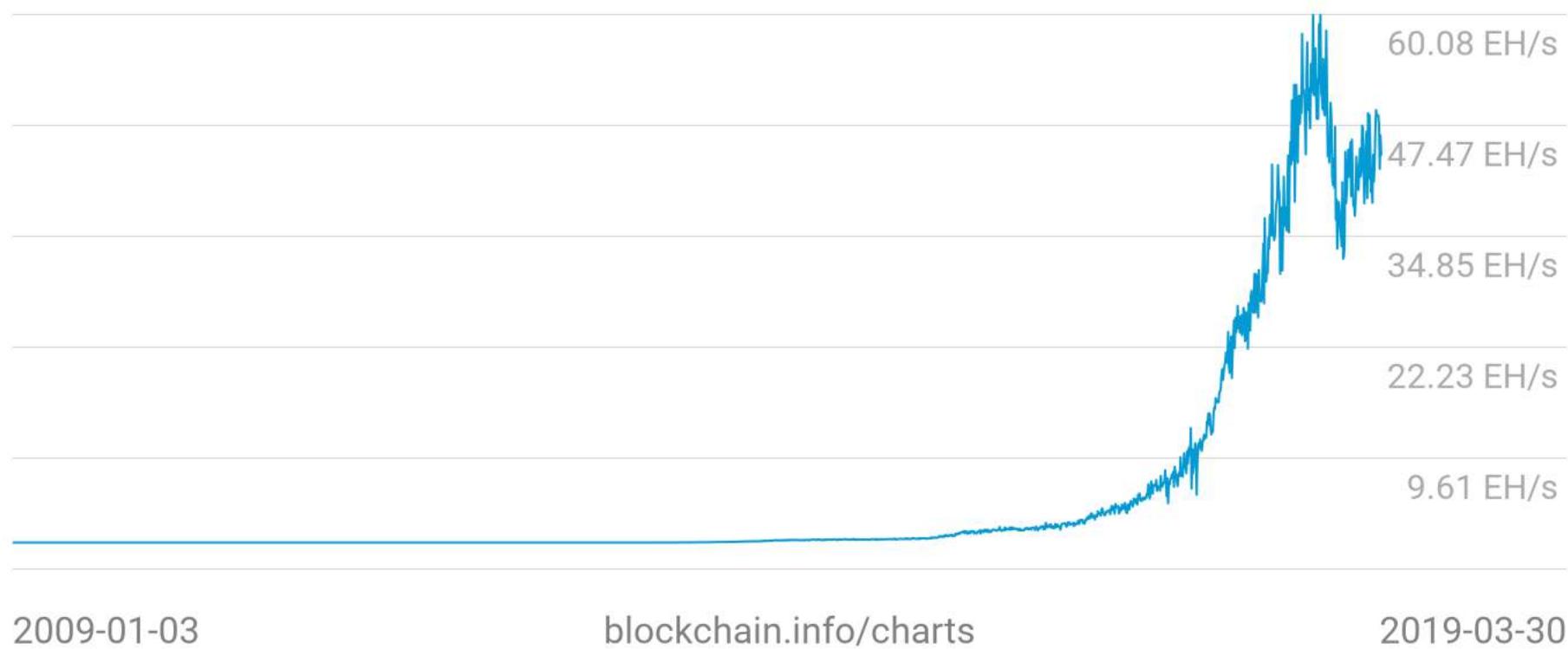


**Hash per second represents SHA-256
algorithms that are used per sec**

MINING DIFFICULTY



Hash Rate
44.08 EH/s



2009-01-03

blockchain.info/charts

2019-03-30

INTERPLAY OF FOUR PROCESSES

Independent verification of each transaction, by every full node, based on a comprehensive list of criteria

Independent aggregation of those transactions into new blocks by mining nodes

Independent verification of the new blocks by every node and assembly into a chain

Independent selection, by every node, of the chain demonstrated through Proof-of-Work

HASH RATE DENOMINATIONS

1 kH/s is 1,000 (one thousand) hashes/sec

1 MH/s is 1,000,000 (one million) hashes/sec

1 GH/s is 1,000,000,000 (one billion) hashes/sec

1 TH/s is 1,000,000,000,000 (one trillion) hashes/sec

1 PH/s is 1,000,000,000,000,000 (one quadrillion) hashes/sec

1 EH/s is 1,000,000,000,000,000,000 (one quintillion)
hashes/sec

2009

0.5 MH/sec-8 MH/sec (16× growth)

2010

8 MH/sec-116 GH/sec (14,500× growth)

2011

16 GH/sec-9 TH/sec (562× growth)

2012

9 TH/sec-23 TH/sec (2.5× growth)

2013

23 TH/sec-10 PH/sec (450× growth)

2014

10 PH/sec-300 PH/sec (3000× growth)

2015

300 PH/sec-800 PH/sec (266× growth)

2016

800 PH/sec-2.5 EH/sec (312× growth)

Mining And Hashrates!





BITCOIN MINING



BLOCK REWARDS

Block 000000 to 209999, total reward = 50

Block 210000 to 419999 total reward = 25

Block 420000 to 629999 total reward = 12.5

Block 630000 to 839999 total reward = 6.25



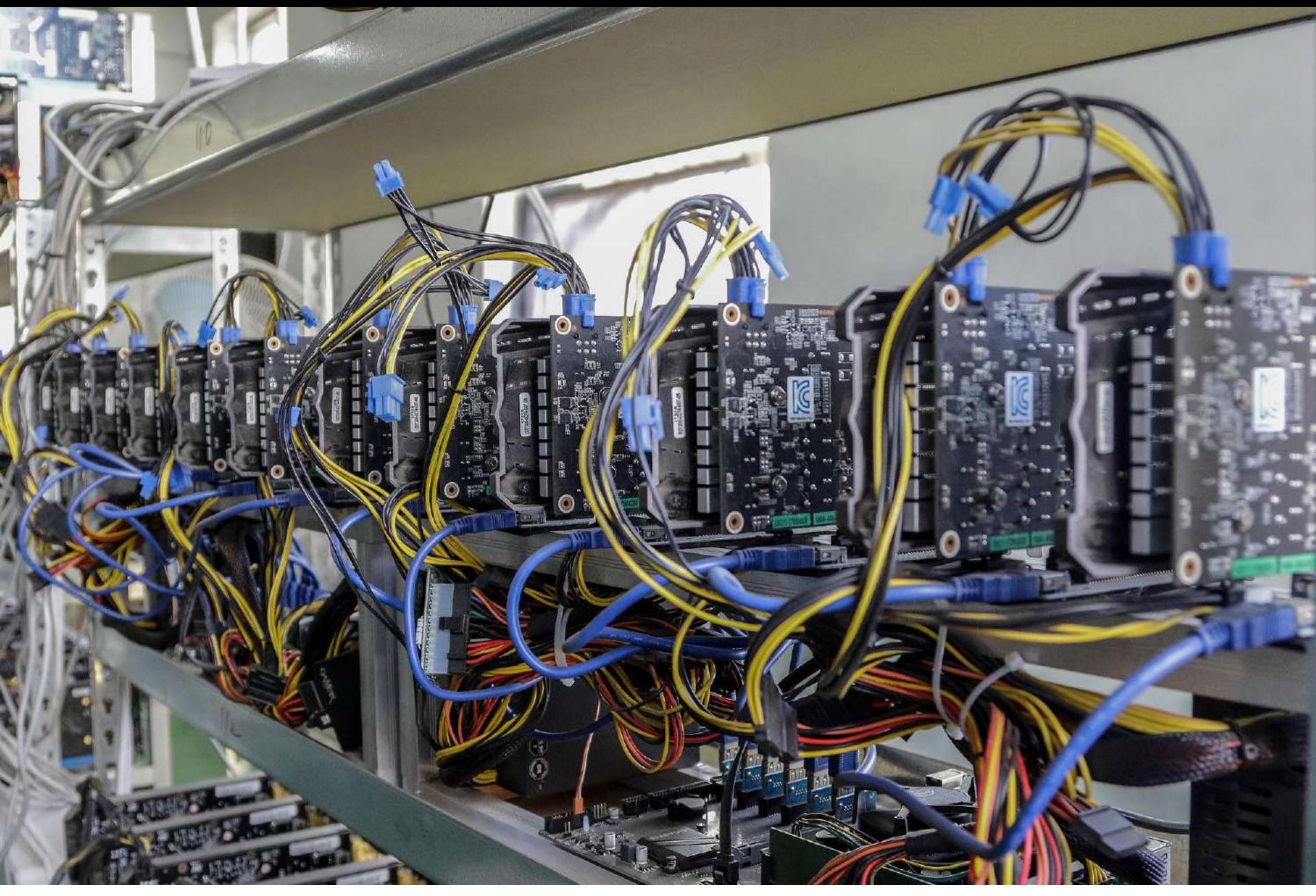
BITCOIN MINING: FEW PICS



BITCOIN MINING: FEW PICS



BITCOIN MINING: FEW PICS



BITCOIN MINING: FEW PICS



BITCOIN MINING: FEW PICS



BITCOIN MINING: FEW PICS



BITCOIN MINING: FEW PICS



BITCOIN MINING: FEW PICS



The First Solar Powered Bitcoin Mining Farm could be in Coal Town Australia



by **Arshmeet Hora** — August 10, 2018 in News

0



BITCOIN MINING: FEW PICS

This Is What Happens When Bitcoin Miners Take Over Your Town

Eastern Washington had cheap power and tons of space. Then the suitcases of cash started arriving.

By PAUL ROBERTS | March/April 2018



<https://www.politico.com/magazine/story/2018/03/09/bitcoin-mining-energy-prices-smalltown-feature-217230/>

BITCOIN MINING

HOME > NEWS > EUROPE

Ukraine plans huge cryptocurrency mining data centers next to nuclear power plants

As much as 2-3GW could be given over to mining bitcoin

February 01, 2021 By: Sebastian Moss  1 Comment

<https://www.datacenterdynamics.com/en/news/ukraine-plans-huge-cryptocurrency-mining-data-centers-next-nuclear-power-plants/>

BITCOIN MINING

A Russian Nuclear Plant Is Renting Space to Energy-Hungry Bitcoin Miners

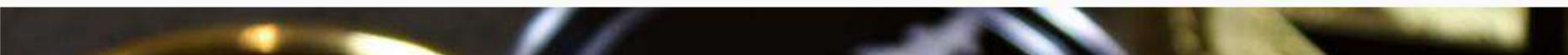
<https://www.coindesk.com/a-russian-nuclear-plant-is-renting-space-to-energy-hungry-bitcoin-miners>

BITCOIN MINING

And You Can't Even Ski On It

A power plant in New York ramped back up to mine Bitcoin, but opponents are pushing back

By Jonathan Hilburg • April 14, 2021 • National, News, Sustainability, Technology



<https://www.archpaper.com/2021/04/greenidge-power-plant-mine-bitcoin-raising-fears-of-a-climate-crash/>

BITCOIN MINING

Iran Seizes 7,000 Illegal Cryptocurrency Mining Computers

Tuesday, 22 Jun 2021 18:00



Iranian police have seized 7,000 illegal cryptocurrency mining computers, their largest haul to date of the energy-guzzling machines that have exacerbated power outages in Iran, state media reported on Tuesday.

In late May, Iran banned the mining of cryptocurrencies such as Bitcoin for nearly four months as part of efforts to reduce the incidence of power blackouts blamed by officials on surging electricity demand during the searingly hot and dry summer.

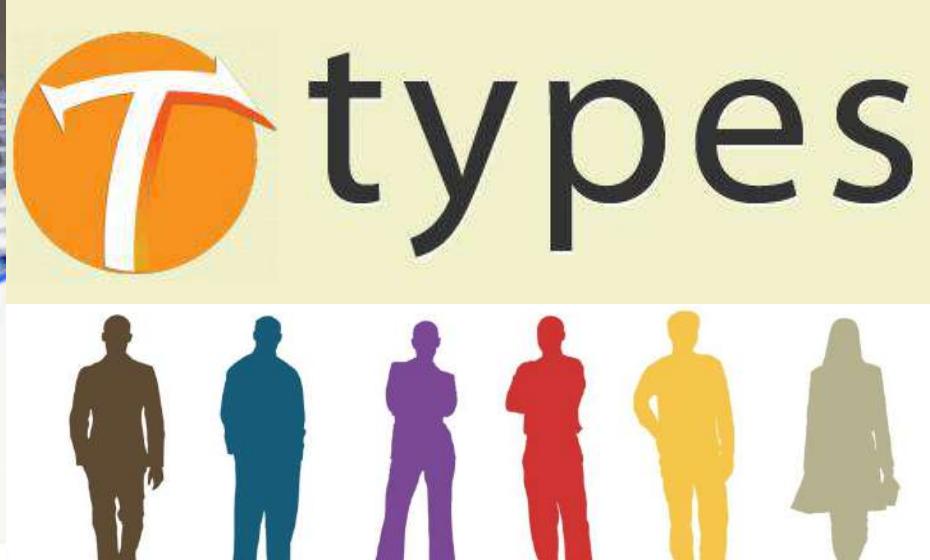
<https://iranintl.com/en/iran-in-brief/iran-seizes-7000-illegal-cryptocurrency-mining-computers>

Huge infrastructure projects in China have created a substantial energy surplus, which in turn has driven down the cost of energy-intensive bitcoin mining





BITCOIN MINING



ELECTRONIC CURRENCIES BUY SERVICES
ORGANIZATION MONEY ONLINE MARKET
TRADING BIT BANKING CRYPTO CURRENCY DIGITAL COIN
ACTION TRADE UNIT & MONEY SECURITY MINING PROFITABILITY
EXPERTISE PROFIT PEER COIN TRADE BUSINESS
LITE COINS EXCHANGE TRANSACTIONS MARKET



SOLO.[®]



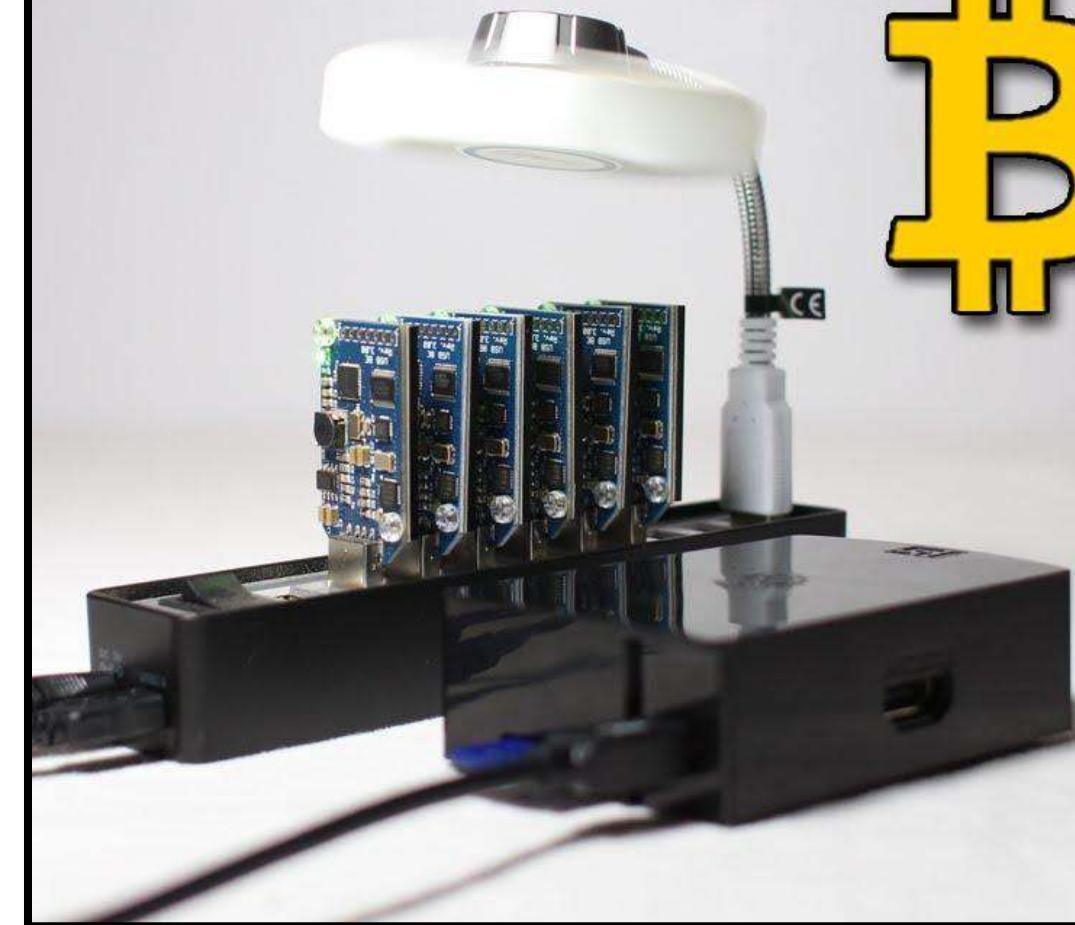
A miner performs the
MINING OPERATIONS
ALONE without joining
a pool.

All mined blocks are generated to
the **MINER'S CREDIT**.

SOLO MINE BITCOIN

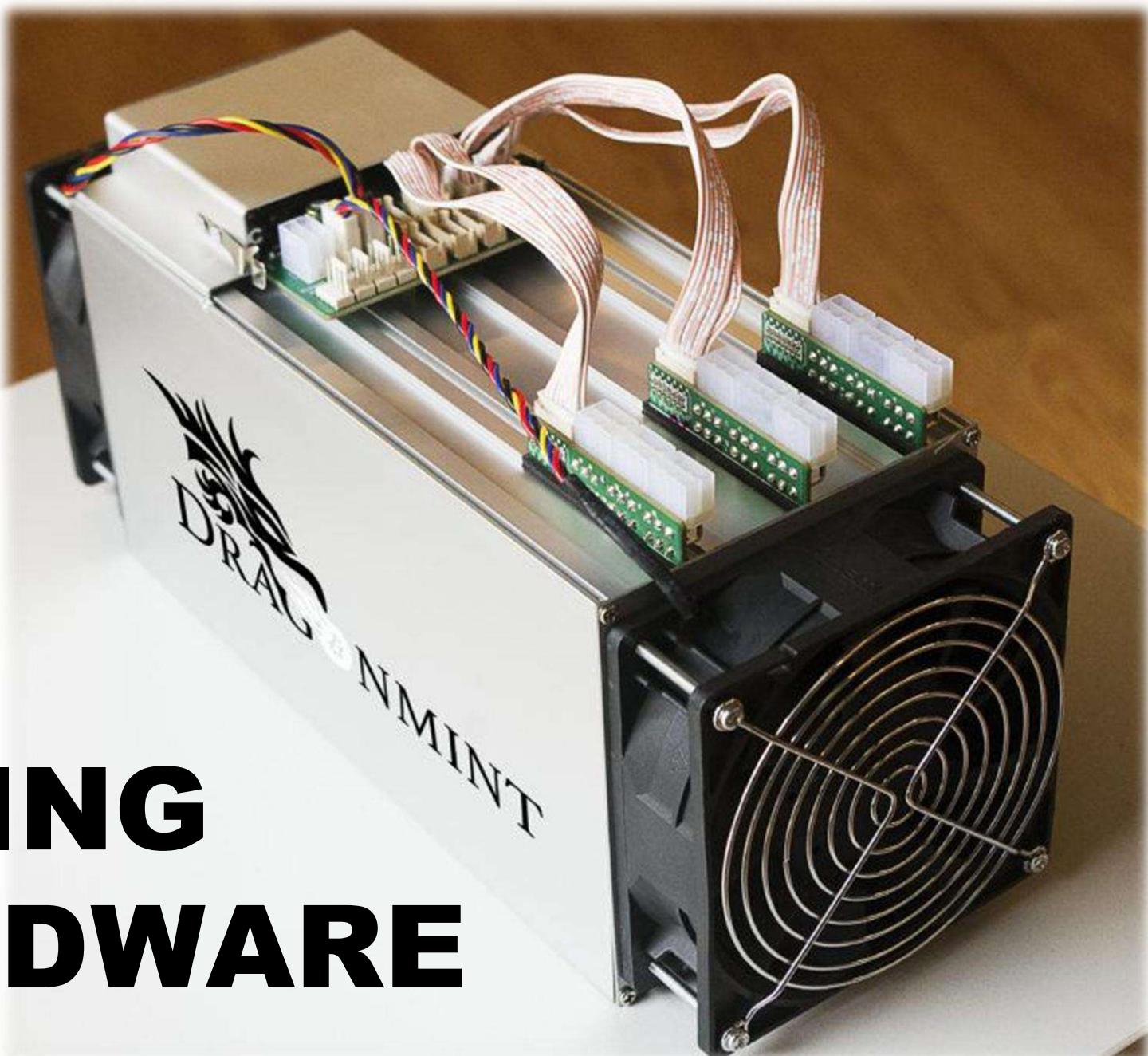
The **current hardware's utilized** for the process of **solo mining** can deliver an experience which is more like **playing the lottery**, but if you do it right you can exit with a **lot of cash**





Bitcoin Mining LOOKS HARDWARE

MINING HARDWARE





**MINING
HARDWARE**



MINING HARDWARE



MINING HARDWARE



 Pooled  **Bitcoin Mining**

POOLED MINING

combines the work of many miners
toward a common goal



Home - F2Pool

Secure | https://www.F2pool.com

f2pool Home Workers Payouts Help

ETH/ETC/ZEC/ASHMIN

BTC: 905 Phash/s LTC: 6107 Ghash/s ETH: 27.9 Thash/s ETC: 1005 Ghash/s ZEC: 46.8 MHash/s SH: 32.9 Thash/s

Welcome to F2Pool

Bitcoin Litecoin Ethereum Zcash

Bitcoin F2Pool Mining Pool

www.F2pool.com/user/home

F2pool BTC/LTC

我的首页 挖矿管理 行业记录 帮助

BTC: 130 Phash/s LTC: 541 Ghash/s

采矿速率图表

2018-01-01

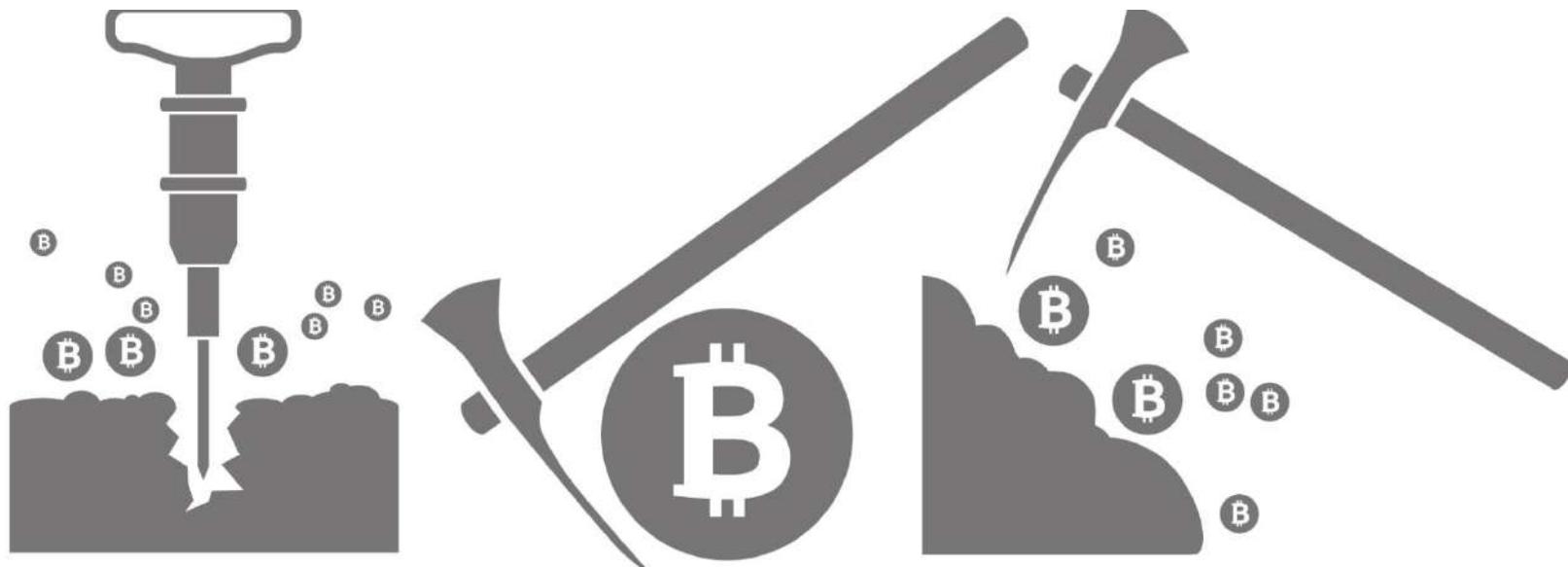
Bitmain (Thash/s) Xaya (Mhash/s)

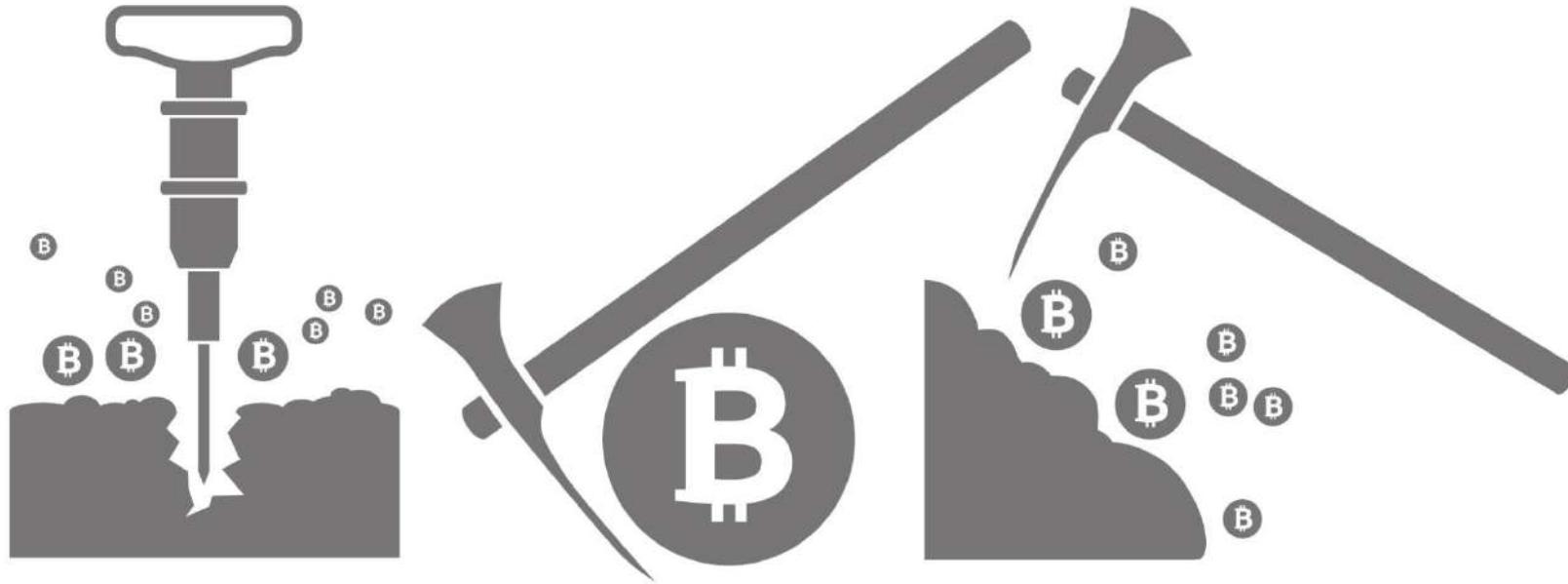
Activate Windows
Go to PC settings to activate Windows.

LJ420



BTCC





BitFury



SLUSHPOOL



BITCOIN CLOUD MINING

Ethereum Mining: Available For Pre-Order!



[HOME](#) [BLOG](#) [PRICING](#) [OUR OFFER](#) [ABOUT US](#) [PRESS](#)
[CUSTOMER SERVICE](#) [DATACENTERS](#)

START BITCOIN MINING TODAY!

It's super simple - Your mining rigs are already set up and running.

As soon as you've set-up your account you can start to earn your first coins from our bitcoin cloud mining service!

[START MINING NOW!](#)

[LEARN MORE](#)



cloud mining

A Beginner's Guide to Bitcoin Cloud Mining

E A S Y

E A S Y

E A S Y

BYZANTINE GENERAL CONSENSUS

**So here we are....THE PROOF OF
WORK...That's how it WORKS FOR THE
BITCOIN**

REMEMBER THESE TERMS?



TRUST

THIRD PARTY NEGATION

HASH CASH

$y^2 = x^3 + 7$

PUBLIC KEY- PRIVATE KEYS

RIPEMD-160

PSEUDONOMOUS

FINITE FIELDS

Secp256k1 standard

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

BLOCK REWARDS

$y^2 = x^3 + ax + b7$

~ 371 GB SIZE BLOCKCHAIN

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

HASH CONNECTED BLOCKS

DISTRIBUTED LEDGER

ADDRESSING

HISTORY

BLOCKS

CHAINS

DIGITAL SIGNATURES

10 MINUTES RULE

CRYPTOGRAPHY

MINING

PROOF OF WORK

BLOCKS

BYZANTINE GENERAL PROBLEM

NONCE

OPENSSL

ECDSA

BITCOIN EQUATION

GPU/FPGA/ASIC

03 Jan 2009

SHA 256

51% ATTACKS OVERVIEW

How Blockchains Can Be Hacked

Block 1

Ledger X = \$100

Block 2a

Ledger X = \$0

Block 2b

Ledger X = \$100

Block 3a

Ledger X = \$0

Block 3b

Ledger X = \$100

Block 4a

Ledger X = \$0

Block 4b

Ledger X = \$100

X

Block 5b

Ledger X = \$100

Step 1

A transaction occurs.

For example, \$100 is spent by attacker.

Step 2

A "double spend" occurs when the original spend record is not recorded in the attacker blockchain.

For example, the attacker (red) block still shows \$100 while the honest (green) block shows \$0.

Step 3

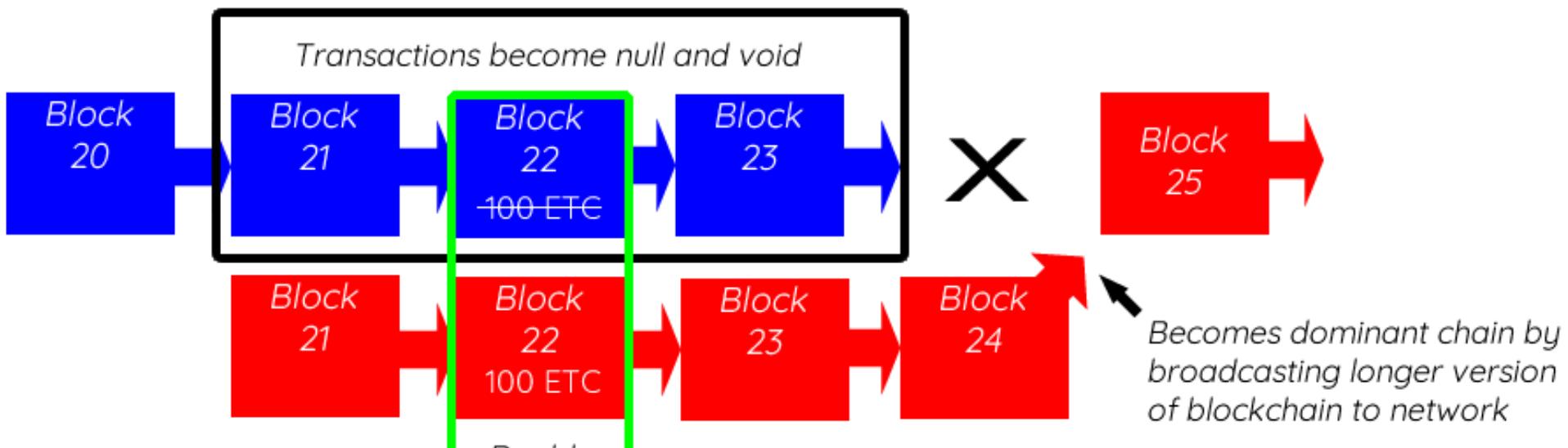
The accepted block chosen according to protocol is the "heaviest" block. However, the heaviest block is the attacker block.

Step 4

The inaccurate block will eventually be accepted if the computing power of perpetrator is more than 50% of the total network hashing power.

The attack yields \$100.

51% Attack (double-spend)



- Original (honest) blockchain <50% hash power
- Malicious blockchain >50% hash power

51 PERCENT ATTACK



▲ During a Bitcoin conference in Amsterdam a local cafe takes advantage of the attending clientele accepting Bitcoins. Photograph: Alamy

Bitcoin has stared down an existential threat, after a consortium of miners briefly gained enough processing power to theoretically destroy the currency.

For a few hours on Friday, mining pool Ghash.io controlled 51% of all the processing power being used to perform the calculations that keep bitcoin secure. If it had abused that power, it would have had the ability to indirectly take money from other users, for instance by buying something and then rewriting history so that the purchase never happened.

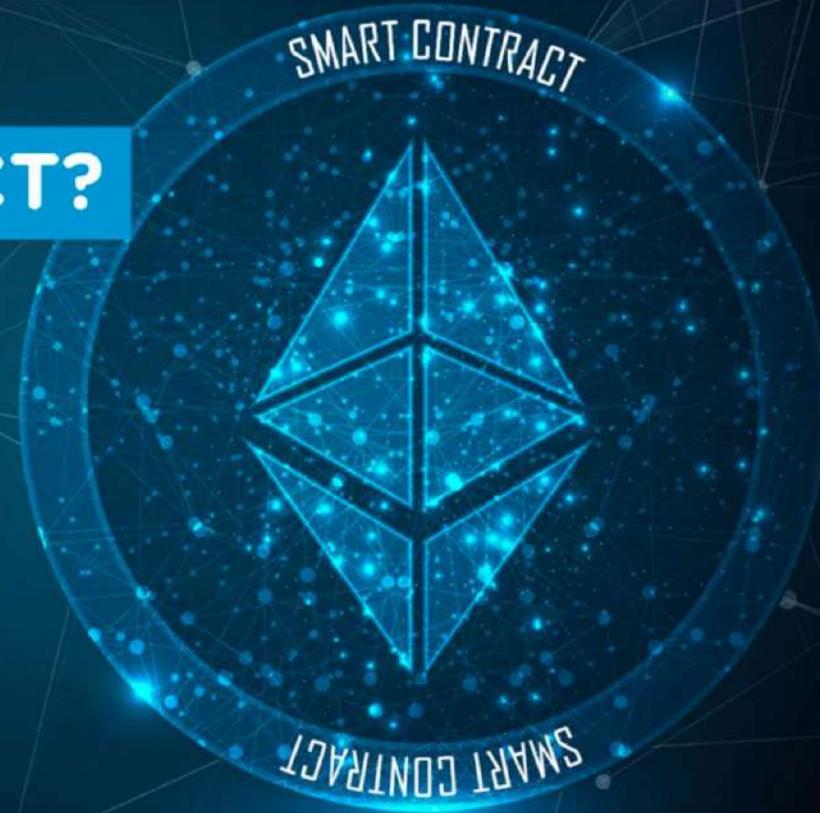
But shortly after the threshold was breached, some members of the mining pool pulled their computing power from the group, averting - or at least, delaying - catastrophe.

51 PERCENT ATTACK

The mining pool gHash.IO briefly exceeded 50% of the **bitcoin** network's computing power in July 2014, leading the pool to voluntarily commit to reducing its share of the network. It said in a statement that it would not reach 40% of the total mining power in the future.

Krypton and Shift, two blockchains based on **ethereum**, suffered 51% attacks in August 2016.

WHAT IS A SMART CONTRACT?



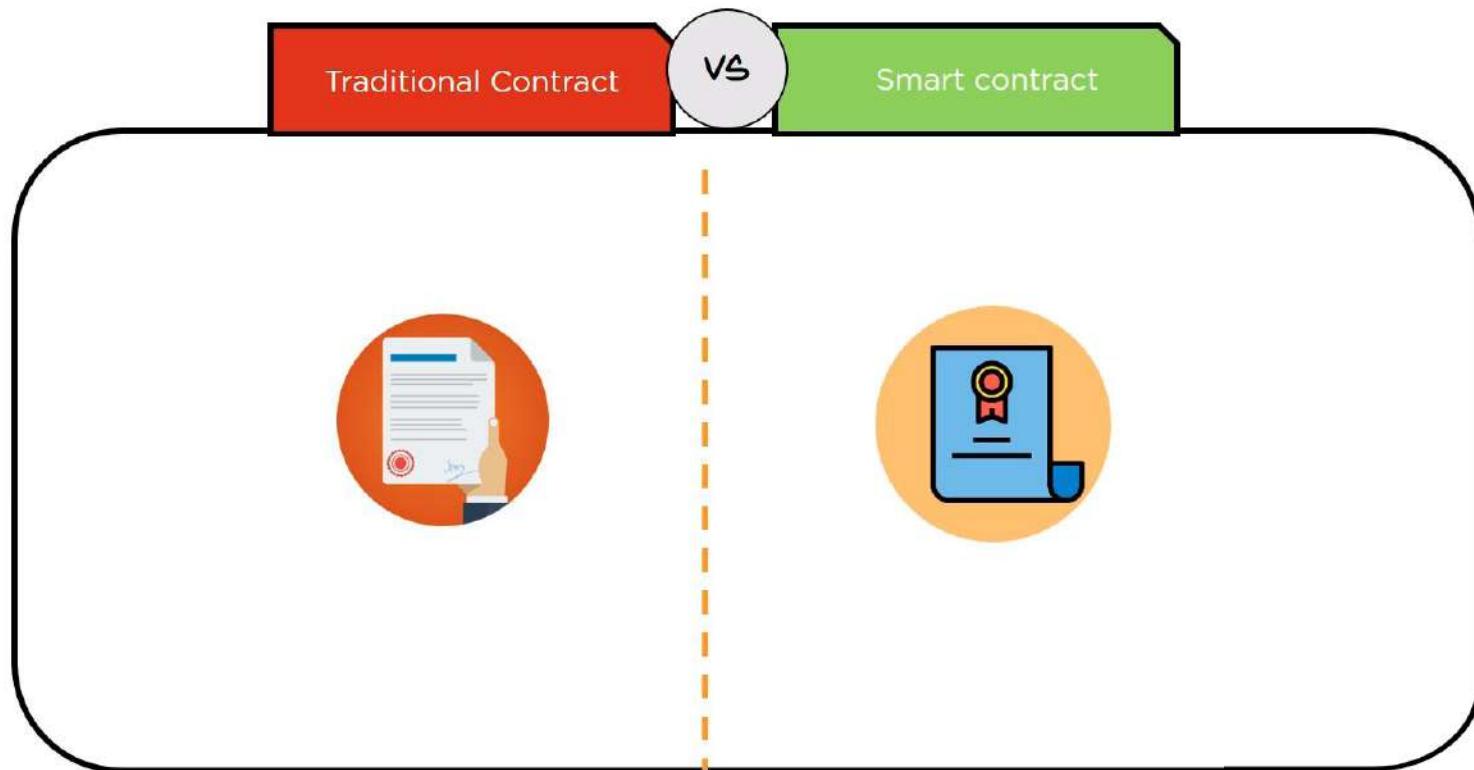
What's in it for you?

- ▶ Why smart contract?
- ▶ What is a smart contract?
- ▶ Solidity for smart contract
- ▶ Advantages of smart contract
- ▶ Blockchain implementation of smart contract

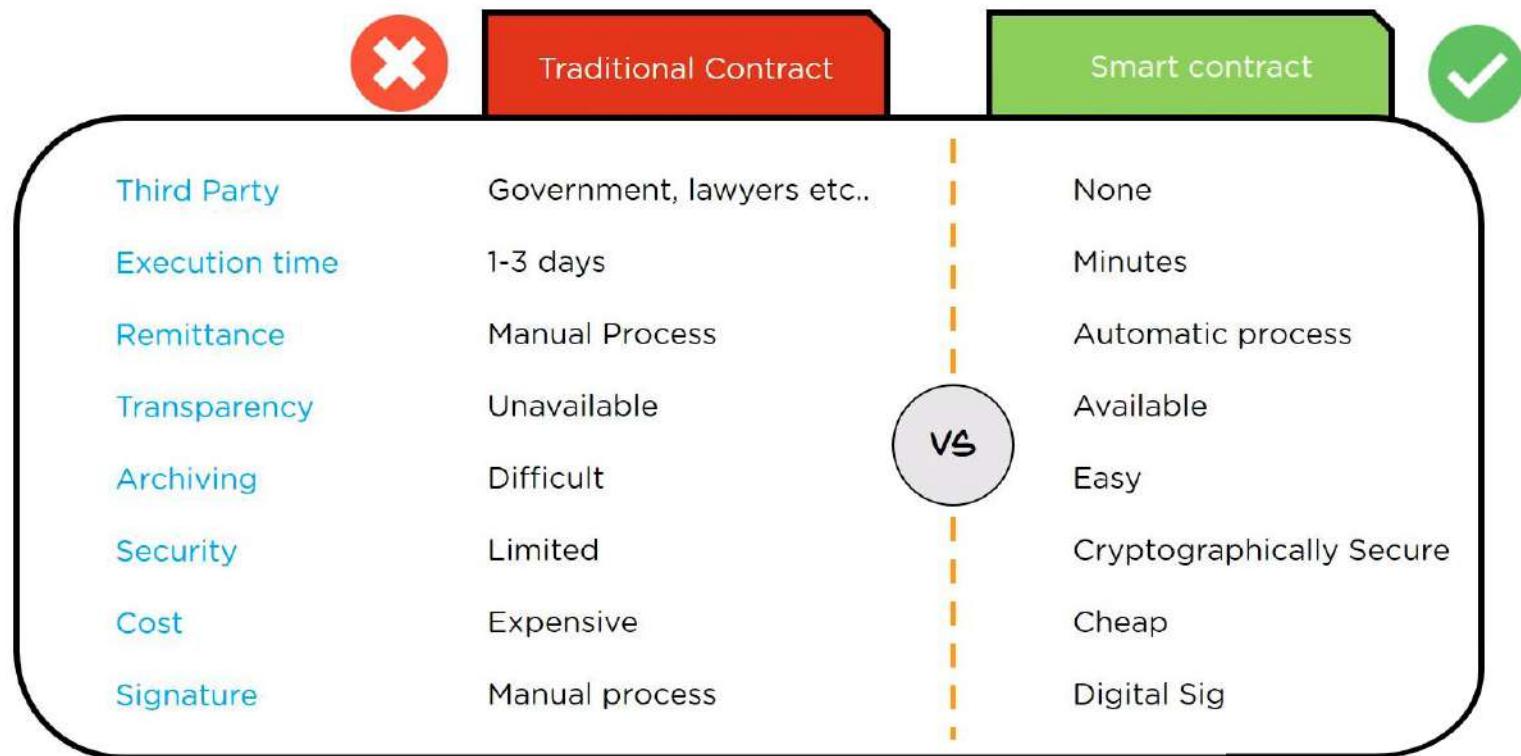
Why smart contract?



Why smart contract?



Why smart contract?



What is a smart contract?

Consider a real life example where you are taking out a chocolate from a vending machine



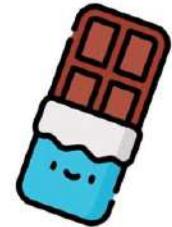
YOU DEPOSIT A \$2 NOTE IN A VENDING MACHINE



AFTER THAT, YOU HIT "A1" BUTTON WHICH IS MAPPED AGAINST THE CHOCOLATE BAR THAT YOU WANT TO BUY

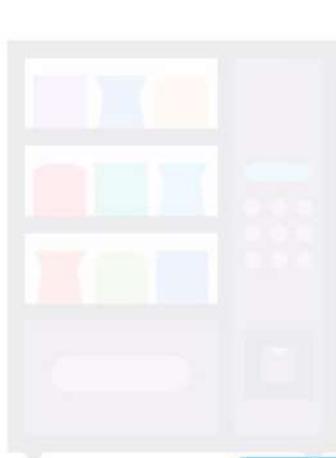


AS A RESULT, A LEVER IN THE VENDING MACHINE MOVES AND PUSHES OUT THE CHOCOLATE



What is a smart contract?

Consider a real life example where you are taking a \$20 bill to a vending machine



Note

A smart contract is very similar to a vending machine

It eliminates the need of intermediaries and escrow services

YOU INSERT A \$20
VENDING MACHINE

IN THE
VES AND
COLATE

What is a smart contract?

Smart contracts are self-executing contracts which contain the terms and conditions of an agreement between the peers

The terms and conditions of an agreement is written in code



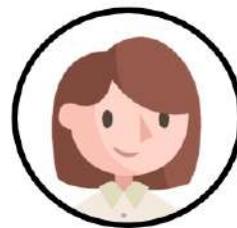
These agreements facilitate the exchange of money, shares, property etc.

It executes in blockchain's decentralized platform

EXAMPLE

What is a smart contract?

Let's consider an example where Rachel is at the airport and her flight is delayed



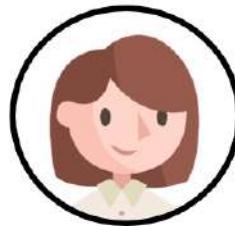
Rachel



What is a smart contract?

Let's consider an example where Rachel is at the airport and her flight is delayed

BUT THIS INCONVENIENCE
COULD HAVE BEEN BENEFICIAL
TO RACHEL, AS SMART
CONTRACT INSURANCE WOULD
ENSURE SHE IS GIVEN A
COMPENSATION FOR THE
FLIGHT'S DELAY



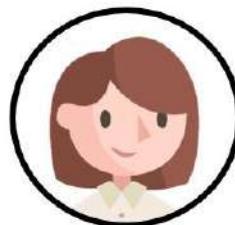
Rachel



What is a smart contract?

Let's consider an example where Rachel is at the airport and her flight is delayed

WONDERING HOW SMART
CONTRACT CAN BE HELPFUL
HERE?



Rachel



What is a smart contract?



