CS48001-SEC532
Blockchain Security & Applications
Section 1 - Cryptography & Crypto Currency

Dr. Enis KARAARSLAN

Muğla Sıtkı Koçman Üniversitesi
Cyber Security AI Disciplines
BcRG - Blockchain Research Group
MvRG - Metaverse Research Group

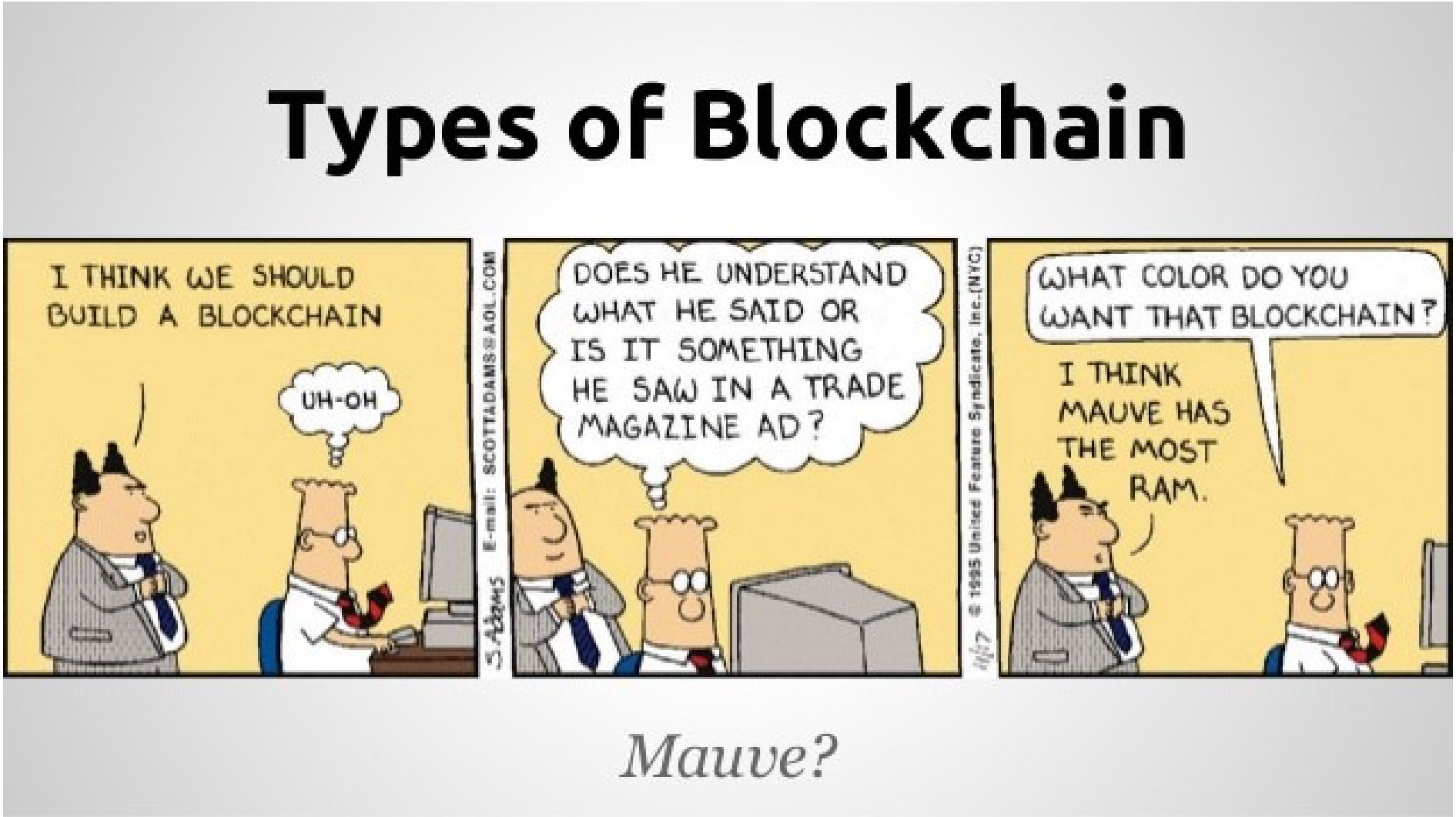
enis.karaarslan@mu.edu.tr

28 Şubat 2022

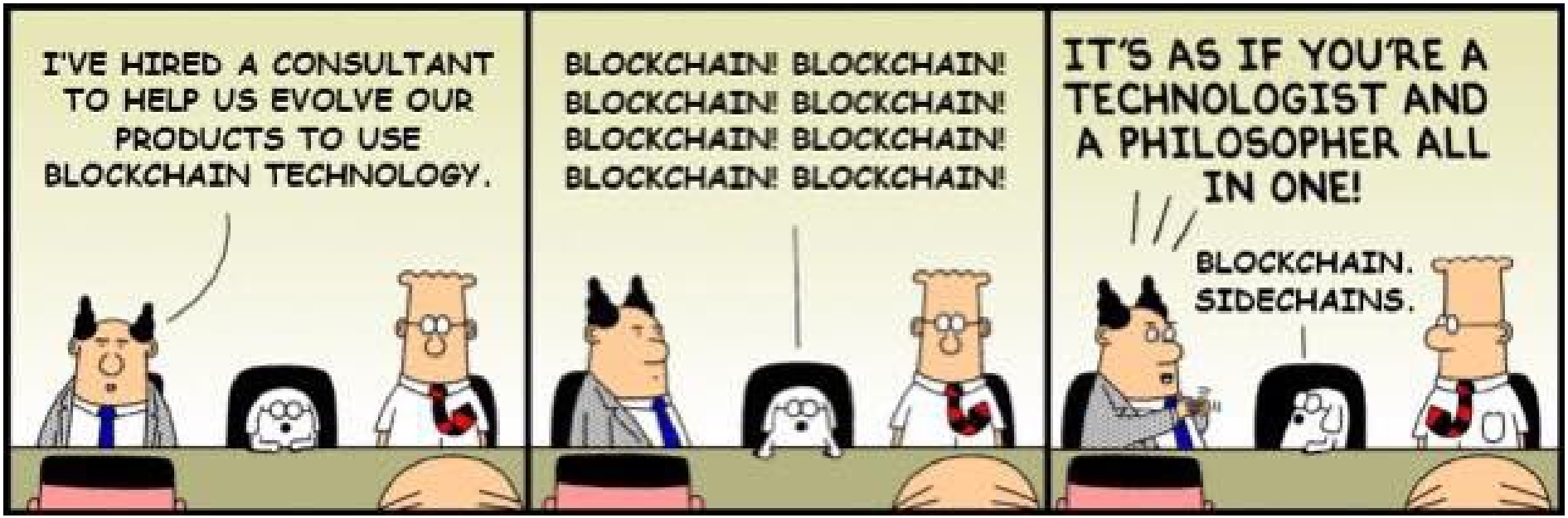
Index

Introduction

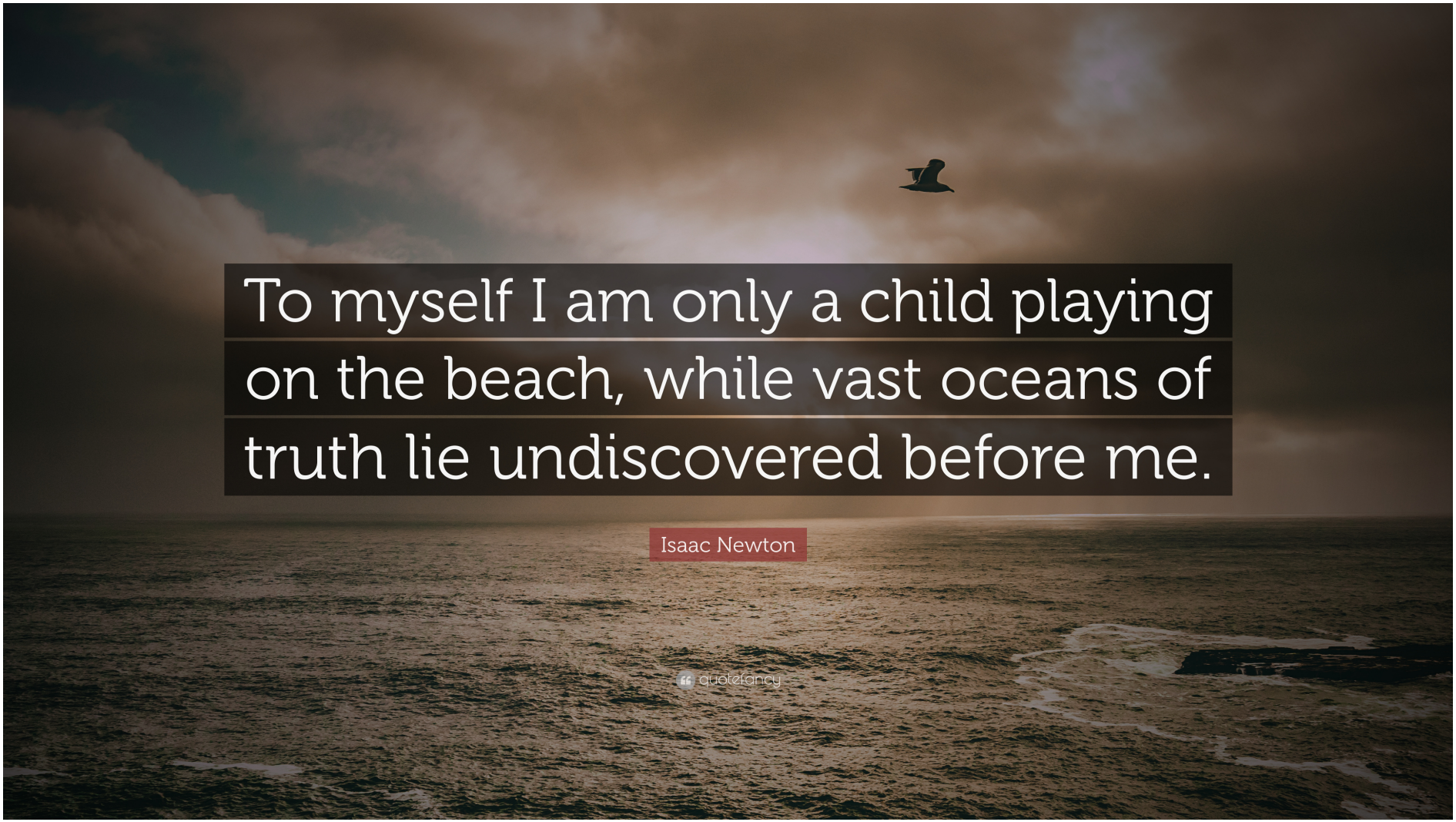
We Should Build a Blockchain Project :)



and everywhere is full of blockchain experts :)



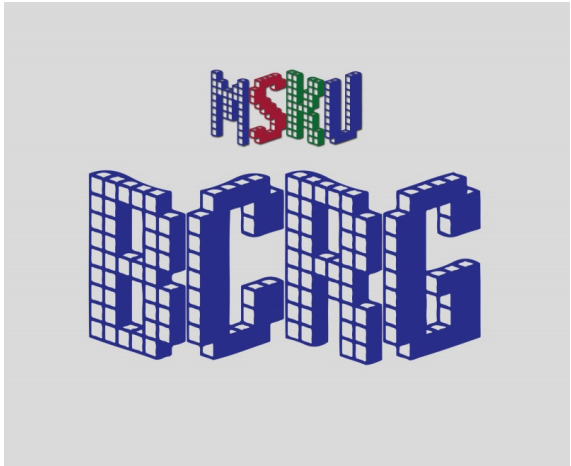
and everywhere is full of blockchain experts :)