AXA flight delay insurance is one of the examples of Ethereum smart contracts



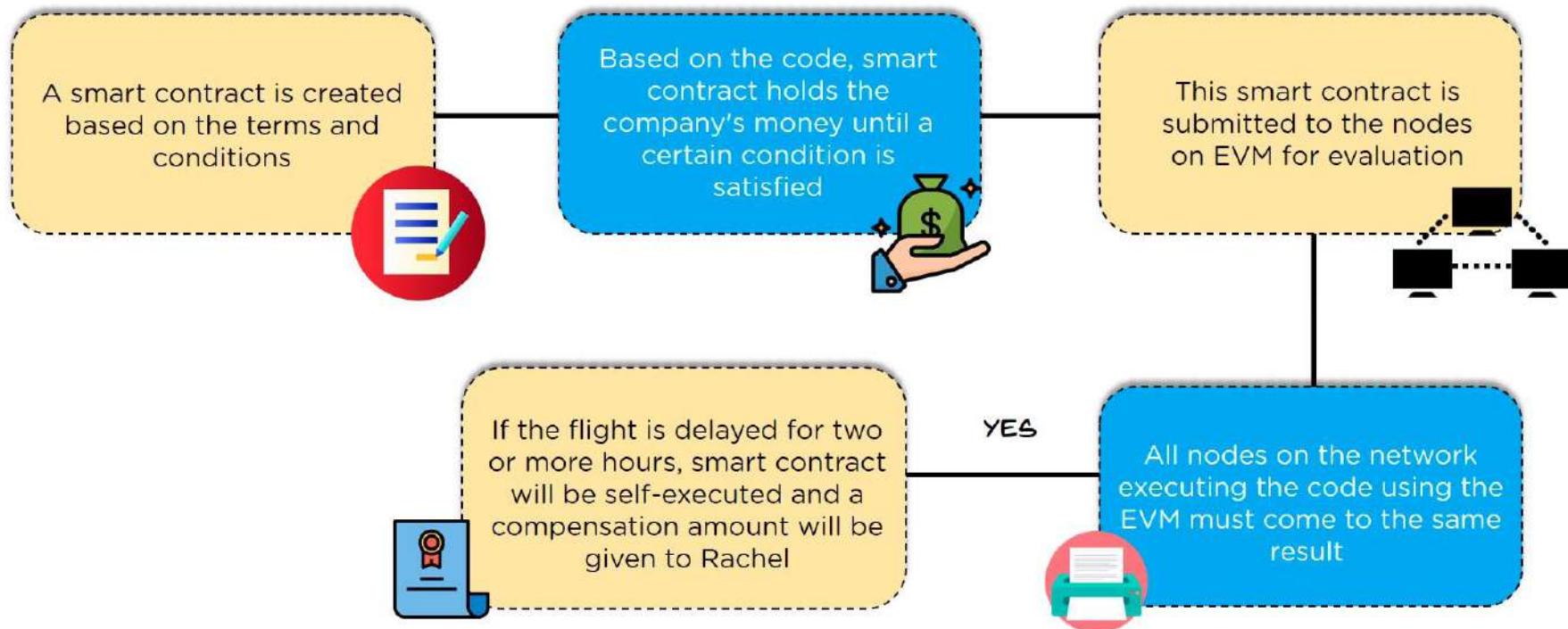
The smart contract is linked to the databases that record flights' status



It enables automatic compensation when there is a delay of two hours or more

Note: AXA is an insurance company

What is a smart contract?



Note: Smart contracts are immutable, so they won't let any person to alter the agreement

What is a smart contract?

A smart
based

Based on the code, smart

Insurance · News

AXA withdraws blockchain flight delay compensation experiment

November 11, 2019 • by Miranda Wood

Contract is
the nodes
evaluation

The network
made using the
to the same

Note: Smart contracts are immutable, so they won't let anyone alter the agreement

Solidity for smart contract

Solidity for smart contract

Here come's the important question!

Q: What programming language does a smart contract use?

Solidity

Serpent

They are the two widely used programming languages for writing Ethereum smart contracts

Solidity for smart contract

Here come's the important question!

Q: What programming language does a smart contract use?



Solidity

Serpent

However, on blockchain platform, **solidity** is widely used for implementing smart contracts

Solidity for smart contract

Solidity



Solidity is a high level programming language used for implementing smart contracts



Note: It enables to check the program at runtime rather than compile-time

MARRIAGE CONTRACT ON BLOCKCHAIN

<http://prenupwithlove.com/>

A painting of a couple in a romantic pose. A man in a suit is kneeling, holding a ring box towards a woman in a dress. The scene is set against a dark background with a warm glow from behind them.

pre-nup
with love

*“First ever pre-nup on the Ethereum Blockchain” -
Now activated!*

"Smart Contract" by Gaurang; Design by Sayalee

MARRIAGE CONTRACT ON BLOCKCHAIN

THE C(OUPLE)REATORS



GAURANG TORVEKAR

Co-Founder & CTO, Attores



SAYALEE KALUSKAR

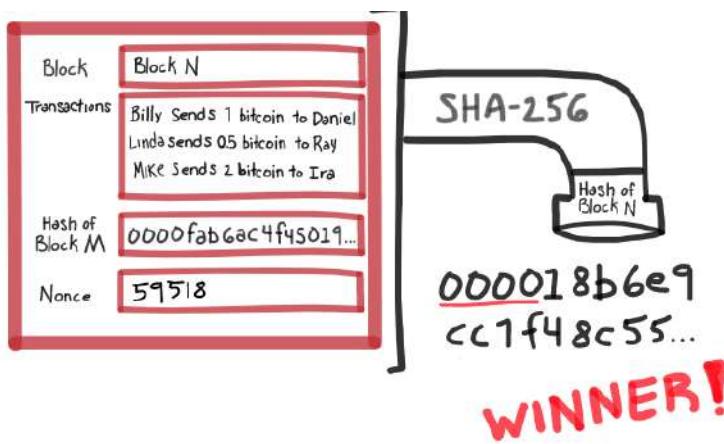
Creative Art Director, honestbee

MARRIAGE CONTRACT ADDRESS ON ETHEREUM MAINNET

0x5657b8d985be88af0f3d2dc064e2db784071ae1c



LET'S GO



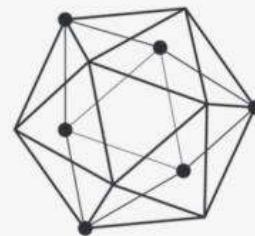
&



**And interesting thing is that
consensus is now available in
pluggable versions**

KAFKA/RAFT
or SUMERAGI

HYPERLEDGER



OVERVIEW



CONCEPTS

Major characteristics of Blockchain



DECENTRALIZATION



TRANSPARENCY



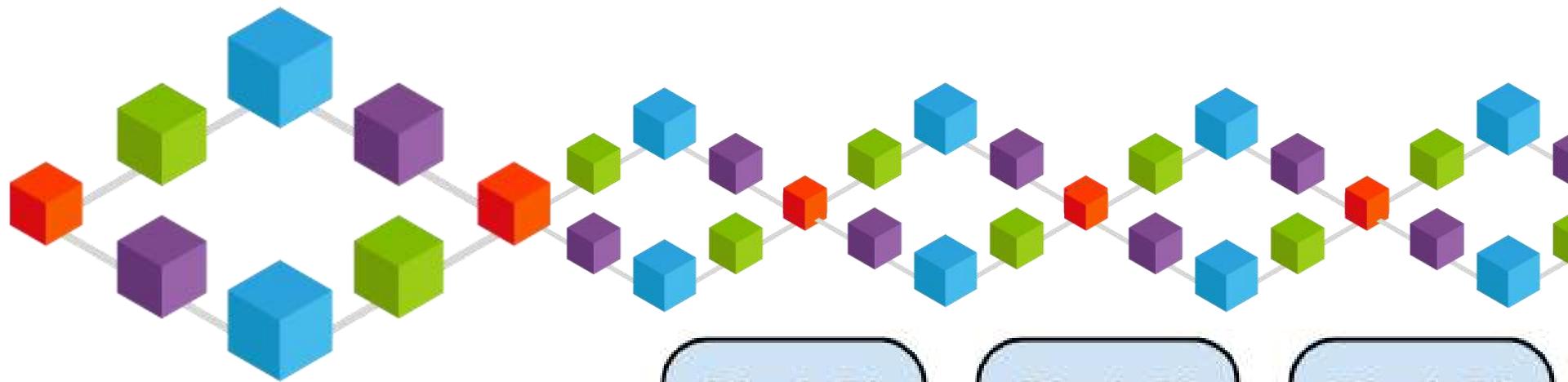
IMMUTABILITY



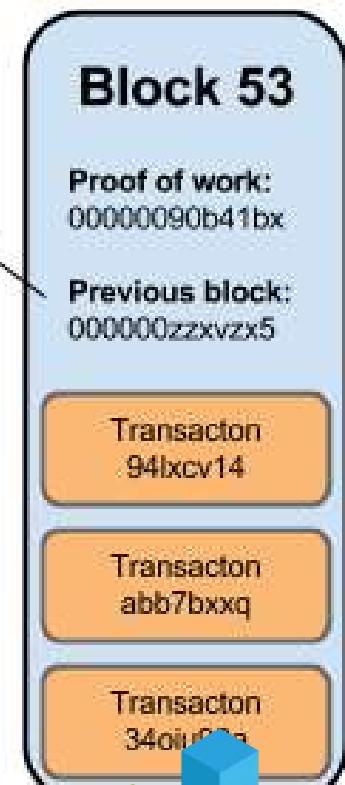
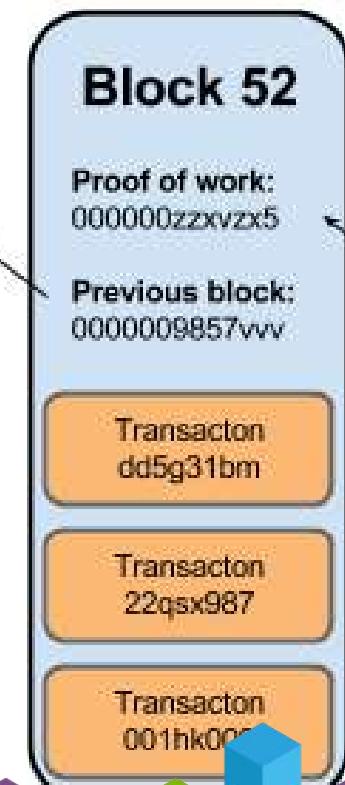
NEUTRALITY



OPEN-ACCESS



WHAT BLOCKCHAIN LOOKS LIKE



PUBLIC LEDGER

Rs 1000/-
A>B Rs 200
B>D Rs 600
C>B Rs 100
B>C Rs 200
A>B Rs 100
C>D Rs 250
B>C Rs 170
D>C Rs 189



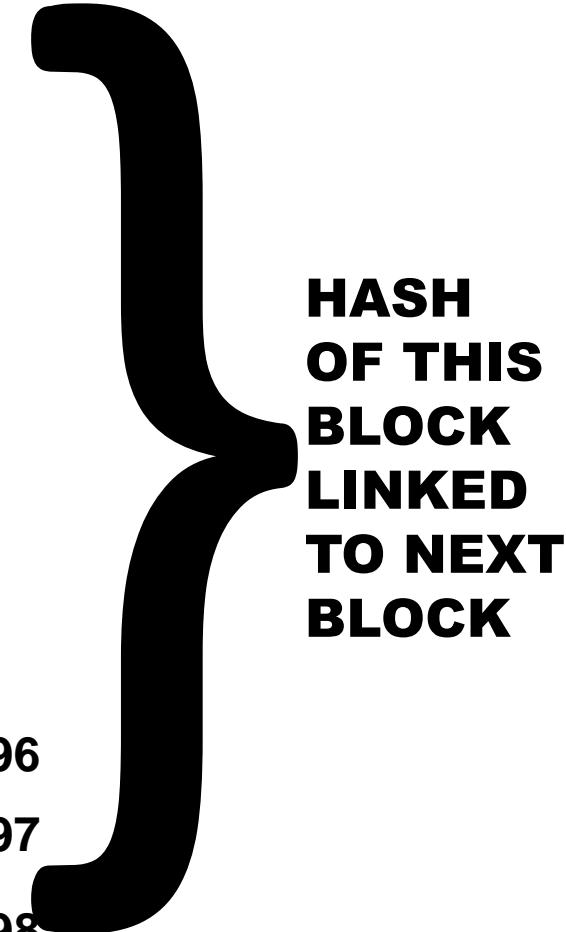
MILLIONS OF
TRANSACTIONS

A>B Rs 100
C>D Rs 250
B>C Rs 170
D>C Rs 189

PUBLIC LEDGER

	Rs 1000/-	
1	A>B Rs 200	Hash of 1
2	B>D Rs 600	Hash of 2
3	C>B Rs 100	Hash of 3
4	B>C Rs 200	Hash of 4
5	A>B Rs 100	Hash of 5
6	C>D Rs 250	Hash of 6
7	B>C Rs 170	Hash of 7
8	D>C Rs 189	

**9-1496
TRANSACTIONS**



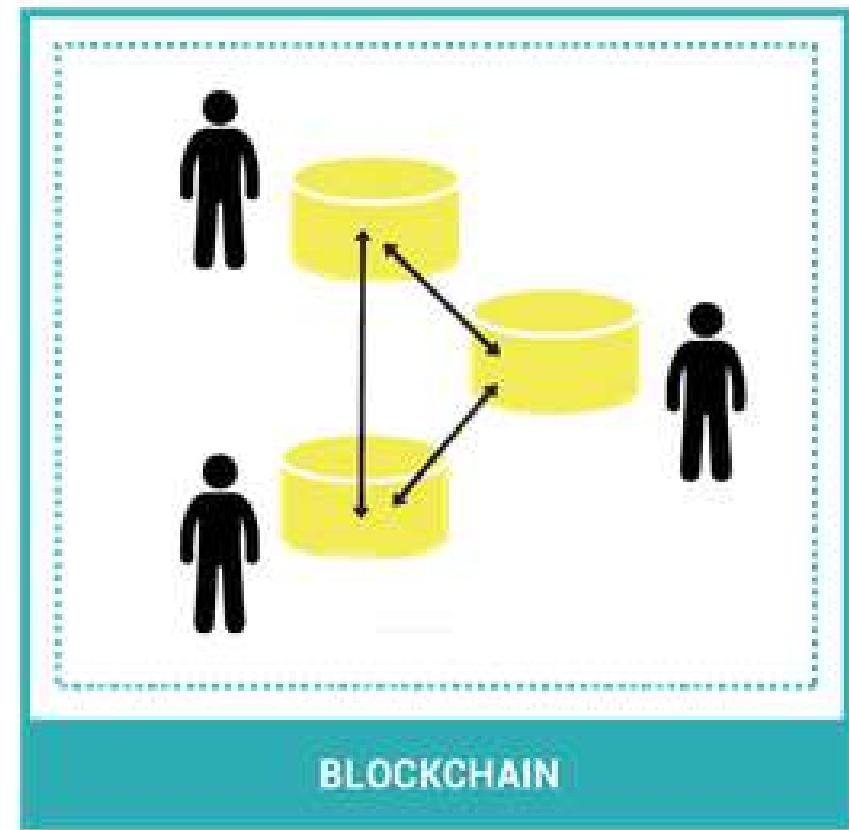
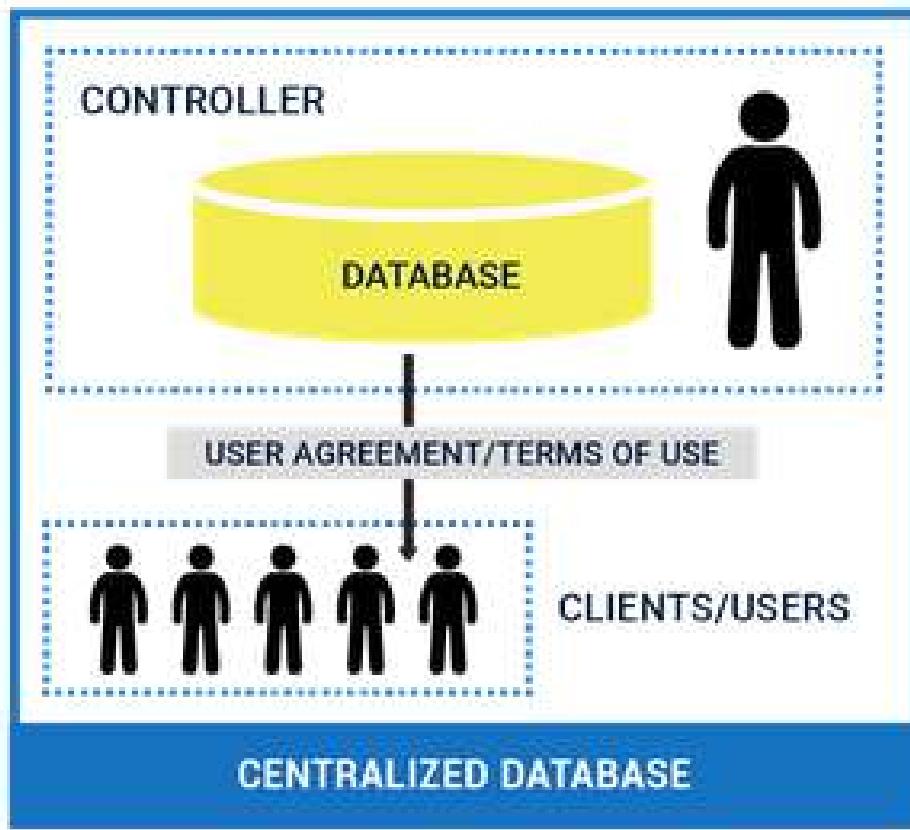
1497	A>B Rs 100	Hash of 1496
1498	C>D Rs 250	Hash of 1497
1499	B>C Rs 170	Hash of 1498
1500	D>C Rs 189	Hash of 1499

CENTRALIZED DATABASES VS. BLOCKCHAIN

What's the
Difference



CENTRALIZED DATABASES VS. BLOCKCHAIN



Simplistic overview

RAW BLOCKCHAIN DATA FILES

Check out on a Live Bitcoin Blockchain

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c8170100000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
....	



Block hash

0000000000000000
e067a478024addfe
cdc93628978aa52d
91fabd4292982a50

RAW BLOCKCHAIN DATA FILES

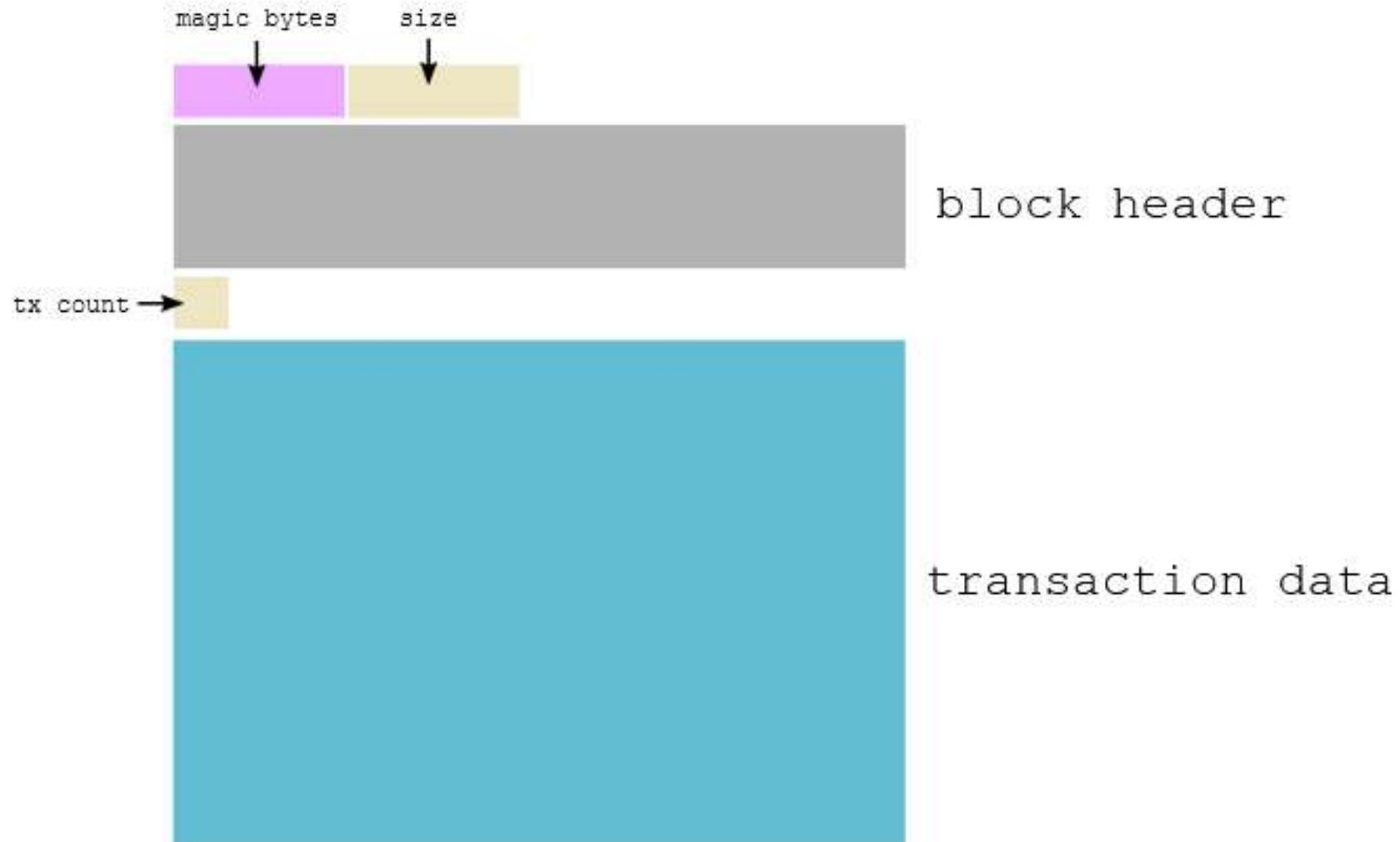
- ❖ For ease of assimilation, we will take a simple example from real bitcoin blockchain
- ❖ I have the ***blk000001.dat*** file which I have ***dd*** into first 1000bytes as ***anupam.dat***

RAW BLOCKCHAIN DATA FILES

Field Sizes

- Nodes on the bitcoin network expect each field to be a certain length. This structured format allows them to run through the transaction data and figure out where each field begins and ends.
- That's why even though the version number is **1**, it's stored as **01000000** because a bitcoin node expects a field that is *4 bytes* in size.
- The inputcount (and signatures) and outputcount (and lockingscripts) can vary in length, which is why special VarInt fields are used to specify their upcoming sizes.

RAW BLOCKCHAIN DATA FILES



Magic bytes : RAW BLOCKCHAIN DATA FILES

Magic bytes are also used to separate block data in the ***blk*.dat*** files.

Network	Magic Bytes
Mainnet	f9beb4d9
Testnet3	0b110907
Regtest	fabfb5da

RAW BLOCKCHAIN DATA FILES

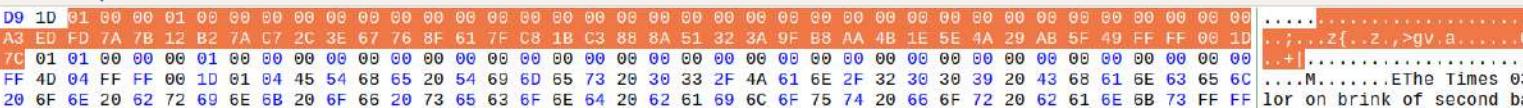
MAGIC NUMBER

RAW BLOCKCHAIN DATA FILES

SIZE OF UPCOMING BLOCK

RAW BLOCKCHAIN DATA FILES

BLOCK HEADER



The screenshot shows a hex editor interface with the following details:

- File Menu:** File, Edit, View, Search, Tools, Help.
- Toolbar:** Includes icons for Open, Save, Find, Replace, Cut, Copy, Paste, and others.
- File Name:** anupam.dat
- Hex View:** The main area displays binary data in hex format. A blue arrow points from the right side of the hex view towards the ASCII view.
- ASCII View:** To the right of the hex view, there is an ASCII dump of the file's content. The text includes various characters, some of which are highlighted in red or orange, and some are underlined.

RAW BLOCKCHAIN DATA FILES

TRANSACTION COUNT

RAW BLOCKCHAIN DATA FILES

TRANSACTION DATA

Magic bytes : RAW BLOCKCHAIN DATA FILES

```
greg@aglaya ~/learnmeabitcoin/github/php-simple-bitcoin-node |
```

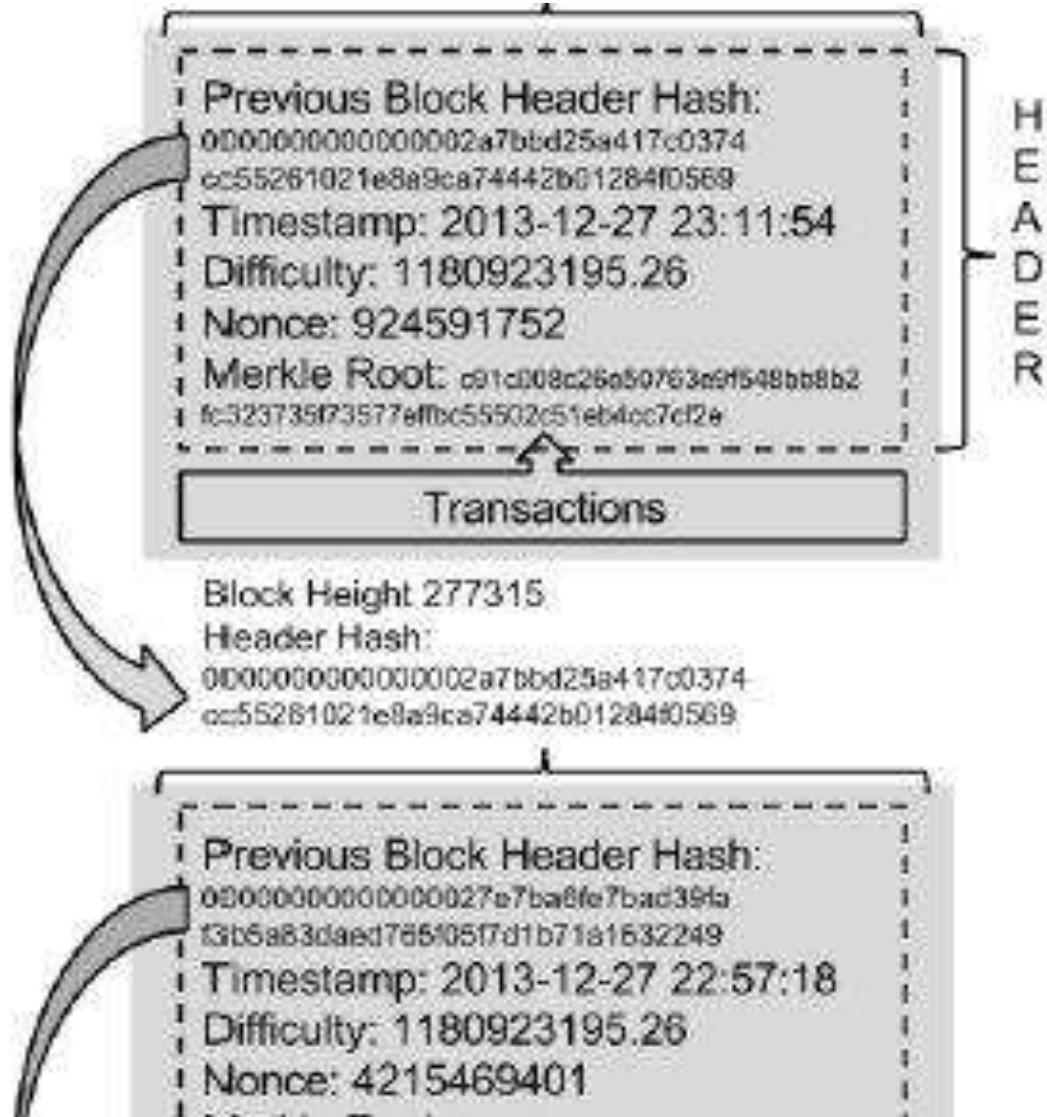
If you are trying to read this data, it's good to have a reliable way of knowing when a new message starts (and ends). This is why a specific set of “**magic bytes**” are used as a “**marker**” so that you can always identify the start of a new message.

So there's nothing actually magical about magic bytes – it's just a way of segmenting data.

Block Header: RAW BLOCKCHAIN DATA FILES

A block header is like the **metadata** at the top of a block of transactions

The fields in the block header provide a **unique summary** of the entire block.



Block Header: RAW BLOCKCHAIN DATA FILES

FIELD	DESCRIPTION
Version	The version of the block.
Previous Block Hash	The Block Hash of the block that this block is being built on top of. This is what “chains” the blocks together.
Merkle Root	All of the transactions in this block, hashed together. Basically provides a single-line summary of all the transactions in this block.
Time	When a miner is trying to mine this block, the <i>Unix</i> time at which this block header is being hashed is noted within the block header itself.
Bits	A shortened version of the Target.
Nonce	The field that miners change in order to try and get a hash of the block header (a Block Hash) that is below the Target.

VarInt: RAW BLOCKCHAIN DATA FILES

VarInt (variable integer) is a field used in transaction data to *indicate the number of upcoming fields*, or the *length of an upcoming field*.

Here's a transaction with the **VarInt** fields highlighted (and if it's referring to a field length, the length of that field is highlighted too)

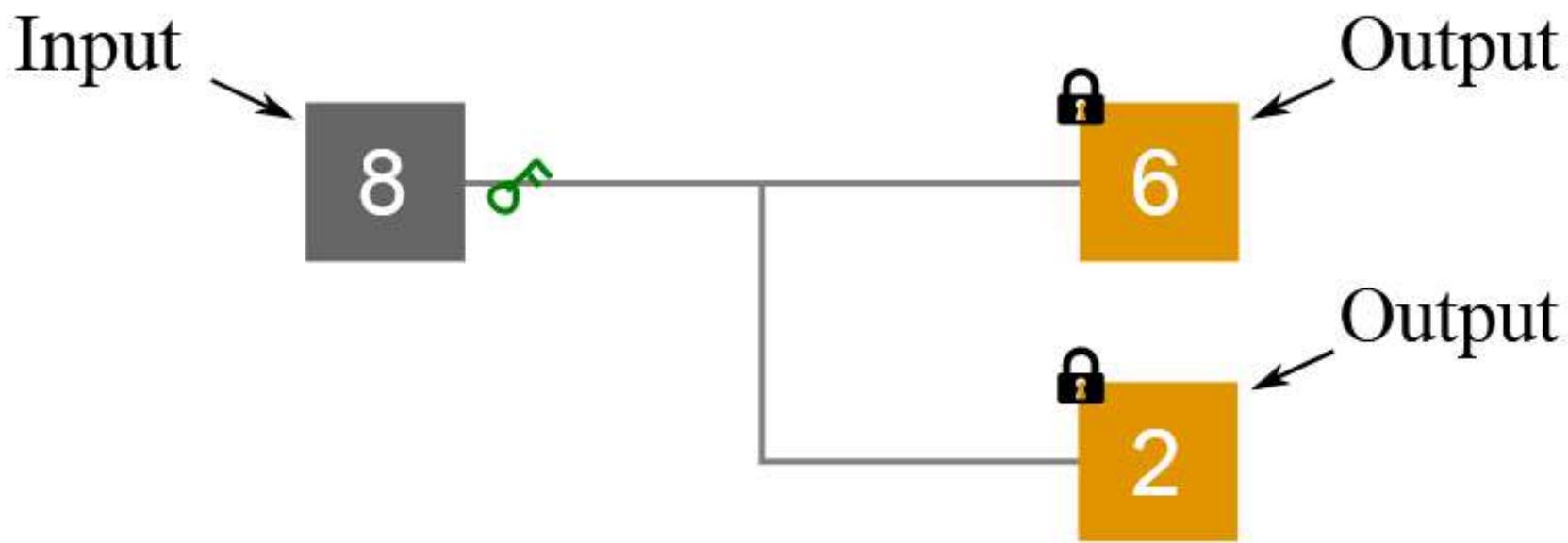
```
01000000017b9c26b765a24997e0f855e5d25e86e6816b213e2bbc67bc918df239bfc20158040000006a47304402200aa5891780e216bf1941b502de  
29890834a2584eb576657e340d1fa95f2c0268022010712e05b30bfa9a9aaa146927fce1819f2ec6d118d25946256770541a8117b6012103d2305c39  
2cbd5ac36b54d3f23f7305ee024e25000f5277a8c065e12df5035926fffffffff028555a700000000001976a914aca504fd373f5f3ba2774a3643d714  
d6419463bc88ac9bc0ba01000000001976a9143bbebbd7a3414f9e5afebe79b3b408bada63cde288ac00000000
```

6a = 106 bytes

47304402200aa5891780e216bf1941b502de29 ... 926

Transaction data : RAW BLOCKCHAIN DATA FILES

A bitcoin transaction is just a bunch of data that describes the movement of bitcoin's



It takes in inputs, and creates new outputs

Transaction OUTPUTS and INPUTS

Transactions are the most important part of the bitcoin ecosystem.

Everything else in bitcoin is designed to ensure that transactions can be created, propagated on the network, validated, and finally added to the global ledger of transactions (the blockchain)

Transaction OUTPUTS and INPUTS

Transactions are data structures that encode the transfer of value between participants in the bitcoin system

Each transaction is a public entry in bitcoin's blockchain, the global double-entry bookkeeping ledger

Transaction **OUTPUTS** and **INPUTS**

In the blockchain network...everything has a **hash value** or for easy assimilation there are **no easy to read human mundane readable dictionary text...**

01	00	F2	05	2A	01	00	00	00	43	41	04	67	8A	FD	B0	FE	55	48	27	19	67	F1	A6	71	30	B7	10	5C	D6	A8	28	E0	39	09	A6	
DE	B6	49	F6	BC	3F	4C	EF	38	C4	F3	55	04	E5	1E	C1	12	DE	5C	38	4D	F7	BA	0B	8D	57	8A	4C	70	2B	6B	F1	1D	5F	AC	00	
D9	D7	00	00	00	01	00	00	00	6F	E2	8C	0A	B6	F1	B3	72	C1	A6	A2	46	AE	63	F7	4F	93	1E	83	65	E1	5A	08	9C	68	D6	19	
20	51	FD	1E	4B	A7	44	BB	BE	68	0E	1F	EE	14	67	7B	A1	A3	C3	54	0B	F7	B1	CD	B6	06	E8	57	23	3E	0E	61	BC	66	49	FF	
99	01	01	00	00	00	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
FF	07	04	FF	FF	00	1D	01	04	FF	FF	FF	FF	01	00	F2	05	2A	01	00	00	00	43	41	04	96	B5	38	E8	53	51	9C	72	6A	2C	91	
13	90	81	3A	62	7C	66	FB	8B	E7	94	7B	E6	3C	52	DA	75	89	37	95	15	D4	E0	A6	04	F8	14	17	81	E6	22	94	72	11	66	BF	
23	42	C8	58	EE	AC	00	00	00	00	F9	BE	B4	D9	D7	00	00	00	01	00	00	00	48	60	EB	18	BF	1B	16	20	E3	7E	94	90	FC	8A	
51	59	AB	86	68	8E	9A	83	00	00	00	00	D5	FD	CC	54	1E	25	DE	1C	7A	5A	DD	ED	F2	48	58	B8	BB	66	5C	9F	36	EF	74	4E	
0F	9B	B0	BC	66	49	FF	FF	00	1D	08	D2	BD	61	01	01	00	00	00	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	FF	FF	FF	FF	07	04	FF	FF	00	1D	01	0B	FF	FF	FF	FF	01	00	F2	05	2A	01	00	00	43	00		
F5	5B	50	52	28	E4	C3	D5	19	4C	1F	CF	AA	15	A4	56	AB	DF	37	F9	B9	D9	7A	40	40	AF	C0	73	DE	E6	C8	90	64	98	4F	03	
C1	3E	23	64	46	B4	17	AB	79	A0	FC	AE	41	2A	E3	31	6B	77	AC	00	00	00	00	F9	BE	B4	D9	D7	00	00	00	01	00	00	00	BD	
A1	B1	08	CE	1A	5D	70	03	8D	0A	96	7B	AC	B6	8B	6B	63	06	5F	62	6A	00	00	00	00	44	F6	72	22	60	90	D8	5D	B9	A9	F2	
B3	87	AF	7B	E5	B7	FB	B7	A1	76	7C	83	1C	9E	99	5D	BE	66	49	FF	FF	00	1D	05	E0	ED	6D	01	01	00	00	00	01	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	FF	FF	FF	07	04	FF	FF	00	1D	01	0E	FF		
05	2A	01	00	00	00	43	41	04	94	B9	D3	E7	6C	5B	16	29	EC	F9	7F	FF	95	D7	A4	BB	DA	C8	7C	C2	60	99	AD	A2	80	66	C6	
CD	89	71	94	A0	8D	0C	27	26	C5	74	7F	1D	B4	9E	8C	F9	0E	75	DC	3E	35	50	AE	9B	30	08	6F	3C	D5	AA	AC	00	00	00	00	00
00	00	01	00	00	00	49	44	46	95	62	AE	1C	2C	74	D9	A5	35	E0	0B	6F	3E	40	FF	BA	D4	F2	FD	A3	89	55	01	00	00	00	00	

Transaction OUTPUTS and INPUTS

Thus a simple transaction with a person "A" transferring some amount to a person "B" or any event transaction...will generally look like in screenshot below

Hash	0787e6e1f742808d2b8400e2c28fb7c6fcba414c8a498354af7018af...	2015-03-01 11:52
	COINBASE (Newly Generated Coins)	1LH3QtVjrQmKemRDaJzoWAibPhvi5v5pvk 1JLRXD8rjRgQtTS9MvfQALfHgGWau9L9ky
Fee	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 158 bytes)	0.00000000 BTC  25.00277017 BTC 

Transaction data : RAW BLOCKCHAIN DATA FILES

Fields

Field	Data	Size	Description																								
Version	01000000 ⓘ	4 bytes	Which version of transaction data structure we're using.																								
Input Count	01 ⓘ	Variable	Indicates the upcoming number of inputs.																								
Input(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>TXID</td><td>796...efc ⓘ</td><td>32 bytes</td><td>Refer to an existing transaction.</td></tr><tr><td>VOUT</td><td>01000000 ⓘ</td><td>4 bytes</td><td>Select one of its outputs.</td></tr><tr><td>ScriptSig Size</td><td>6a ⓘ</td><td>Variable</td><td>Indicates the upcoming size of the unlocking code.</td></tr><tr><td>ScriptSig</td><td>473...825</td><td></td><td>A script that unlocks the input.</td></tr><tr><td>Sequence</td><td>ffffffff ⓘ</td><td>4 bytes</td><td></td></tr></tbody></table>			Field	Data	Size	Description	TXID	796...efc ⓘ	32 bytes	Refer to an existing transaction.	VOUT	01000000 ⓘ	4 bytes	Select one of its outputs.	ScriptSig Size	6a ⓘ	Variable	Indicates the upcoming size of the unlocking code.	ScriptSig	473...825		A script that unlocks the input.	Sequence	ffffffff ⓘ	4 bytes	
Field	Data	Size	Description																								
TXID	796...efc ⓘ	32 bytes	Refer to an existing transaction.																								
VOUT	01000000 ⓘ	4 bytes	Select one of its outputs.																								
ScriptSig Size	6a ⓘ	Variable	Indicates the upcoming size of the unlocking code.																								
ScriptSig	473...825		A script that unlocks the input.																								
Sequence	ffffffff ⓘ	4 bytes																									
Output Count	01 ⓘ	Variable	Indicates the upcoming number of outputs.																								
Output(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>Value</td><td>4ba...000000000000 ⓘ</td><td>8 bytes</td><td>The value of the output in satoshis.</td></tr><tr><td>ScriptPubKey Size</td><td>19 ⓘ</td><td>Variable</td><td>Indicates the upcoming size of the locking code.</td></tr><tr><td>ScriptPubKey</td><td>76a9...88ac</td><td></td><td>A script that locks the output.</td></tr></tbody></table>			Field	Data	Size	Description	Value	4ba...000000000000 ⓘ	8 bytes	The value of the output in satoshis.	ScriptPubKey Size	19 ⓘ	Variable	Indicates the upcoming size of the locking code.	ScriptPubKey	76a9...88ac		A script that locks the output.								
Field	Data	Size	Description																								
Value	4ba...000000000000 ⓘ	8 bytes	The value of the output in satoshis.																								
ScriptPubKey Size	19 ⓘ	Variable	Indicates the upcoming size of the locking code.																								
ScriptPubKey	76a9...88ac		A script that locks the output.																								
Locktime	00000000 ⓘ	4 bytes	Set a minimum block height or Unix time that this transaction can be included in.																								

Transaction data : RAW BLOCKCHAIN DATA FILES

```
01000000017967a5185e907a25225574544c31f7b059c1a191d65b53dcc1554d339c4f9efc010000006a47304402206a2eb16b7b92051d0fa38c133e67684ed064effada1d7f925c  
842da401d4f22702201f196b10e6e4b4a9fff948e5c5d71ec5da53e90529c8dbd122bff2b1d21dc8a90121039b7bcd0824b9a9164f7ba098408e63e5b7e3cf90835cce19868f54f  
8961a825fffffffff014baef21000000000001976a914db4d1141d0048b1ed15839d0b7a4c488cd368b0e88ac00000000
```

Transaction: [c1b4e695098210a31fe02abffe9005cffc051bbe86ff33e173155bcbdc5821e3](#)

Transaction data : RAW BLOCKCHAIN DATA FILES

01000000017967a5185e907a25225574544c31f7b059c1a191d65b53dcc1554d339c4f9efc01000006a47304402206a2eb16b7b92051d0fa38c133e67684ed064effada1d7f925c
d4f22702201f196b10e6e4b4a9fff948e5c5d71ec5da53e90529c8dbd122bff2b1d21dc8a90121039b7bcd0824b9a9164f7ba098408e63e5b7e3cf90835cce19868f54f
fffffffff014baf2100000000001976a914db4d1141d0048b1ed15839d0b7a4c488cd368b0e88ac00000000

Version

Fields

Field	Data	Size	Description																								
Version	01000000	4 bytes	Which version of transaction data structure we're using.																								
Input Count	01	Variable	Indicates the upcoming number of inputs.																								
Input(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>TXID</td><td>796...efc</td><td>32 bytes</td><td>Refer to an existing transaction.</td></tr><tr><td>VOUT</td><td>01000000</td><td>4 bytes</td><td>Select one of its outputs.</td></tr><tr><td>ScriptSig Size</td><td>6a</td><td>Variable</td><td>Indicates the upcoming size of the unlocking code.</td></tr><tr><td>ScriptSig</td><td>473...825</td><td></td><td>A script that unlocks the input.</td></tr><tr><td>Sequence</td><td>fffffff0</td><td>4 bytes</td><td></td></tr></tbody></table>			Field	Data	Size	Description	TXID	796...efc	32 bytes	Refer to an existing transaction.	VOUT	01000000	4 bytes	Select one of its outputs.	ScriptSig Size	6a	Variable	Indicates the upcoming size of the unlocking code.	ScriptSig	473...825		A script that unlocks the input.	Sequence	fffffff0	4 bytes	
Field	Data	Size	Description																								
TXID	796...efc	32 bytes	Refer to an existing transaction.																								
VOUT	01000000	4 bytes	Select one of its outputs.																								
ScriptSig Size	6a	Variable	Indicates the upcoming size of the unlocking code.																								
ScriptSig	473...825		A script that unlocks the input.																								
Sequence	fffffff0	4 bytes																									
Output Count	01	Variable	Indicates the upcoming number of outputs.																								
Output(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>Value</td><td>4baf210000000000</td><td>8 bytes</td><td>The value of the output in satoshis.</td></tr><tr><td>ScriptPubKey Size</td><td>19</td><td>Variable</td><td>Indicates the upcoming size of the locking code.</td></tr><tr><td>ScriptPubKey</td><td>76a9...88ac</td><td></td><td>A script that locks the output.</td></tr></tbody></table>			Field	Data	Size	Description	Value	4baf210000000000	8 bytes	The value of the output in satoshis.	ScriptPubKey Size	19	Variable	Indicates the upcoming size of the locking code.	ScriptPubKey	76a9...88ac		A script that locks the output.								
Field	Data	Size	Description																								
Value	4baf210000000000	8 bytes	The value of the output in satoshis.																								
ScriptPubKey Size	19	Variable	Indicates the upcoming size of the locking code.																								
ScriptPubKey	76a9...88ac		A script that locks the output.																								
Locktime	00000000	4 bytes	Set a minimum block height or Unix time that this transaction can be included in.																								

Transaction data : RAW BLOCKCHAIN DATA FILES

0100000001 7967a5185e907a25225574544c31f7b059c1a191d65b53dcc1554d339c4f9efc 010000006a47304402206a2eb16b7b92051d0fa38c133e67684ed064effada1d7f925c
842da401d4f22702201f196b10e6e4b4a9fff94 71ec5da53e90529c8dbd122bfff2b1d21dc8a90121039b7bcd0824b9a9164f7ba098408e63e5b7e3cf90835cce19868f54f
8961a825fffffffff014baef21000000000001976a d1141d0048b1ed15839d0b7a4c488cd368b0e88ac00000000

Input

TXID

Fields

Field	Data	Size	Description																								
Version	01000000 ⓘ	4 bytes	Which version of transaction data structure we're using.																								
Input Count	01 ⓘ	Variable	Indicates the upcoming number of inputs.																								
Input(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>TXID</td><td>796...efc ⓘ</td><td>32 bytes</td><td>Refer to an existing transaction.</td></tr><tr><td>VOUT</td><td>01000000 ⓘ</td><td>4 bytes</td><td>Select one of its outputs.</td></tr><tr><td>ScriptSig Size</td><td>6a ⓘ</td><td>Variable</td><td>Indicates the upcoming size of the unlocking code.</td></tr><tr><td>ScriptSig</td><td>473...825</td><td></td><td>A script that unlocks the input.</td></tr><tr><td>Sequence</td><td>fffffff ⓘ</td><td>4 bytes</td><td></td></tr></tbody></table>			Field	Data	Size	Description	TXID	796...efc ⓘ	32 bytes	Refer to an existing transaction.	VOUT	01000000 ⓘ	4 bytes	Select one of its outputs.	ScriptSig Size	6a ⓘ	Variable	Indicates the upcoming size of the unlocking code.	ScriptSig	473...825		A script that unlocks the input.	Sequence	fffffff ⓘ	4 bytes	
Field	Data	Size	Description																								
TXID	796...efc ⓘ	32 bytes	Refer to an existing transaction.																								
VOUT	01000000 ⓘ	4 bytes	Select one of its outputs.																								
ScriptSig Size	6a ⓘ	Variable	Indicates the upcoming size of the unlocking code.																								
ScriptSig	473...825		A script that unlocks the input.																								
Sequence	fffffff ⓘ	4 bytes																									
Output Count	01 ⓘ	Variable	Indicates the upcoming number of outputs.																								
Output(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>Value</td><td>4baef210000000000 ⓘ</td><td>8 bytes</td><td>The value of the output in satoshis.</td></tr><tr><td>ScriptPubKey Size</td><td>19 ⓘ</td><td>Variable</td><td>Indicates the upcoming size of the locking code.</td></tr><tr><td>ScriptPubKey</td><td>76a9...88ac</td><td></td><td>A script that locks the output.</td></tr></tbody></table>			Field	Data	Size	Description	Value	4baef210000000000 ⓘ	8 bytes	The value of the output in satoshis.	ScriptPubKey Size	19 ⓘ	Variable	Indicates the upcoming size of the locking code.	ScriptPubKey	76a9...88ac		A script that locks the output.								
Field	Data	Size	Description																								
Value	4baef210000000000 ⓘ	8 bytes	The value of the output in satoshis.																								
ScriptPubKey Size	19 ⓘ	Variable	Indicates the upcoming size of the locking code.																								
ScriptPubKey	76a9...88ac		A script that locks the output.																								
Locktime	00000000 ⓘ	4 bytes	Set a minimum block height or Unix time that this transaction can be included in.																								

Transaction data : RAW BLOCKCHAIN DATA FILES

Fields

Field	Data	Size	Description																								
Version	01000000 	4 bytes	Which version of transaction data structure we're using.																								
Input Count	01	Variable	Indicates the upcoming number of inputs.																								
Input(s)	<table border="1"> <thead> <tr> <th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr> </thead> <tbody> <tr> <td>TXID</td><td>796...efc </td><td>32 bytes</td><td>Refer to an existing transaction.</td></tr> <tr> <td>VOUT</td><td>01000000 </td><td>4 bytes</td><td>Select one of its outputs.</td></tr> <tr> <td>ScriptSig Size</td><td>6a</td><td>Variable</td><td>Indicates the upcoming size of the unlocking code.</td></tr> <tr> <td>ScriptSig</td><td>473...825</td><td></td><td>A script that unlocks the input.</td></tr> <tr> <td>Sequence</td><td>ffffffffff </td><td>4 bytes</td><td></td></tr> </tbody> </table>			Field	Data	Size	Description	TXID	796...efc 	32 bytes	Refer to an existing transaction.	VOUT	01000000 	4 bytes	Select one of its outputs.	ScriptSig Size	6a	Variable	Indicates the upcoming size of the unlocking code.	ScriptSig	473...825		A script that unlocks the input.	Sequence	ffffffffff 	4 bytes	
Field	Data	Size	Description																								
TXID	796...efc 	32 bytes	Refer to an existing transaction.																								
VOUT	01000000 	4 bytes	Select one of its outputs.																								
ScriptSig Size	6a	Variable	Indicates the upcoming size of the unlocking code.																								
ScriptSig	473...825		A script that unlocks the input.																								
Sequence	ffffffffff 	4 bytes																									
Output Count	01	Variable	Indicates the upcoming number of outputs.																								
Output(s)	<table border="1"> <thead> <tr> <th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Value</td><td>4ba...000000000000 </td><td>8 bytes</td><td>The value of the output in satoshis.</td></tr> <tr> <td>ScriptPubKey Size</td><td>19</td><td>Variable</td><td>Indicates the upcoming size of the locking code.</td></tr> <tr> <td>ScriptPubKey</td><td>76a9...88ac</td><td></td><td>A script that locks the output.</td></tr> </tbody> </table>			Field	Data	Size	Description	Value	4ba...000000000000 	8 bytes	The value of the output in satoshis.	ScriptPubKey Size	19	Variable	Indicates the upcoming size of the locking code.	ScriptPubKey	76a9...88ac		A script that locks the output.								
Field	Data	Size	Description																								
Value	4ba...000000000000 	8 bytes	The value of the output in satoshis.																								
ScriptPubKey Size	19	Variable	Indicates the upcoming size of the locking code.																								
ScriptPubKey	76a9...88ac		A script that locks the output.																								
Locktime	00000000 	4 bytes	Set a minimum block height or Unix time that this transaction can be included in.																								

Transaction data : RAW BLOCKCHAIN DATA FILES

Input

01000000017967a5185e907a25225574544c31f7b059c1a191d65b53dcc1554d339c4f9efc010000006a47304402206a2eb16b7b92051d0fa38c133e67684ed064effada1d7f925c
842da401d4f22702201f196b10e6e4b4a9fff948e5c5d71ec5da53e90529c8dbd122bff2b1d21dc8a90121039b7bcd0824b9a9164f7ba098408e63e5b7e3cf90835ccce19868f54f
8961a825ffffffff014baf21000000000001976a914db4d1141d0048b1ed15839d0b7a4c488cd368b0e88ac00000000

scriptSig

action: c1b4e695098210a31fe02abffe9005cfffc051bbe86ff33e173155bcbdc5821e3

Fields

Field	Data	Size	Description																								
Version	01000000	4 bytes	Which version of transaction data structure we're using.																								
Input Count	01	Variable	Indicates the upcoming number of inputs.																								
Input(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>TXID</td><td>796...efc</td><td>32 bytes</td><td>Refer to an existing transaction.</td></tr><tr><td>VOUT</td><td>01000000</td><td>4 bytes</td><td>Select one of its outputs.</td></tr><tr><td>ScriptSig Size</td><td>6a</td><td>Variable</td><td>Indicates the upcoming size of the unlocking code.</td></tr><tr><td>ScriptSig</td><td>473...825</td><td></td><td>A script that unlocks the input.</td></tr><tr><td>Sequence</td><td>fffffff</td><td>4 bytes</td><td></td></tr></tbody></table>			Field	Data	Size	Description	TXID	796...efc	32 bytes	Refer to an existing transaction.	VOUT	01000000	4 bytes	Select one of its outputs.	ScriptSig Size	6a	Variable	Indicates the upcoming size of the unlocking code.	ScriptSig	473...825		A script that unlocks the input.	Sequence	fffffff	4 bytes	
Field	Data	Size	Description																								
TXID	796...efc	32 bytes	Refer to an existing transaction.																								
VOUT	01000000	4 bytes	Select one of its outputs.																								
ScriptSig Size	6a	Variable	Indicates the upcoming size of the unlocking code.																								
ScriptSig	473...825		A script that unlocks the input.																								
Sequence	fffffff	4 bytes																									
Output Count	01	Variable	Indicates the upcoming number of outputs.																								
Output(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>Value</td><td>4baf210000000000</td><td>8 bytes</td><td>The value of the output in satoshis.</td></tr><tr><td>ScriptPubKey Size</td><td>19</td><td>Variable</td><td>Indicates the upcoming size of the locking code.</td></tr><tr><td>ScriptPubKey</td><td>76a9...88ac</td><td></td><td>A script that locks the output.</td></tr></tbody></table>			Field	Data	Size	Description	Value	4baf210000000000	8 bytes	The value of the output in satoshis.	ScriptPubKey Size	19	Variable	Indicates the upcoming size of the locking code.	ScriptPubKey	76a9...88ac		A script that locks the output.								
Field	Data	Size	Description																								
Value	4baf210000000000	8 bytes	The value of the output in satoshis.																								
ScriptPubKey Size	19	Variable	Indicates the upcoming size of the locking code.																								
ScriptPubKey	76a9...88ac		A script that locks the output.																								
Locktime	00000000	4 bytes	Set a minimum block height or Unix time that this transaction can be included in.																								

Transaction data : RAW BLOCKCHAIN DATA FILES

01000000 Input 185e907a25225574544c31f7b059c1a191d65b53dcc1554d339c4f9efc01000006a47304402206a2eb16b7b92051d0fa38c133e67684ed064effada1d7f925c
842da401d... 0201f196b10e6e4b4a9fff948e5c5d71ec5da53e90529c8dbd122bff2b1d21dc8a90121039b7bcd0824b9a9164f7ba098408e63e5b7e3cf90835cc...
8961a825fffff014ba... 00000000

Sequence

Transaction: [c1b4e695098210a31fe02abffe9005cffc051bbe86ff33e173155bcbdc5821e3](#)

Fields

Field	Data	Size	Description																								
Version	01000000	4 bytes	Which version of transaction data structure we're using.																								
Input Count	01	Variable	Indicates the upcoming number of inputs.																								
Input(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>TXID</td><td>796...efc </td><td>32 bytes</td><td>Refer to an existing transaction.</td></tr><tr><td>VOUT</td><td>01000000 </td><td>4 bytes</td><td>Select one of its outputs.</td></tr><tr><td>ScriptSig Size</td><td>6a</td><td>Variable</td><td>Indicates the upcoming size of the unlocking code.</td></tr><tr><td>ScriptSig</td><td>473...825</td><td></td><td>A script that unlocks the input.</td></tr><tr><td>Sequence</td><td>fffff...ffff </td><td>4 bytes</td><td></td></tr></tbody></table>			Field	Data	Size	Description	TXID	796...efc	32 bytes	Refer to an existing transaction.	VOUT	01000000	4 bytes	Select one of its outputs.	ScriptSig Size	6a	Variable	Indicates the upcoming size of the unlocking code.	ScriptSig	473...825		A script that unlocks the input.	Sequence	fffff...ffff	4 bytes	
Field	Data	Size	Description																								
TXID	796...efc	32 bytes	Refer to an existing transaction.																								
VOUT	01000000	4 bytes	Select one of its outputs.																								
ScriptSig Size	6a	Variable	Indicates the upcoming size of the unlocking code.																								
ScriptSig	473...825		A script that unlocks the input.																								
Sequence	fffff...ffff	4 bytes																									
Output Count	01	Variable	Indicates the upcoming number of outputs.																								
Output(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>Value</td><td>4ba...0000000000 </td><td>8 bytes</td><td>The value of the output in satoshis.</td></tr><tr><td>ScriptPubKey Size</td><td>19</td><td>Variable</td><td>Indicates the upcoming size of the locking code.</td></tr><tr><td>ScriptPubKey</td><td>76a9...88ac</td><td></td><td>A script that locks the output.</td></tr></tbody></table>			Field	Data	Size	Description	Value	4ba...0000000000	8 bytes	The value of the output in satoshis.	ScriptPubKey Size	19	Variable	Indicates the upcoming size of the locking code.	ScriptPubKey	76a9...88ac		A script that locks the output.								
Field	Data	Size	Description																								
Value	4ba...0000000000	8 bytes	The value of the output in satoshis.																								
ScriptPubKey Size	19	Variable	Indicates the upcoming size of the locking code.																								
ScriptPubKey	76a9...88ac		A script that locks the output.																								
Locktime	00000000	4 bytes	Set a minimum block height or Unix time that this transaction can be included in.																								

Transaction data : RAW BLOCKCHAIN DATA FILES

01000000017967a5185e907a25225574544c31f7b059c1a191d65b53dcc1554d339c4f9efc010000006a47304402206a2eb16b7b92051d0fa38c133e67684ed064effada1d7f925c
842da401d4f22702201f196b10e6e4b4a9fff948e5c5d71ec5da53e90529c8dbd122bff2b1d21dc8a90121039b7bcd0824b9a9164f7ba098408e63e5b7e3cf90835cccb19868f54f
8961a825fffffffff014baf2100000000001976a914db4d1141d0048b1ed15839d0b7a4c488cd368b0e88ac00000000

Output Count

Transaction: [c1b4e695098210a31fe02abffe9005cffc051bbe86ff33e173155bcbdc5821e3](#)

Fields

Field	Data	Size	Description																								
Version	01000000 	4 bytes	Which version of transaction data structure we're using.																								
Input Count	01	Variable	Indicates the upcoming number of inputs.																								
Input(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>TXID</td><td>796...efc </td><td>32 bytes</td><td>Refer to an existing transaction.</td></tr><tr><td>VOUT</td><td>01000000 </td><td>4 bytes</td><td>Select one of its outputs.</td></tr><tr><td>ScriptSig Size</td><td>6a</td><td>Variable</td><td>Indicates the upcoming size of the unlocking code.</td></tr><tr><td>ScriptSig</td><td>473...825</td><td></td><td>A script that unlocks the input.</td></tr><tr><td>Sequence</td><td>ffffffffff </td><td>4 bytes</td><td></td></tr></tbody></table>			Field	Data	Size	Description	TXID	796...efc 	32 bytes	Refer to an existing transaction.	VOUT	01000000 	4 bytes	Select one of its outputs.	ScriptSig Size	6a	Variable	Indicates the upcoming size of the unlocking code.	ScriptSig	473...825		A script that unlocks the input.	Sequence	ffffffffff 	4 bytes	
Field	Data	Size	Description																								
TXID	796...efc 	32 bytes	Refer to an existing transaction.																								
VOUT	01000000 	4 bytes	Select one of its outputs.																								
ScriptSig Size	6a	Variable	Indicates the upcoming size of the unlocking code.																								
ScriptSig	473...825		A script that unlocks the input.																								
Sequence	ffffffffff 	4 bytes																									
Output Count	01	Variable	Indicates the upcoming number of outputs.																								
Output(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>Value</td><td>4ba<ins>f210000000000</ins> </td><td>8 bytes</td><td>The value of the output in satoshis.</td></tr><tr><td>ScriptPubKey Size</td><td>19</td><td>Variable</td><td>Indicates the upcoming size of the locking code.</td></tr><tr><td>ScriptPubKey</td><td>76a9...88ac</td><td></td><td>A script that locks the output.</td></tr></tbody></table>			Field	Data	Size	Description	Value	4ba <ins>f210000000000</ins> 	8 bytes	The value of the output in satoshis.	ScriptPubKey Size	19	Variable	Indicates the upcoming size of the locking code.	ScriptPubKey	76a9...88ac		A script that locks the output.								
Field	Data	Size	Description																								
Value	4ba <ins>f210000000000</ins> 	8 bytes	The value of the output in satoshis.																								
ScriptPubKey Size	19	Variable	Indicates the upcoming size of the locking code.																								
ScriptPubKey	76a9...88ac		A script that locks the output.																								
Locktime	00000000 	4 bytes	Set a minimum block height or Unix time that this transaction can be included in.																								

Transaction data : RAW BLOCKCHAIN DATA FILES

01000000017967a5185...
25574544c31f7b059c1a191d65b53dcc1554d339c4f9efc01000006a47304402206a2eb16b7b92051d0fa38c133e67684ed064effada1d7f925c
842da401d4f22702201...
5e4b4a9fff948e5c5d71ec5da53e90529c8dbd122bff2b1d21dc8a90121039b7bcd0824b9a9164f7ba098408e63e5b7e3cf90835cc...
8961a825fffffffff014ba...
f104baf21000000000001976a914db4d1141d0048b1ed15839d0b7a4c488cd368b0e88ac00000000

Output

Value

Transaction: [c1b4e695098210a31fe02abffe9005cffc051bbe86ff33e173155bcbdc5821e3](#)

Fields

Field	Data	Size	Description																								
Version	01000000 	4 bytes	Which version of transaction data structure we're using.																								
Input Count	01 	Variable	Indicates the upcoming number of inputs.																								
Input(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>TXID</td><td>796...efc </td><td>32 bytes</td><td>Refer to an existing transaction.</td></tr><tr><td>VOUT</td><td>01000000 </td><td>4 bytes</td><td>Select one of its outputs.</td></tr><tr><td>ScriptSig Size</td><td>6a </td><td>Variable</td><td>Indicates the upcoming size of the unlocking code.</td></tr><tr><td>ScriptSig</td><td>473...825</td><td></td><td>A script that unlocks the input.</td></tr><tr><td>Sequence</td><td>ffffffffff </td><td>4 bytes</td><td></td></tr></tbody></table>			Field	Data	Size	Description	TXID	796...efc 	32 bytes	Refer to an existing transaction.	VOUT	01000000 	4 bytes	Select one of its outputs.	ScriptSig Size	6a 	Variable	Indicates the upcoming size of the unlocking code.	ScriptSig	473...825		A script that unlocks the input.	Sequence	ffffffffff 	4 bytes	
Field	Data	Size	Description																								
TXID	796...efc 	32 bytes	Refer to an existing transaction.																								
VOUT	01000000 	4 bytes	Select one of its outputs.																								
ScriptSig Size	6a 	Variable	Indicates the upcoming size of the unlocking code.																								
ScriptSig	473...825		A script that unlocks the input.																								
Sequence	ffffffffff 	4 bytes																									
Output Count	01 	Variable	Indicates the upcoming number of outputs.																								
Output(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>Value</td><td>4ba...0000000000 </td><td>8 bytes</td><td>The value of the output in satoshis.</td></tr><tr><td>ScriptPubKey Size</td><td>19 </td><td>Variable</td><td>Indicates the upcoming size of the locking code.</td></tr><tr><td>ScriptPubKey</td><td>76a9...88ac</td><td></td><td>A script that locks the output.</td></tr></tbody></table>			Field	Data	Size	Description	Value	4ba...0000000000 	8 bytes	The value of the output in satoshis.	ScriptPubKey Size	19 	Variable	Indicates the upcoming size of the locking code.	ScriptPubKey	76a9...88ac		A script that locks the output.								
Field	Data	Size	Description																								
Value	4ba...0000000000 	8 bytes	The value of the output in satoshis.																								
ScriptPubKey Size	19 	Variable	Indicates the upcoming size of the locking code.																								
ScriptPubKey	76a9...88ac		A script that locks the output.																								
Locktime	00000000 	4 bytes	Set a minimum block height or Unix time that this transaction can be included in.																								

Transaction data : RAW BLOCKCHAIN DATA FILES

01000000017967a5185e907a25225574544c21f7b059c1a191d65b53dcc1554d339c4f9efc01000006a47304402206a2eb16b7b92051d0fa38c133e67684ed064effada1d7f925c
842da401d4f22702201f196b10e6e4b4 Output 1e5c5d71ec5da53e90529c8dbd122bff2b1d21dc8a90121039b7bcd0824b9a9164f7ba098408e63e5b7e3cf90835cccb19868f54f
8961a825fffffffff014baf2100000000001976a914db4d1141d0048b1ed15839d0b7a4c488cd368b0e88ac00000000

scriptPubKey Size

Transaction: [c1b4e695098210a31fe02abffe9005cffc051bbe86ff33e173155bcbdc5821e3](#)

Fields

Field	Data	Size	Description																								
Version	01000000	4 bytes	Which version of transaction data structure we're using.																								
Input Count	01	Variable	Indicates the upcoming number of inputs.																								
Input(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>TXID</td><td>796...efc</td><td>32 bytes</td><td>Refer to an existing transaction.</td></tr><tr><td>VOUT</td><td>01000000</td><td>4 bytes</td><td>Select one of its outputs.</td></tr><tr><td>ScriptSig Size</td><td>6a</td><td>Variable</td><td>Indicates the upcoming size of the unlocking code.</td></tr><tr><td>ScriptSig</td><td>473...825</td><td></td><td>A script that unlocks the input.</td></tr><tr><td>Sequence</td><td>ffffffffff</td><td>4 bytes</td><td></td></tr></tbody></table>			Field	Data	Size	Description	TXID	796...efc	32 bytes	Refer to an existing transaction.	VOUT	01000000	4 bytes	Select one of its outputs.	ScriptSig Size	6a	Variable	Indicates the upcoming size of the unlocking code.	ScriptSig	473...825		A script that unlocks the input.	Sequence	ffffffffff	4 bytes	
Field	Data	Size	Description																								
TXID	796...efc	32 bytes	Refer to an existing transaction.																								
VOUT	01000000	4 bytes	Select one of its outputs.																								
ScriptSig Size	6a	Variable	Indicates the upcoming size of the unlocking code.																								
ScriptSig	473...825		A script that unlocks the input.																								
Sequence	ffffffffff	4 bytes																									
Output Count	01	Variable	Indicates the upcoming number of outputs.																								
Output(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>Value</td><td>4baf210000000000</td><td>8 bytes</td><td>The value of the output in satoshis.</td></tr><tr><td>ScriptPubKey Size</td><td>19</td><td>Variable</td><td>Indicates the upcoming size of the locking code.</td></tr><tr><td>ScriptPubKey</td><td>76a9...88ac</td><td></td><td>A script that locks the output.</td></tr></tbody></table>			Field	Data	Size	Description	Value	4baf210000000000	8 bytes	The value of the output in satoshis.	ScriptPubKey Size	19	Variable	Indicates the upcoming size of the locking code.	ScriptPubKey	76a9...88ac		A script that locks the output.								
Field	Data	Size	Description																								
Value	4baf210000000000	8 bytes	The value of the output in satoshis.																								
ScriptPubKey Size	19	Variable	Indicates the upcoming size of the locking code.																								
ScriptPubKey	76a9...88ac		A script that locks the output.																								
Locktime	00000000	4 bytes	Set a minimum block height or Unix time that this transaction can be included in.																								

Transaction data : RAW BLOCKCHAIN DATA FILES

01000000017967a5185e907a25225574544c31f7b9efc1a191d65b53dcc1554d339c4f9efc01000006a47304402206a2eb16b7b92051d0fa38c133e67684ed064effada1d7f925c
842da401d4f22702201f196b10e6e4b4a9fff948 Output c5da53e90529c8dbd122bff2b1d21dc8a90121039b7bcd0824b9a9164f7ba098408e63e5b7e3cf90835ccce19868f54f
8961a825fffffffff014baf2100000000001976a914db4d1141d0048b1ed15839d0b7a4c488cd368b0e88ac00000000

scriptPubKey

Transaction: [c1b4e695098210a31fe02abffe9005cffc051bbe86ff33e173155bcbdc5821e3](#)

Fields

Field	Data	Size	Description																								
Version	01000000 	4 bytes	Which version of transaction data structure we're using.																								
Input Count	01	Variable	Indicates the upcoming number of inputs.																								
Input(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>TXID</td><td>796...efc </td><td>32 bytes</td><td>Refer to an existing transaction.</td></tr><tr><td>VOUT</td><td>01000000 </td><td>4 bytes</td><td>Select one of its outputs.</td></tr><tr><td>ScriptSig Size</td><td>6a</td><td>Variable</td><td>Indicates the upcoming size of the unlocking code.</td></tr><tr><td>ScriptSig</td><td>473...825</td><td></td><td>A script that unlocks the input.</td></tr><tr><td>Sequence</td><td>ffffffffff </td><td>4 bytes</td><td></td></tr></tbody></table>			Field	Data	Size	Description	TXID	796...efc 	32 bytes	Refer to an existing transaction.	VOUT	01000000 	4 bytes	Select one of its outputs.	ScriptSig Size	6a	Variable	Indicates the upcoming size of the unlocking code.	ScriptSig	473...825		A script that unlocks the input.	Sequence	ffffffffff 	4 bytes	
Field	Data	Size	Description																								
TXID	796...efc 	32 bytes	Refer to an existing transaction.																								
VOUT	01000000 	4 bytes	Select one of its outputs.																								
ScriptSig Size	6a	Variable	Indicates the upcoming size of the unlocking code.																								
ScriptSig	473...825		A script that unlocks the input.																								
Sequence	ffffffffff 	4 bytes																									
Output Count	01	Variable	Indicates the upcoming number of outputs.																								
Output(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>Value</td><td>4baf210000000000 </td><td>8 bytes</td><td>The value of the output in satoshis.</td></tr><tr><td>ScriptPubKey Size</td><td>19</td><td>Variable</td><td>Indicates the upcoming size of the locking code.</td></tr><tr><td>ScriptPubKey</td><td>76a9...88ac</td><td></td><td>A script that locks the output.</td></tr></tbody></table>			Field	Data	Size	Description	Value	4baf210000000000 	8 bytes	The value of the output in satoshis.	ScriptPubKey Size	19	Variable	Indicates the upcoming size of the locking code.	ScriptPubKey	76a9...88ac		A script that locks the output.								
Field	Data	Size	Description																								
Value	4baf210000000000 	8 bytes	The value of the output in satoshis.																								
ScriptPubKey Size	19	Variable	Indicates the upcoming size of the locking code.																								
ScriptPubKey	76a9...88ac		A script that locks the output.																								
Locktime	00000000 	4 bytes	Set a minimum block height or Unix time that this transaction can be included in.																								

Transaction data : RAW BLOCKCHAIN DATA FILES

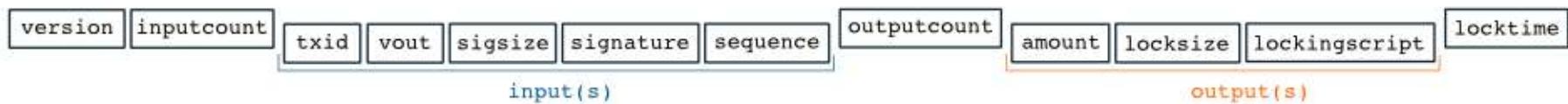
01000000017967a5185e907a25225574544c31f7b059c1a191d65b53dcc1554d339c4f9efc010000006a47304402206a2eb16b7b92051d0fa38c133e67684ed064effada1d7f925c
842da401d4f22702201f196b10e6e4b4a9fff948e5c5d71ec5da53e90529c8dbd122bff2b1d21dc8a90121039b7bcd0824b9a9164f7ba098408e63e5b7e3cf90835cccb19868f54f
8961a825fffffffff014baef2100000000001976a914db4d1141d0048b1ed15839d0b7a4c488cd368b0e88ac00000000

Transaction: c1b Locktime 0a31fe02abffe9005cffc051bbe86ff33e173155bcbdc5821e3

Riclus

Field	Data	Size	Description																								
Version	01000000 ⓘ	4 bytes	Which version of transaction data structure we're using.																								
Input Count	01 ⓘ	Variable	Indicates the upcoming number of inputs.																								
Input(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>TXID</td><td>796...efc ⓘ</td><td>32 bytes</td><td>Refer to an existing transaction.</td></tr><tr><td>VOUT</td><td>01000000 ⓘ</td><td>4 bytes</td><td>Select one of its outputs.</td></tr><tr><td>ScriptSig Size</td><td>6a ⓘ</td><td>Variable</td><td>Indicates the upcoming size of the unlocking code.</td></tr><tr><td>ScriptSig</td><td>473...825</td><td></td><td>A script that unlocks the input.</td></tr><tr><td>Sequence</td><td>ffffffffff ⓘ</td><td>4 bytes</td><td></td></tr></tbody></table>			Field	Data	Size	Description	TXID	796...efc ⓘ	32 bytes	Refer to an existing transaction.	VOUT	01000000 ⓘ	4 bytes	Select one of its outputs.	ScriptSig Size	6a ⓘ	Variable	Indicates the upcoming size of the unlocking code.	ScriptSig	473...825		A script that unlocks the input.	Sequence	ffffffffff ⓘ	4 bytes	
Field	Data	Size	Description																								
TXID	796...efc ⓘ	32 bytes	Refer to an existing transaction.																								
VOUT	01000000 ⓘ	4 bytes	Select one of its outputs.																								
ScriptSig Size	6a ⓘ	Variable	Indicates the upcoming size of the unlocking code.																								
ScriptSig	473...825		A script that unlocks the input.																								
Sequence	ffffffffff ⓘ	4 bytes																									
Output Count	01 ⓘ	Variable	Indicates the upcoming number of outputs.																								
Output(s)	<table border="1"><thead><tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr></thead><tbody><tr><td>Value</td><td>4baef210000000000 ⓘ</td><td>8 bytes</td><td>The value of the output in satoshis.</td></tr><tr><td>ScriptPubKey Size</td><td>19 ⓘ</td><td>Variable</td><td>Indicates the upcoming size of the locking code.</td></tr><tr><td>ScriptPubKey</td><td>76a9...88ac</td><td></td><td>A script that locks the output.</td></tr></tbody></table>			Field	Data	Size	Description	Value	4baef210000000000 ⓘ	8 bytes	The value of the output in satoshis.	ScriptPubKey Size	19 ⓘ	Variable	Indicates the upcoming size of the locking code.	ScriptPubKey	76a9...88ac		A script that locks the output.								
Field	Data	Size	Description																								
Value	4baef210000000000 ⓘ	8 bytes	The value of the output in satoshis.																								
ScriptPubKey Size	19 ⓘ	Variable	Indicates the upcoming size of the locking code.																								
ScriptPubKey	76a9...88ac		A script that locks the output.																								
Locktime	00000000 ⓘ	4 bytes	Set a minimum block height or Unix time that this transaction can be included in.																								

Transaction data : RAW BLOCKCHAIN DATA FILES



Transaction data tells **how to unlock existing packages of bitcoins** (from previous transactions), and how to lock them up *again* in to new packages

INDEPENDENT VERIFICATION OF TRANSACTIONS

- The transaction's syntax and data structure must be correct.
- Neither lists of inputs or outputs are empty.
- The transaction size in bytes is less than MAX_BLOCK_SIZE.
- Each output value, as well as the total, must be within the allowed range of values

(less than 21m coins, more than the dust threshold).

- None of the inputs have hash=0

Bitcoin Core considers a transaction output to be dust, when its value is lower than the cost of spending it at the dustRelayFee rate.

TRANSACTION INTERNALS

.....Lets check a hash

MULTICHAIN BLOCKCHAIN



MultiChain

<https://www.multichain.com/developers/>



MultiChain

Bitcoin SCRIPT

SCRIPT

Mini programming language used as a locking mechanism for outputs

A locking script is placed on every output

**An unlocking script must be provided to unlock an output
(i.e. when you're using it as an input)**

It consists of two types of things:

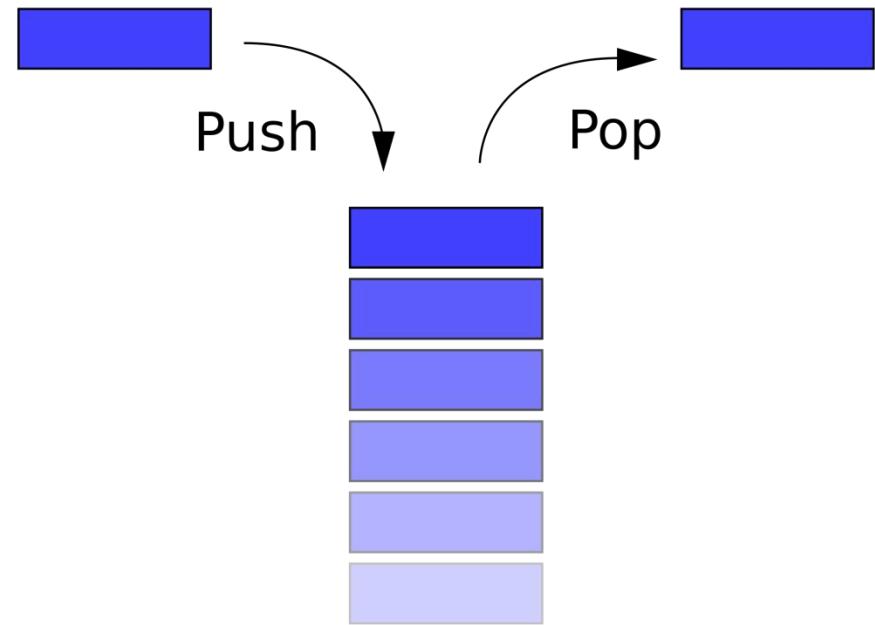
- **Data - For example; public keys and signatures.**
- **OPCODES - Simple functions that operate on the data**

SCRIPT IS STACK BASED

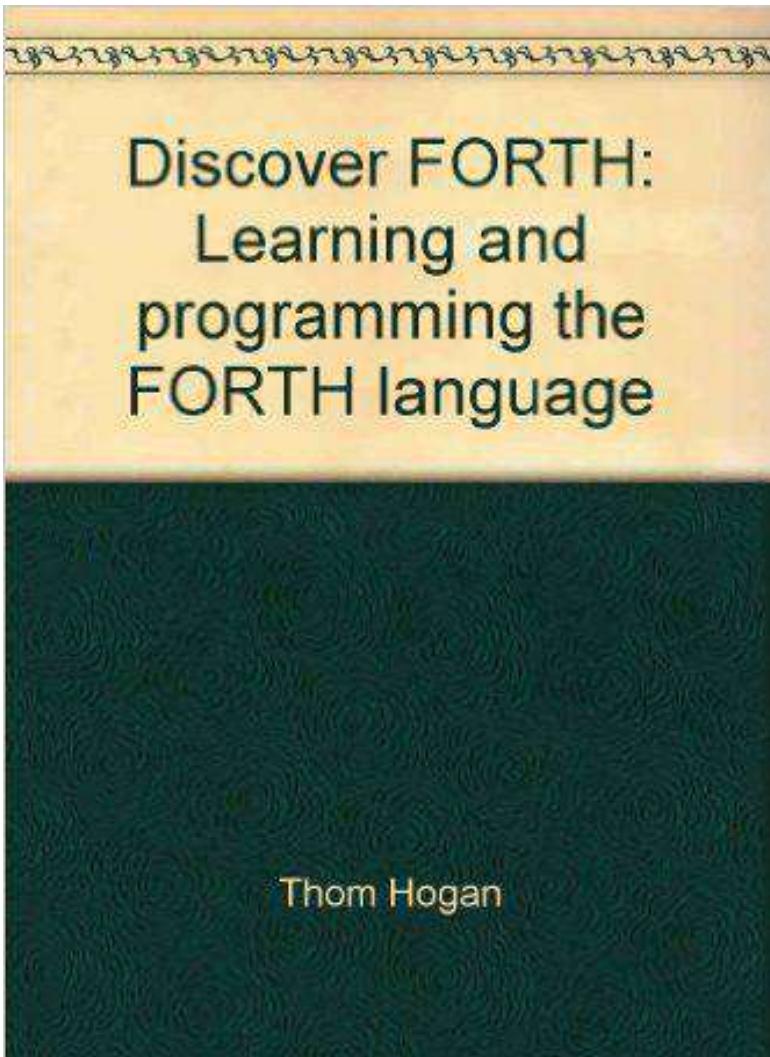
Bitcoin Script uses a data structure that can be thought of as a linear structure represented by a physical stack or pile.

Items at the top of the stack can be added (pushed) or removed (popped) in a “Last In, First Out (LIFO)” queue.

Imagine stacking three books: Book A (top), Book B (middle), and Book C (bottom). With Bitcoin Script, Book A would need to be the first taken out of the stack (popped), followed by Book B and Book C, to put anything at the bottom of the stack (pushed).



SCRIPT IS FORTH LIKE



Script resembles **Forth**, a programming language that first appeared in 1970

Forth is used in the **Open Firmware Bootloader**, space applications (including the Philae spacecraft), and a variety of other embedded systems involving interactions with hardware

SCRIPT IS Reverse-Polish Notation (RPN)

Also known as postfix notation, RPN is a method of placing the operation function at the end of a sentence. For example, adding 5 and 6 in Script must be written as “5 6 +” rather than “5 + 6.”

Reverse Polish Notation

Reverse Polish Notation (RPN), also known as polish postfix notation or simply postfix notation, is a mathematical notation in which operators follow their operands.

For example, the infix expression P1: $5 + ((1 + 2) * 4) - 3$ can be written like this in *Reverse Polish Notation*: P2: 5 1 2 + 4 * + 3 -

In terms of the operation, the expression P1 and P2 can be evaluated as

P1	P2
$5 + ((1 + 2) * 4) - 3$	5 1 2 + 4 * + 3 -
$5 + (3 * 4) - 3$	5 3 4 * + 3 -
$5 + 12 - 3$	5 12 + 3 -
$17 - 3$	17 3 -
14	14

The reverse polish notation has many advantages, such as there is no bracket in the expression and no priority is needed for the operators, most importantly, the evaluation process is quite simple. The reverse polish notation could be evaluated by using a stack.

Evaluation Algorithm

Input	Operation	Stack	Remark
5	Push	5	
1	Push	5,1	
2	Push	5,1,2	
+	Addition	5,3	Pop (1,2), do addition, push in the result (3)
4	Push	5,3,4	
*	Multiplication	5,12	Pop (3,4), do multiplication, push in the result (12)
+	Addition	17	Pop (5,12), do addition, push in the result (17)
3	Push	17,3	
-	Subtraction	14	Pop (17,3), do subtraction, push in the result (14)

SCRIPT IS TURING INCOMPLETE



Turing incomplete means that Script does not allow infinite loops.

Other blockchains developed since Bitcoin have mainly chosen to be Turing Complete, or at least have a high degree of Turing completeness.

HOW DOES BITCOIN SCRIPT WORK?

Bitcoin Script can be thought of as a **list of instructions** recorded with each transaction that describes **how the recipient of the funds can gain access to them**. Most Bitcoin transactions only require simple scripts, but more complex scripts can be implemented



SCRIPT TYPES

- P2PK (Pay To Pubkey)
- P2PKH (Pay To Pubkey Hash)
- P2MS (Pay To Multisig)
- P2SH (Pay To Script Hash)
- NULL DATA



SCRIPT TYPES



Pay to Public Key Hash (P2PKH)

P2PKH is the most commonly used transaction type and is used to send transactions to the bitcoin addresses.

SCRIPT TYPES

Pay to Script Hash (P2SH)

P2SH is used in order to send transactions to a script hash (that is, the addresses starting with 3) and was standardized in BIP16.



SCRIPT TYPES



MultiSig (Pay to MultiSig):

A **complex type** of script where it is **possible to construct a script that required multiple signatures to be valid in order to redeem a transaction.**

Various complex transactions such as escrow and deposits can be built using this script.

SCRIPT TYPES

Null data/OP_RETURN

This script is used to store arbitrary data on the blockchain for a fee. The limit of the message is 40 bytes. The output of this script is unredeemable because OP_RETURN will fail the validation in any case.



BITCOIN SCRIPTS

scriptPubKey is a locking script placed on the output of a Bitcoin transaction that requires certain conditions to be met in order for a recipient to spend his/her bitcoins.

scriptSig is the unlocking script that satisfies the conditions placed on the output by the *scriptPubKey* and is what allows it to be spent.



Bitcoin Improvement Proposal (BIP)

***B**itcoin
Improvement
Proposals*

Bitcoin Improvement Proposal (BIP)

A standard for proposing changes to the
Bitcoin protocol

*Bitcoin
Improvement
Proposals*

Bitcoin Improvement Proposal (BIP)

BIPs can include **consensus-critical changes** (like soft fork and hard fork protocol upgrades) but also other changes **that benefit from coordination across different Bitcoin software implementations**, such as changes to the peer-to-peer layer or new backup seed formats.

*Bitcoin
Improvement
Proposals*

WHO CREATED BIP?

First developed and introduced by early **Bitcoin developer Amir Taaki** who believed that the Bitcoin development process would benefit from becoming more structured and accountable.

Taaki **submitted the first BIP (BIP 0001) on August 19, 2011**, which described the BIP process itself. It was heavily based on the process for improving Python, a programming language, described in Python Enhancement Proposal 0 (PEP 0).

*Bitcoin
Improvement
Proposals*

How Does a BIP Get Adopted (or Rejected)?

As a draft, **the BIP can be changed and improved by the author(s), based on community feedback.** In the case of Bitcoin protocol changes, it will also require a reference implementation, in code. **If the proposal reaches community consensus, it will be considered final.**

*Bitcoin
Improvement
Proposals*

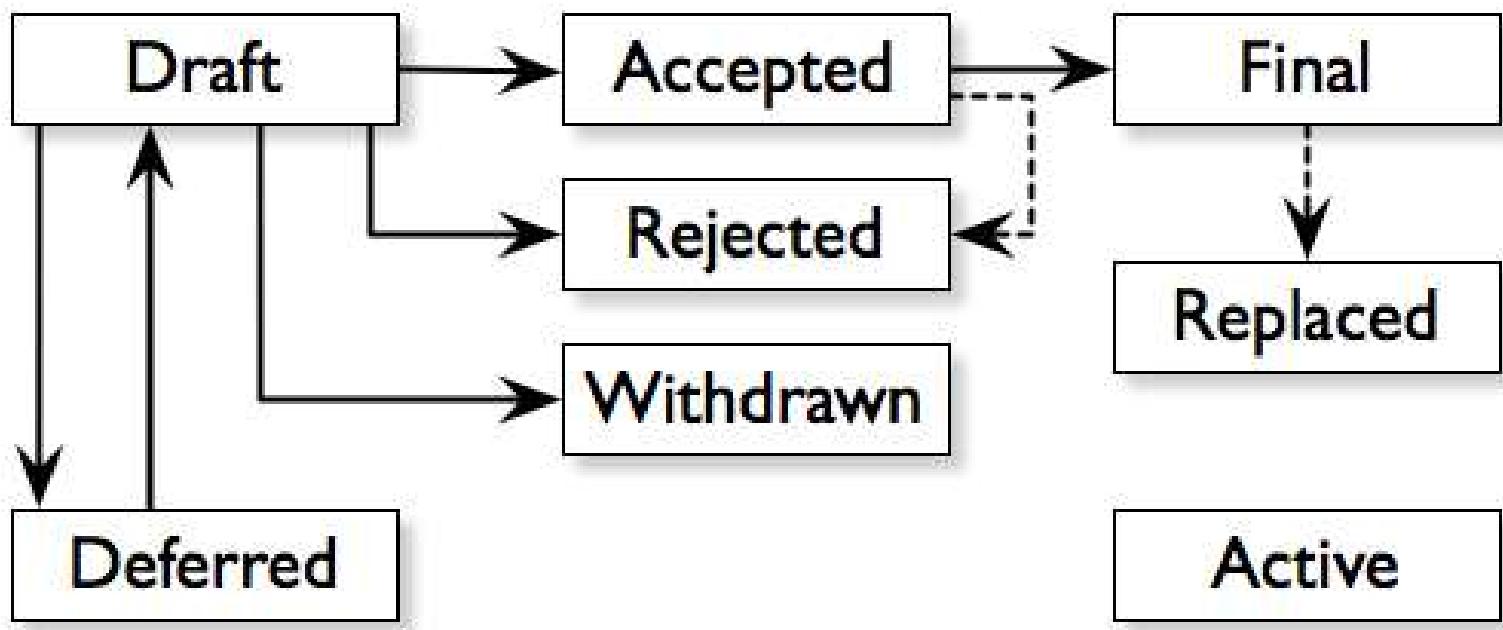
How Does a BIP Get Adopted (or Rejected)?

Every BIP **starts as a draft, submitted by one or several authors.** (Although, even before a BIP is a draft, it's typically discussed more informally on the **Bitcoin development mailing list, Internet Relay Chat (IRC) channels and/or other venues.**)

*Bitcoin
Improvement
Proposals*

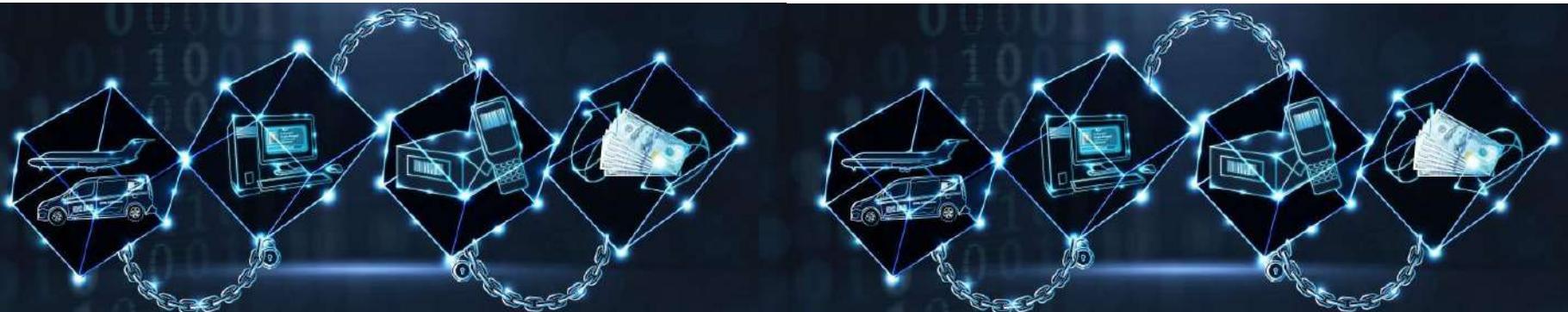
How Does a BIP Get Adopted (or Rejected)?

Picture below is the BIP process as taken from BIP 0001.



<https://github.com/bitcoin/bips>

Types of Blockchain



Public

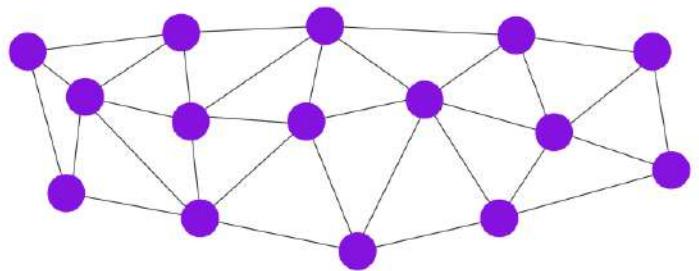
Private

Hybrid

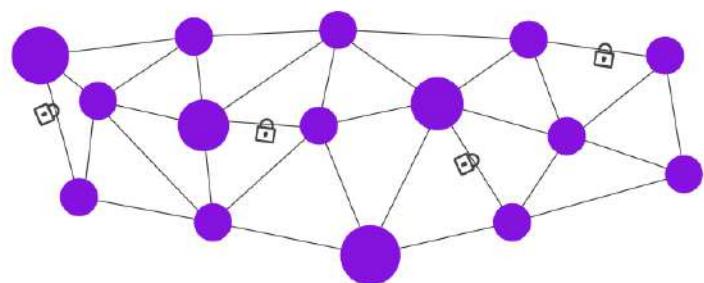
Types of Blockchain

Consortium

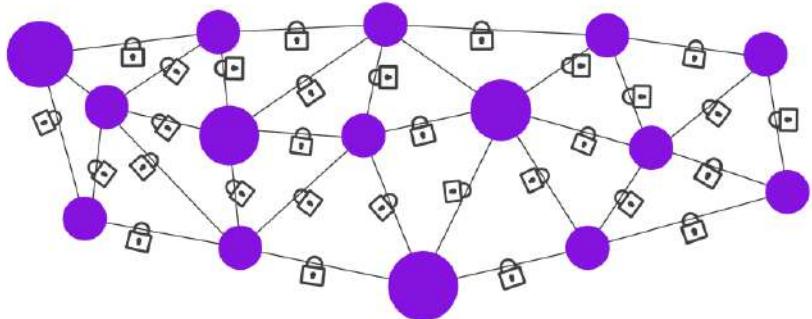




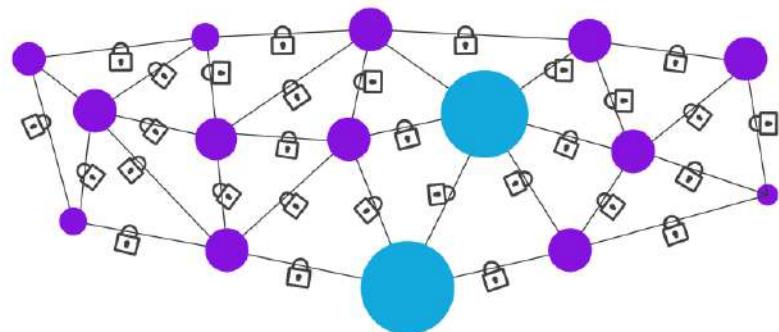
Public Blockchain



Semi Private Blockchain



Private Blockchain



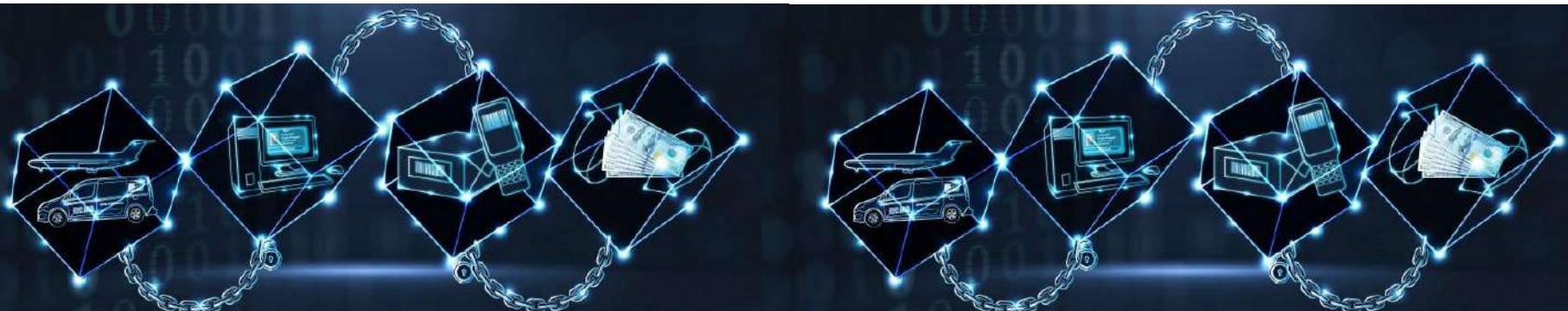
Consortium Blockchain





Public blockchains

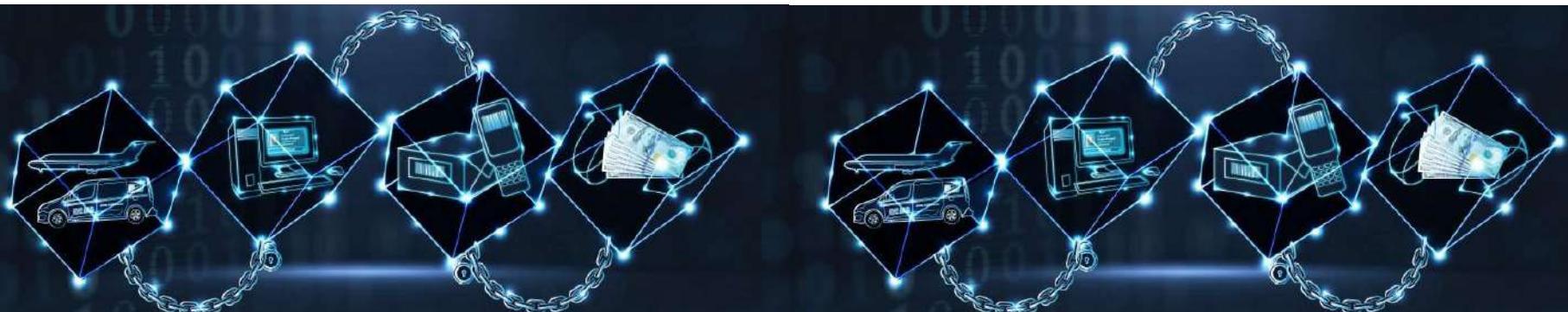
As the name suggests, public blockchains are not owned by anyone. They are open to the public, and anyone can participate as a node in the decision-making process. Users may or may not be rewarded for their participation. All users of these *permissionless* or *unpermissioned* ledgers maintain a copy of the ledger on their local nodes and use a distributed consensus mechanism to decide the eventual state of the ledger. Bitcoin and Ethereum are both considered public blockchains.