Dr. Enis Karaarslan

MSKÜ Cyber Security & AI Disciplines

- Academician and consultant
- My specialization: Cybersecurity, blockchain, data science
- Blockchain and Artificial Intelligence studies in various fields (health, national security, tourism)
- cybersecurity model,
- Effective use in terms of data science
- Testing
- Metaverse



Dr. Enis Karaarslan : enis.karaarslan@mu.edu.tr

MSKU Blockchain Research Group - http://wiki.netseclab.mu.edu.tr/index.php?title=MSKU_BcRG

MSKU Blockchain Research Group (MSKU BcRG)

- 20 Invited Speech, Panel, Seminar
- 10 Education (Bosnia and Herzegovina, Ankara, Muğla, Eskişehir)
- 6 Live Stream (MSKU Blockchain presentations and chats)
- Blockchain Summer Internship (17 students, 12 experts)
- 1 Blockchain Research Network (DS4H - nodes in 4 different cities)
- 2 Tübitak/ITEA Project Consultancy
- 1 Patents + 1 Patent Application
- 6 Articles
- 14 Papers
- 4 (+2 in print) Book Chapter
- 2 Undergraduate Course (Ceng 3550 - Decentralized Sys.& Appl.)
- 9 Graduation Thesis (1 M.Sc., 8 Bachelor Thesis)
- 7 Awards (Teknofest - Tübitak 2242 Turkey 2nd, 3rd, 4th prizes)
- 1 Magazine Publication, 1 Interview, videos, presentations, drawings

... Turkish content ...

Blokzinciri yayını 2017 :)

Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:3, No:2, S:16-21, 2017

BLOKZİNCİRİ TABANLI SİBER GÜVENLİK SİSTEMLERİ

Enis Karaarslan[1], Muhammet Fatih Akbaş[2]
[1]Muğla Sıtkı Koçman Üniversitesi, Bilgisayar Mühendisliği Bölümü, Muğla, Türkiye
[2]İzmir Kâtip Çelebi Üniversitesi, Bilgi İşlem Daire Başkanlığı, İzmir, Türkiye
enis.karaarslan@mu.edu.tr, mfatih.akbas@ikc.edu.tr

ÖZET

Kripto paralar (cryptocurrency), eşler arası (Peer-to-Peer) mimaride birbirine bağlı madenci düğümü adı verilen bilgisayarlara ve blokzinciri yapısında tutulan kayıt sistemine dayanmaktadır. Bu sistemler sadece bir para birimi sağlamamakta, bu altyapılar üzerinde çeşitli 'merkezi olmayan' (decentralized), dağıtık (distributed) sistemler/yazılımlar tasarlanmaktadır. Bu çalışmada blokzinciri sisteminin nasıl çalıştığı, sağladığı veri bütünlüğü, kullanılabilirlik, mahremiyet gibi güvenlik servisleri ve hata toleransı incelenmektedir. Blokzinciri yapısının; nesnelerin interneti (Internet of Things), akıllı şehirler, kişisel verilerin korunması, bilgisayar ağları için kullanımı gibi siber güvenlik konularındaki çalışmalar ele alınmaktadır. Blokzinciri uygulamalarındaki temel sorunlara ve olası çözümler gözden geçirilmiştir. Bu tür çözümlerin ağ güvenliğinde kullanımına dair önerilere yer verilmiştir.

Anahtar Kelimeler: Blokzinciri, Siber Güvenlik, Kripto Para

Let's start ...

Starting with Cryptocurrencies...