Private blockchains

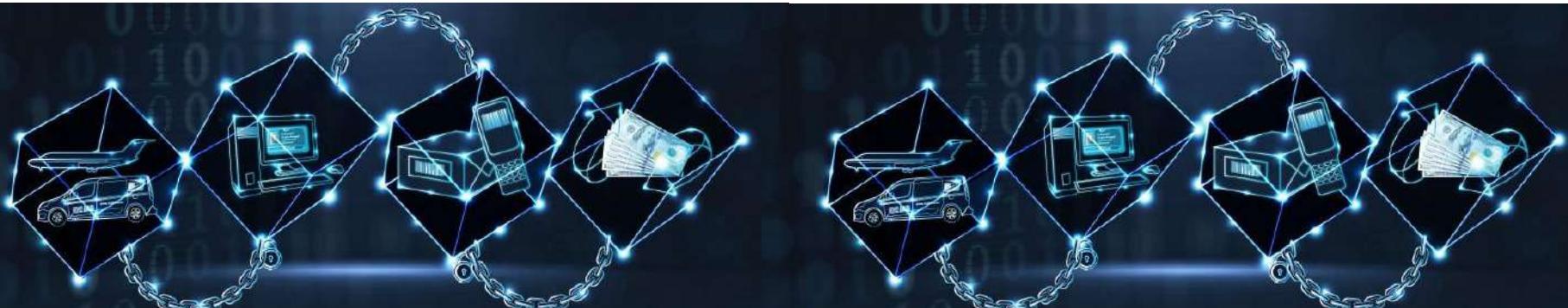
As the name implies, private blockchains are just that—private. That is, they are open only to a consortium or group of individuals or organizations who have decided to share the ledger among themselves. There are various blockchains now available in this category, such as HydraChain and Quorum. Optionally, both of these blockchains can also run in public mode if required, but their primary purpose is to provide a private blockchain.

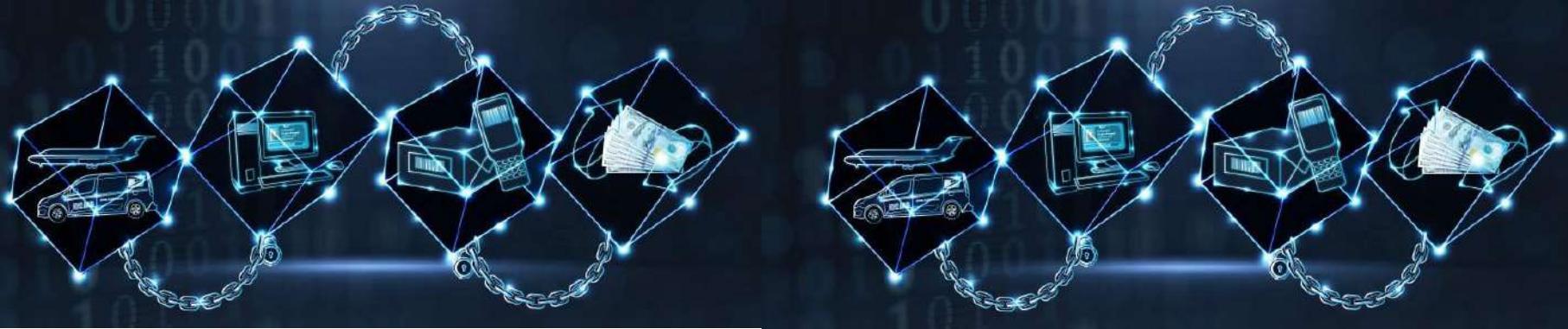




Semiprivate blockchains

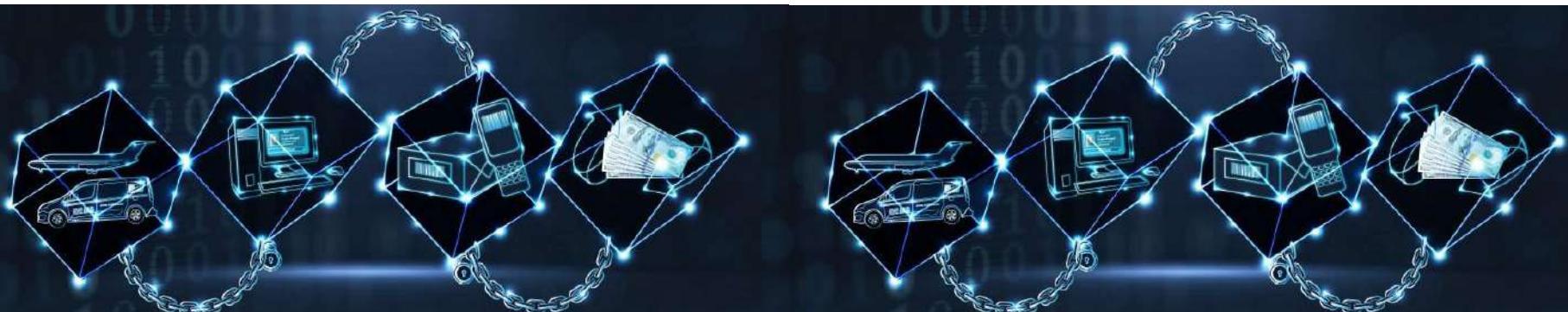
With *semiprivate blockchains*, part of the blockchain is private and part of it is public. Note that this is still just a concept today, and no real world POCs have yet been developed. With a semi-private blockchain, the private part is controlled by a group of individuals, while the public part is open for participation by anyone.





Sidechains

More precisely known as *pegged sidechains*, this is a concept whereby coins can be moved from one blockchain to another and moved back again. Typical uses include the creation of new *altcoins* (alternative cryptocurrencies) whereby coins are burnt as a proof of an adequate stake. *Burnt* or *burning the coins* in this context means that the coins are sent to an address which is unspendable and this process makes the *burnt* coins irrecoverable. This mechanism is used to bootstrap a new currency or introduce scarcity which results in increased value of the coin.

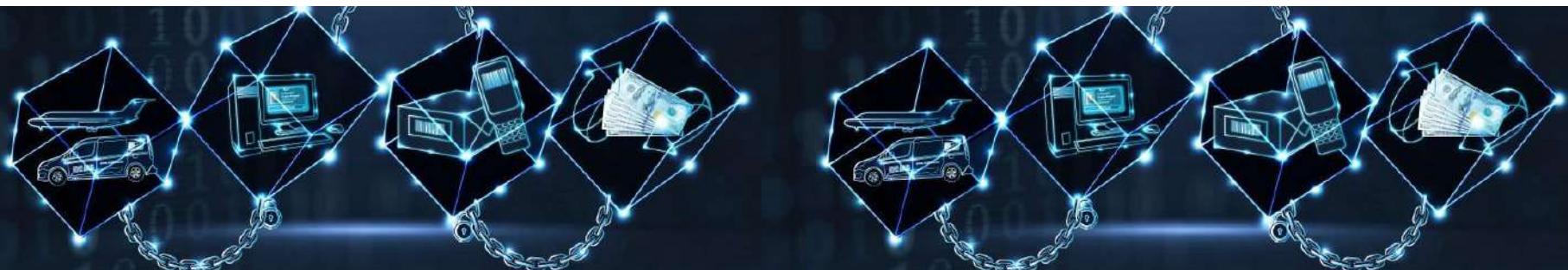




Fully private and proprietary blockchains

There is no mainstream application of these types of blockchains, as they deviate from the core concept of decentralization in blockchain technology. Nonetheless, in specific private settings within an organization, there could be a need to share data and provide some level of guarantee of the authenticity of the data.

An example of this type of blockchain might be to allow for collaboration and the sharing data between various government departments. In that case, no complex consensus mechanism is required, apart from simple state machine replication and an agreement protocol with known central validators. Even in private blockchains, tokens are not really required, but they can be used as means of transferring value or representing some real-world asset.

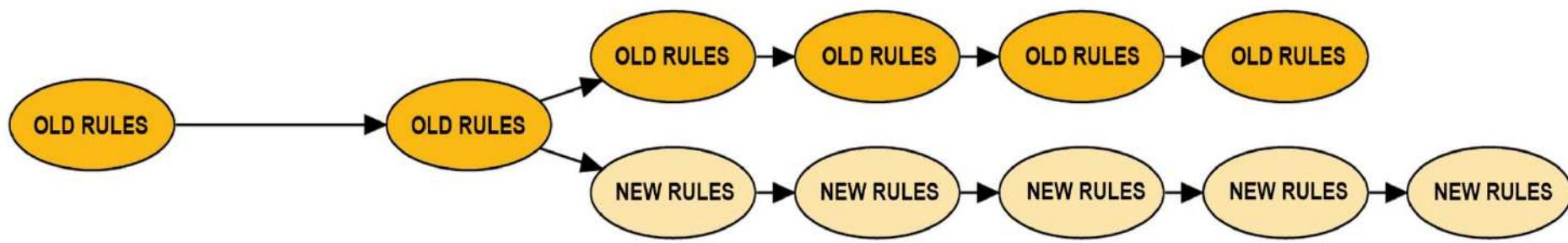


BITCOIN FORK



THE BITCOIN FORK

A BLOCKCHAIN FORK



THE BITCOIN FORK

Blockchain is a DECENTRALIZED DATA STRUCTURE, different copies of it are not always consistent

Blocks may ARRIVE at DIFFERENT NODES at different times, causing nodes to have different perspectives of the blockchain

THE BITCOIN FORK

To resolve this, each node always **SELECTS** and **ATTEMPTS** to extend the chain of blocks that represents the most Proof-of-Work, also known as the **LONGEST CHAIN** or greatest cumulative difficulty chain



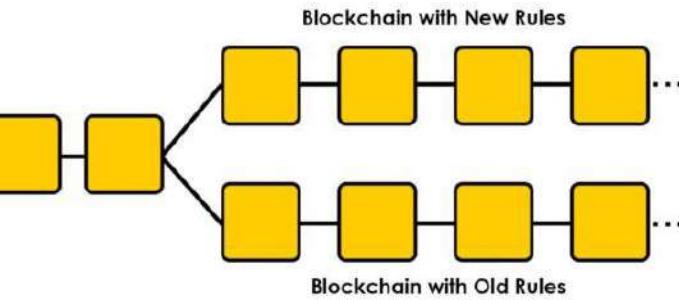
THE BITCOIN FORK

LONGEST CHAIN RULE

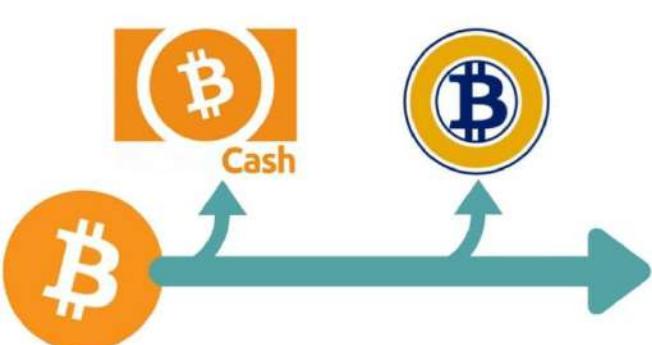
By **SUMMING** the **DIFFICULTY RECORDED** in each block in a chain, a node can calculate the **TOTAL AMOUNT** of **Proof-of-Work** that has been expended to create that chain

THE BITCOIN FORK

Next few diagrams, progress of a “**FORK**” event across the network is seen

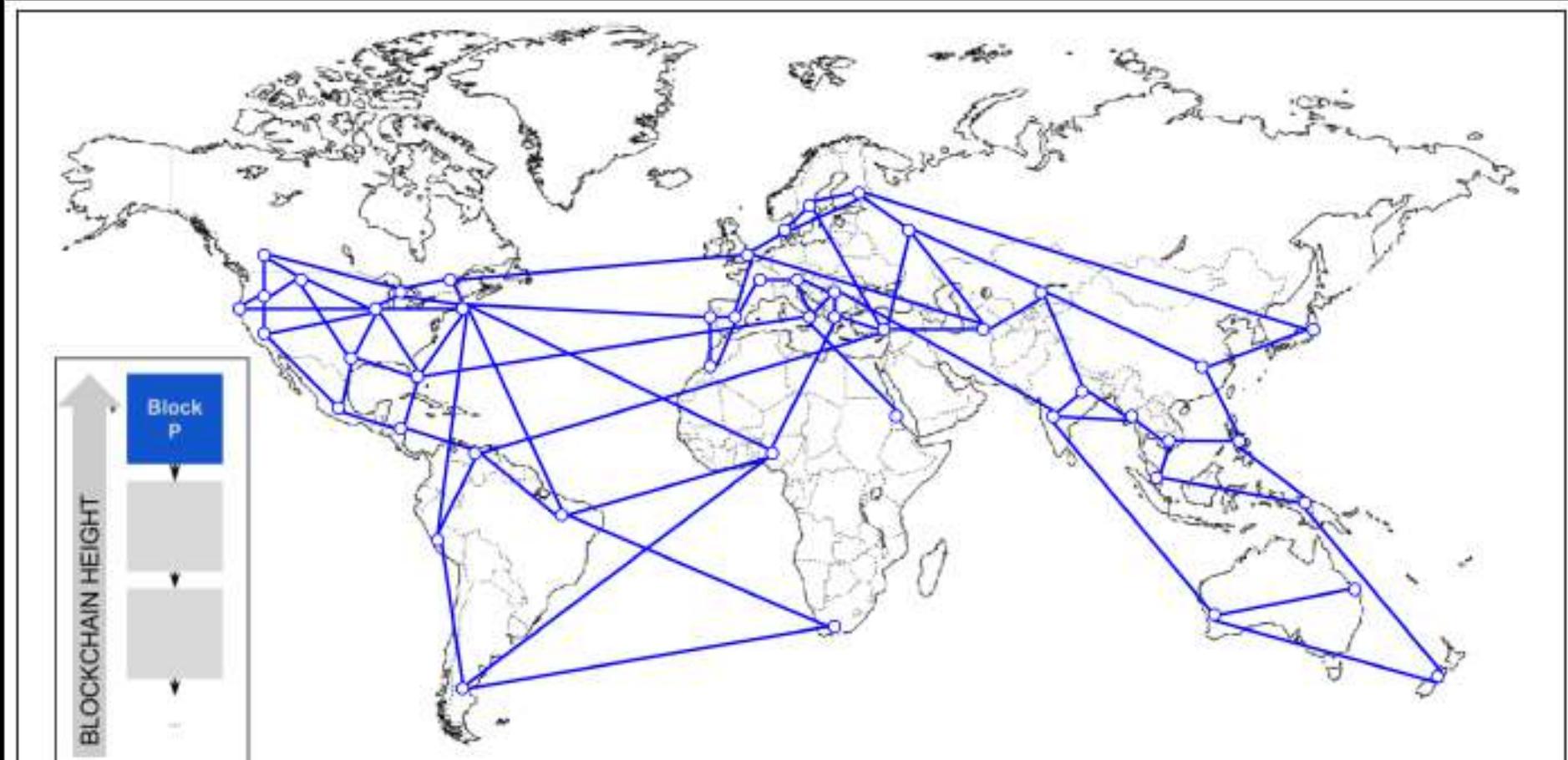


The figures are **SIMPLIFIED REPRESENTATION** of Bitcoin global network



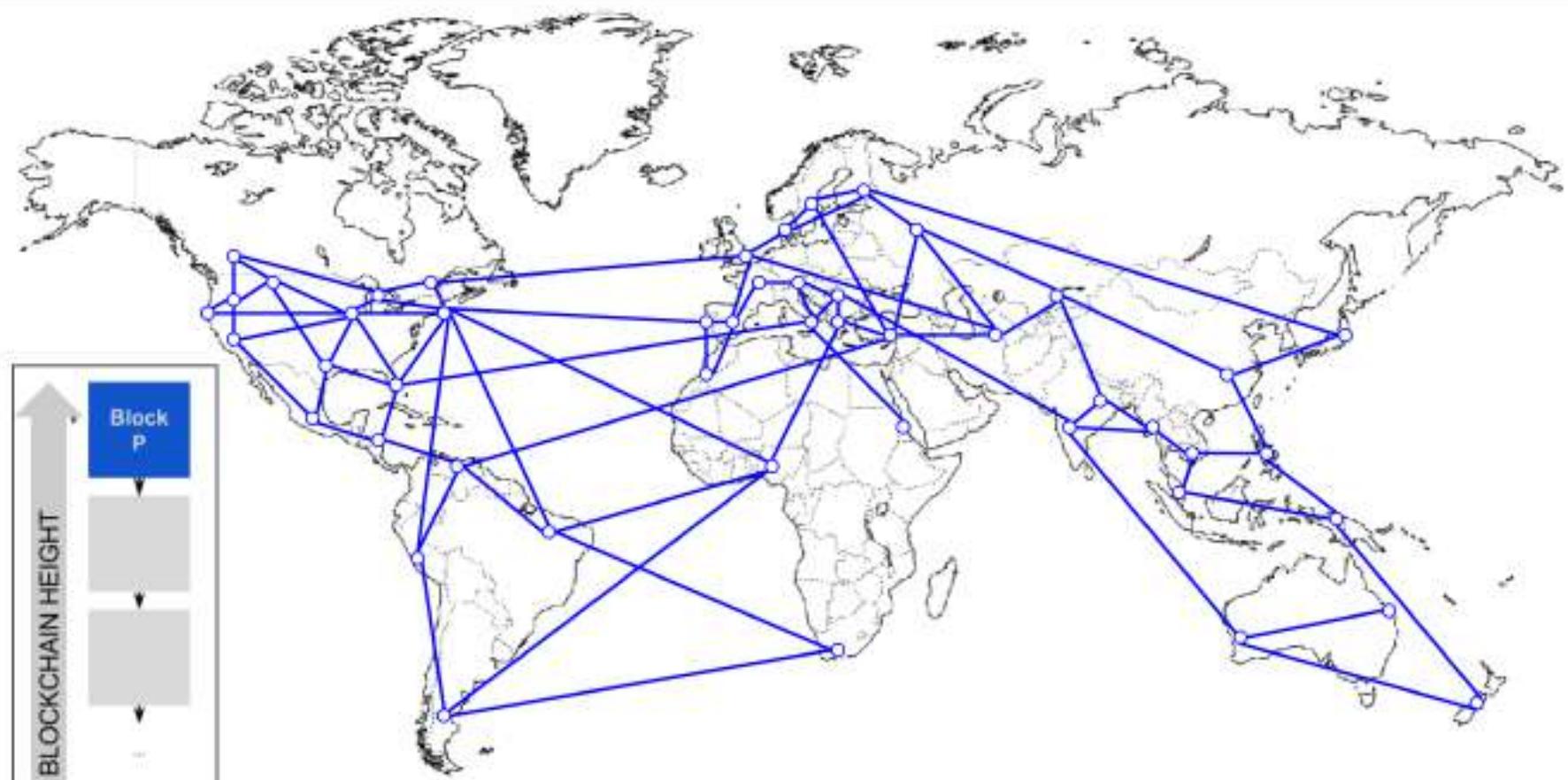
In reality, the Bitcoin network's topology is not organized geographically

THE BITCOIN FORK



For illustration purposes, different blocks are shown as different colors, spreading across the network and coloring the connections they traverse

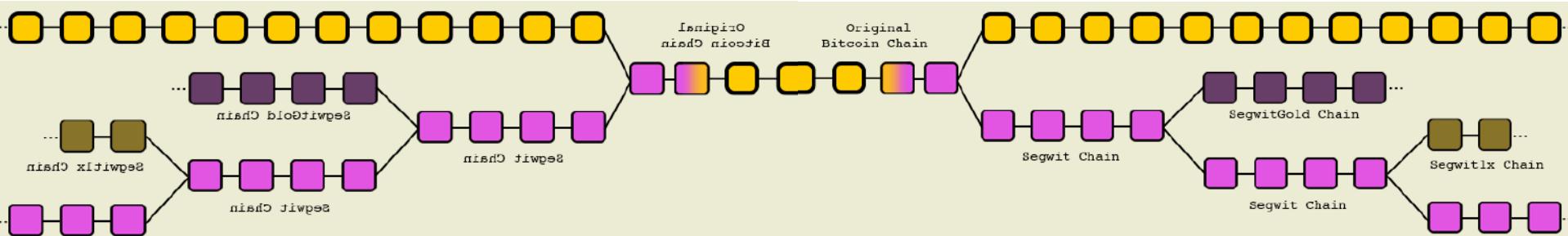
THE BITCOIN FORK



First figure shows that **NETWORK** has a unified perspective of the blockchain, with the **BLUE BLOCK** as the tip of the main chain.

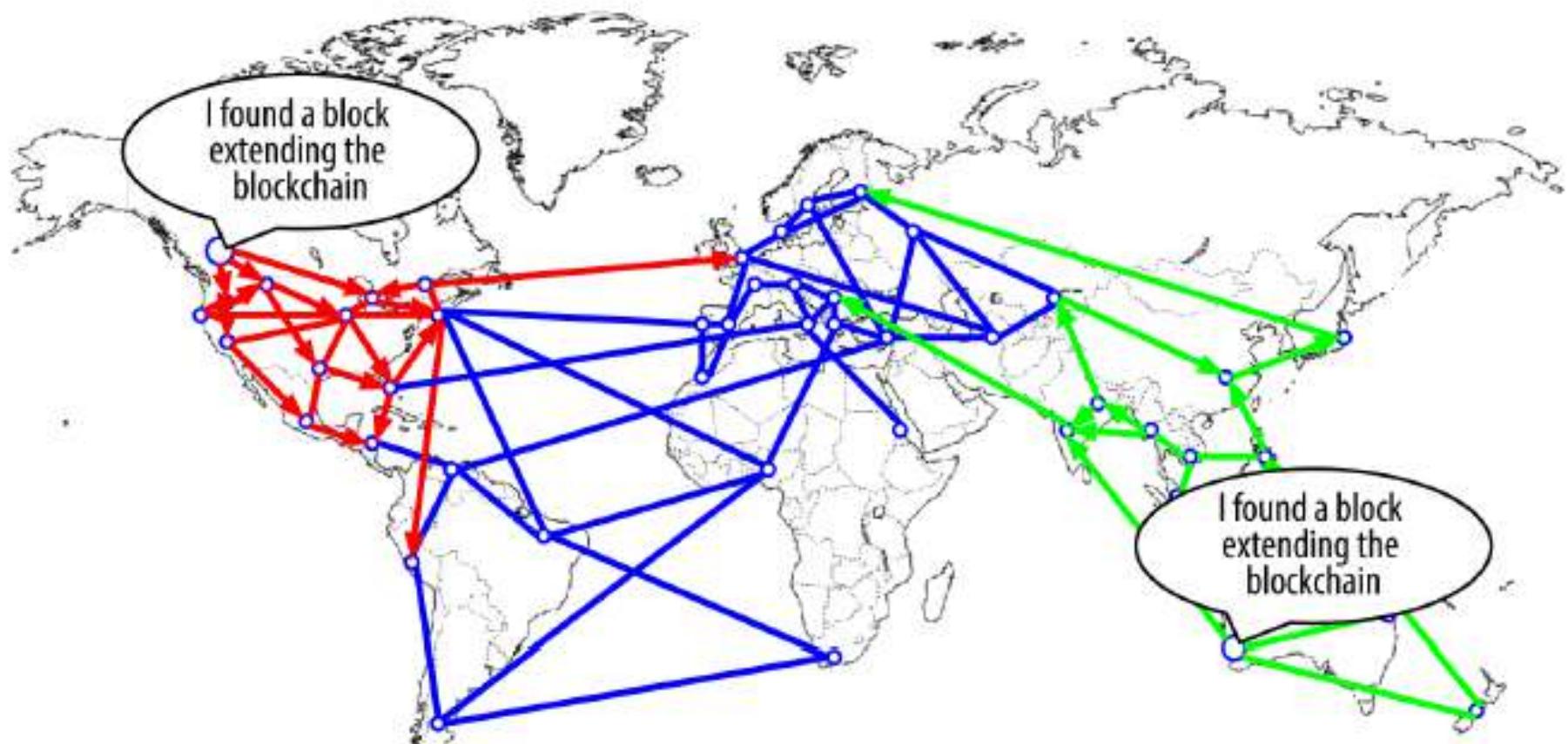
THE BITCOIN FORK

A Fork occurs **under normal conditions** wherein two miners solve the Proof-of-Work algorithm within a short period of time from each other`



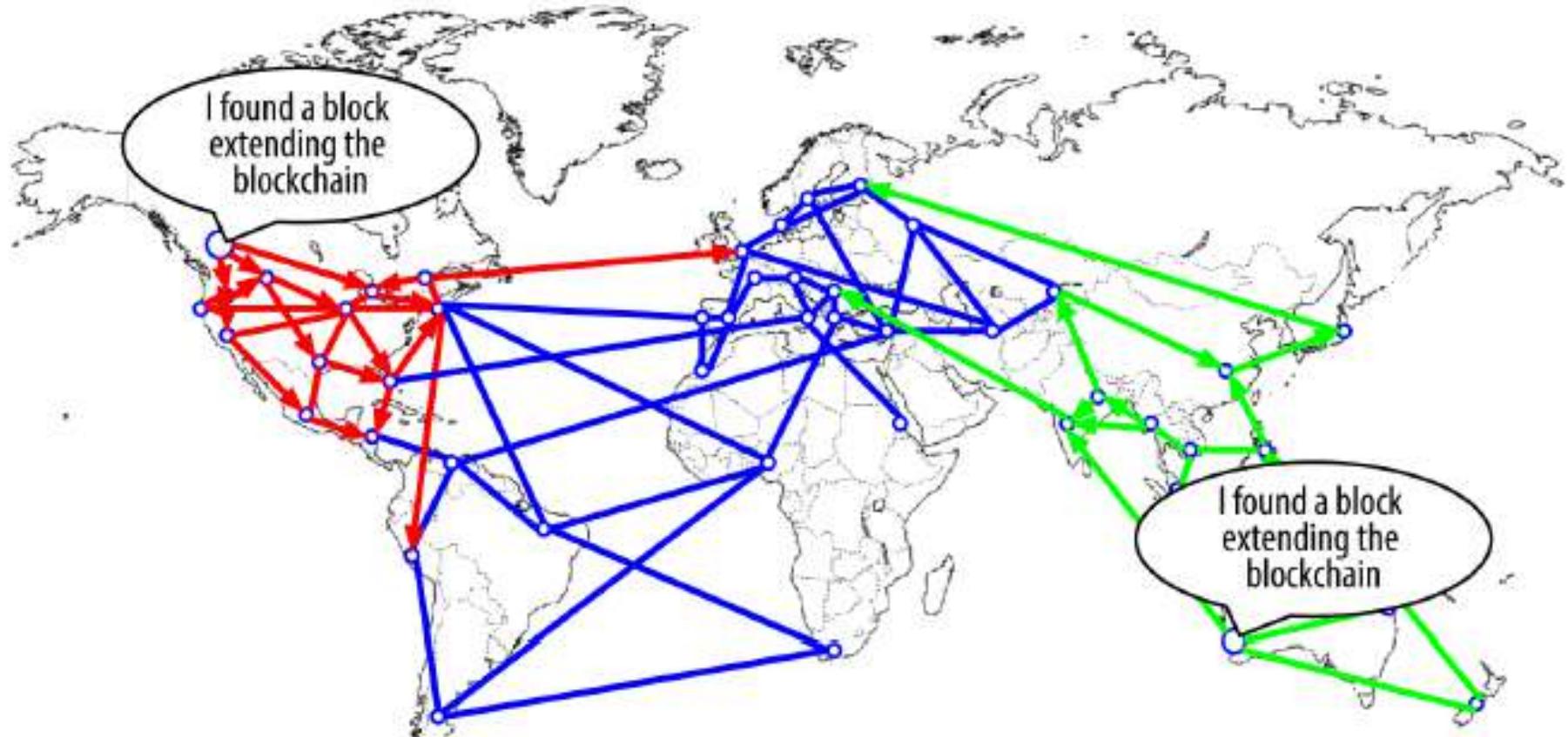
As both miners discover a solution for their respective candidate blocks, they immediately broadcast their own “**WINNING**” block to their immediate neighbors who begin propagating the block across the network

THE BITCOIN FORK



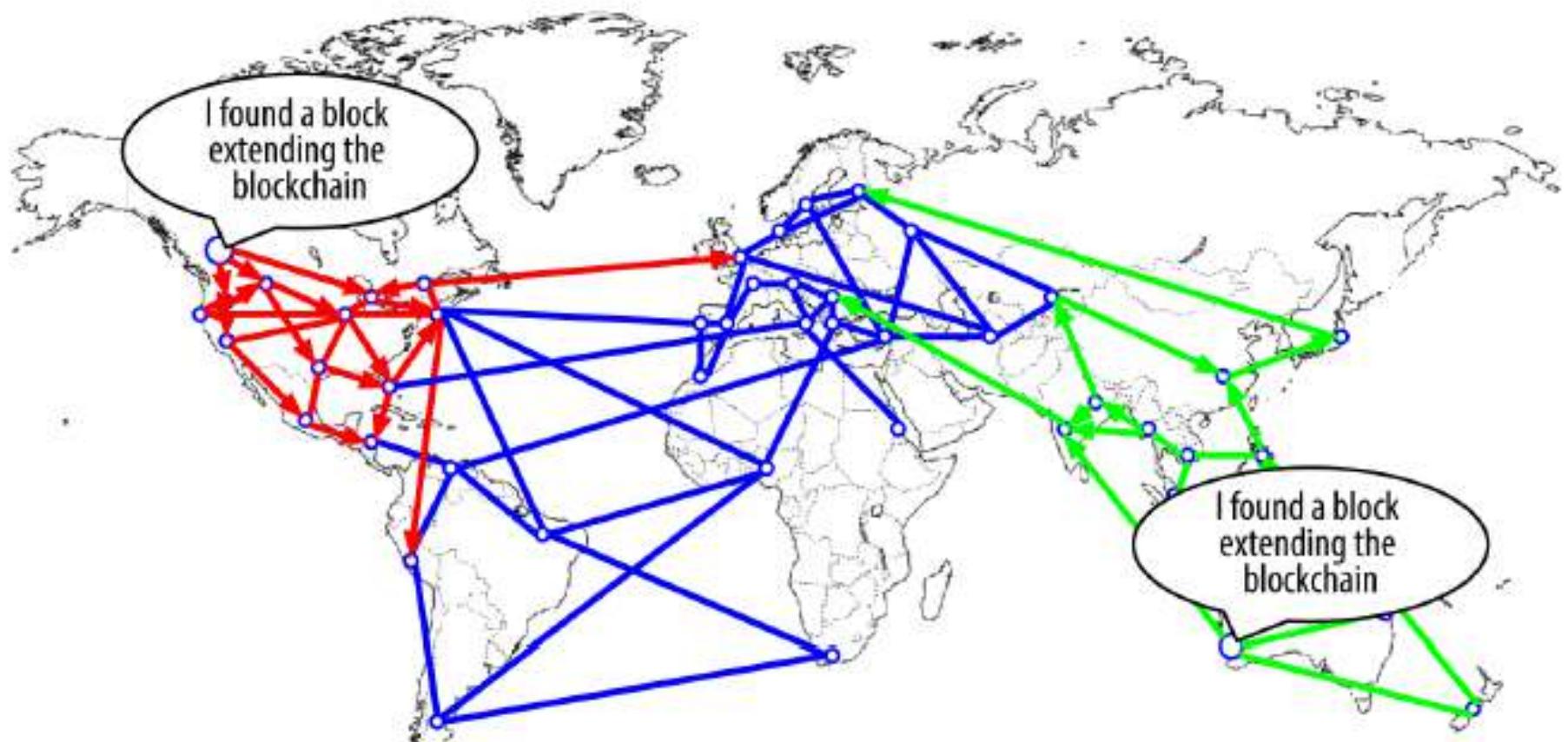
Two miners mine TWO DIFFERENT BLOCKS almost simultaneously & children of the BLUE BLOCK, and building on top of the blue block

THE BITCOIN FORK



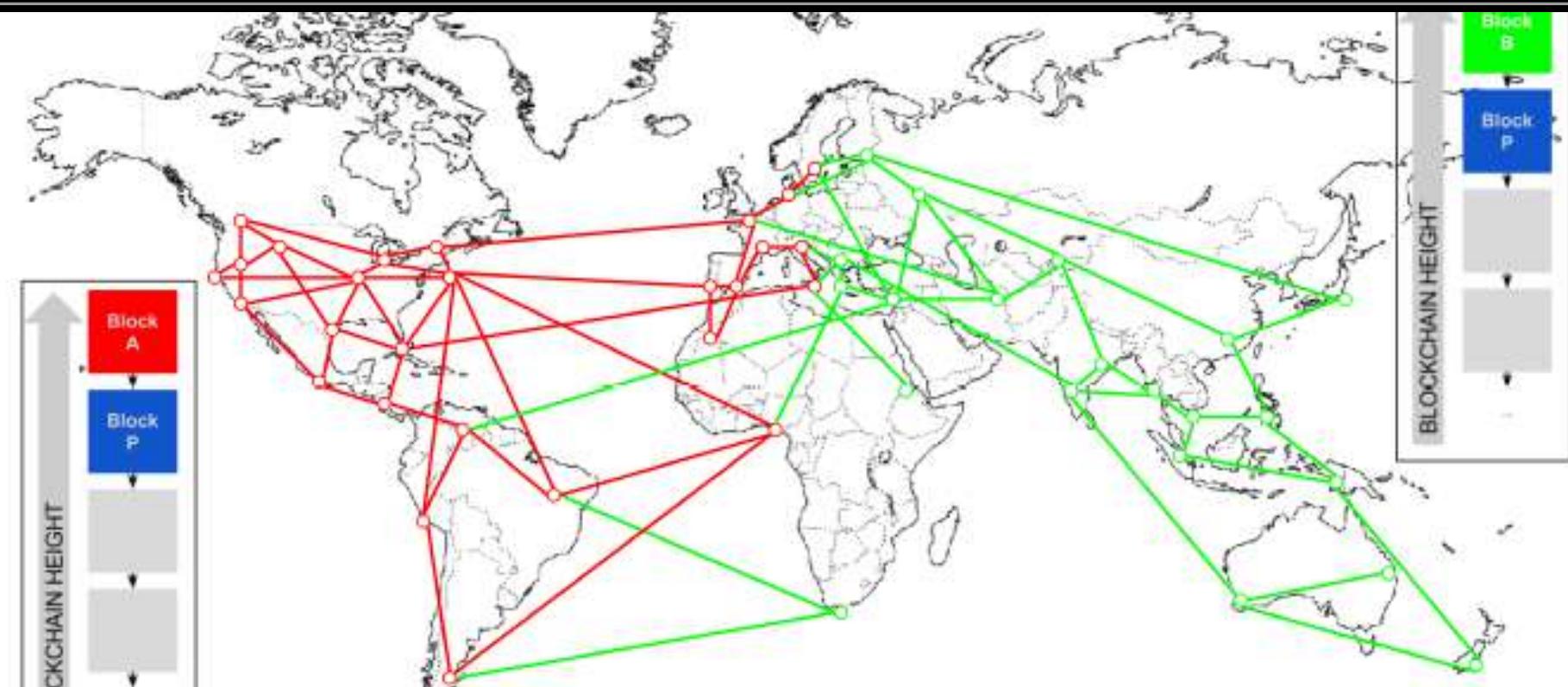
Both blocks are VALID, both blocks contain a VALID SOLUTION to the proof of work, blocks EXTEND THE SAME PARENT

THE BITCOIN FORK



Both blocks likely contain most of the same transactions, with only perhaps a few differences in the order of transactions

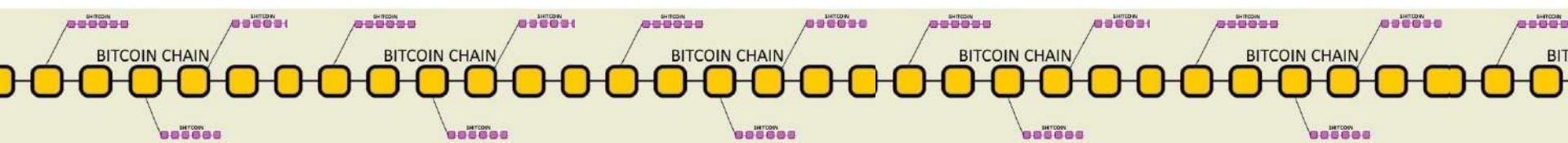
THE BITCOIN FORK



Both **BLOCKS PROPAGATE**, some nodes receive block "**RED**" & some receive block "**GREEN**" & network splits in two different perspectives

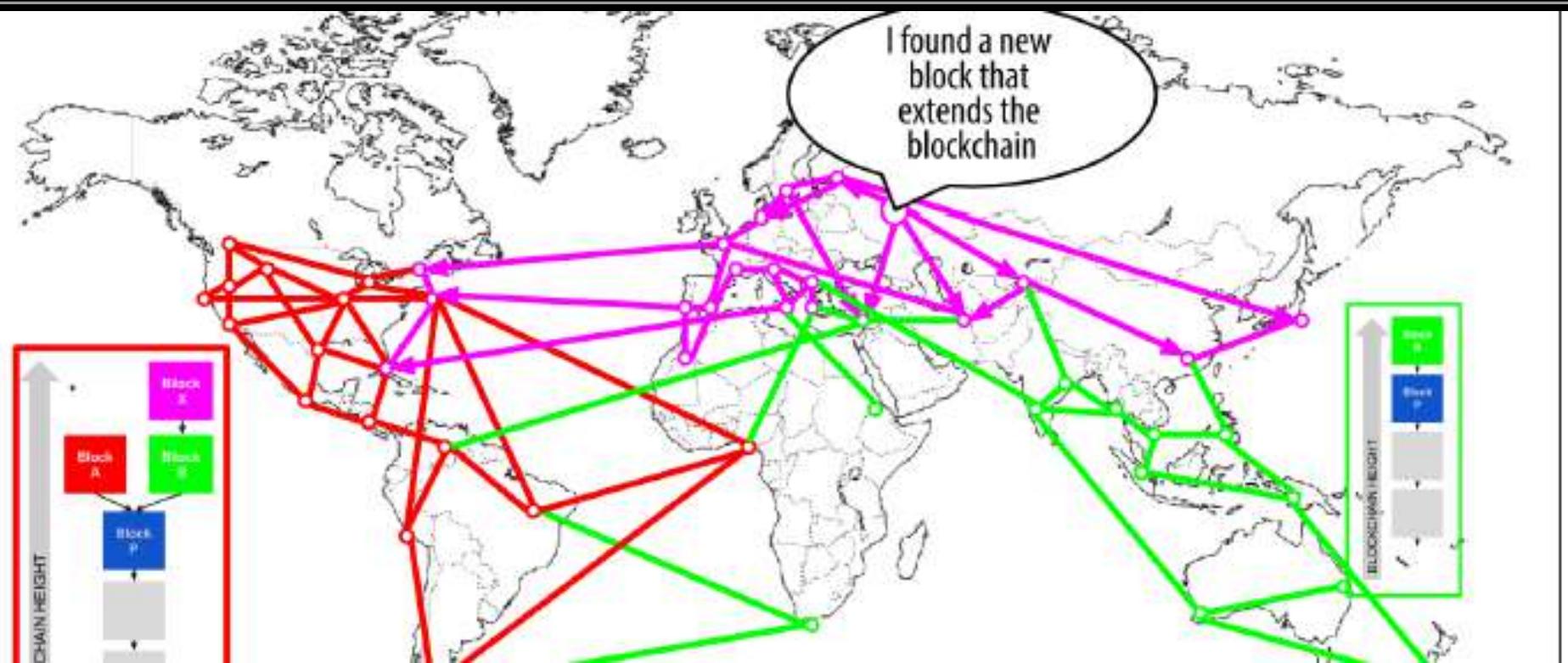
THE BITCOIN FORK

From this moment, the Bitcoin network nodes closest (**TOPOLOGICALLY, NOT GEOGRAPHICALLY**) to the Canadian node will hear about block “red” first and will create a new greatest-cumulative-difficulty blockchain with “red” as the last block in the chain (e.g. blue-red), ignoring the candidate block “green” that arrives a bit later



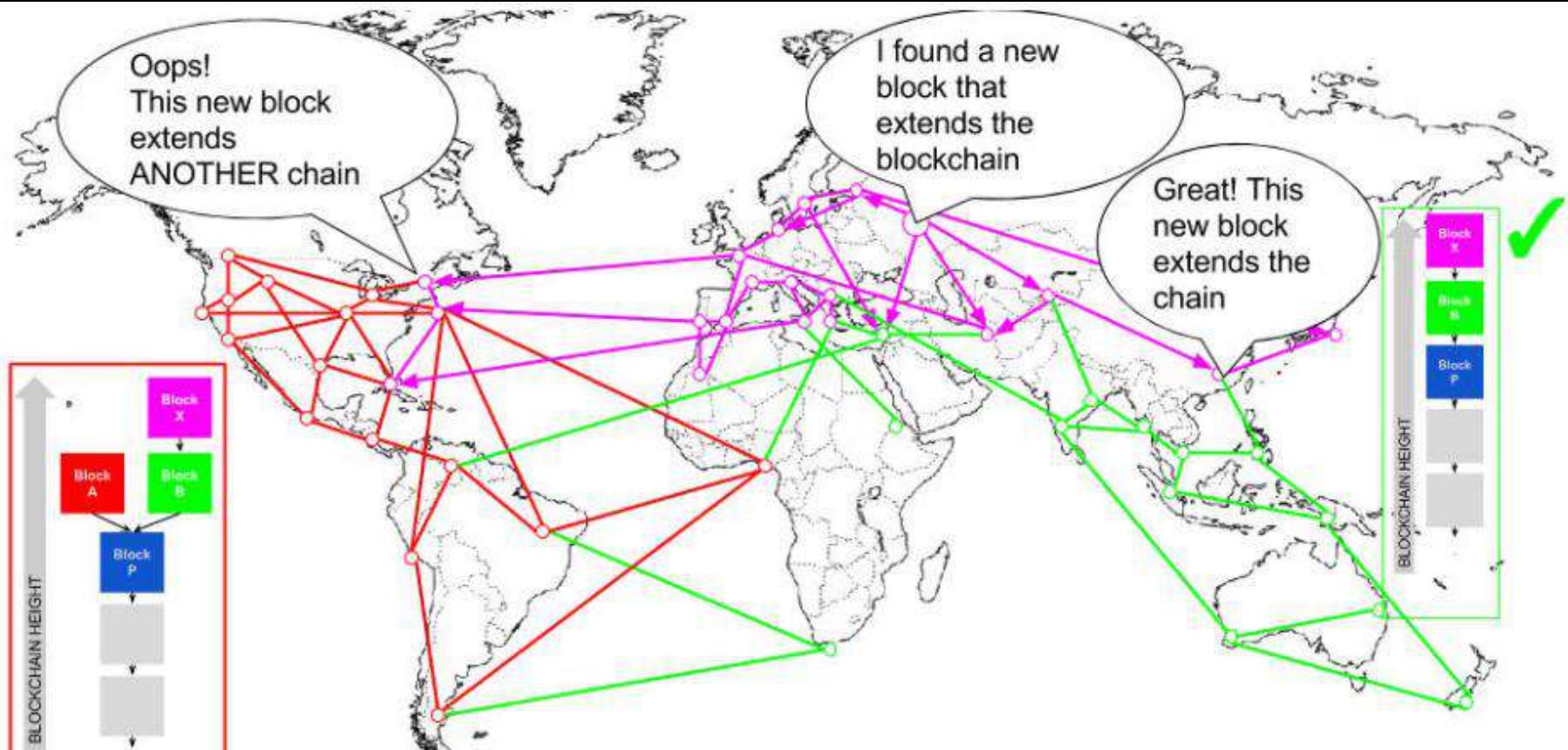
Node closer to the Australian node will take that block as the winner and extend the blockchain with “green” as the last block (e.g. blue-green), ignoring “red” when it arrives a few seconds later

THE BITCOIN FORK



Miners building on top of “GREEN” find a new block “PINK” that extends the chain and immediately propagate this new block and the entire network sees it as a valid solution.

THE BITCOIN FORK



Chain **BLUE-GREEN-PINK** is now longer
than the chain **BLUE-RED**



Incidents

Case Studies

Crypto Crimes and Fiascos

**An important link in all crypto crimes is
the access to wallet....let's first see
variety in CRYPTO WALLETS**



bitcoin *wallet*

SIGN UP FOR A BITCOIN WALLET



WALLET is basically
the **Bitcoin Equivalent**
of a **Bank account.**

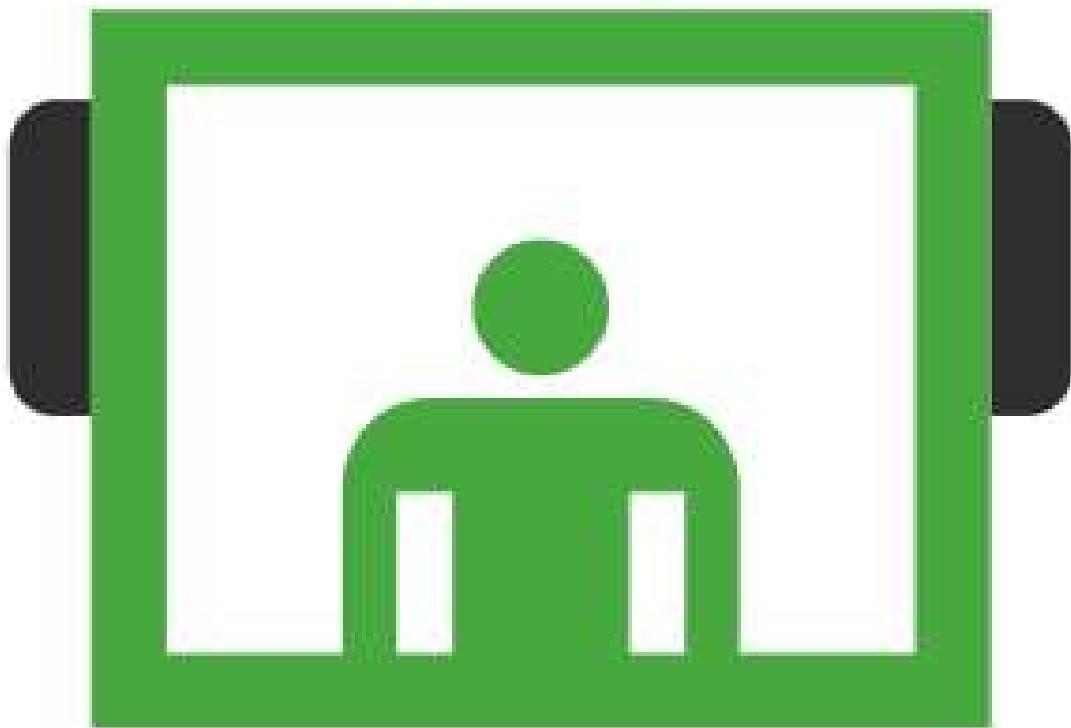


Allows to **RECEIVE** BITCOINS,
STORE(!!!!) them, and then
SEND them to others

airtel
money

!dea MONEY™

UNLIKE



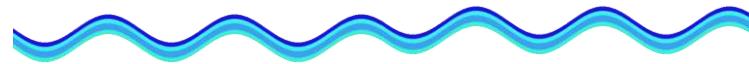
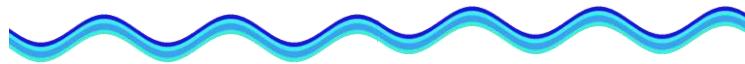
TY^{YES}

Cold Wallets & Hot Wallets

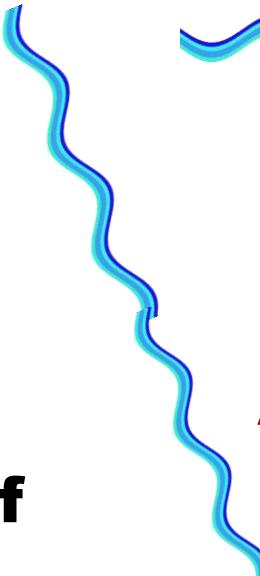


COLD implies it is **Offline** or **Disconnected** from the **Internet**

Connected to the **Internet** or is **online** is said to be **HOT**



Cold is considered most **Secure** & suitable for **Storing Large Amounts** of bitcoins



Hot is suitable for **Frequently Accessed** funds

Designed to be **downloaded**
& used on **Laptops/PCs**



Easy to Access.

Available for **Different OS**

– Windows, Mac OS and Ubuntu.



Windows



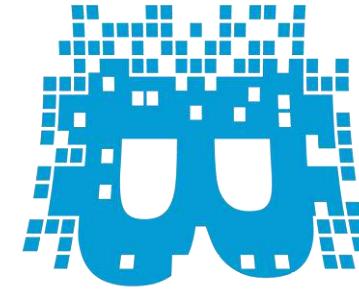
Mac OS X



Linux

Armory, Multibit, Msigna
and **Hive** to mention a FEW

MOBILE WALLETS



BLOCKCHAIN

ONLINE WEB WALLETS

coinbase

Coinbase is the world's most popular place to buy and sell bitcoin.



CIRCLE

bitcoin

PHYSICAL WALLETS

**Paper Wallets can
Securely hold your BITCOINS
in Cold Storage form for a
long time**



**Bitaddress.org
or Blockchain.info**

**Once they are generated, you
print them out on a piece of
paper**



BitcoinQt is the **First** ever built
bitcoin **CLIENT WALLET**



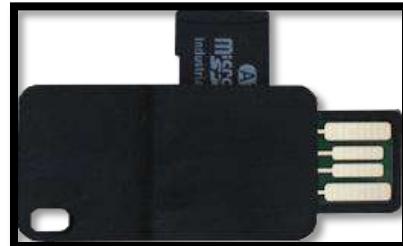
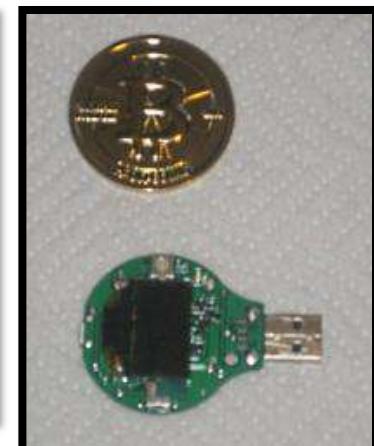
Original bitcoin
wallet used by the
Pioneers of the
currency

COMPUTERS installed with these wallets
FORM PART OF THE CORE
NETWORK & have **access to all**
transactions on the blockchain

BITCOIN
WALLETS
CLIENTS

HARDWARE WALLETS





BRAIN WALLET

A **brainwallet** refers to the concept of storing Bitcoins in one's own mind by memorizing a [seed phrase](#).

If the seed is not recorded anywhere, the Bitcoins can be thought of as being held only in the mind of the owner.

If a brainwallet is forgotten or the person dies or is permanently incapacitated, the Bitcoins are lost forever.

To create a brainwallet, use Bitcoin wallet software to generate a seed phrase and then memorize it. Such seeds are generated by wallets like [Electrum](#), [Armory](#) and [Mycelium](#).

Crypto exchange may have lost \$145 mn after CEO dies in India



Hong Kong, Feb 6 (IANS) The death of Canadian entrepreneur Gerald Cotten, died due to complications with Crohn's disease while travelling in India in December, has left a huge stash of cryptocurrencies locked off from the people who own them.

Quadriga, Canada's biggest cryptocurrency exchange, said it's unable to gain access to \$145 million of bitcoin and other digital assets after the death of Cotten, its 30-year old CEO and Co-Founder.

Many of the digital currencies held by Quadriga are stored offline in accounts known as "cold wallets," a way of protecting them from hackers. Cotten appears to have been the only person with access to the wallets, according to court documents cited by Canadian media and posted online by cryptocurrency news site CoinDesk, CNN reported.

The unusual case highlights the risks investors face looking after their assets in the thinly regulated industry.

Cotten's death has plunged Quadriga into crisis and left it struggling to figure out how to refund more than 100,000 of its users. The company filed for creditor protection in the Nova Scotia Supreme Court on Thursday.

"For the past weeks, we have worked extensively to address our liquidity issues, which include attempting to locate and secure our very significant cryptocurrency reserves held in cold wallets. Unfortunately, these efforts have not been successful," Quadriga said in a statement on its website.

PAPER WALLETS



choice



Choose your Bitcoin wallet

Find your wallet and start making payments with merchants and users.

Desktop

Hardware

Mobile

Web



ArcBit



Bitcoin
Knots



Bitcoin
Core



BitGo



Green
Address



mSIGNA



Armory



Bither



Electrum

FULL NODE CLIENT

LIGHT WEIGHT CLIENT

THIRD PARTY CLIENT



types



Windows



ANDROID



APPLE



Ubuntu



ORACLE



OS X



Linux



Xen



Debian | Gentoo | SUSE | Mandriva | Gentoo



VMWare



Red Hat



Fedora



CentOS



Debian



Sun



Mint



SUSE



Mageia



Arch Linux



Slackware



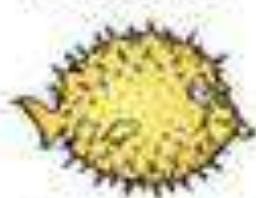
Mandriva



Gentoo



FreeBSD



OpenBSD



NetBSD



DragonFly BSD

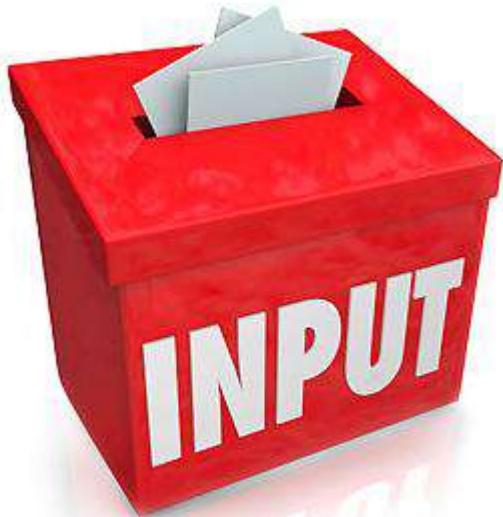


Darwin



GOOGLE CHROME OS

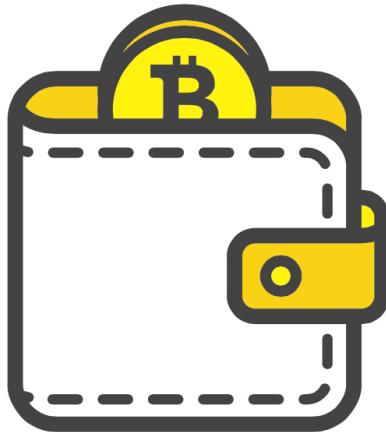
WHAT WALLETS



NUMBER

Transactions

A user for **CONDUCTING TRANSACTIONS** utilizing **BITCOIN**, he or she must first **DOWNLOAD** and setup a **BITCOIN WALLET**



BITCOIN WALLET can show the total **BALANCE** of all **BITCOINS** it **CONTROLS** and let **A USER PAY** a specified **AMOUNT**



Once wallet is **INSTALLED & CONFIGURED**, an **ADDRESS** is **GENERATED** which is **SIMILAR** to an **E-MAIL** or **PHYSICAL ADDRESS**

WALLET contains a **USER'S PRIVATE KEY**, which **ALLOWS FOR THE SPENDING** of the **BITCOINS**, which are located in the **BLOCK CHAIN**



A reward system, in the form of a website or app, that dispenses rewards in the form of a **satoshi, for visitors to claim in exchange for completing a **captcha or task as described by the website.****



TOP Bitcoin Faucets

SATOSHI : 1/100th of a Millionth BITCOIN

Why Is Recognizing Wallets Important?

For the investigator, recognizing wallets is essential to be able to investigate the movement of a suspect's funds within cryptocurrencies and potentially seize assets



The potential insecurities of each method of storage can also work into the hands of the investigator, enabling private keys to be found and seized and hence gain control of funds

MNEMONIC CODES

Private keys can also be in the form of a string of mnemonic code words often called a seed. Electrum wallet and the Trezor hardware key are examples

1 toe	7 little	13 globe	19 cousin
2 miss	8 wink	14 thank	20 vibrant
3 arrive	9 any	15 clump	21 hockey
4 bonus	10 knee	16 connect	22 wave
5 gallery	11 exhaust	17 second	23 fragile
6 fan	12 below	18 bicycle	24 cricket

MNEMONIC CODES

If you find such words, you can reverse the seed back into the private key by using the appropriate software tool by entering them into an online recovery engine, which will then provide the private key

BIP39 MNEMONIC WORDS

emotion

develop

win

pave

upgrade



allow junior

volcano

box

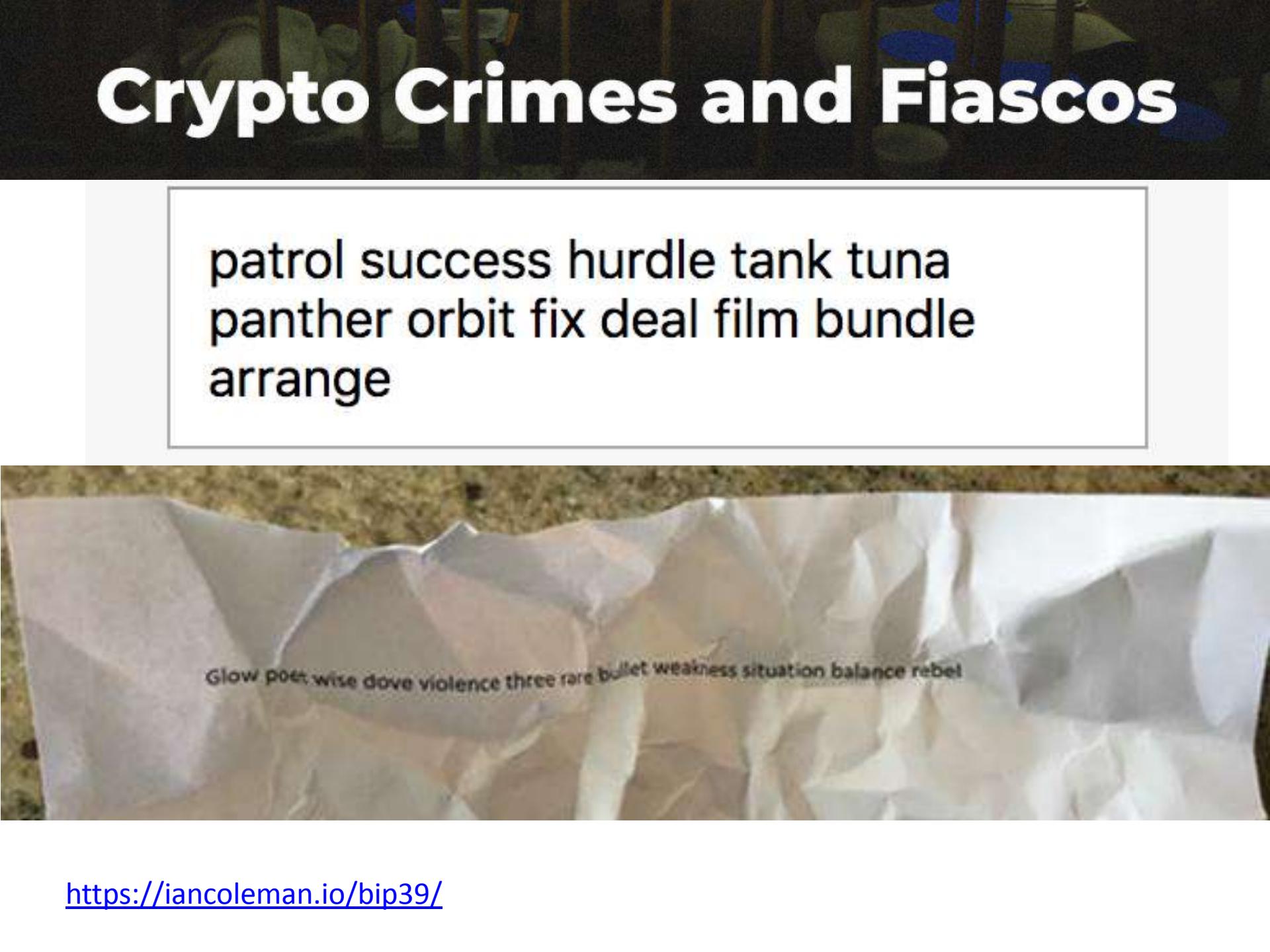
dirt

question

athlete

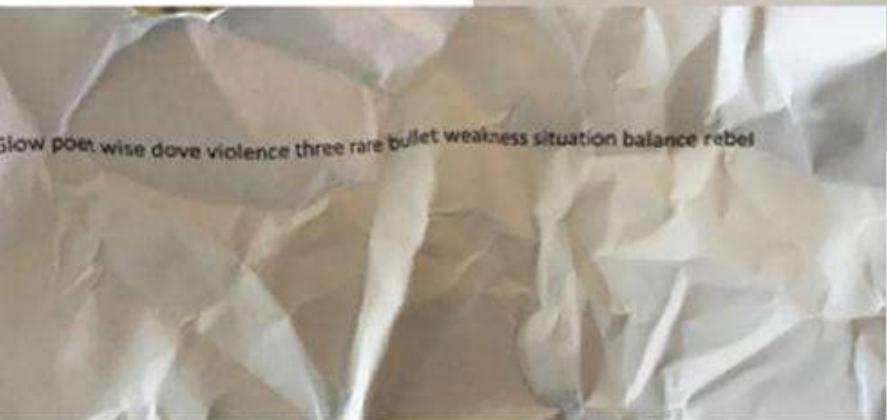
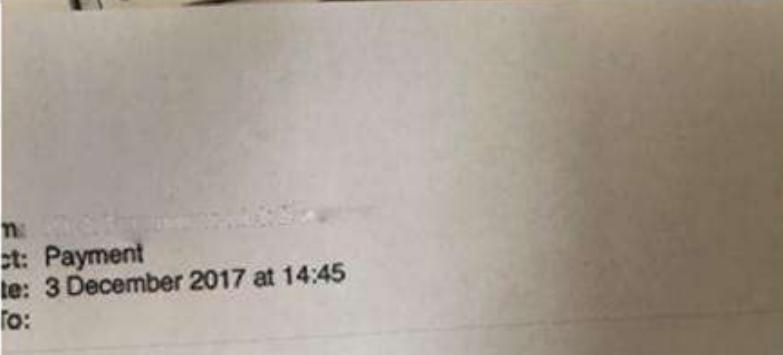
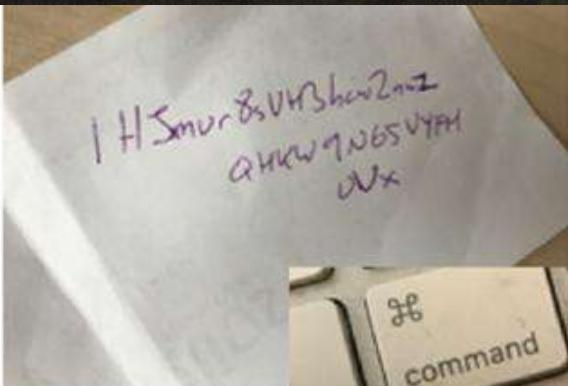
Crypto Crimes and Fiascos

patrol success hurdle tank tuna
panther orbit fix deal film bundle
arrange



Glow poet wise dove violence three rare bullet weakness situation balance rebel

Crypto Crimes and Fiascos



BTC:

1PZ5Ebvd43dvRRqR1gBhsy2Pwts14Cv

- Call John
- 1:30 Meeting

Crypto Crimes and Fiascos

BITCOIN ADDRESSES start with the character 1 or 3, are 34 characters long, and are formatted as Base58. For example:

1AM9ufiK76JwP6DzEGyB9ruddBxQhM1oeZE

ETHEREUM ADDRESSES start with 0x and are 42 characters long. For example:

0x78febmkmc377e2ee0b997c72b76d12c4aa2ce9be

Crypto Crimes and Fiascos

Ethereum **PRIVATE KEYS** are 64 characters long. For example:

**Aba7e63318ebe4450911b62d5e79139310ad3554533
8bb89fcb7183365cc3375**

Ethereum **PUBLIC KEYS** are 42 characters long and start with 0x. For example:

0x310B065125DDBACeB4822CA5e4F130025F8c9f07

Extracting the Wallet File

If possible, it's best to try to find and recover the wallet file

The wallet contains everything you need to investigate Bitcoin usage, private keys, and addresses, records of transactions, and other metadata

**CRYPTOCURRENCY
WALLET**



If you can get a wallet from a suspect's computer, it's time to celebrate!

Extracting the Wallet File

Bitcoin Core

Windows XP

C:\Documents and Settings\<username>\ Applicationdata\ Bitcoin

Windows Vista through Windows 10

C:\Users\<username>\Appdata\Roaming\Bitcoin

Linux

~/.bitcoin/

Mac

~/Library/Application Support/Bitcoin

Extracting the Wallet File

Litecoin

Linux

/home/<username>/.litecoin.conf

Mac

/Users//<username>/Library/Application Support/litecoin.conf

Windows XP

c:\Documents and Settings\<username>\Application
Data\Litecoin\litecoin.conf

Windows Vista through Windows 10

c:\Users\<username>\AppData\Roaming\Litecoin\litecoin.conf

Armory

%appdata%\Armory (.wallet)

Bitcoin Unlimited/Classic/XT/Core

%appdata%\Bitcoin (wallet.dat)

Extracting the Wallet File

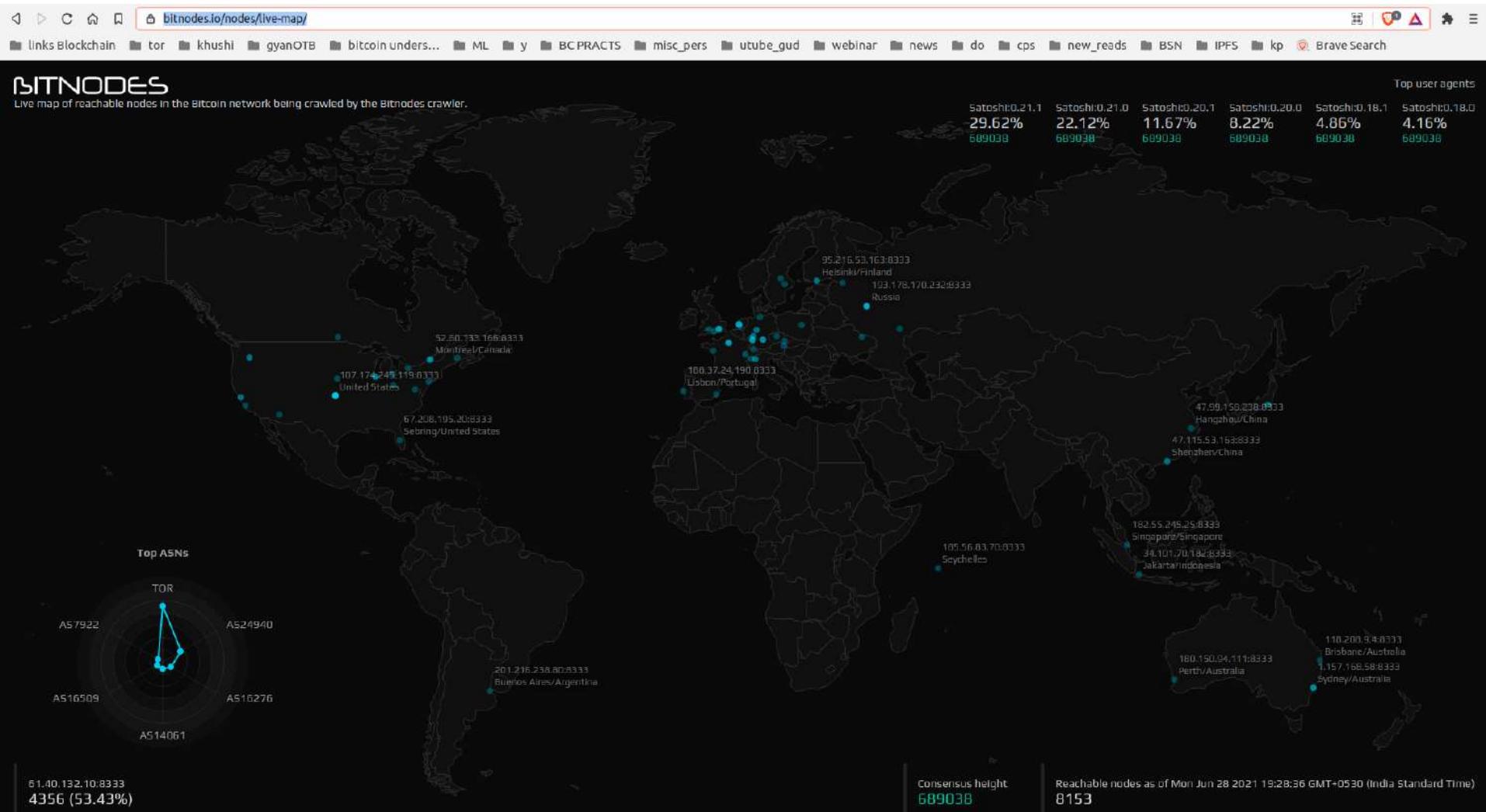
One method is to search for a “magic number” that always exists inside the `wallet.dat` file

Magic number (4 bytes) is an identifier for the Blockchain network. It has a constant value of `0xD9B4BEF9` and indicates a) Start of the block

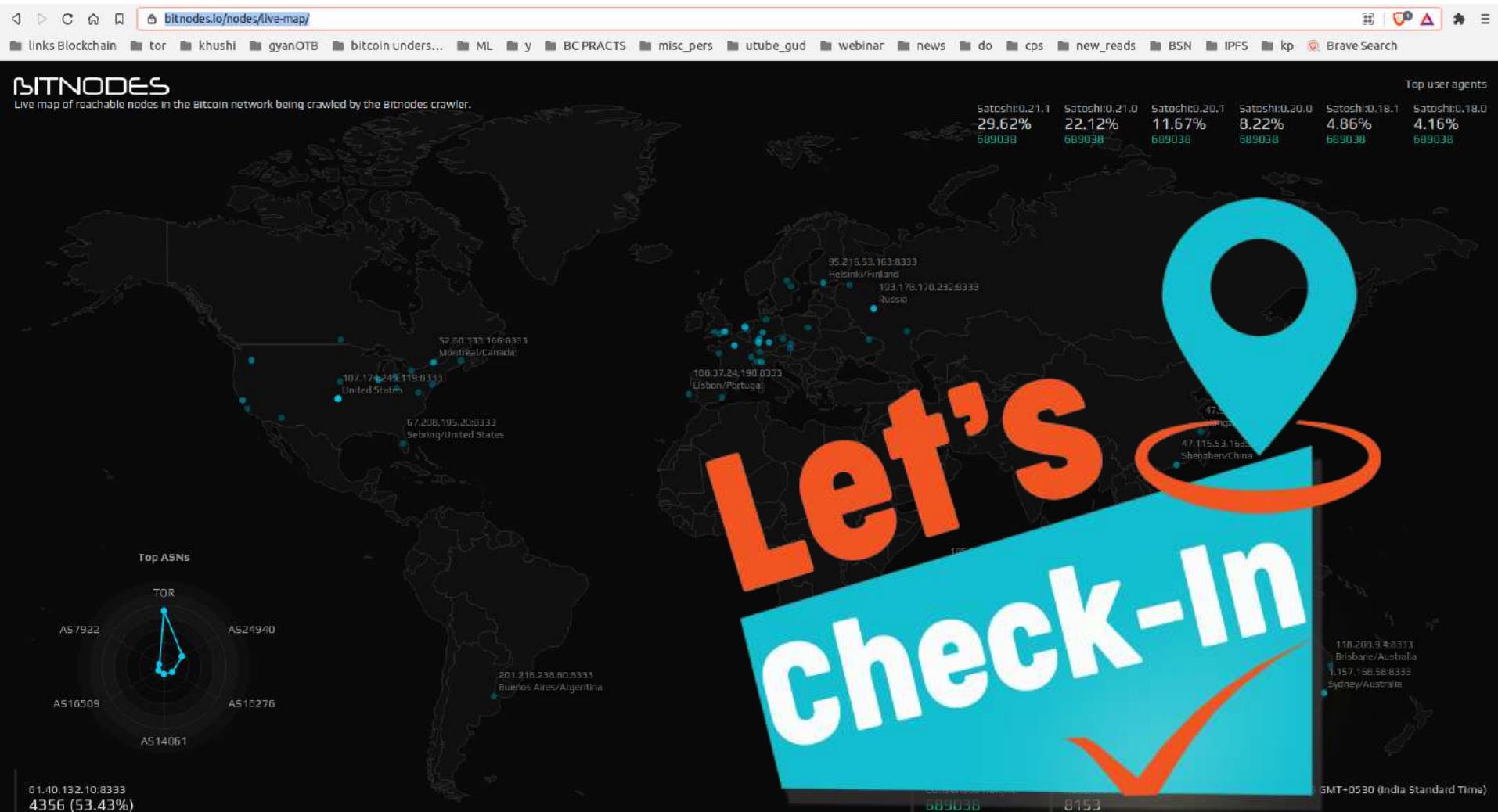
Live Nodes: BITCOIN

<https://bitnodes.io/nodes/live-map/>

Live Nodes: BITCOIN

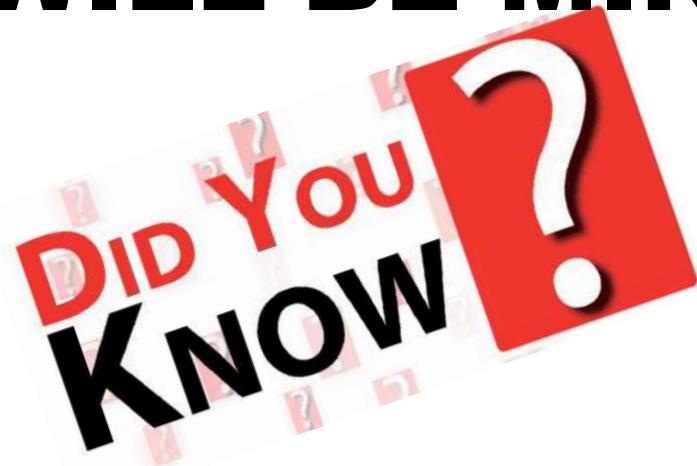


Live Nodes: BITCOIN



<https://bitnodes.io/nodes/live-map/>

THE LAST BITCOIN (PROBABLY 21 MILLIONTH COIN) WILL BE MINED IN THE YEAR



2140



21 million

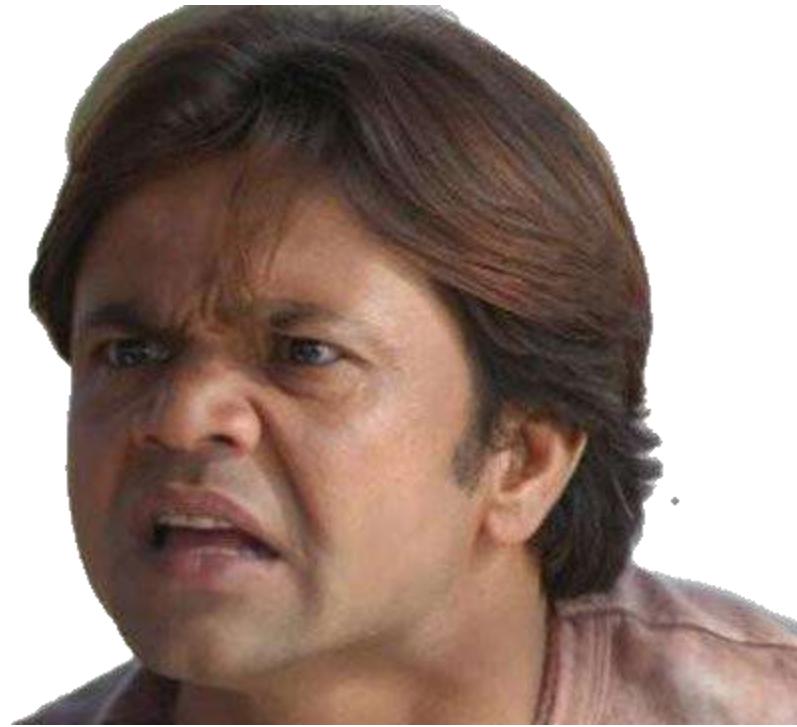
Do you own any coins in any CRYPTOEXCHANGE ?

सर, मेरे पास भी कुछ
bitcoin/ethereum हैं, फिर
कहाँ हैं **PRIVATE KEYS/ PUBLIC
KEYS/ HASHES** and all **NONCES**
जो आपने बताये, मुझे तो इसमें
से किसी की ज़रूरत नहीं पड़ी?



Do you own any coins in any CRYPTOEXCHANGE ?

सर, मेरे पास भी कुछ
bitcoin/ethereum हैं, फिर
कहाँ हैं **PRIVATE KEYS/ PUBLIC
KEYS/ HASHES** and all **NONCES**
जो आपने बताये, मुझे तो इसमें
से किसी की ज़रूरत नहीं पड़ी?



**" If you store your crypto on an exchange, you don't have a private key
then the EXCHANGE OWNS THE PRIVATE KEY AND THE COINS. What you
own is a PROMISE FROM THE EXCHANGE that they will give you your
coins when you ask for them, exactly the same as you have for "real"
money in a "real" bank. As long as you don't own your own private keys,
you don't own your coins. You are merely allowed access to them on
someone else's conditions.**

EXCHANGE HACKS

Crypto Crimes and Fiascos

Business News › Markets › Cryptocurrency › S.Africa crypto exchange brothers disappear after \$3.6 bn vanishes from platform, lawyers say

S.Africa crypto exchange brothers disappear after \$3.6 bn vanishes from platform, lawyers say

Reuters • Last Updated: Jun 27, 2021, 12:38 PM IST

SHARE  FONT SIZE  SAVE  PRINT 

JOHANNESBURG, June 25 (Reuters) - Lawyers for investors in a cryptocurrency exchange in South Africa, which told clients in April their accounts had been hacked, say \$3.6 billion has disappeared from the platform and that the two brothers who ran it cannot be traced.

If confirmed, Africrypt's losses would rank among the biggest crypto losses yet. For the whole of 2020, losses in the crypto sector through fraud and other crime were \$1.9 billion, down from a record of \$4.5 billion in 2019, according to crypto intelligence company CipherTrace. [read more](#)

Source: <https://www.reuters.com/technology/safrica-crypto-exchange-brothers-disappear-after-client-cash-vanishes-lawyers-2021-06-25/>

Crypto Crimes and Fiascos

Cryptocurrency exchange Liquid confirms hack

Zack Whittaker @zackwhittaker / 8:01 PM GMT+5:30 • November 18, 2020

 Comment

Cryptocurrency exchange Liquid has confirmed it was hacked, but that the scope of the incident is still under investigation.

The company's chief executive Mike Kayamori said in [a blog post](#) the attack happened on November 13. The hacker gained access to the company's domain records, allowing the hacker to take control of several employee email accounts, and later compromised the company's network.

Kayamori said that while cryptocurrency funds are "accounted for," the hacker may have accessed the company's document storage. "We believe the malicious actor was able to obtain personal information from our user database. This may include data such as your email, name, address and encrypted password," he said.

SOURCE: <https://techcrunch.com/2020/11/18/cryptocurrency-exchange-liquid-confirms-hack/>

Crypto Crimes and Fiascos

KuCoin cryptocurrency exchange hacked for \$150 million

KuCoin said an intruder drained all its hot wallets today.

Singapore-based cryptocurrency exchange KuCoin disclosed today a mega hack. In a [statement](#) posted on its website, the company confirmed that a threat actor breached its systems and emptied its hot wallets of all funds.

Hot wallets are cryptocurrency management apps that are connected to the internet. Cold wallets are stored offline.

Cryptocurrency exchanges like KuCoin use hot wallets as their temporary storage systems for assets that are currently being exchanged on the platform, and they are used to power conversion operations and funds transfers.

Source: <https://www.zdnet.com/article/kucoin-cryptocurrency-exchange-hacked-for-150-million/>

Crypto Crimes and Fiascos

Yet another crypto exchange has fallen victim to a massive hack

By Barclay Ballard December 22, 2020

A cryptocurrency exchange with a 24-hour trading volume of nearly \$52 million has been hacked. UK-based EXMO revealed that cryptocurrency assets, including Bitcoin, Ripple, Ethereum, and others, were stolen from its hot wallets. Collectively, around 5% of EXMO's total assets were withdrawn.

EXMO has explained that the incident is still being investigated but it has identified the wallet addresses where the stolen funds were deposited. The crypto exchange has reported the theft to the relevant authorities and asked other crypto services to block all accounts connected to the attack. In addition, EXMO has reiterated that all losses related to this incident will be refunded.

Source: <https://www.techradar.com/in/news/yet-another-crypto-exchange-has-fallen-victim-to-a-massive-hack>

Crypto Crimes and Fiascos

7 FEB 2020

NEWS

Crypto Exchange Loses "Almost All Funds" in Hack

Cyber-criminals have stolen "almost all funds" entrusted to crypto exchange platform **Altsbit**.

The Italian exchange announced it had become the target of a devastating hack yesterday on **Twitter**. According to their posts, criminals made off with 1,066 Komodo (KMD) tokens and 283,375 Verus (VRSC) "coins" with a combined value of \$27,000.

Funds kept in cold storage—crypto coins whose private keys are stored on devices that exist in an offline environment—were not swiped in the cyber-heist.

In a statement released on Twitter at 2:24 a.m. on February 6, Altsbit wrote: "Dear users, unfortunately we have to notify you with the fact that our exchange was hacked during the night and almost all funds from BTC, ETH, ARRR and VRSC were stolen. A small part of the funds are safe on cold wallets."

Source: <https://www.infosecurity-magazine.com/news/crypto-exchange-loses-almost-all/>

Crypto Crimes and Fiascos

Cryptocurrency exchange Eterbase hacked, \$5.4 million worth of funds stolen



GRAHAM CLULEY

[FOLLOW @GCLULEY](#)

SEP 10, 2020

IT SECURITY AND DATA PROTECTION

European cryptocurrency exchange platform Eterbase has announced that it has suffered a security breach which saw malicious hackers access its network and steal funds worth US \$5.4 million.

In a [message](#) posted on Telegram, the Slovakian cryptocurrency exchange listed the six hot wallets plundered by cybercriminals for their Ether, Tezos, Bitcoin, ALGO, Ripple, and TRON riches.

The majority of the cryptocurrency funds stolen from the hot wallets were in the form of Ether, making up almost \$3.9 million of the almost \$5.4 million stolen.

	Address	approx. USD Value
ETH / ERC-20	0x7860F7b2874e77E80bE0fC6EbfB9414f89781aD9	\$3,945,664
TRX	TPdhhbCHqXzrDyUiQnHApS7VL2UxB8Qhna	\$45,148
XTZ	tz1hnoxVgc8Z1DUa6D18EUkPCXmNbaHwmLRc	\$471,559
BTC	1ANLZZ2YFGumRXaD3EMii92zWQqvX2CK9c	\$114.954

Crypto Crimes and Fiascos

A Crypto Exchange Hacked Here, Another There: Do You Know Where Your Crypto Is Tonight?



by [Tim Sloane](#) — December 24, 2020

Mercator research has documented the security of the Bitcoin network but we also identified that all operations outside of that Bitcoin network are by nature very insecure – especially wallets, exchanges and ATM implementations. Put another way the Bitcoin network is in essence the bank and everything else is a mattress stuffed with money.

Ledger, a secure hardware wallet provider, was hacked in July and lost 272,000 customer records. So while the crypto remains safe in a protected thumb drive, the individual customers are now the targets for a large amount of criminal activity. All of the stolen customer records were dumped onto RaidForum this month and the customers now face a tidal wave of social engineering hacks which have already [begun](#).

<https://www.paymentsjournal.com/a-crypto-exchange-hacked-here-another-there-do-you-know-where-your-crypto-is-tonight/>

Crypto Crimes and Fiascos

Cryptocurrency Exchange Hotbit Hacked: Systems Paralyzed, 2 Million Users Affected

A cryptocurrency exchange with about 2 million users worldwide announced that it has “suffered a serious cyber attack.” A number of basic services are paralyzed and the attacker tried to access the exchange’s wallets. Consequently, the platform has shut down, stating that it needs to perform a “comprehensive inspection” which is expected to last one to two weeks.

Crypto Crimes and Fiascos

SHOWCAUSE TO WAZIRX

ED issues show cause notice to WazirX, directors under FEMA

Our Bureau | Mumbai | Updated on June 11, 2021

No audit trail

The main concern for the investigative agency is that none of these transactions is available on blockchain for any audit/investigation. Also, It was found that WazirX customers could transfer 'valuable' crypto-currencies to any person irrespective of his/her location and nationality without any documentation, making it a safe haven for those looking to launder money or for other illegitimate activities.

<https://www.thehindubusinessline.com/money-and-banking/ed-issues-show-cause-notice-to-wazirx-directors-under-fema/article34787774.ece>

Crypto Crimes and Fiascos

सर,
आखिर ये हैकर
BITCOIN लेकर
गए कहाँ?



Crypto Crimes and Fiascos



सर,
आखिर ये हैकर
BITCOIN लेकर
गए कहाँ?



Ye raaz bhi usi ke saath chala gaya

Crypto Crimes and Fiascos

सर,
आखिर ये हैकर
BITCOIN लेकर
गए कहाँ?



**True for most of the
cases, but then there is
HOPE too**

Ye raaz bhi usi ke saath chala gaya

Colonial Pipeline

Jul 1, 2021, 04:34pm EDT | 350 views

Colonial Pipeline As A Case Study On Cryptocurrency Risks



Gideon Pell Contributor

Fintech

I write about the intersection of finance, risk and technology.

Follow

Colonial Pipeline

Jul 1, 2021, 04:34pm EDT | 350 views

Colonial Pipeline As A Case Study On Cryptocurrency Risks



Gideon Pell Contributor

Fintech

I write about the intersection of finance, risk and technology.

Follow

The ransomware attack on Colonial Pipeline hit the headlines in May

Colonial Pipeline decided to pay the hackers who invaded their systems nearly \$5 million (75 bitcoins) to regain access

Colonial Pipeline

Jul 1, 2021, 04:34pm EDT | 350 views

Colonial Pipeline As A Case Study On Cryptocurrency Risks



Gideon Pell Contributor

Fintech

I write about the intersection of finance, risk and technology.

Follow

Over the next several weeks, the FBI traced the address of the wallet the criminals gave to Colonial to make the payment

At that point, federal law enforcement seized the assets, recovering 2.3 million worth of bitcoins transferred

Colonial Pipeline

Jul 1, 2021, 04:34pm EDT | 350 views

Colonial Pipeline As A Case Study On Cryptocurrency Risks



Gideon Pell Contributor

Fintech

I write about the intersection of finance, risk and technology.

Follow

The FBI said in its request for a warrant that its investigators had in their possession the private key for that cryptocurrency wallet

How they obtained the private key which is closely held is unclear

Colonial Pipeline

Jul 1, 2021, 04:34pm EDT | 350 views

Colonial Pipeline As A Case Study On Cryptocurrency Risks



Gideon Pell Contributor

Fintech

I write about the intersection of finance, risk and technology.

Follow

One scenario is that hackers had made the choice to entrust the private key for their Bitcoin to a cryptocurrency exchange which was forced to hand over the funds to the FBI

<https://www.forbes.com/sites/gideonpell/2021/07/01/colonial-pipeline-as-a-case-study-on-cryptocurrency-risks/?sh=8638db34d547>

Mt. Gox (Magic The Gathering Online Exchange)

**World's largest Bitcoin intermediary
handling 70% of the world's Bitcoin
exchanges**

**Mt. Gox lost about 740,000 Bitcoin
(6% of all Bitcoin in existence at the
time)**





Mark Karpeles



Mark Karpelès (second from right)
announcing Mt. Gox's bankruptcy in 2014



Kim Nilsson, the software engineer



Kolin Burges, a cryptocurrency
trader, protesting the loss of Mt.
Gox's Bitcoins



Alexander Vinnik (center), the
Russian accused

CYBER CRIMES LINKED TO CRYPTOCURRENCIES



WHO IS DD4BC?

DDOS ATTACK

An **extortionist group responsible for many BITCOIN involving DDoS demands** extortion campaigns attacks and ransom

**DDoS “4” Bitcoin – has ATTACKED
over 150+ COMPANIES since its
emergence in 2014.**



**Other groups, INSPIRED BY THEIR
SUCCESS, are jumping on the
bandwagon. Is this form of extortion
here to stay?**

SAMPLE

NOTICE OF EXTORTION

Your business, **900 Degrees Neapolitan Pizzeria**, has been targeted for extortion. The selection process is random, and was not triggered by any event under your control.

Should you fail to pay the one-time monetary tribute, by the deadline provided below, your business will be severely and irreparably damaged. The following methods are commonly employed in cases of non-compliance:

- Negative Online Reviews
- BBB Complaints
- Harassing Telephone Calls
- Fraudulent Delivery Orders
- Telephone Denial-of-Service
- Bomb Threats
- Vandalism
- Mercury Contamination

Anonymous Reports of:

- Health Code Violations
- OSHA Violations
- Criminal Tax Evasion
- Money Laundering
- Illegal Drug Sales
- Marijuana Grow Operations
- Methamphetamine Production
- Terrorist Training Activity

**Nitrogen Sports is dedicated to its
INTERNATIONAL USERBASE & offers
SPORTS BETTING for dedicated
fans to make some extra side money**



**When you visit the site, a unique
Bitcoin address is generated
for your use**

NITROGEN SPORTS

Nitroger × F Using B × Bitcoin × D How Biti × G dd4bc p × Microsoft × Bitcoin f × S

Secure | https://nitogensports.eu

Cloud Forensics bitcoin block anupam Quotes | A-Z education misc bc communication BC g

Error 1009

Ray ID: 3f9f786efb832dbb • 2018



What happened?

The owner of this website (nitrogen.sports) has blocked access from your country or region. Your IP address has been banned by the Indian government (IN) from accessing this website.

in
INDIA

ONLINE SPORTS BETTING

NitrogenSports | Best Bitcoin Sportsbook, Blackjack, Dice, and Poker for Browsers

Nitrogen Sports | Be... +

S! 🔍 ⌂ ⓘ 🔒 https://nitogensports.eu | x Search

 NITROGENSPORTS



Sportsbook

Play Poker

Casino

 Nitrogen

 Affiliates

 Starting Soon

 NITROGENSPORTS

Welcome to Nitrogen Sports! We're the largest and most trusted bitcoin sportsbook and casino. Before playing, please be sure you agree to the following:

- You must be over 18 to play at Nitrogen Sports
- Please confirm that this type of gambling is legal in your jurisdiction
- By playing at Nitrogen Sports you agree to all of our Terms and Conditions

I Agree, Create my anonymous account

Log in to existing account

ONLINE SPORTS BETTING



Ultra Secure

We offer anonymous accounts; you don't need to give us any personal information. We also offer 2-factor authentication to provide maximum security for your account.



Lightning Fast Transactions

Lightning fast deposits and withdrawals are our standard, and most games are graded minutes after they end.



More Choices

From major sports and leagues down to cricket and eSports, we have you covered.



Competitive Odds

Made by gamblers for gamblers, we realize that competitive odds are king!



Fun Promos

Check out our monthly Parlay Promotion and NFL Survivor Pools. Grab a piece of the Jackpots for yourself!