Bitcoin: A Peer-to-Peer Electronic Cash System

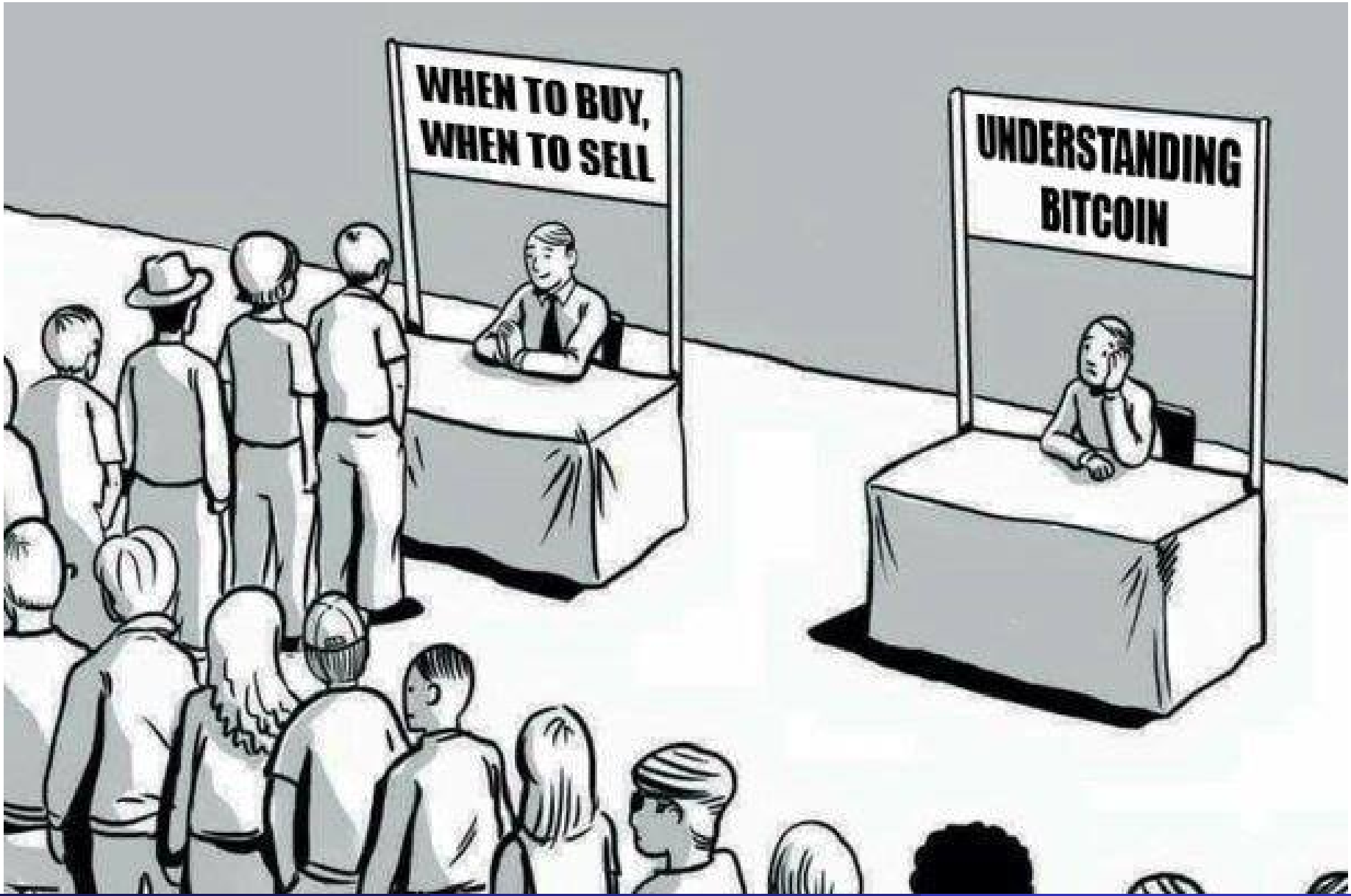
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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

1 Introduction

Cryptocurrency

Humor



Decentralized systems

- Systems where intermediaries are removed (or intermediaries of which we are unaware)
- Freedom?
- Trust?