Superior Support

With our built-in chat and support ticket system, you can get immediate help with any issues.



฿ 0.00000000 (฿ 0.000000)



Elias Samson [644435] Im a United fan so i hope Wenger stays for 20 mo

Sportsbook

Play Poker

Casino

Nitrogen

Affiliates

Starting Soon

In-Play Live

eSports



the future of betting

When you arrived, we automatically created an account for you! We suggest you add a username and password to keep it secure:

Username

Password

Password Again

Add Username / Password

or Sign In

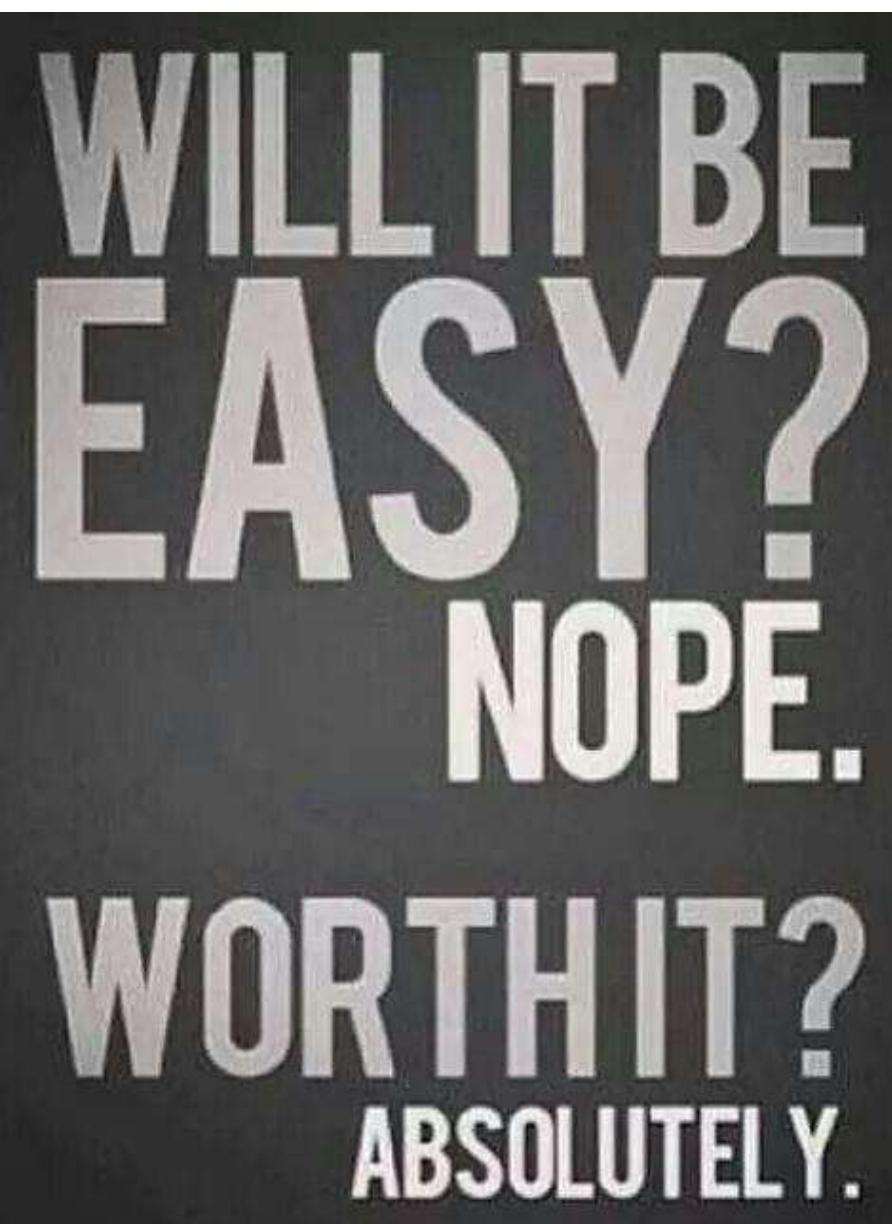
YOU'VE BEEN HACKED!

Hacker Strikes,
Again!



SECURITY BREACH

Operation Pleiades



DD4BC

European Union's law enforcement agency investigators from **Europol, Bosnia, Herzegovina, Germany, France, Japan, Romania, Switzerland, the UK and the US** contributed in tracking down the hacking group

CRYPTOJACKING is the
unauthorized use of someone
else's computer to mine



CRYPTOJACKING

**Getting the victim to click on a
malicious link in an email that loads
crypto mining code on the
computer, or by infecting a website
or online ad with JavaScript code**

CRYPTOJACKING

**Research has found
53,000 + websites
running crypto mining
scripts**

What is it?

**Estimated that those site
had a BILLION combined
monthly visitors**

Cryptojacking



researchers discovered the Smominru crypto mining botnet, which targeted Windows servers to mine Monero, and cybersecurity firm estimated that it had generated as much as \$3.6 million in value as of January.



TECH

Customer of an electronics retailer in UAE claims to have mined ~\$2,500 worth of cryptocurrency using display laptops of the store

By MB Staff - October 10, 2017 - Like & Follow Us Like Follow @menabytes Follow

mb

HACKED

SharafDG charged me 18AED for a delivery that I didn't receive, So I earned 9000AED using their display laptops

Not Gonna Tell ;) • October 10, 2017

CRYPTOJACKING

Home | Cryptocurrency | Cryptocurrency News | Gamers Particularly Targeted in Cryptojacking Avast Malware Researcher Daniel Benes Explains Why

Gamers Particularly Targeted in Cryptojacking - Avast Malware Researcher Daniel Benes Explains Why

A recent research published by Avast pointed out that hackers have been particularly targeting gamers with 'Crackonosh', a cryptojacking malware.

By [Jasmin Jose](#) | Updated: 2 July 2021 16:54 IST

Cryptojacking is a growing problem and gamers are particularly being targeted by malware that uses their computers to mine for cryptocurrency, according to recent research published by security firm Avast. According to the research, cyber criminals have been targeting gamers with 'Crackonosh', a cryptojacking malware. Crackonosh was installed into the gamers' system while free versions of games like NBA 2K19, Grand Theft Auto V, Far Cry 5, The Sims 4, and Jurassic World Evolution were downloaded from unreliable sources like torrents.

<https://gadgets.ndtv.com/cryptocurrency/news/cryptojacking-malware-gamers-avast-crackonosh-cryptocurrency-mining-hackers-2477846>



Ooops, your files have been encrypted!

English

not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

Ransomware attack

Your files will be lost on

1/8/1970 00:00:00

Time Left

00:00:00:00:00

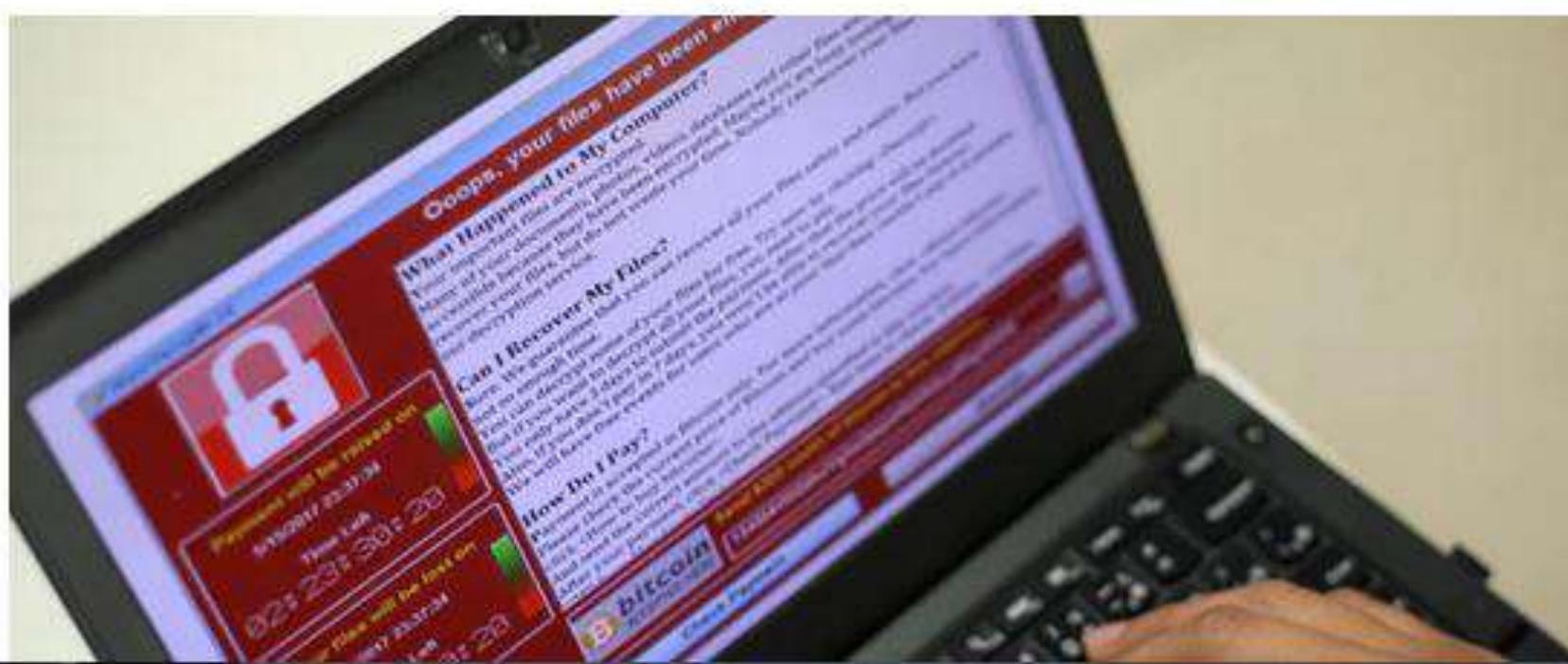
Contact

If you need our assistance, send a message by clicking <[Contact Us](#)>.

We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

WannaCry: hackers withdraw £108,000 of bitcoin ransom

Digital wallets linked to ransomware attack that crippled NHS hospitals are cleaned out, as law enforcement tries to track owners





Sigma Ransomware



**DECRYPT
CrySis
RANSOMWARE**

BEHAVIOR ALERT!

File name: C:\Users\Sarah\Desktop\Rakhni.exe

View details

Diagnosis: **Program is attempting to modify your documents in a suspicious manner**

Allow

If you are sure this behavior is safe, click Allow. If you continue to receive this message, click Block.

Block

Terminate this program now, but do not move it to quarantine.

Allow always

Allow this behavior now and in the future.

Quarantine (recommended)

Stop the action immediately and prevent the program from being executed again.

RAKHNI

DHARMA RANSOMWARE

amagnus@india.com



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail amagnus@india.com. You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send to us up to 3 files for free decryption. Please note that files must NOT contain valuable information and their total size must be less than 10Mb.

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.

https://localbitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

<http://www.coindesk.com/information/how-can-buy-bitcoins/>

RobinHood Ransomware Is “Honest” And Promises To “Respect Your Privacy”

By **Adarsh Verma** - April 15, 2019





What makes RobinHood interesting are some surprising claims made by its creators. The ransomware's .Onion payment page mentions that the developers care about the privacy of the users.

"Your privacy is important for us, all of your records including IP address and Encryption keys will be wiped out after your payment," it says.

The page further mentions that the **bitcoin address** used for the ransom payment is **created freshly** for every victim, so there's no way to track it.



Ransomware

4rw5w, 777, 7ev3, ST, AES-Matrix, AES-
Namrood, Al-Nar, AngryDuck, Anubi, A-
Apocalypse (New), Crypter, aZaZeL, Bad-
BadRabbit, Bam!, BananaCrypt, BandarChor, Bart, Bart v2.0, BitCrypt, BitCrypt 2.0, BitCryptor, BitKangoroo, Bitpayer, Bitshifte-
Feather, Black Shades, Blackout, BlackRuby, Blind, Blind 2, Blocatto, BlockFile12, Blooper, Booyah, BrainCrypt, Brazilian Ransom-
BTCamant, BTCWare, BTCWare Aleta, BTCWare Gryphon, BTCWare Master, BTCWare PayDay, Bubble, Bucbi, Bud, BugWare, Bu-
Cancer, Cerber, Cerber 2.0, Cerber 3.0, Cerber 4.0 / 5.0, CerberTear, Chimera, ChinaYunLong, CHIP, ClicoCrypter, Clouded, Cock-
Locker, CoinVault, Comrade Circle, Conficker, CorruptCrypt, Coverton, CradleCore, Cripton, Cry128, Cry36, Cry9, Cryakl, CryFile, Cry-
CrypMic, CrypMic, Crypren, Crypt0, Crypt0L0cker, Crypt12, Crypt38, CryptConsole, CryptFuck, CryptInfinite, CryptoDefense, Cry-
CryptoFinancial, CryptoFortress, CryptoGod, CryptoHasYou, CryptoHitman, CryptoJacky, CryptoJoker, CryptoLocker3, CryptoLoc-
CryptoLuck, CryptoMix, CryptoMix Revenge, CryptoMix Wallet, Crypton, CryptON, CryptorBit, CryptoRoger, CryptoShield, Crypt-
CryptoTorLocker, CryptoViki, CryptoWall 2.0, CryptoWall 3.0, CryptoWall 4.0, CryptoWire, CryptXXX, CryptXXX 2.0, CryptXXX 3.0, Cry-
CryPy, CrySiS, Crystal, CTB-Faker, CTB-Locker, Damage, DarkoderCryptor, DataKeeper, Dctr, DCry, DCry 2.0, Deadly, DeathNote-
Defender, Defray, DeriaLock, **Dharma (.cezar)**, Dharma (.dharma), Dharma (.onion), Dharma (.wallet), Digisom, DilmaLocker, D-
Locker, DMA Locker 3.0, DMA Locker 4.0, DMALocker Imposter, Domino, Done, DoNotChange, DoubleLocker, DriedSister, Dviid-
Crypt, eBayWall, ECLR Ransomware, EdgeLocker, EduCrypt, El Polocker, EnCrypt, EncrypTile, EncryptoJJS, Encryptor RaaS, Enigm-

BITCOINING IT IN Criminals are cashing in on Bitcoins for illegal activity from buying drugs, hiring hitmen and forging passports on the Dark Web

A Sun investigation has now proved that Bitcoin is linked to a range of serious crimes on the Dark Web

NEWS OCTOBER 27, 2017 17:43

UK Government Reports Currencies Pose a Threat to Cybercrime

WARNING: ISIS using cryptocurrency to fund reign of terror as Bitcoin price soars

AS the Bitcoin price soars, grotesque organisations are using the cryptocurrency to fund its reign of terror.

Digital gold: why hackers love Bitcoin

The WannaCry ransomware attackers demanded payment in the cryptocurrency. But its use in the 'clean' economy is growing, too, and could revolutionise how we use money

Bitcoin fraud triples as criminals target cryptocurrency boom

CYBERSECURITY

Rise of Bitcoin Will Result in Increased Cybercrime in 2018

How cybercriminals are exploiting the bitcoin craze



Daniel Howley
Tech reporter



PONZI!





2018
Loading


\$32 million RAISED
2,31,93,60,000 Rs

2018

Loading



PinCoin

\$660 million RAISED

47,83,68,00,000 Rs

[ABOUT](#)[INVESTMENT](#)

PRE-ICO SALE IS

15% BONUS ENDS IN

14

.

22

.

26

.

22

The Smominru Miner



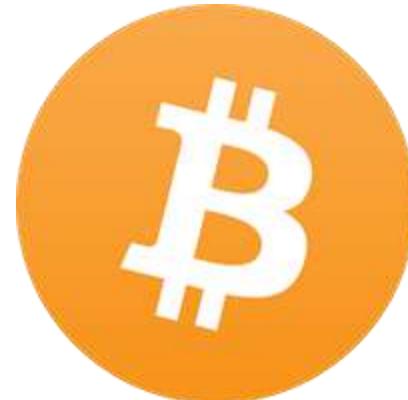
5 LAKH USERS INFECTED

EXCHANGE HACKS

65,66,68,80,000 Rs

worth of cryptocurrencies have been lost so far, with most of these losses happening through exchanges (Aug 2018)

majority



Ross Ulbricht

Ross Ulbricht

S
I
L
K



R
O
U
T
E

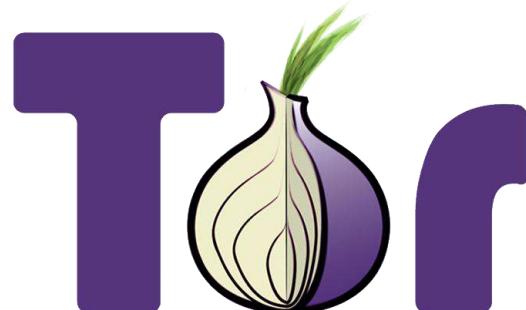
**American Drug trafficker and Darknet
Market Operator**

**CURRENTLY SERVING
A DOUBLE
LIFE SENTENCE PLUS
FORTY YEARS
WITHOUT THE
POSSIBILITY OF
PAROLE**

SilkRoad

BUY ANYTHING
SELL ANYTHING

Stay Anonymous



SERVERS

THE CLOUD

AMAZON

WIKIPEDIA

THE WEB SEA

Google

PORN

CONTINENTAL CONTENTS

DEEP WEB

GOVERNMENT

UNDETECTED



ILLEGAL PORN



Guide On How To Access The Silk Road 3.0 (3.1)

If you've heard about darknet markets, you have heard about the Silk Road. From the original Silk Road, which was basically the forefather of the current online black market, to the Silk Road 2, Silk Road 3.0 now Silk Road 3.1, the name has become synonymous with buying drugs on the net.

And that was possibly the downfall of the first and second version. They were so well known and popular, it put a huge bullseye on their back for the law enforcement agencies determined to shut them down.

I'm going to walk you through step-by-step as I set up Tor and my VPN, create an account at Silk Road 3.0 and Silk Road 3.1 (as the two sites are almost identical clones), and browse through a market that includes everything from hard drugs, weapons, to access to porn sites.

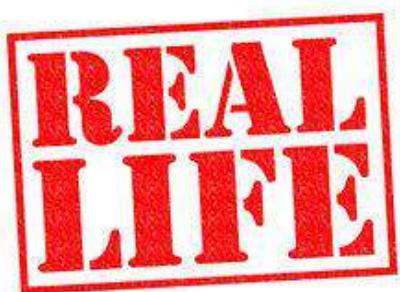
SilkRoad

**Rs 87,55,80,00,000
/1.2 billion\$ turnover**

9,60,000 USERS

HOW WAS HE CAUGHT?

Boasted about running his
International Multimillion Dollar
drugs marketplace on his LinkedIn
profile



He used a real photograph of himself for a fake ID to rent servers to run his international multimillion dollar drugs marketplace

In March 2012, a user registered on the coding Q&A site Stack Overflow with Ulbricht's email address and the **username** '**Ross Ulbricht**'. He then proceeded to post the question "**How can I connect to a Tor hidden service using curl in php?**"



He sought **contacts in courier firms, presumably to work out how to best ship things** from his international multimillion dollar drugs marketplace, on Google+, where his real name, real face and real YouTube profile were visible

An FBI report leaked back in 2012 titled "[Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity](#)" is a prime example of how law enforcement was seeing Bitcoin at the time. In the report, the FBI expresses concerns surrounding the anonymity of Bitcoin and how it "...might logically attract money launderers, human traffickers, terrorists, and other criminals". The FBI was quick to identify possible early use cases of Bitcoin, mostly unsavoury, but continued to note that Bitcoin is not fully untraceable and cited research from the University College of Dublin focusing on the limits to Bitcoins anonymity. It's around this time that people, outside the developers and fanatics, were slowly beginning to notice that Bitcoin wasn't the untraceable currency they once thought, and this wasn't a secret.

In the court proceedings of Ulbricht, the FBI was able to use Bitcoin's Blockchain and strategically correlate transactions leading to a set of servers they had previously seized. [The over 3500 transactions](#), open to view in Bitcoins public ledger, were found to have been from the seized servers and traceable directly back to Ulbricht's personal Samsung 700z laptop, also under seizure from the FBI.

In the case of the Silk Road, Bitcoins anonymity was challenged as the security and privacy ended at the public keys. Ross Ulbricht's pseudonyms were his public keys, each with a trackable and verifiable history of activity and transactions. The success of the FBI was in linking the pseudonymous public keys to the then anonymous Ross Ulbricht.

**~144,000
BITCOINS**

1FfmbHfnpaZjKFvyi1okTJJusN455paPH

SLEEPING SINCE 5 YEARS NOW

BTC BITCOIN ANALYSIS SEPTEMBER 16, 2018 16:46 CET

This Dormant \$720 Million Bitcoin Wallet Has Woken Up – But Who Owns It?



SEPT 16, 2018

Address 0.11138308 BTC

Address 1FfmbHfnpaZjKFvyi1okTJJusN455paPH

Summary confirmed

Total Received	144341.64743243 BTC
Total Sent	144341.53604935 BTC
Final Balance	0.11138308 BTC
No. Transactions	655



Transactions

033138d73850f009339a26

mined Jan 16, 2017 10:57:34 AM

But it doesn't end there.

BITCOINS



**IT'S JUST THE
BEGINNING**





THE
TIP
OF THE
ICEBERG

January 03, 2018

Cybercriminals dropping Bitcoin for more private cryptocurrencies



News › Business › Business Analysis & Features

Bitcoin is being dropped by criminals in favour of privacy coins like monero

Some coins post fake blockchain entries to hamper surveillance

Olga Kharif | Tuesday 2 January 2018 12:03 GMT | 0 comments

More SUCH unknown currency UPCOMING



MONERO



Bitcoin Private



Dash
Digital Cash



CASH



BYTECOIN



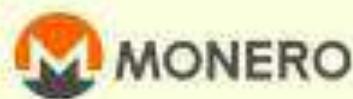
ZCLASSIC



COMPARISON OF

ANONYMOUS

CRYPTOS



MONERO



bitcoin



CASH



DASH



VERGE



LET'S TALK



Monero

Safe, Secure & Misunderstood



MONERO

brother IT'S





Vs

**Monero****Bitcoin**

Founder	Group of 7 core developers	Satoshi Nakamoto
Release Date	18 April, 2014	9 Jan 2008
Release Method	Crowdfunded group of 7 core developers	Genesis Block Mined
Total Coin Supply	18.4 Million XMR + 0.3 XMR/minute	21 Million
Blockchain Protocol	Proof of work	Proof of work
Usage	Digital Currency	Digital Currency
Privacy	Untraceable	Yes
Trackable	No	Yes
Cryptocurrency Used	Monero	Bitcoin(Satoshi)
Cryptocurrency Symbol	(XMR)	(BTC)
Transaction Fee	0.004-0.02 XMR/kB	Varies based on load on blockchain
Algorithm	CrptoNote	SHA-256
Blocks Time	120 seconds	at least 10 minutes
Mining	GPUs, CPU	Pools,ASIC miners
Scalable	Yes	Yes



MONERO

Why?

UNTRACEABLE

RING SIGNATURES

In cryptography, a ring signature is a type of digital signature that can be performed by any member of a group of users that each have keys.

ANONYMOUS
MONERO

A dark blue background featuring a grid of binary digits (0s and 1s) and several thin, light blue lines connecting specific digits, resembling a circuit board or a network diagram.

RING SIGNATURES

Ring signatures enable a sending participant to conceal his identity from other participants in a group

Anonymous digital signatures from one member of the group, its is not revealed which member signed the transaction

**ANONYMOUS
MONERO**

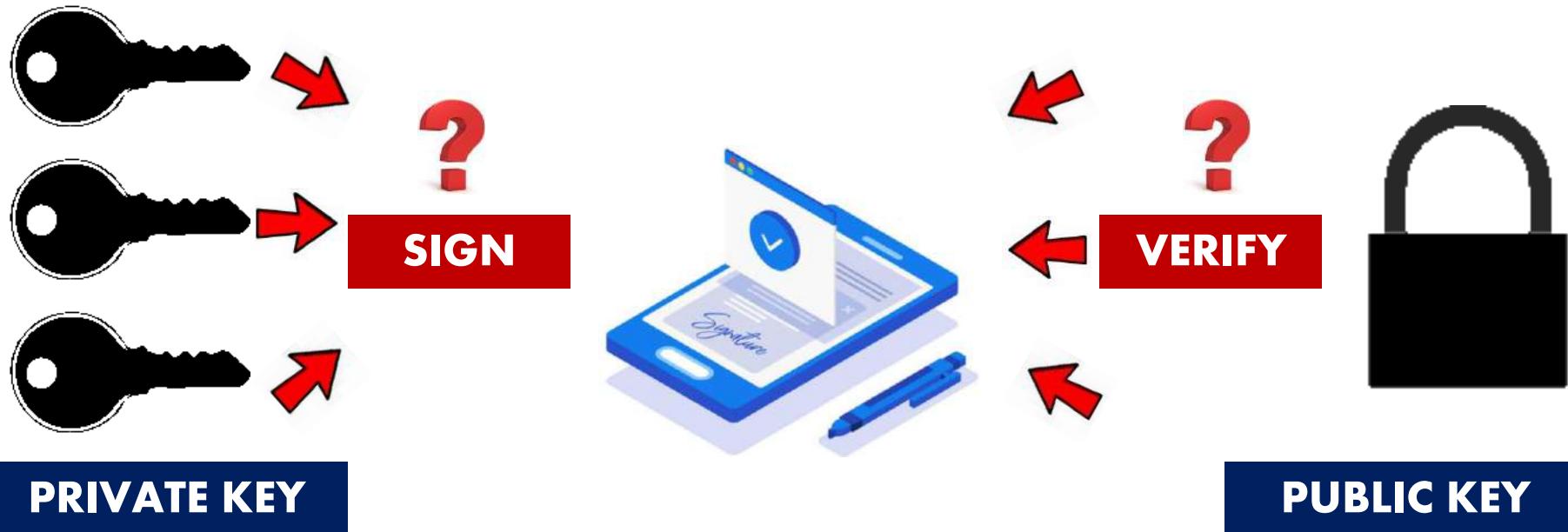
A dark blue background featuring a grid of binary digits (0s and 1s) and a small white stick figure walking across the left side.

ORDINARY SCENE - SIGNATURES



ANONYMOUS MONERO

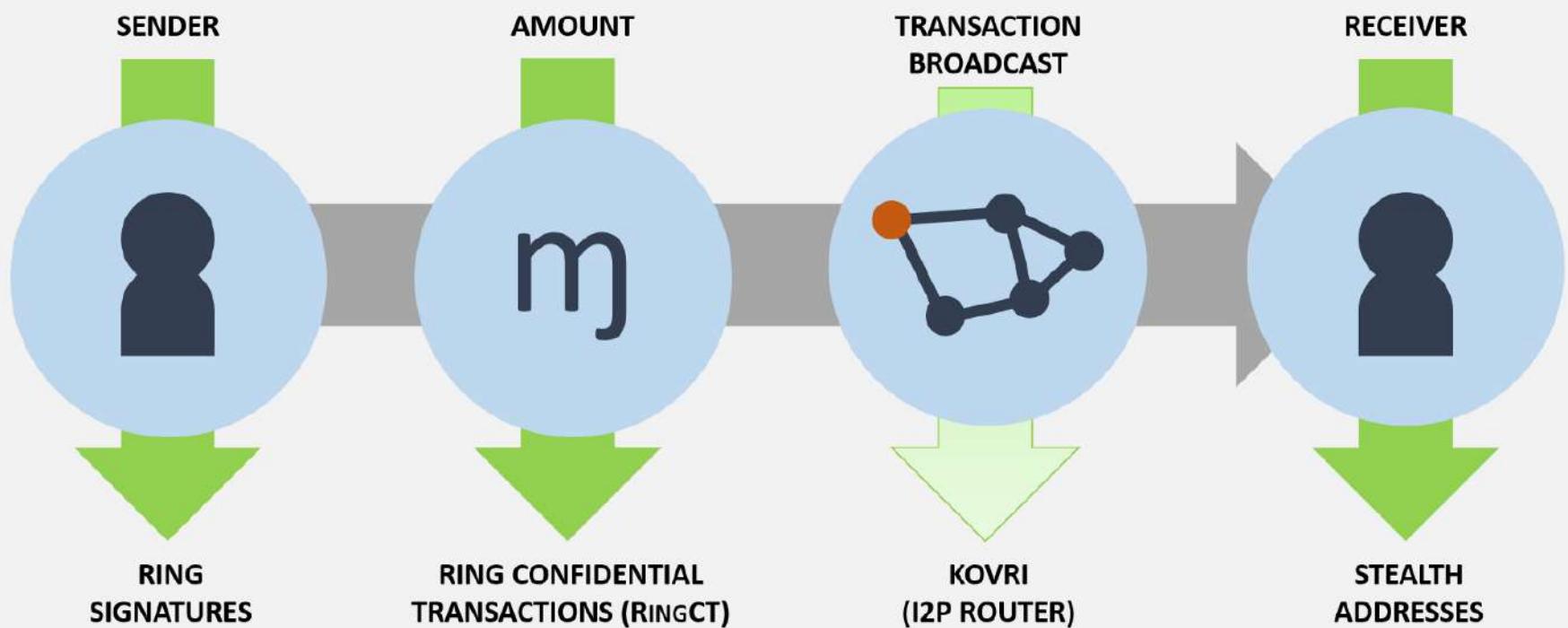
RING SCENE - SIGNATURES



ANONYMOUS MONERO

REASON

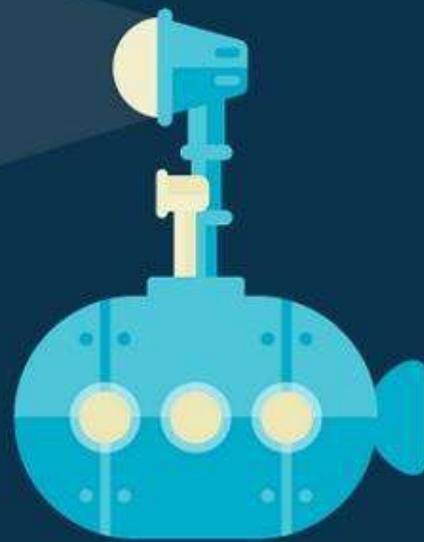
The Monero Difference



Luminati Anonymity Network

Highly secure, low latency Internet anonymity

Dive in



1 0
1 0 1
1 0 0
1 0 1



Riffle Anonymity Network

Cover your Digital Footprints Better than Tor



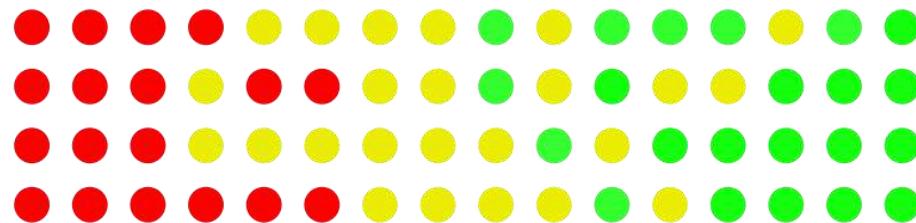
Tor-Like Anonymous Browsing

High Speed Network @ 93GBps

A glowing blue network of lines and dots forms a globe, symbolizing global connectivity and a distributed network. The lines represent data flow or connections between nodes, which are represented by small glowing blue dots. The globe is centered on Earth, showing continents and oceans, with the network density appearing higher over landmasses.

INVISIBLE INTERNET PROJECT (I₂P)
is an anonymous network layer that
allows for censorship-resistant, peer
to peer communication

I2P



**Kovri is a FREE, DECENTRALIZED,
ANONYMITY TECHNOLOGY developed
by Monero**



**Kovri uses both GARLIC ENCRYPTION
AND GARLIC ROUTING to create a
private, protected overlay-network across
the internet.**



**Effectively HIDES GEOGRAPHICAL
LOCATION and internet IP address.**

REASON

With **BITCOIN**, you reveal your real
“**HOME ADDRESS**” in order to send and
receive **BITCOIN**

Stealth

Monero, uses the **EQUIVALENT OF A**
“POST OFFICE BOX” as address to
send and receive **Monero**.

VIRTUAL P.O. box
instead of actual
address

ADDRESS

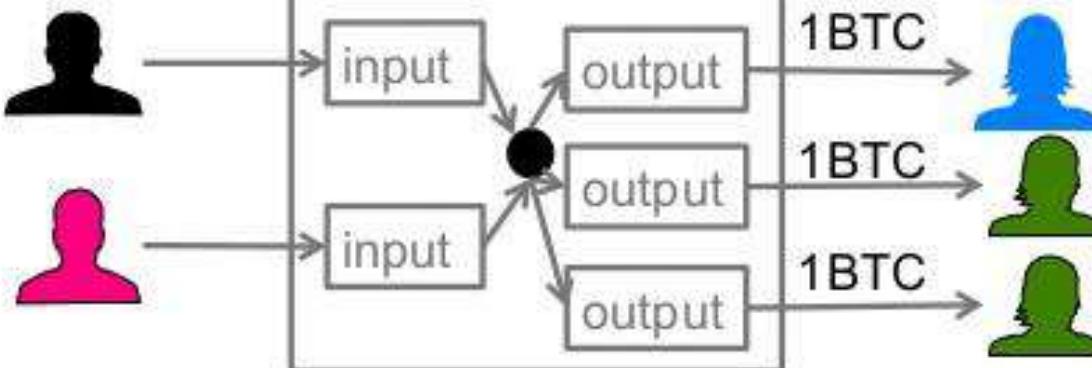
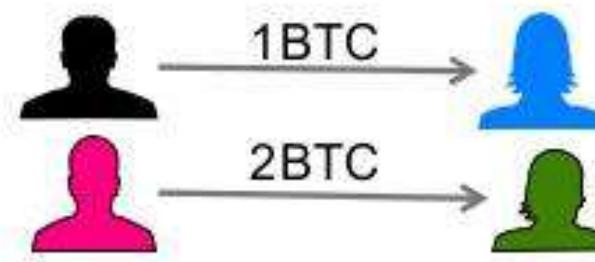
REASON



Signature[®]

**Ring signature is a WAY TO MAKE
SURE A TRANSACTION CAN'T BE
TIED BACK to a specific individual**

CoinJoin is ANONYMIZATION method for bitcoin TRANSACTIONS



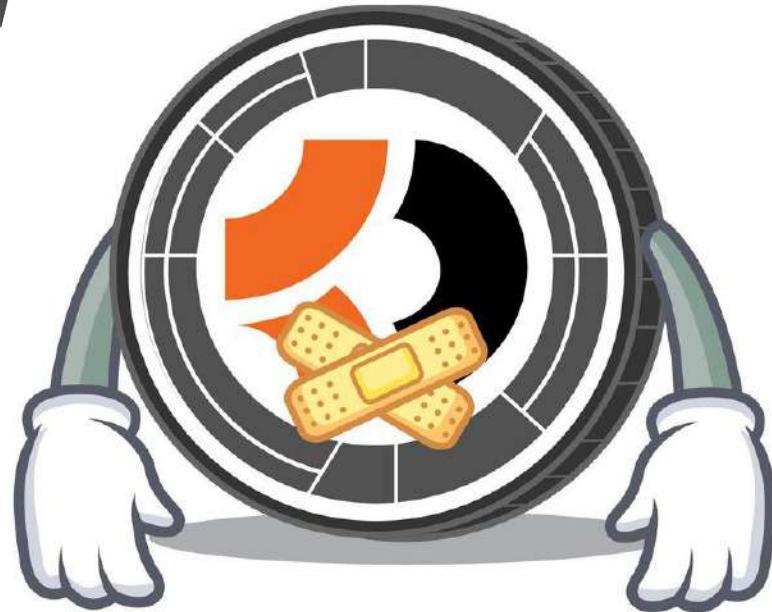
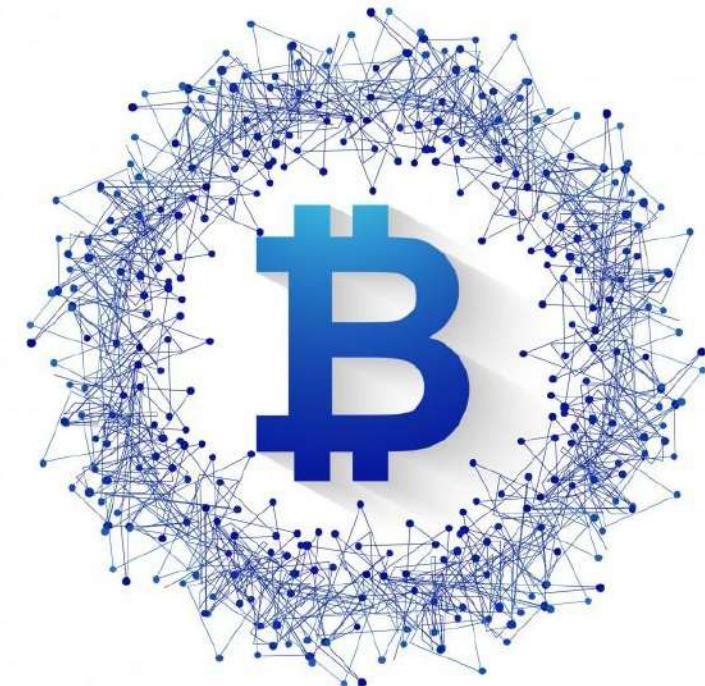
**"When you want to make a payment,
find someone else who also wants to
make a payment and make a joint
payment together."**



**When making a
joint payment,
there is no way
to relate input
and outputs in
one BITCOIN
transaction**

SILENT

 *bitcoin*



**Silent Bitcoin is a DIGITAL VOUCHER
CURRENCY 100% backed by bitcoins.**



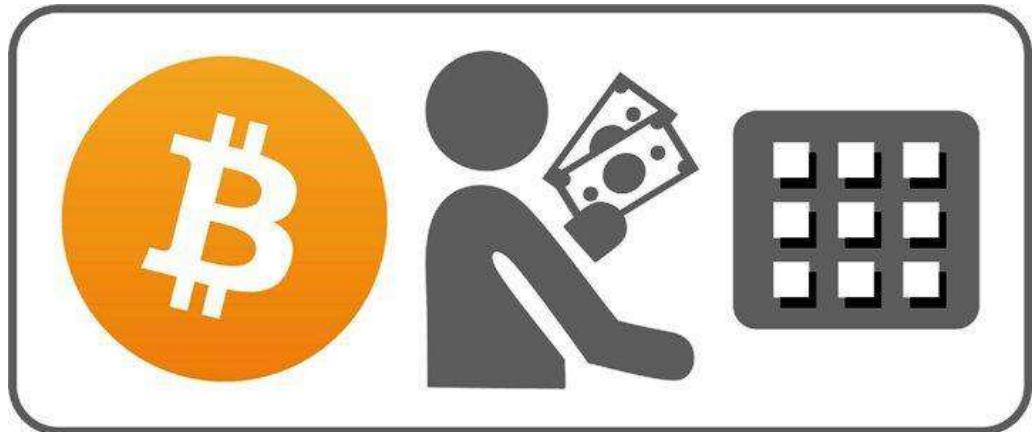
**Means that 1.0 SBC
equals 1.0 BTC.**



**However the base
units for SBC vouchers
are mBTC, or milli-
bitcoin (0.001 BTC).**



When a user spends BTC to a wallet hash controlled by SilentVault, they receive in exchange a voucher (a cryptographically signed XML object) for the same amount in SBC.





tumblebit



TumbleBit, a new unidirectional unlinkable payment hub



Allows parties to make fast, anonymous, OFF-BLOCKCHAIN payments through an untrusted intermediary called the Tumbler

No one, not even the Tumbler, can link a payment from its payer to its payee

1.46×10^{48} possible Bitcoin Addresses

ऊपर वाला जब देता है तो छपर फाड़ के देता है



**that gives every
person on Earth
 2.05×10^{38} Different
Addresses**

The background of the image shows a wide, open landscape with a golden-yellow field in the foreground and a clear, light blue sky above. The sky has a few wispy, white clouds near the horizon.

MIND
BOGGLING

BITCOIN MIXER



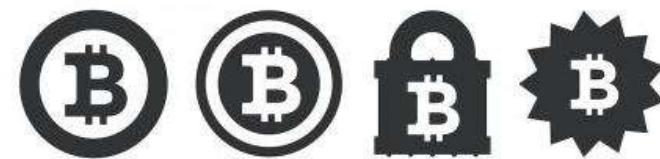
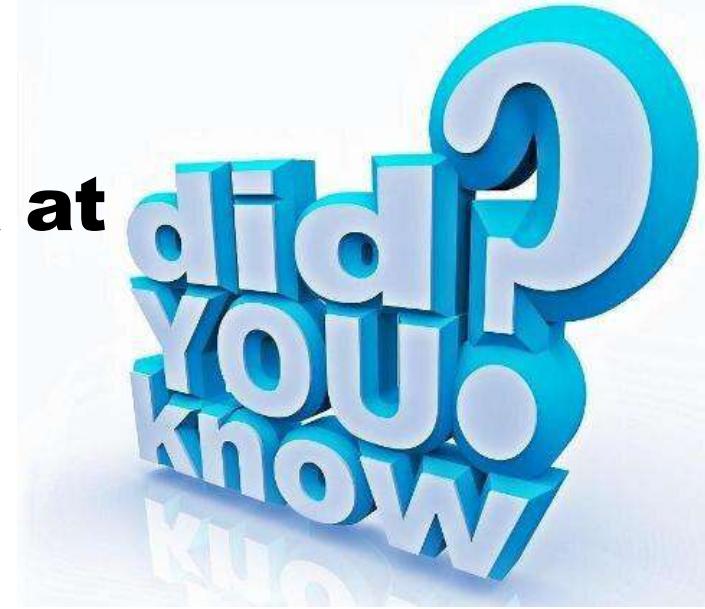


Bitcoin Mixer is an **Anonymous Service**, that confuses the trails of Bitcoin transactions.



 **bitcoin**  **mixer**

When we say **SOMEONE HAS BITCOINS & you look at a **PARTICULAR BITCOIN ADDRESS**, there are **NO DIGITAL BITCOINS held AGAINST that ADDRESS****

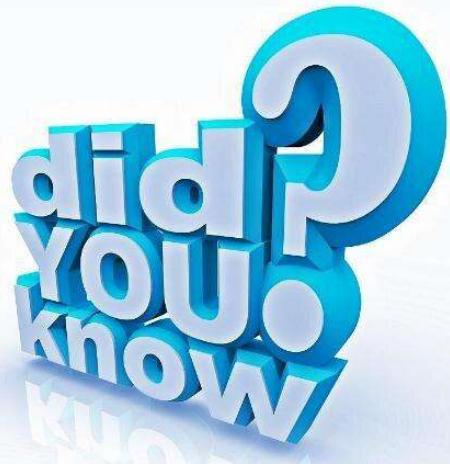


BITCOIN
DIGITAL CURRENCY



CALCULATED.





Bitcoin Account

BALANCE of any **BITCOIN**
address **ISN'T HELD** at
that **ADDRESS**; one **MUST**
RECONSTRUCT it by
looking at the

BALANCE **BLOCKCHAIN**

DARKNET

A SIMPLE GUIDE TO SAFELY AND EFFECTIVELY TUMBLING (MIXING) BITCOINS.

POSTED ON JULY 10, 2015

NEWS

Bitcoin tumbling, also referred to as Bitcoin mixing or Bitcoin laundering, is the process of using a third party service to break the connection between a Bitcoin address sending coins and the address(s) they are sent to. Since the Bitcoin blockchain is a public ledger that records every transaction, mixing coins is critical for anyone who doesn't want the entire world to know exactly where they send and store their BTC, or from where they receive it.



TUTITION 4 ALL



10 Best Bitcoin Tumbler (Mixer) Services – Review 2019



Bitcoin Laundry

BitMix.Biz

BestMixer.io

Bitcoin Blender

CryptoMixer

Bitcoin Fog

Blender.io

MixTum.io



BITCOIN FOG

LONGEST running, most established
BITCOIN MIXER, yet gossips are
they are selectively **SCAMMING**
their users. If you send a high
enough amount to them, you will not
see it again

HOLD YOUR BREATH



**World's first Blockchain satellite
on February 2, 2018**

SpaceChain successfully launches first Blockchain Node into low earth orbit

By News Desk - 02/26/2018



Singapore: SpaceChain launched its first blockchain node into orbit. The satellite was carried by CZ-2D rocket at 3:51 pm local time from Jiuquan Satellite Launch Center in the Gobi desert, China. It was equipped with a Raspberry Pi hardware development board that runs a full-node program on the Qtum blockchain.

This launch could go down in history as the beginning of a new era in privately funded space exploration. There is no doubt that SpaceChain is entering an area that has been nearly inaccessible for most. This decentralized, open source space



<https://www.forbes.com/sites/leonhardweese/2017/08/18/why-one-startups-plan-to-use-satellites-to-beam-bitcoin-data-around-the-world-might-anger-china/#2528f8f11a88>



Blockstream

Broadcasts real-time Bitcoin Blockchain data from a group of communication satellites in space to ALMOST EVERYONE ON THE PLANET

**Enables further participation in
Bitcoin, including the billions of
people in the world **WITHOUT
INTERNET ACCESS****



**Access to people in places
where **BANDWIDTH**
PRICES/SPEED make
participating cost prohibitive**



chal e ga

Blockstream Launches 5th Satellite Streaming Bitcoin Blockchain From Space

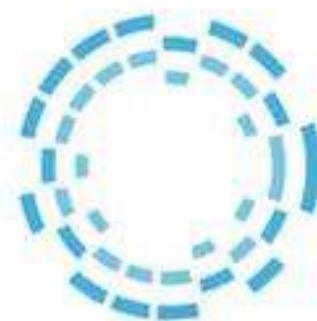
12444 Total views

353 Total shares

Listen to article



2:07



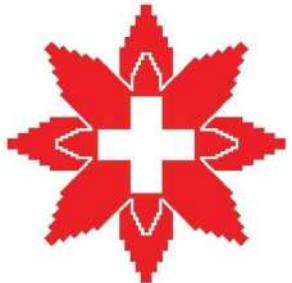
Blockstream





JUST NOT BITCOIN

Community-based space platform that is integrating **BLOCKCHAIN+SPACE** to lower barriers of entry to space and promote collaboration within the space community



* switzerland



Japan



SOUTH
AMERICA



DANMARK



KYRGYZSTAN

USA

Uzbekistan



Russia

China Lifts Bitcoin Ban; Individuals and Businesses Can Now Own Cryptocurrencies Legally

By Bada Adedamola - November 8, 2018
Last Updated: November 9, 2018 at 6:58 PM EST



DOUBTFUL



Japan

Since 1643...
Organized crimes



Japan Penalizes Crypto Exchanges - Yakuza Involvement Confirmed

The Japanese regulator has issued business improvement orders to six of the country's 16 fully-licensed crypto exchanges including Bitflyer, Quoine, and Tech Bureau. The agency confirmed to news.Bitcoin.com that at least one of the six exchanges has some form of involvement with the Yakuza. Responding to the improvement order, Bitflyer has halted new account registrations.

Headache



FORENSICS

DIGITAL SCI

INVESTIGATE GATHERING EVIDENCE

CRIME

SCIENTIFIC ARTS

LIFE DETERMINATION

TIMES ANTHROPOLOGY

ZATION DICTIONARIES DIVERSE

RECOGNITION INVOLVE ACCELERANT

EXTERNAL SHOEPRINTS

EXPLOSIONS KNOWN

DETERMINE IMPORTANT CIVIL

APPROACH EFFICIENCY

PATTERNS POTENTIAL

MATTERS

PSYCHOLOGY CIRCUMSTANCES

EXAMINATIONS

PETROLEUM

BEHAVIORAL

SPECIALISTS

CONCERN

EVALUATION

THEORETICAL

COMPUTING

OSTEOLOGY

SOLUTIONS

EXAMINING

DEALS

SUSPECTS

PATHOLOGY

PROCESSES

PRODUCTS

TYPICALLY

ORDER

CELESTIAL

GENERATE

TEST

ORGANISMS

UNIVERSITY

OPTOMETRY

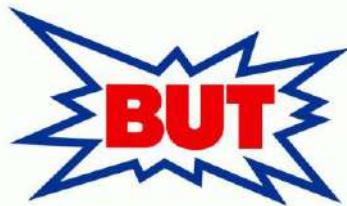
LINGUISTICS

ORGANISMS

**Currently
Not Available**



Software Tools



**COMING
SOON!**

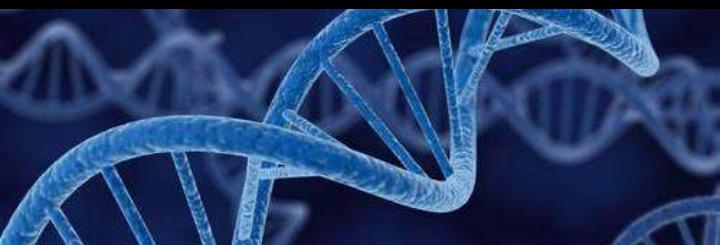




bitcoin is FORENSICK!!



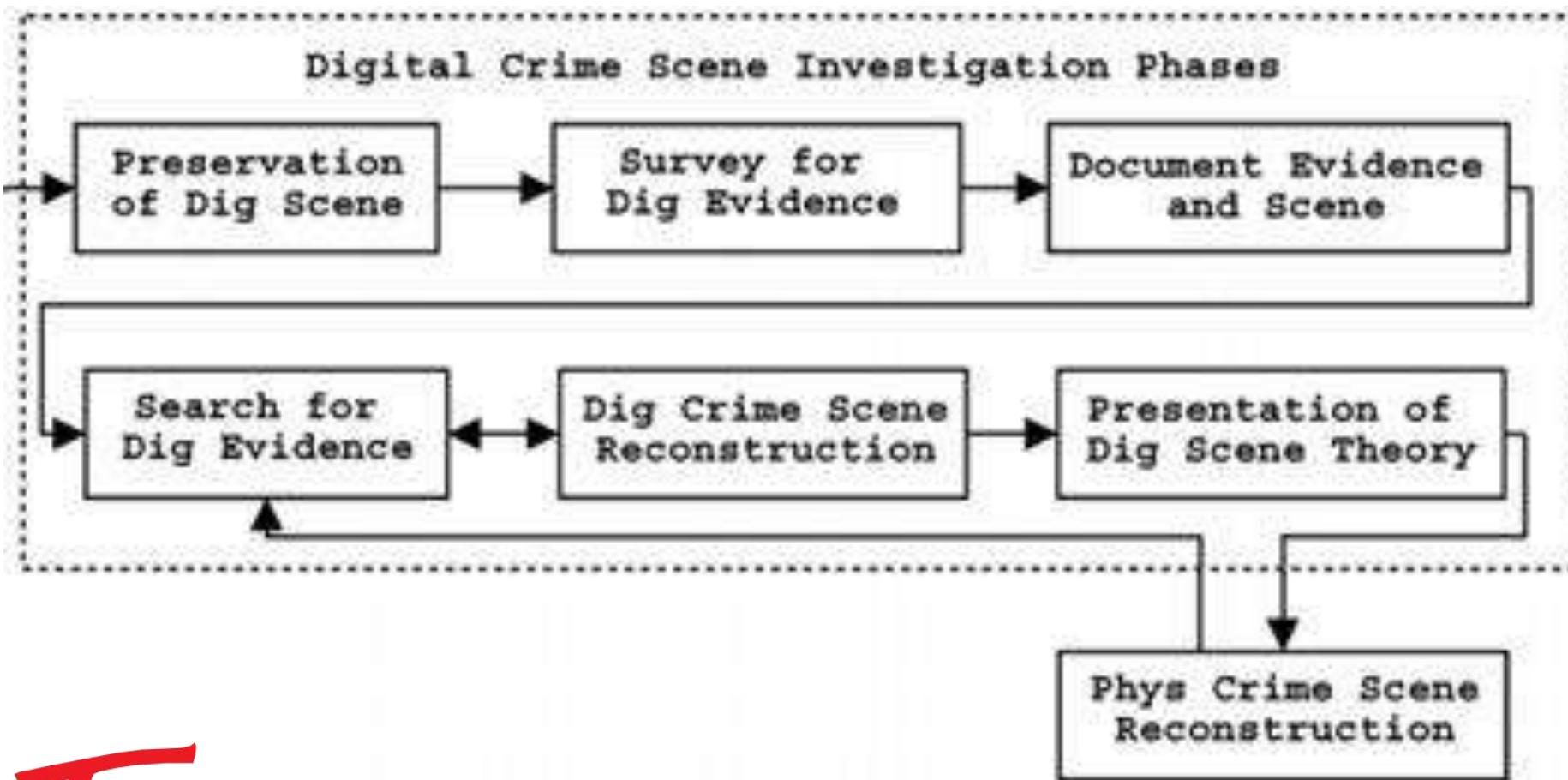
But Keep Calm & Trust Forensics



By : ANUPAM TIWARI

EMAIL: anupamtiwari@protonmail.com

BITCOIN ARTIFACTS



True
BASIC[®] stand

History Network



Everyone on the NETWORK knows about a TRANSACTION and THE HISTORY OF A TRANSACTION can be TRACED BACK to the point where the BITCOINS were produced





Secure

<https://blockexplorer.com>

Secure | <https://blockexplorer.com/blocks>

do bitcoin transa [Satoshi's](#) A Forensic Look at Bit [How bitcoin mining works](#) [what is Proof of Work](#) [Explainer](#)

Bitcoin Blocks Status *Search for block, transaction or address*


Blocks mined on:
2017-02-22 UTC 
Today

Blocks by date.

Height	Timestamp
454170	Feb 22, 2017 5:20:12 PM
454169	Feb 22, 2017 5:15:42 PM
454168	Feb 22, 2017 4:59:36 PM
454167	Feb 22, 2017 4:54:47 PM
454166	Feb 22, 2017 4:54:21 PM
454165	Feb 22, 2017 4:44:35 PM
454164	Feb 22, 2017 4:36:51 PM
454163	Feb 22, 2017 4:23:56 PM

Conduct a
SEARCH based
on **BLOCK
NUMBER,**
ADDRESS,
BLOCK HASH,
**TRANSACTION
HASH** or
PUBLIC KEY



Block #486639

Summary

Number Of Transactions 114

Output Total 280.16081729 BTC

Estimated Transaction Volume 9.20195291 BTC

Transaction Fees 0.01014514 BTC

Height [486639 \(Main Chain\)](#)

Timestamp 2017-09-23 15:36:19

Received Time 2017-09-23 15:36:19

Relayed By [Bixin](#)

Difficulty 1,103,400,932,964.29

Bits 402718488

Size 47.435 kB

Hashes

Hash 00000000000000000000000000000000cbbcffd1d3eb363485f7f2d51464e045edefef730c20e40

Previous Block 000000000000000000000000a27d02b6d05dca6eeef0414705a8289ff98ab75219629de

Next Block(s)

Merkle Root 0b4d74832afc7df3e5872209768c1a90e8dd6478d4bd307a41cf727bcb2e5d28

Bitcoin GAMES

✓ 7 GAMES

✓ HUGE JACKPOTS

✓ INSTANT PAYOUT

✓ NO REGISTRATION

99% Or Better Expected Return

100% WIN RATE | 100% FAIR | 100% SECURE

Blockchain Luxembourg S.A.R.L (LU) | https://blockchain.info/ip-log

Quillpad - Typing in In... Your download should... http://192.168.56.1/ow...

Bitcoin Nodes Log List of bitcoin nodes blockchain.info has connected to in the past.

Total Unique Ip Addresses: 29,627

Ip Address or Hostname

IP	Port	Last Connected	Location	Hostname
139.99.131.171	8333	2017-08-24 17:44:34	AU (Sydney)	ns537674.ip-139-99-131.net
65.96.105.154	8333	2017-08-24 17:44:33	US (Canton)	c-65-96-105-154.hsd1.ct.comcast.net
96.244.205.42	8333	2017-08-24 17:44:29	US (Bel Air)	pool-96-244-205-42.bltmmd.fios.verizon.net



SOURCE : <https://blockchain.info/ip-log>



search

Bitcoin Charts & Graphs × bitcoin EXPLORER SEARCH × Bitcoin Nodes Log ×

Blockchain Luxembourg S.A.R.L [LU] | <https://blockchain.info/ip-log>

Apps Bookmarks Cloud Forensics bitcoin block anupam Quotes | A-Z Blockchain Demo 2/3 Of All Bitcoins Has IoT on the blockchain A Secure Model of Io education

Bitcoin Nodes Log

List of bitcoin nodes blockchain.info has connected to in the past.

Total Unique Ip Addresses: 29,627

Ip Address or Hostname

IP	Last Connected	Location	Hostname
139.99.131.171	2017-08-24 17:44:34	AU (Sydney)	ns537674.ip-139-99-131.net
65.96.105.154	2017-08-24 17:44:33	US (Canton)	c-65-96-105-154.hsd1.ct.comcast.net
96.244.205.42	2017-08-24	US (Bel Air)	pool.96-244-205-42.bltmmd.fios.verizon.net

A large, stylized orange and white logo resembling a dollar sign (\$) or a Bitcoin symbol is positioned on the left side of the screen, partially cut off by the frame.

Bitcoin-Qt

Version v0.8.6-beta

© 2009-2013 The Bitcoin developers

one



Loading block index...

File Settings Help

Overview

Send

Receive

Transactions

Balances

Available: 0.00000000 B

Pending: 0.00000000 B

Total: 0.00000000

Recent transactions

Synchronizing with network...

4 years and 26 weeks behind

Synchronizing with network...

4 years and 39 weeks behind

Synchronizing with network...

4 years and 40 weeks behind

Synchronizing with network...

5 years and 0 weeks behind

Synchronizing with network...

5 years and 0 weeks behind

BTC



elBox

windows_blockchain [Running] - Oracle VM VirtualBox

Bitcoin Core - Wallet

File Settings Help

Overview Send Receive Transactions

Balances Available Pending Total:

Recent transactions

! Recent transactions may not yet be visible, and therefore your wallet's balance might be incorrect. This information will be correct once your wallet has finished synchronizing with the bitcoin network, as detailed below.

Attempting to spend bitcoins that are affected by not-yet-displayed transactions will not be accepted by the network.

Number of blocks left 233698

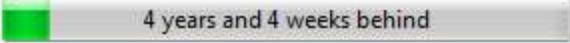
Last block time Tue Aug 13 21:15:50 2013

Progress 8.61% 

Progress increase per hour 0.40%

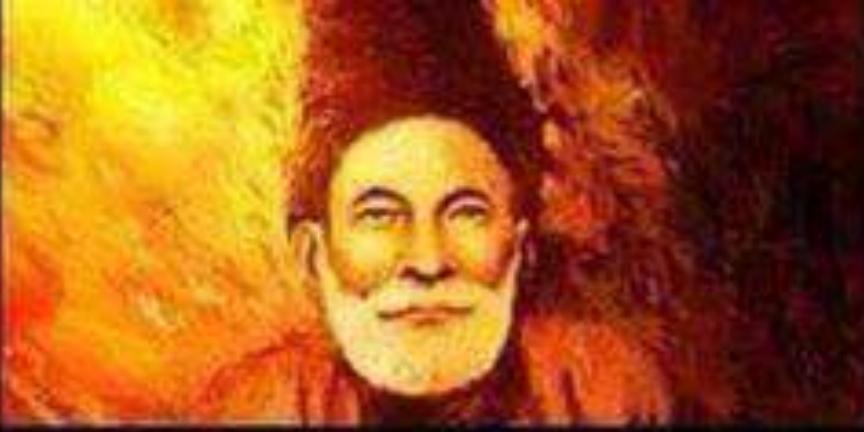
Estimated time left until synced 9 days

Hide

Synchronizing with network...  4 years and 4 weeks behind

BTC HD 

FORENSIC INVESTIGATOR



किसी ने गालिब से पूछा....

" कैसे हो ? "

गालिब ने हँसकर कहा ;-

" जिंदगी में गम है " ...

" गम में दर्द है "

" दर्द में मज़ा है "

और मजे में "हम" है। "

**CRIMINAL
FORENSIC
INVESTIGATOR**

**NOBODY CARES,
WORK HARDER.**

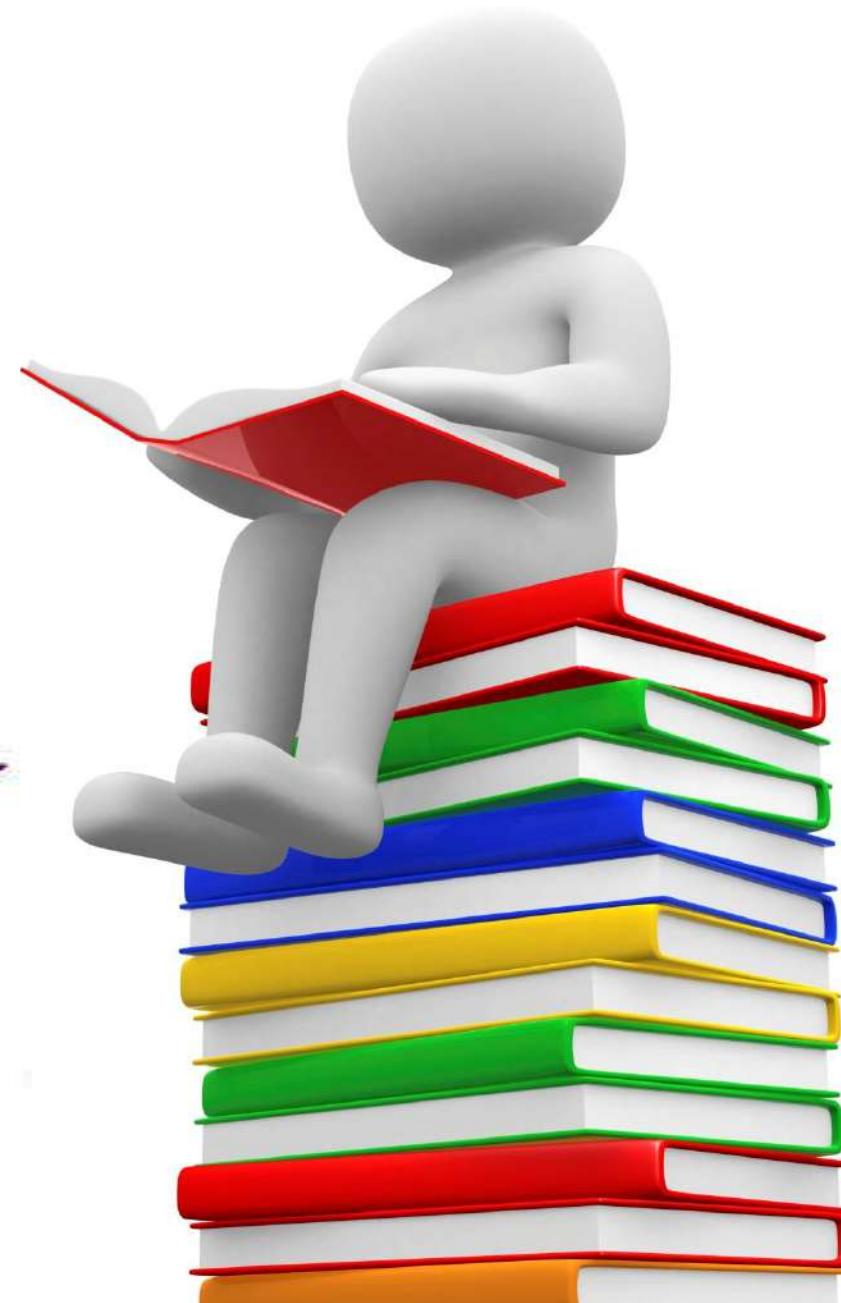
**PROBLEM BATANA
ASAAN HAI....**

It's EASY!



Never
stop
learning

SOLUTION



**DIG DEEP IN THE
TECHNOLOGY &
PRODUCE
EXPERTS**



....NOT just BUY TOOLS

H₄O₁P₃E₁

Largest Bitcoin Mixing Service Down

By Richard - July 27, 2017

The news that Bitmixer.io, the Bitcoin

Sudden Bitmixer Shutdown a Red Flag for Bitcoin 'Anonymity'

1460 Views

July 25, 2017 by Jon Southurst – 8 Comments

One of the oldest and most popular Bitcoin "mixing" services, Bitmixer, has announced it's shutting operations. While operators were vague on reasons, it appears they may be spooked by recent law enforcement activity against dark net marketplaces

BUSINESS GUEST

BitMixer shuts down to 'make Bitcoin ecosystem more clean'

RUPERT HACKETT, BUYABITCOIN.COM.AU | @RUPERTH | JULY 25, 2017 5:05 PM



World's Largest Bitcoin Tumbling Announces Sudden Shutdown

20152 Total views

Crypto
Popular Bitcoin Mixing Service Bitmixer.io Shuts Down Immediately
Bitmixer.io Shuts Down Immediately

July 25, 2017

Crypto, News

Off-The-Shelf Software



Numisight



Bitcoin is a highly interconnected network of transactions.

Numisight gives you the tools you need to view
the forest, the trees, and all the levels of detail in between.

[Download the Public Alpha](#)

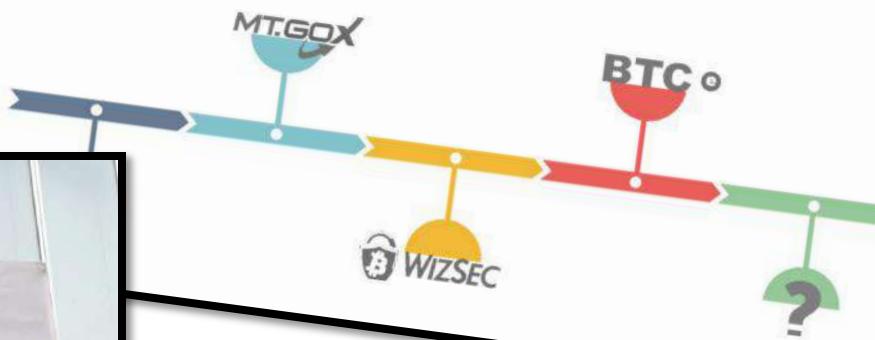


bloq



CHAINALYSIS

MtGox, BTC-e, and the Missing Coins: A living timeline of the greatest cyber crime ever



New “Know-Your-Transaction” Tool Enables Enhanced Blockchain Investigation



bitcoin





elliptic



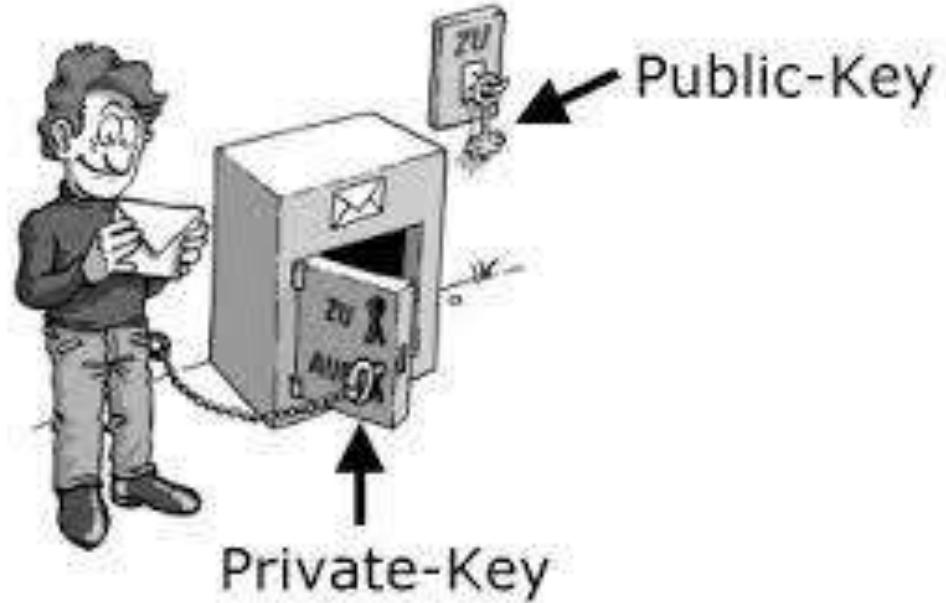
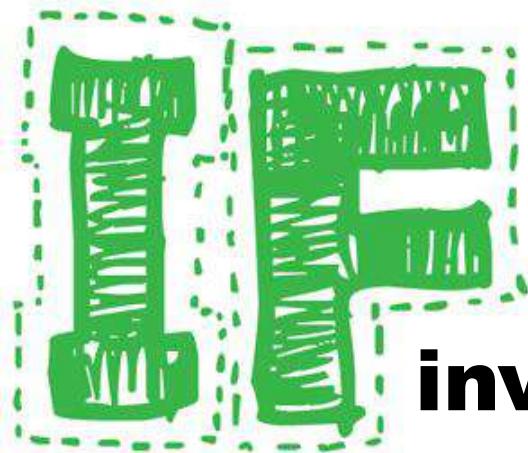
BLOCKCYPHER



PROJECT TITANIUM : Main thrust of the European Union's Titanium Project is to *Monitor blockchains, deanonymize wallet addresses, surveil dark net markets, and block terrorists and money launderers.* TITANIUM, which stands for **T**ools for the **I**nvestigation of **T**ransactions in **U**nderground Markets

ADVANCES IN MAPPING TRACE





**investigator has the Bitcoin
Private key of the suspect, they can
search for that particular key on the
Blockchain to Trace the purchases
to other potential Suspects.**

Hijacking Bitcoin: Routing Attacks on Cryptocurrencies

<https://btc-hijack.ethz.ch>

Maria Apostolaki
ETH Zürich
apmaria@ethz.ch

Aviv Zohar
The Hebrew University
avivz@cs.huji.ac.il

Laurent Vanbever
ETH Zürich
lvanbever@ethz.ch



Attacking Bitcoin via the Internet infrastructure using routing attacks

As Bitcoin connections are routed over the Internet—in clear text and without integrity checks—any third-party can eavesdrop, drop, modify, inject, or delay Bitcoin messages

Border Gateway Protocol
(BGP)

Detecting such attackers is CHALLENGING
any day

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Forensic Look at Bitcoin Cryptocurrency

The increased use of cryptocurrencies such as Bitcoin among private users and some businesses has opened a new avenue of research in the field of digital forensics involving cryptocurrencies. Since the creation of Bitcoin in 2008, cryptocurrencies have begun to make a presence in the world of ecommerce. Cryptography serves as the underlying foundation for Bitcoin, which gives it the benefits of confidentiality, integrity, nonrepudiation and authentication. Having been designed and built upon the foundation of the...



pro-
substantia
research paper
critical think
d in

BITCOIN FORENSIC ARTIFACT EXAMINATION



SOFTWARE
HARDWARE

The background of the text is composed of a grid of binary digits (0s and 1s) in various colors, including black, white, blue, green, red, and yellow, creating a digital or data-oriented visual texture.

Windows 7 Professional

Multibit

Bitcoin-Qt

Bitminter

Basic USB ASIC Bitcoin

Gateway laptop ML6720

120 GB WD hard drive

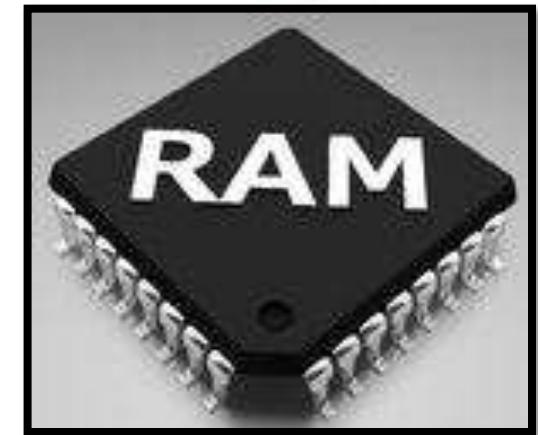
(4) USB ASIC Mining drives

USB powered cooling fan

32 GB USB thumb drive

COLLECTION OF BITCOIN ARTIFACTS

- **System Info**
- **Info about Logged users**
- **Registry Info**
- **Remnants of Chats**
- **Web browsing Activities**
- **Recent Communications**
- **Info from Cloud Services**
- **Decryption Keys for encrypted volumes mounted**



Sarah Meiklejohn, a Bitcoin focused Computer Researcher



Extensive Research in Bitcoin Blockchain

pre-substantive
research paper
critical thinking
air

Utilizing the data from

344

transactions,
Meiklejohn able to
identify the owners of
more than a million
Bitcoin addresses

**Found that by looking
blockchain an
investigator can
uncover who owns a
Bitcoin addresses**

2015

Bitcoin over Tor isn't a good idea

Alex Biryukov

University of Luxembourg

Email: alex.biryukov@uni.lu

Ivan Pustogarov

University of Luxembourg

Email: ivan.pustogarov@uni.lu

*"In this paper we show that combining **TOR** and **BITCOIN** creates an **ATTACK VECTOR** for the stealthy man-in-the-middle attacks. A **LOW-RESOURCE ATTACKER** gain **FULL CONTROL** of information flows between all users who chose to use Bitcoin over **TOR**. In particular the attacker **CAN LINK TOGETHER** USER'S **TRANSACTIONS** regardless of pseudonyms used"*

COLLECTION OF BITCOIN ARTIFACTS

Bitcoin transactions occur via a Network Connection, an investigator should seize any Physical Object that can connect to the Internet in addition to the hard drive





Find, Organize, & Analyze Computer Evidence

ACCESSIONDATA

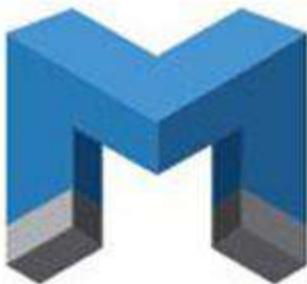
FTK™

FORENSIC TOOLKIT™

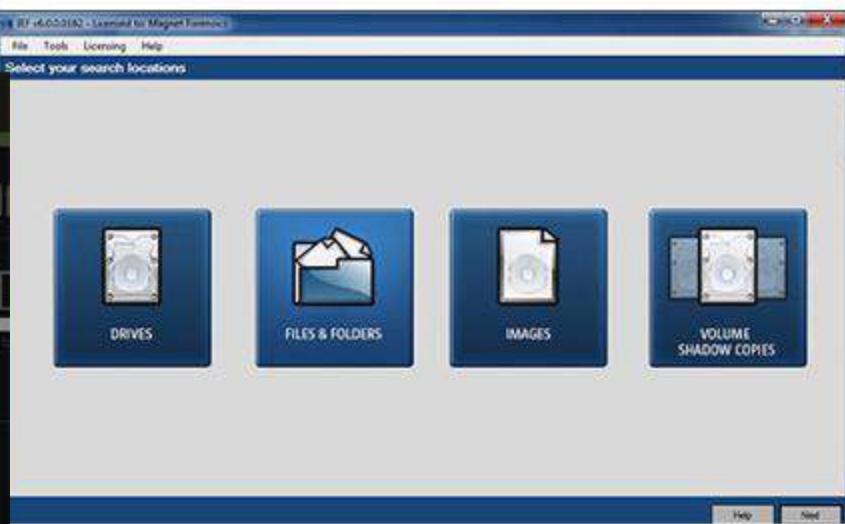
[FTK Install](#)

[Distributed Engine](#) [View Readme](#)

[View User Guide](#) [Other Products](#)



INTERNET EVIDENCE FINDER™



GDPR Threatens to Impair Cryptocurrency Crime Investigations



General Data
Protection Regulation

<https://whois.icann.org/en>

BLOCKCHAIN

WHERE
TO
START
?

Read the “**SATOSHI PAPER**”

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

At the onset of your blockchain journey, though just 9 pages, you will find it hard to understand in the first few reads....DON'T WORRY on this...but just READ and move ahead. Keep reading this paper as you slowly build your concepts ahead.

Getting confused or Not able to understand is the first step to clarity on subject

PRELIMS TO LEARNING BLOCKCHAIN

Don't HURRY UP TO LEARN

Please understand this very **DELIBERATELY** that there is no need to hurry and learn all the blockchain essentials in a hurried manner.

Every thing takes time. Be deliberate to understand nuts and bolts first. Ensure **that you understand** what you **feel you have understood**.



The capacity to learn is a gift; the ability to learn is a skill; the willingness to learn is a choice.

**DON'T TRY TO
UNDERSTAND
EVERYTHING.
SOMETIMES IT IS
NOT MEANT TO BE
UNDERSTOOD,
JUST ACCEPTED.**

PRELIMS TO LEARNING BLOCKCHAIN

GET SAVVY WITH LINUX

While there are few and there will be GUIs platform sooner for performing blockchain operations, **but it is always advised that you learn all the dirty things of CLI and commands** via Linux command interface on TERMINAL. Any flavor of Linux will be ok.



PRELIMS TO LEARNING BLOCKCHAIN

GET SAVVY WITH LINUX

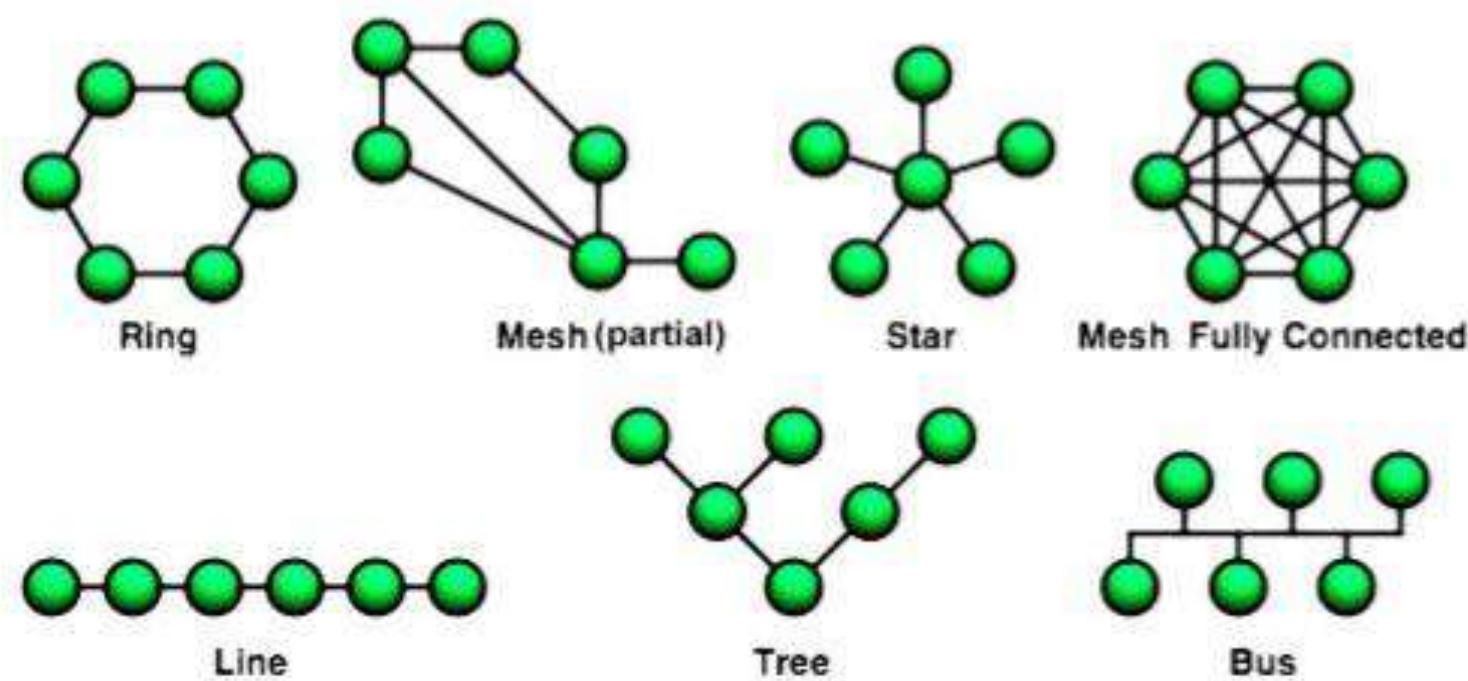
Best way to get hands-on with linux is to install it as a host OS and soon you will get conversant with the essentials. But also remember this is **NOT WITHOUT TEETHING TROUBLES**



PRELIMS TO LEARNING BLOCKCHAIN

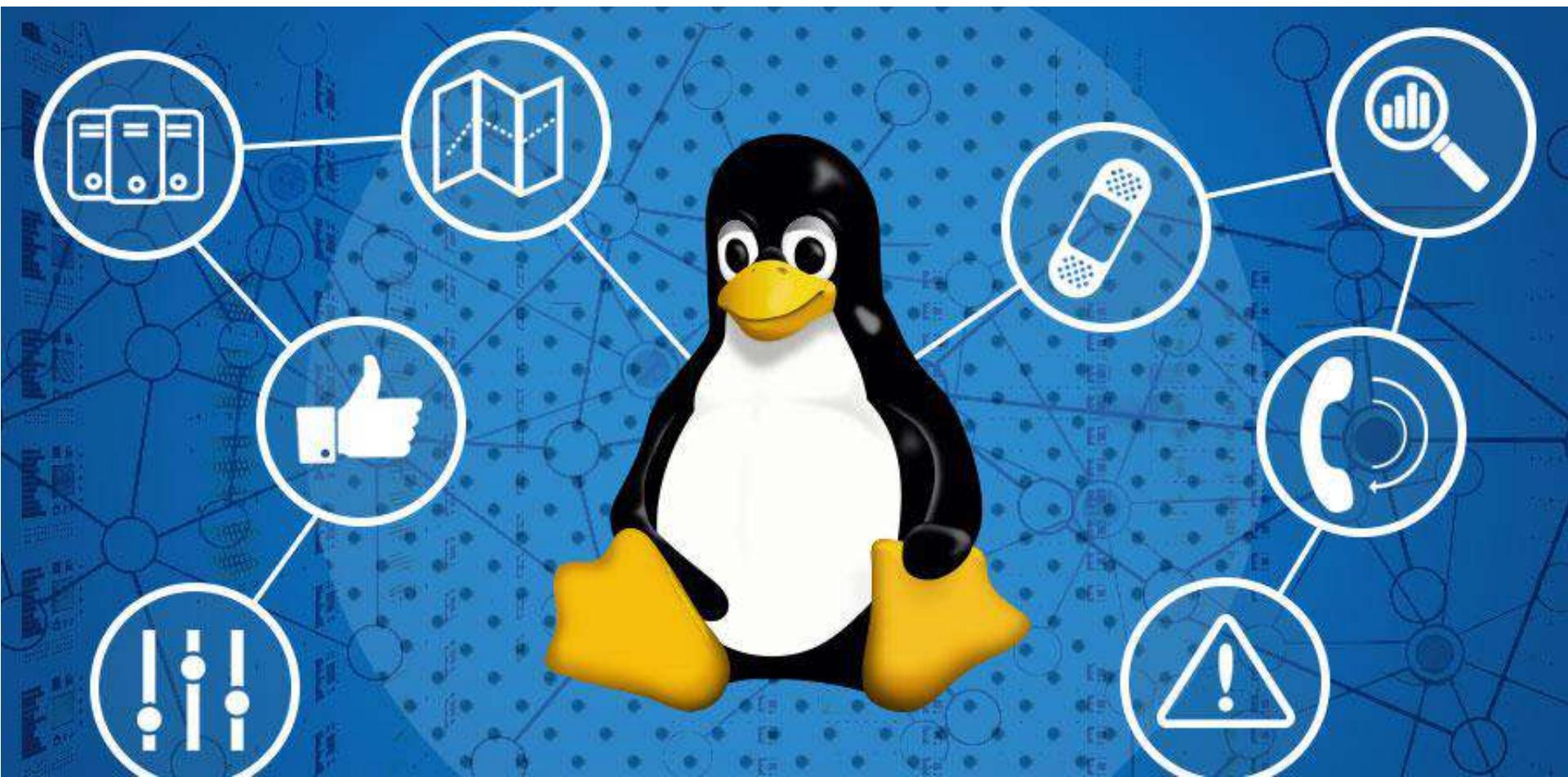
BASIC NETWORKING CONCEPTS

Another **important thing to get absolute clear** will be basic networking which will come handy in creating and configuring machines on a network



PRELIMS TO LEARNING BLOCKCHAIN

BASIC NETWORKING COMMANDS



PRELIMS TO LEARNING BLOCKCHAIN

GET SAVVY WITH SCRIPTING

Scripting here means not deep script programming but you should get savvy with basic **VIM/Vi editor**



PRELIMS TO LEARNING BLOCKCHAIN

CRYPTOGRAPHY & BASIC COMMANDS

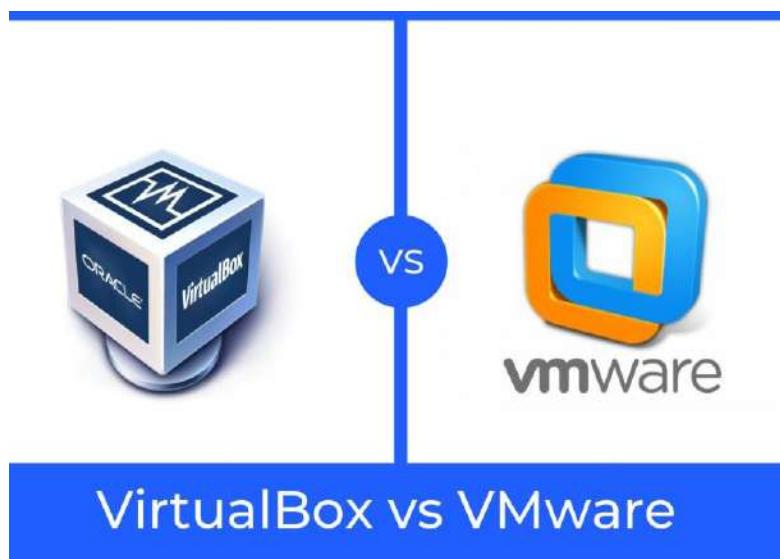
Building further upon **Linux/CLI**, one should get hands dirty with very basic cryptography to begin with. Understand PKI, HASH techniques, encryption and decryption of files, salting, algorithm applications of AES 256, SHA256, ECDSA etc

```
Desktop  Downloads  Pictures  Templates  yeahhub.txt.gpg
Documents  Music  Public  Videos
root@kali:~# gpg yeahhub.txt.gpg ← --- 
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
root@kali:~# ls
Desktop  Downloads  Pictures  Templates  yeahhub.txt
Documents  Music  Public  Videos  yeahhub.txt.gpg
root@kali:~# cat yeahhub.txt
Hello this is a secret text
root@kali:~#
```

PRELIMS TO LEARNING BLOCKCHAIN

USING VIRTUAL MACHINES

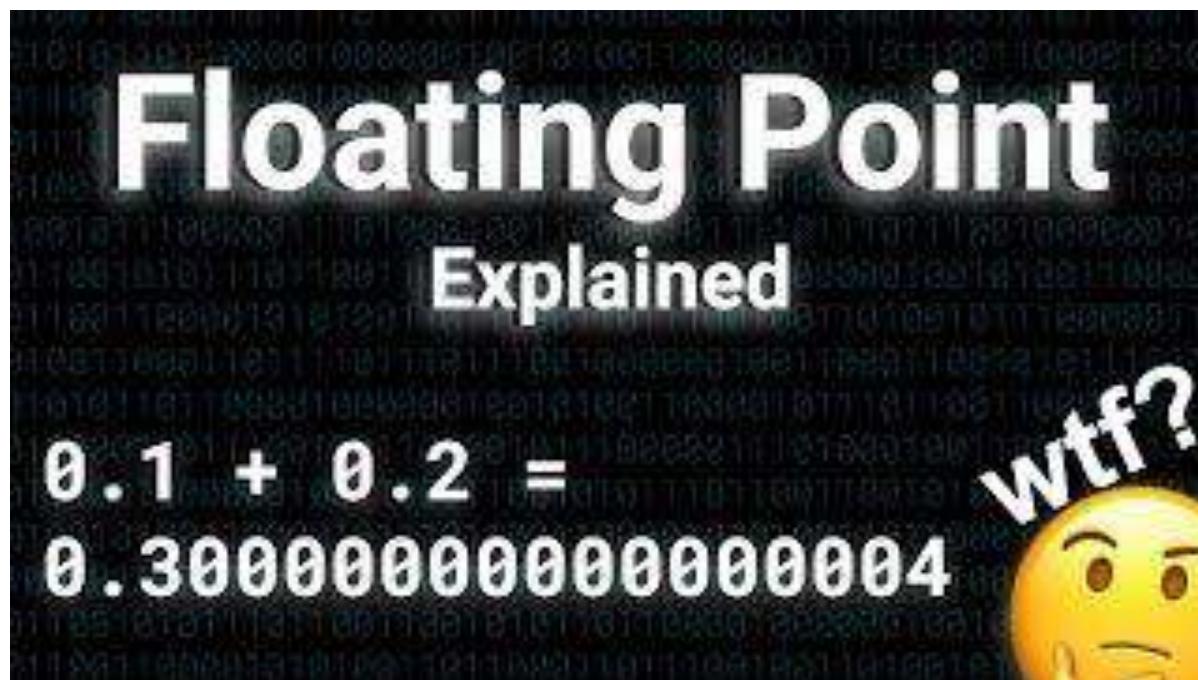
To begin with, getting familiar with VMs will be a big help. Instead of expecting huge IT labs or multiple PCs to simulate P2P nodes on blockchain, VMs will easily facilitate your test benches



PRELIMS TO LEARNING BLOCKCHAIN

BASICS OF FINITE MATHS

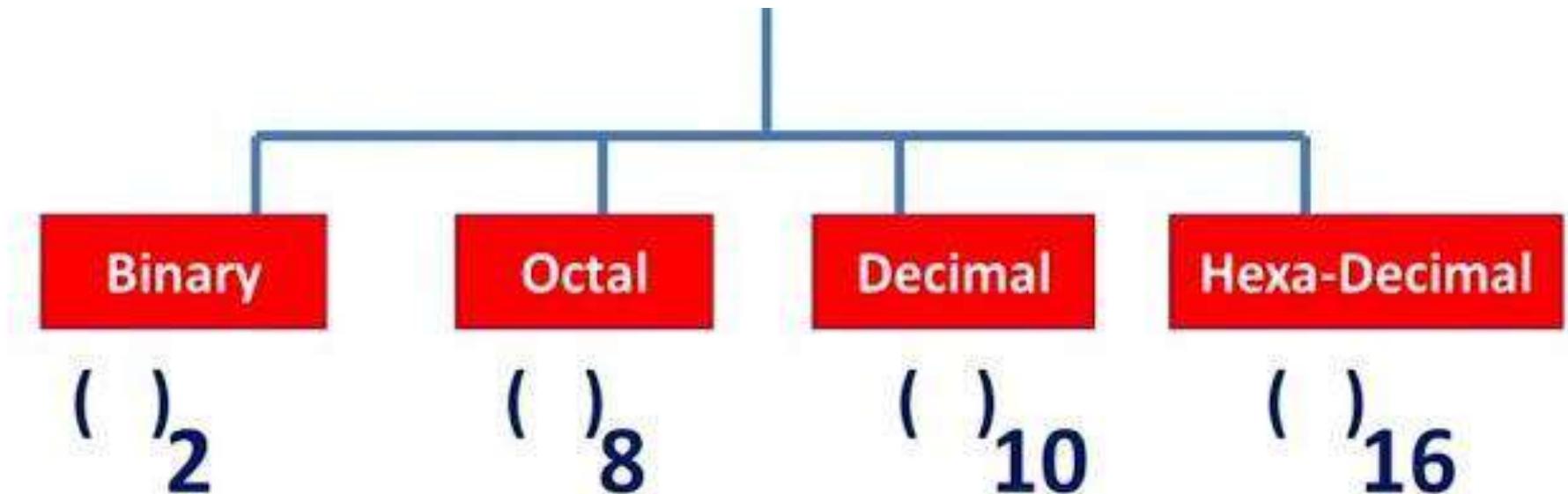
If ever you get a question why learn this subject, just add 0.1+0.2 in python or any computer language and find the reason why the answer is not 0.3 ?



PRELIMS TO LEARNING BLOCKCHAIN

BINARY/OCTA/HEX NUMBER SYSTEMS

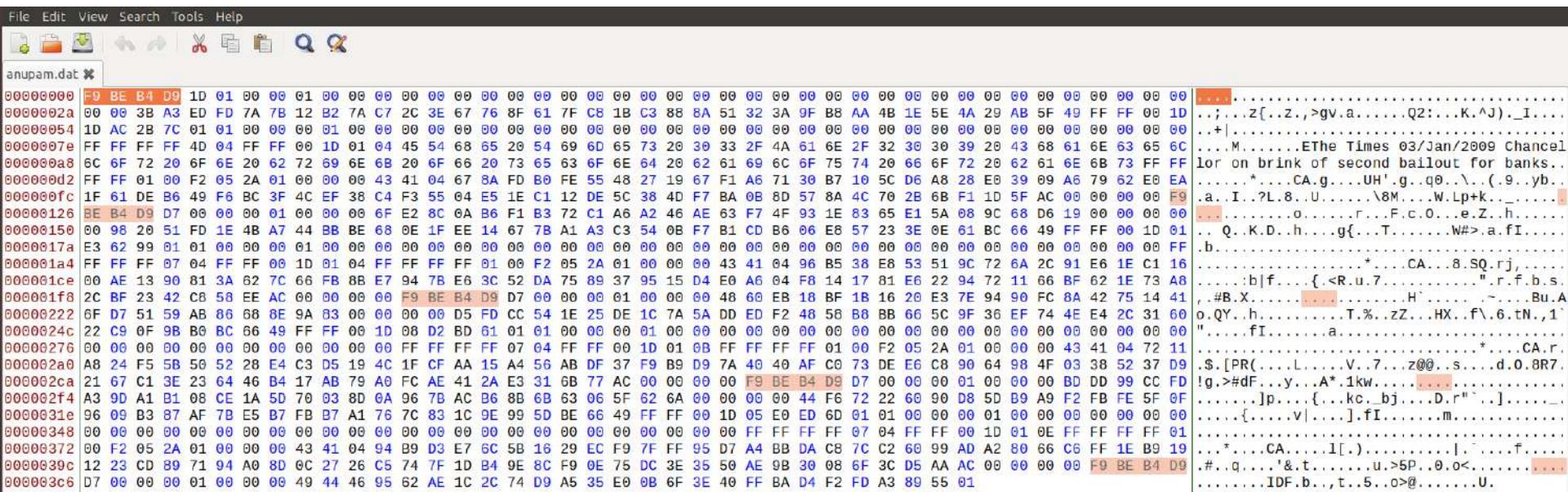
Another absolute must to begin with. As you explore the bitcoin blockchain, you will **realise everything stored on blockchain is in either of these numbering systems.**



PRELIMS TO LEARNING BLOCKCHAIN

UNDERSTANDING HEX EDITORS

While in the beginning ,one jumps inside a typical bitcoin block, **Hex editors** knowledge will be handy in opening and understanding the content



PRELIMS TO LEARNING BLOCKCHAIN

BASIC PYTHON

Another must if you wish to program smart contracts and get playful with **querying blockchain** as you progress in the domain



PRELIMS TO LEARNING BLOCKCHAIN

GOOD MACHINE

A **host OS Ubuntu kind with i3/i5 processor, 16 GB RAM and basic 500 HDD/SSD** will be good to begin and experiment with. This machine can be installed with VMs on which you can create nodes and work to simulate mechanics



PRELIMS TO LEARNING BLOCKCHAIN

KEEP READING GOOD JOURNAL PAPERS & FOLLOW INFORMATIVE BLOGS

Now also keep a watch on what is happening in the research world. At the onset when you read these papers, it is highly likely that you won't understand, but over a period of time as you dwell on internals and practise hands on , you will gradually become conversant with most



PRELIMS TO LEARNING BLOCKCHAIN

YOUTUBE: A SEA OF INFORMATION

Make it a practice to keep watching youtube videos available on blockchain intermittently. Keep noting what you understand, keep exploring what you don't understand, follow up with that you don't understand. 2 Hours daily in parts spread over day....It is again inevitable that you might not understand few, no problem but keep watching

Getting confused or Not able to understand is the first step to clarity on subject

PRELIMS TO LEARNING BLOCKCHAIN

TOOLS & PLATFORM

Lets play with a SIMULATED BLOCKCHAIN



Ganache

*Simulated
Blockchain*



*Kovan Test network
faucets*



Remix IDE is an open
source web and
desktop application



Wallet



MultiChain

This will be one of the easiest platform to create and play with a custom blockchain. Once you are through with basic components as addressed earlier in this slide including Linux, cryptography, CLI commands, Vim, virtual machines etc, this will be an awesome platform to practice

<https://www.multichain.com/developers/>

FEW USEFUL BOOKS



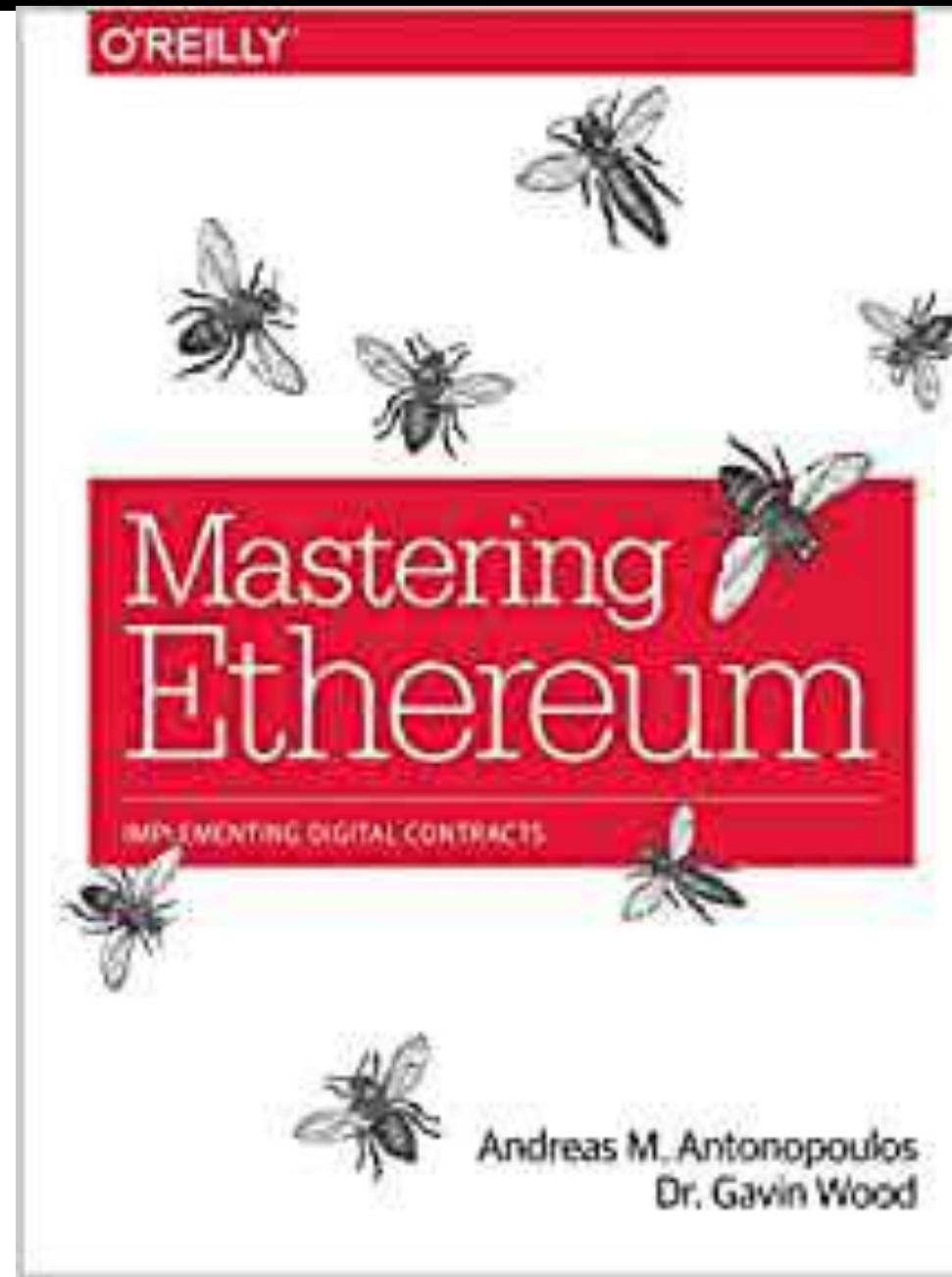
FEW USEFUL BOOKS

The books I have shared ahead it is not expected that you buy all of these together but you may plan to refer them in the beginning in online editions and depending on how you find them you can get them in paperback editions gradually

I AM A **TRADITIONAL BOOK LOVER...& NOT FIND** reading in KINDLE comfortable ...so you can get e-books if you comfortable

FEW USEFUL BOOKS

This book is peculiar to the domain of ethereum only....a good to begin with kind



FEW USEFUL BOOKS

One of my strongly recommended book if you are fresh to this ecosystem of blockchain. I have two books...First and second version. More recently the author has come up with the third edition which is more enriched with content.



FEW USEFUL BOOKS

A very good book to build concepts of blockchain from scratch

Everyday Cryptography

FUNDAMENTAL PRINCIPLES & APPLICATIONS



KEITH MARTIN

FEW USEFUL BOOKS

**Another light reading
on history and present
state of
blockchain eco system**

ATTACK OF THE 50 FOOT BLOCKCHAIN

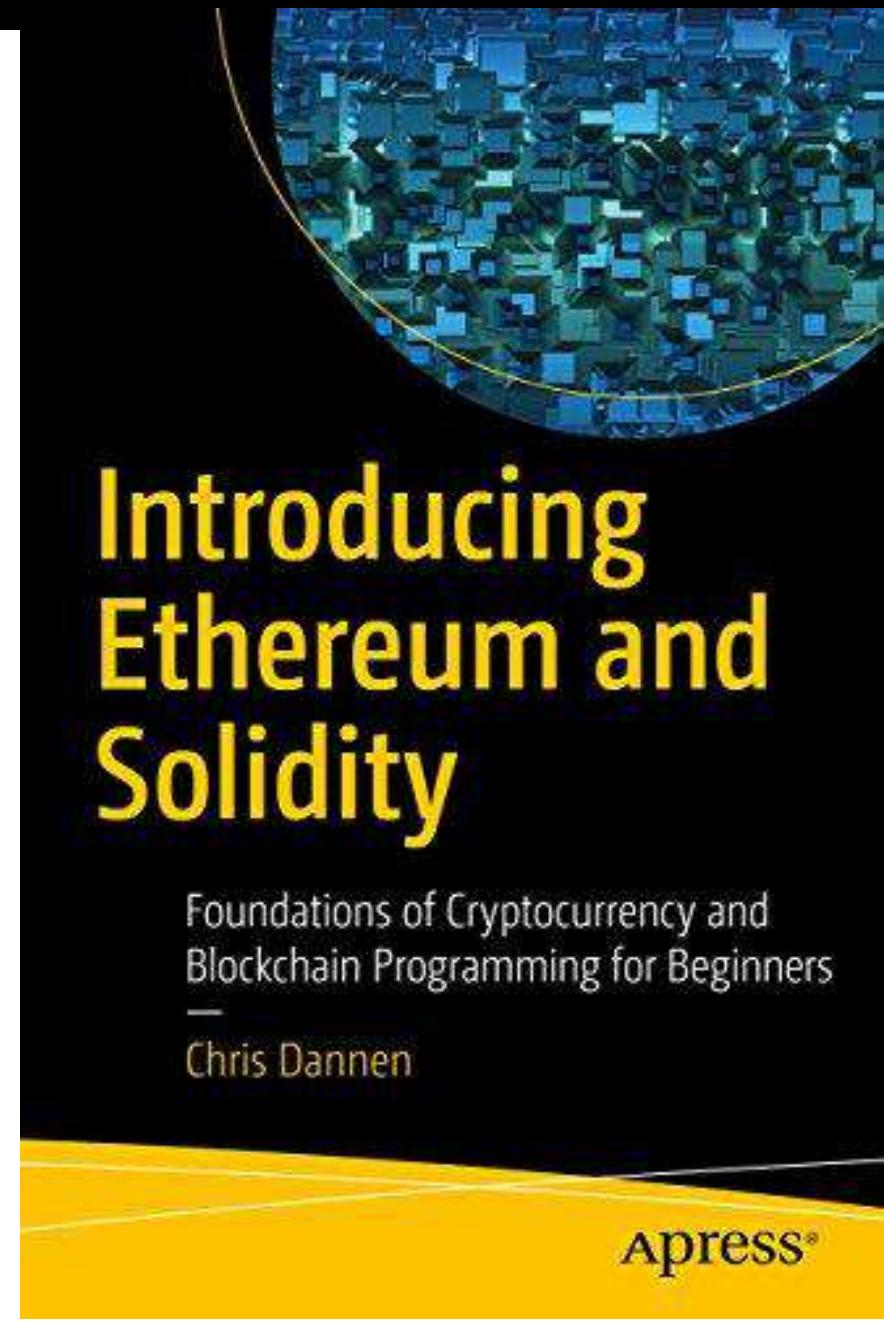


**BITCOIN, BLOCKCHAIN,
ETHEREUM & SMART CONTRACTS**

DAVID GERARD

FEW USEFUL BOOKS

This is
peculiar
to the
domain
of
ethereum
and
smart
contracts



apress®

FEW USEFUL BOOKS

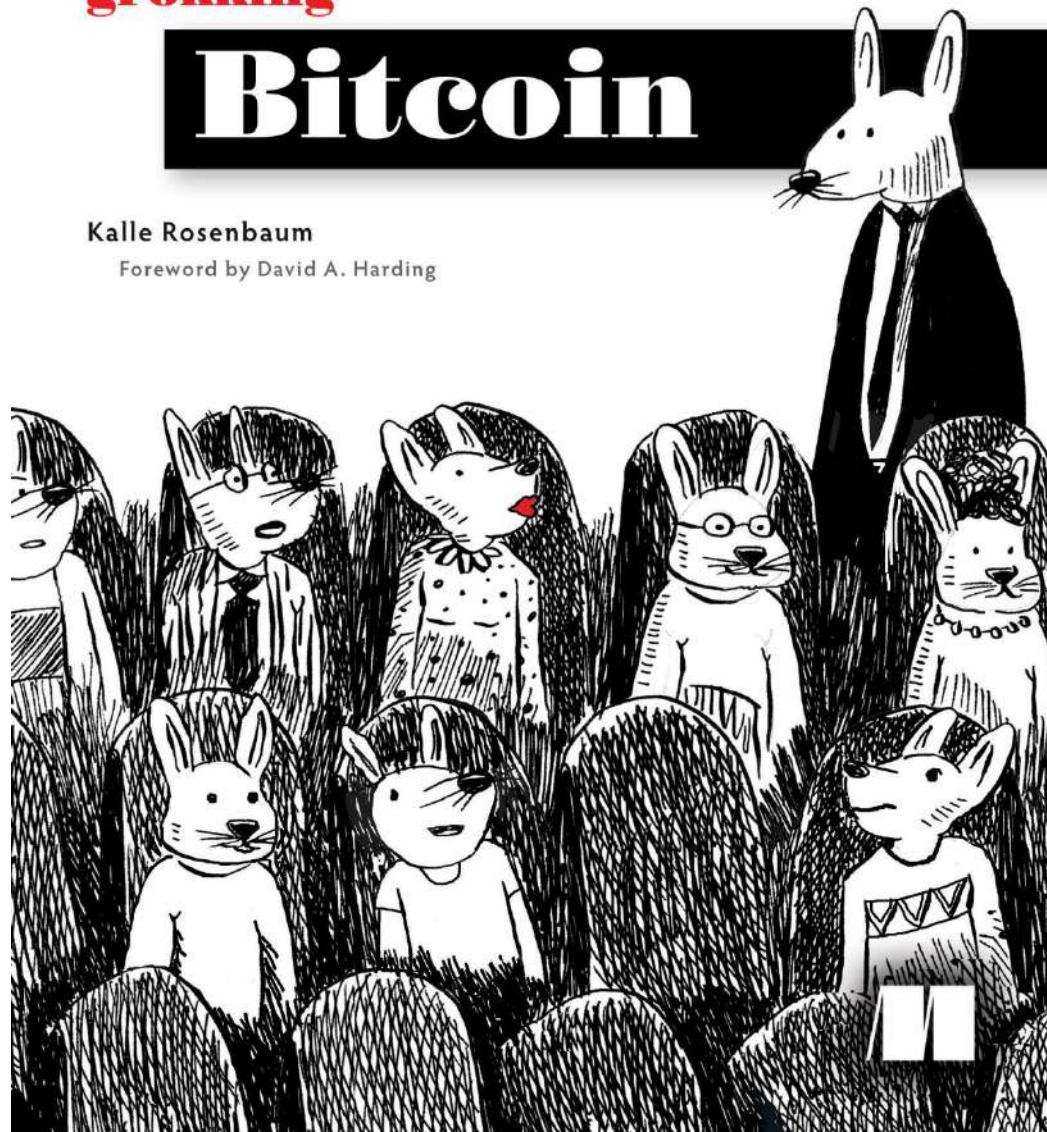
Another truly awesome in-depth bible of internal mechanics of Bitcoin blockchain

grokking

Bitcoin

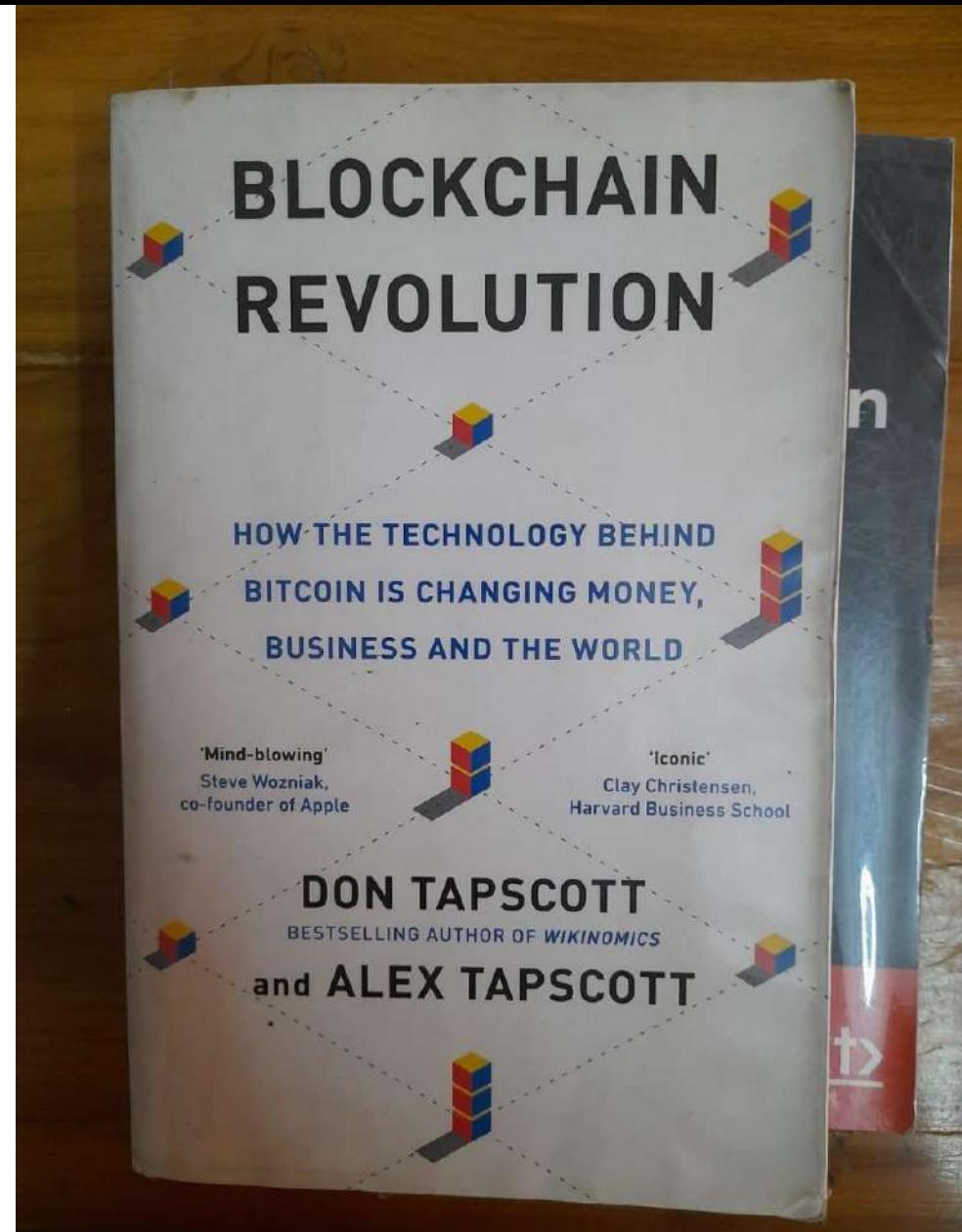
Kalle Rosenbaum

Foreword by David A. Harding



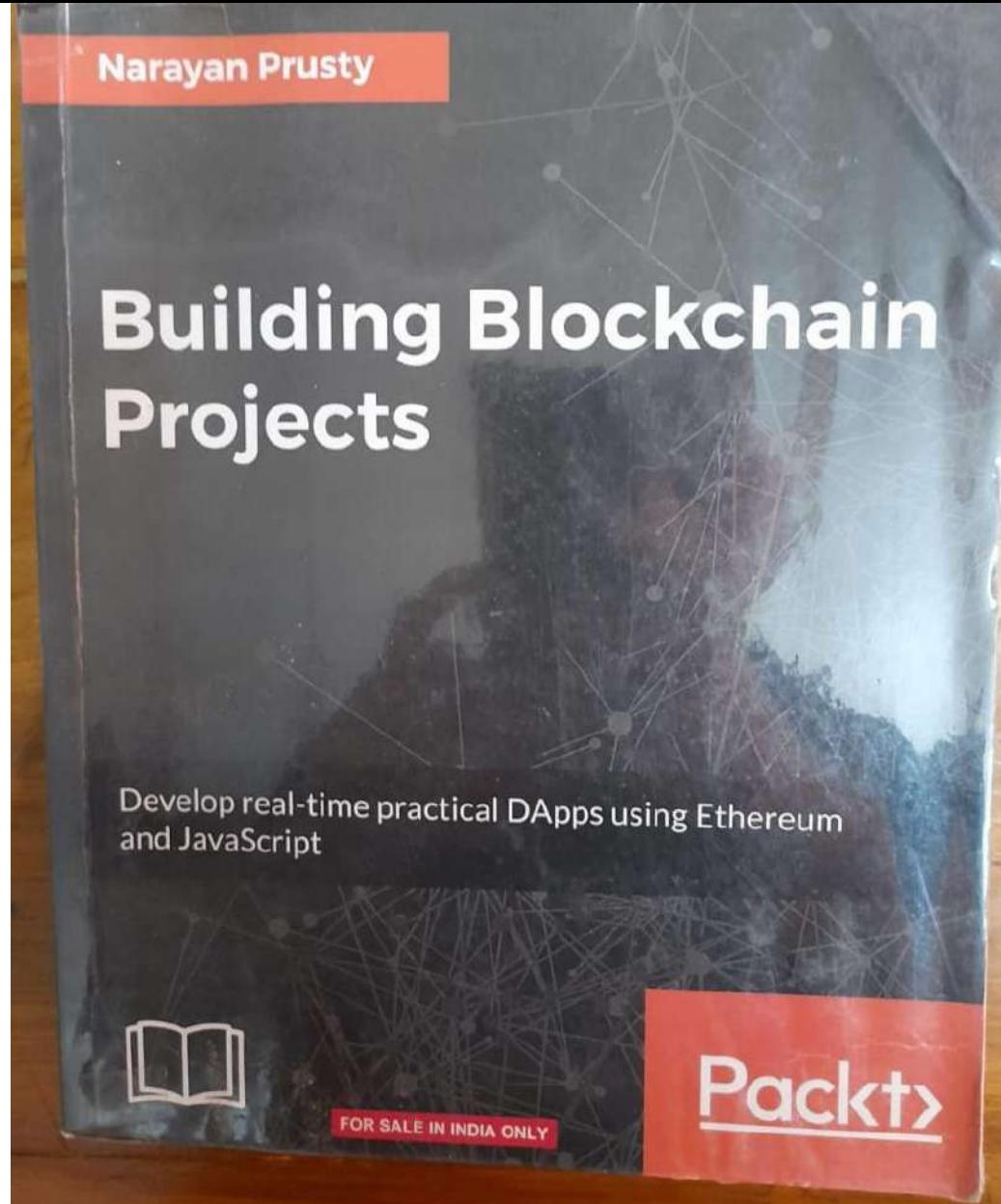
FEW USEFUL BOOKS

**Applications of
Blockchain....a
world renowned
book**



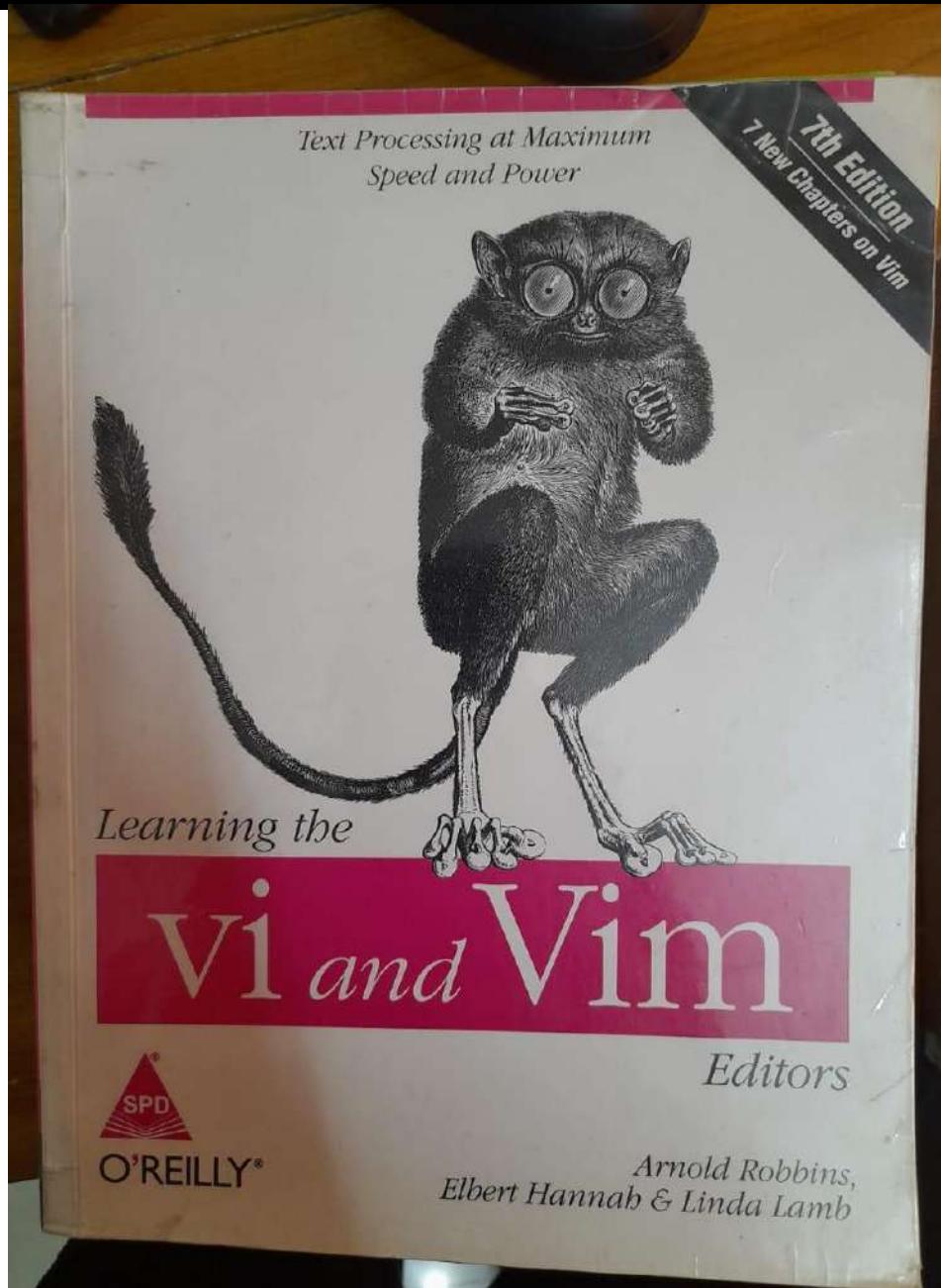
FEW USEFUL BOOKS

**Beginners
world to
basic
blockchain
projects**



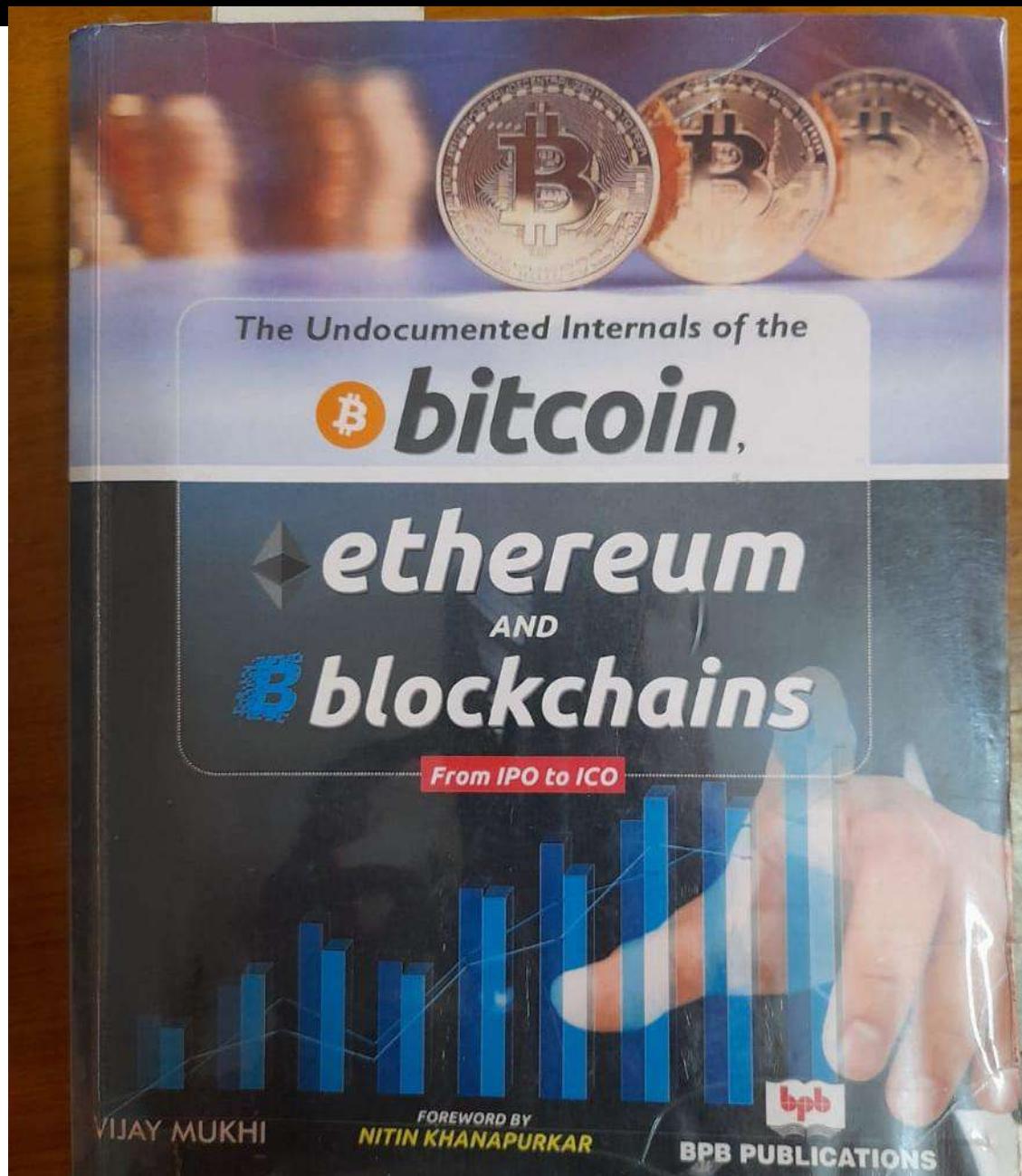
FEW USEFUL BOOKS

**Basic VI and
VIM...will be
helpful in long
run and
routine
configurations
and testing**



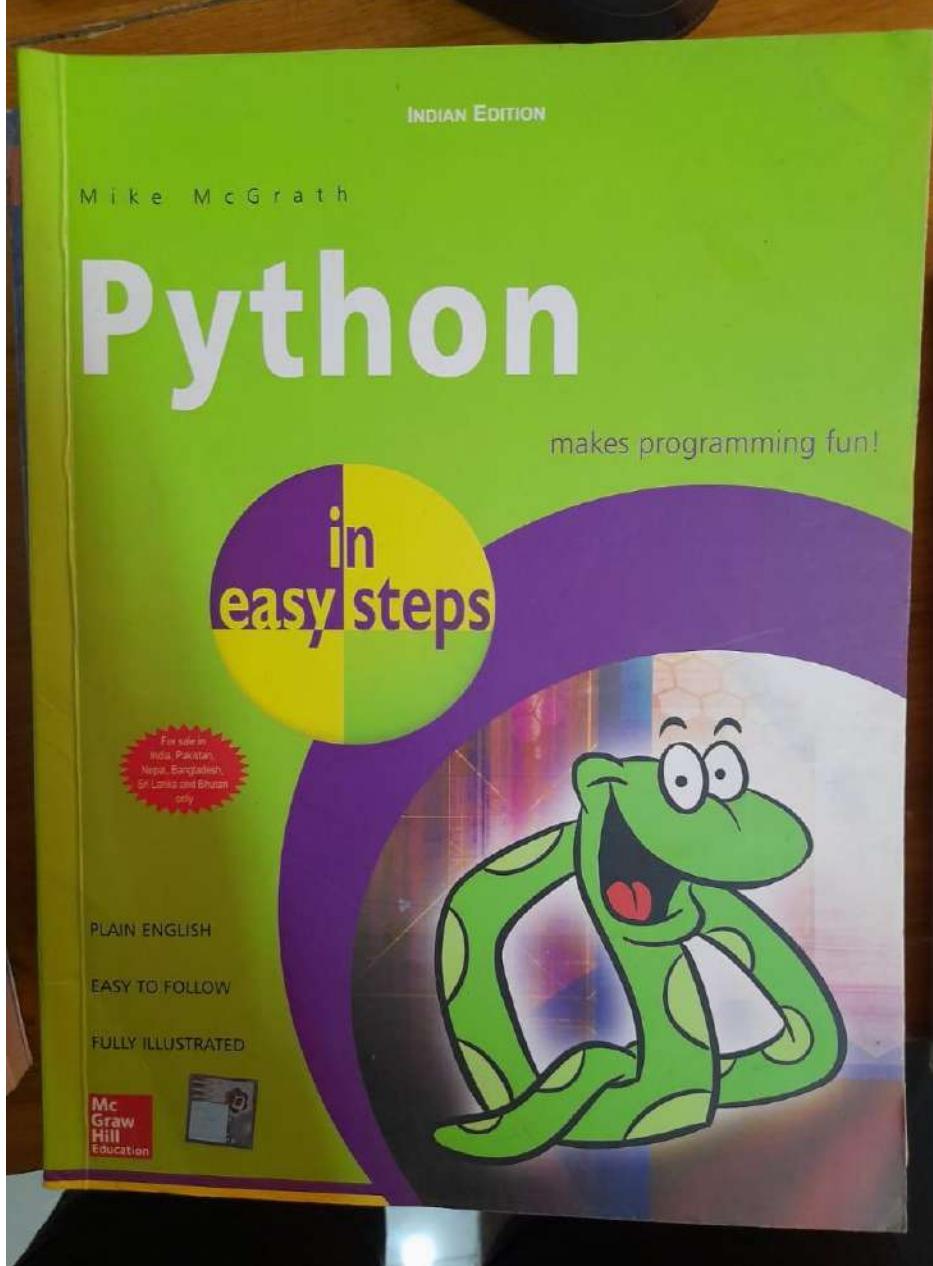
FEW USEFUL BOOKS

One truly awesome in-depth bible of internal mechanics of Bitcoin and Ethereum blockchain



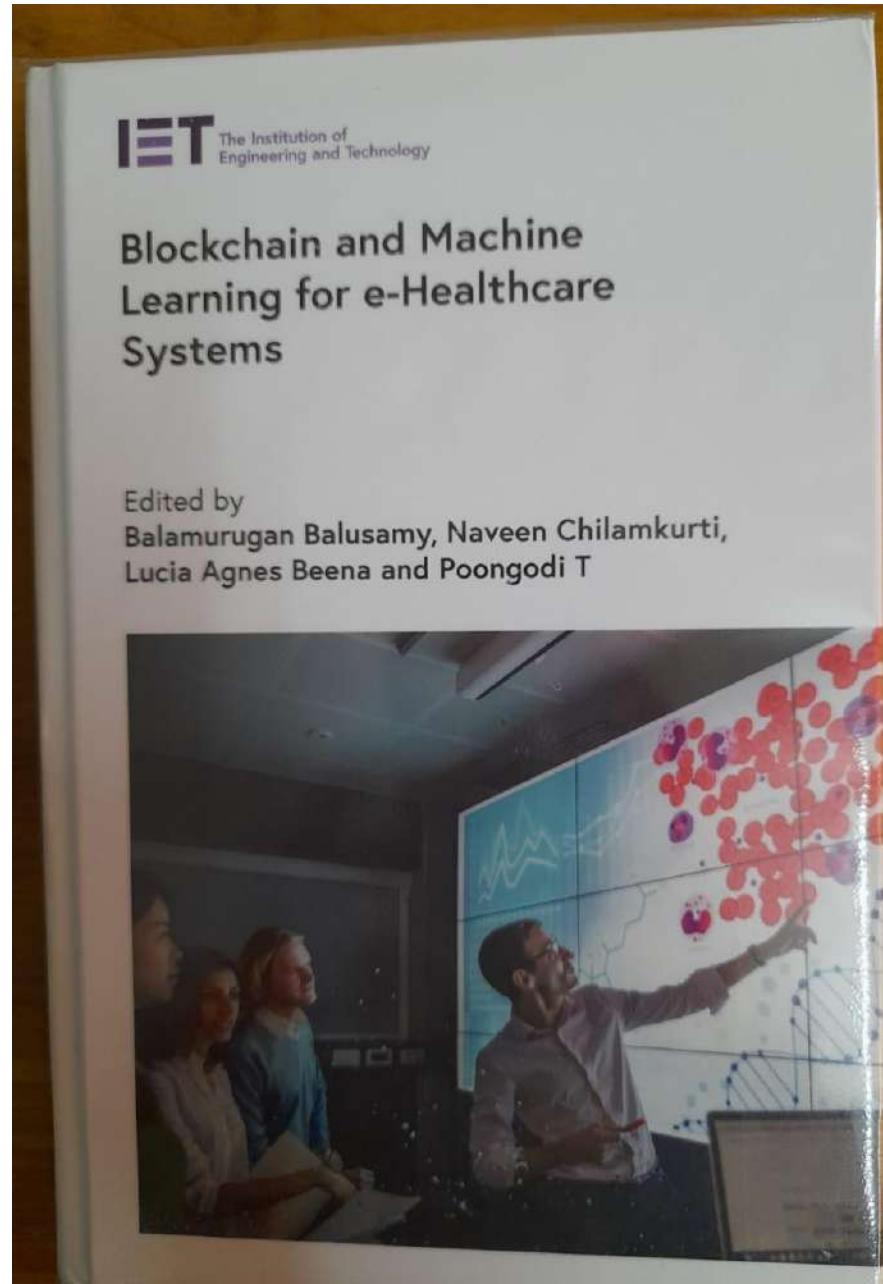
FEW USEFUL BOOKS

**First step
into
Python...**



FEW USEFUL BOOKS

**Recommended ☺
coz this book has
one chapter on
blockchain by me**



FEW USEFUL LINKS

**Sharing few links which are not in any order
of merit or subject but random links I have
pursued and liked over my journey of learning**

FEW USEFUL LINKS

<https://bitcoin.org/bitcoin.pdf>

https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf

<https://anyhash.com/>

<https://prathamudeshmukh.github.io/merkle-tree-demo/>

<https://www.cs.usfca.edu/~galles/visualization/Trie.html>

<https://www.cs.usfca.edu/~galles/visualization/RadixTree.html>

<https://www.blockchain.com/explorer>

<https://explorer.bitcoin.com/btc>

<https://bitcoin.org/en/download>

<https://www.desmos.com/calculator/kkj2efqk5x>

<https://andersbrownworth.com/blockchain/>

<https://andersbrownworth.com/blockchain/public-private-keys/>

FEW USEFUL LINKS

<https://learnmeabitcoin.com/>

<https://www.binaryhexconverter.com/hex-to-decimal-converter>

<https://hackernoon.com/if-we-lived-in-a-bitcoin-future-how-big-would-the-blockchain-have-to-be-bd07b282416f>

<https://www.datadriveninvestor.com/2019/11/21/a-decomposition-of-the-bitcoin-block-header/>

<https://www.scadacore.com/tools/programming-calculators/online-hex-converter/>

<https://www.epochconverter.com/>

<https://www.rapidtables.com/convert/number/hex-to-decimal.html>

<https://medium.com/@stolman.b/how-to-hash-the-genesis-block-like-a-pro-3cc437a4a237>

<https://medium.com/hackergirl/how-to-calculate-the-hash-of-a-block-in-bitcoin-8f6aebb0dc6d>

<https://www.youtube.com/watch?v=ci1jFDRPoCw>

<https://www.hyperledger.org/use/cactus>

FEW USEFUL LINKS

<https://www.youtube.com/watch?v=qN8LP1cY6K4>

<https://www.youtube.com/watch?v=dNRDvLACg5Q>

https://www.youtube.com/watch?v=iB3HcPgm_FI&list=PLzctEq7iZD-7-DgJM604zsndMapn9ff6q&index=24

<https://www.youtube.com/watch?v=8afbTaA-gOQ>

<https://popeller.io/index.php/blog/>

<https://gobittest.appspot.com/Address>

<https://anyhash.com/>

<https://prathamudeshmukh.github.io/merkle-tree-demo/>

<https://www.cs.usfca.edu/~galles/visualization/Trie.html>

<https://www.cs.usfca.edu/~galles/visualization/RadixTree.html>

<https://www.blockchain.com/explorer>

FEW USEFUL LINKS

<https://andersbrownworth.com/blockchain/blockchain>

<https://bitcoin.org/en/download>

<https://kjur.github.io/jrsasign/sample/sample-ecdsa.html>

<https://www.desmos.com/calculator/kkj2efqk5x>

<https://gobittest.appspot.com/Address>

<https://andersbrownworth.com/blockchain/tokens>

<https://metamask.io/>

<https://www.trufflesuite.com/ganache>

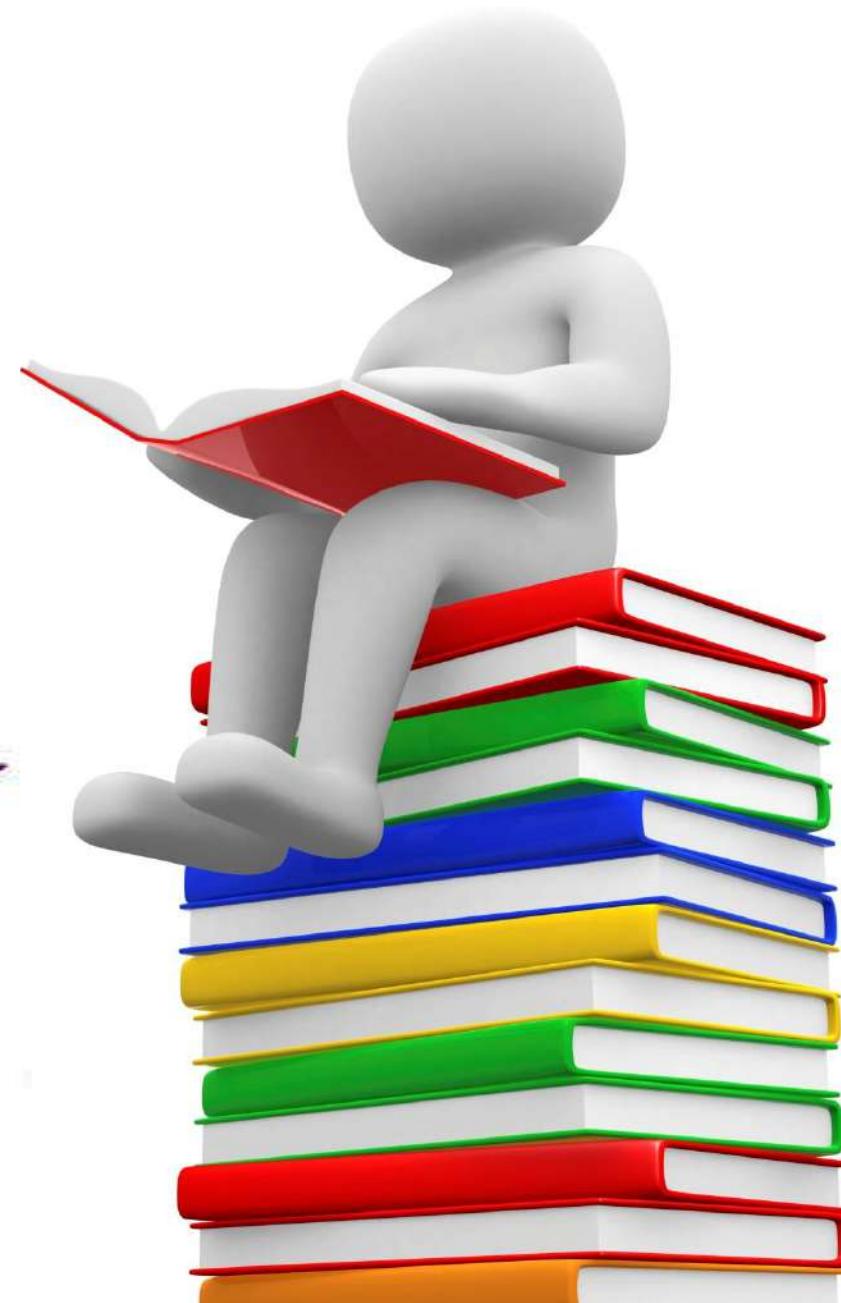
<https://bitcoin-rpc.github.io/en/doc/0.17.99/rpc/blockchain/getblockchaininfo/>

<https://www.calculator.net/big-number-calculator.html>

http://www.save-editor.com/tools/wse_hex.html

Never
stop
learning

SOLUTION



Domain



LOTS! Learn





OPEN SOURCE



KNOWLEDGE IS POWER



Share Your knowledge {



ALWAYS
SEEK
KNOWLEDGE



My JOURNEY in BLOCKCHAIN DOMAIN

My ASSUMPTIONS as a LEARNER

100%

80%

60%

40%

20%

I know 60-70
percent
Blockchain
Technology

Aug
2015



My ASSUMPTIONS as a LEARNER

100%

80%

60%

40%

20%

I know 60-70 percent Blockchain Technology

Increasing trend

So I thought....

I will know 90 percent blockchain technology

Mereko Sab Ata Hai..
Mai Expert Hun

Aug
2015

•

•

•

→



My **REALISATION** as a LEARNER

100%

80%

60%

40%

20%

I know 60-70 percent Blockchain Technology

I know “**May be**” 1-2 percent about Blockchain technology

“The more I learn, the more I realize how much I don't know.” — Albert Einstein

Aug
2015

July
2021



ANUPAM TIWARI

B.E, M.Tech, Research Scholar, FIE, FIETE

CERTIFICATIONS

- CDAC certified Cyber Security Professional
- GFSU certified Cyber Security Professional
- Certified Ethical Hacker
- PG in Information Security
- PG in ERP
- PG in Operations and systems

MEMBER OF TECHNICAL SOCIETIES

- Fellow, IETE
- Fellow, Institution of Engineers
- Senior Member, Computer Society of India
- Advanced Computing & Communications society
- Indian Science Congress Association

E-mail : anupam.blockchain@gmail.com

Blog : <https://anupriti.blogspot.com/> LinkedIn : www.linkedin.com/in/anupam-t-3848883

Research work : I have been exploring the domain of Blockchain and Cryptocurrencies for about 5 years plus now. My research work is focused on exploiting **Blockchain** for **Cyber physical systems** domains like **Internet of Vehicles, Smart Cities , Smart Buildings ,Smart Grids and Cyber physical Medical systems** etc

International Conference Papers and Technical articles in magazines

30+

Speaker in conferences

45+

THANK YOU!

E-Mail: anupam.blockchain@gmail.com

LinkedIn : www.linkedin.com/in/anupam-t-3848883

Blog at <https://anupriti.blogspot.com/>