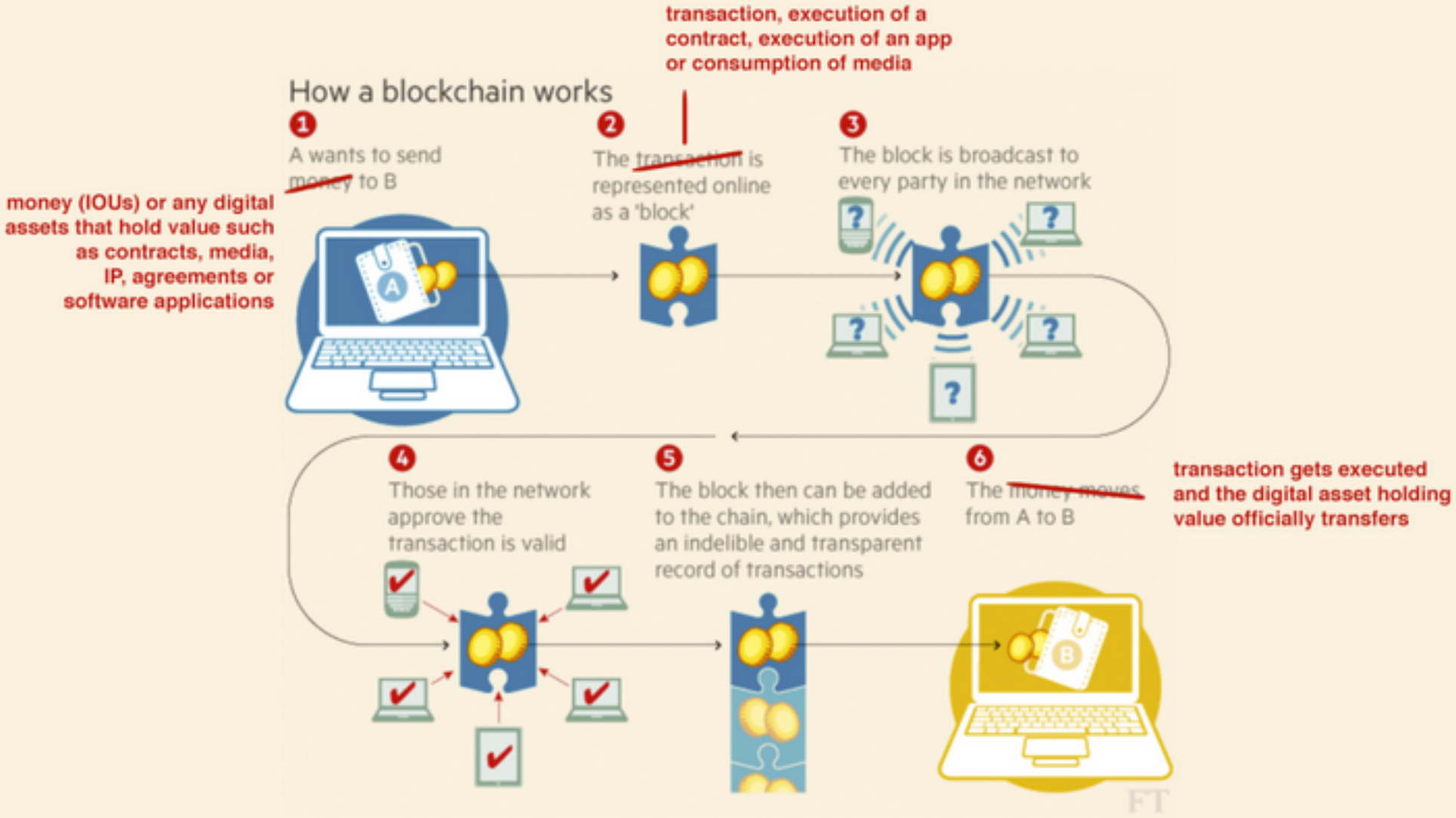
Or Totally Emotional

Intermediaries ...

What's different in Blockchain?

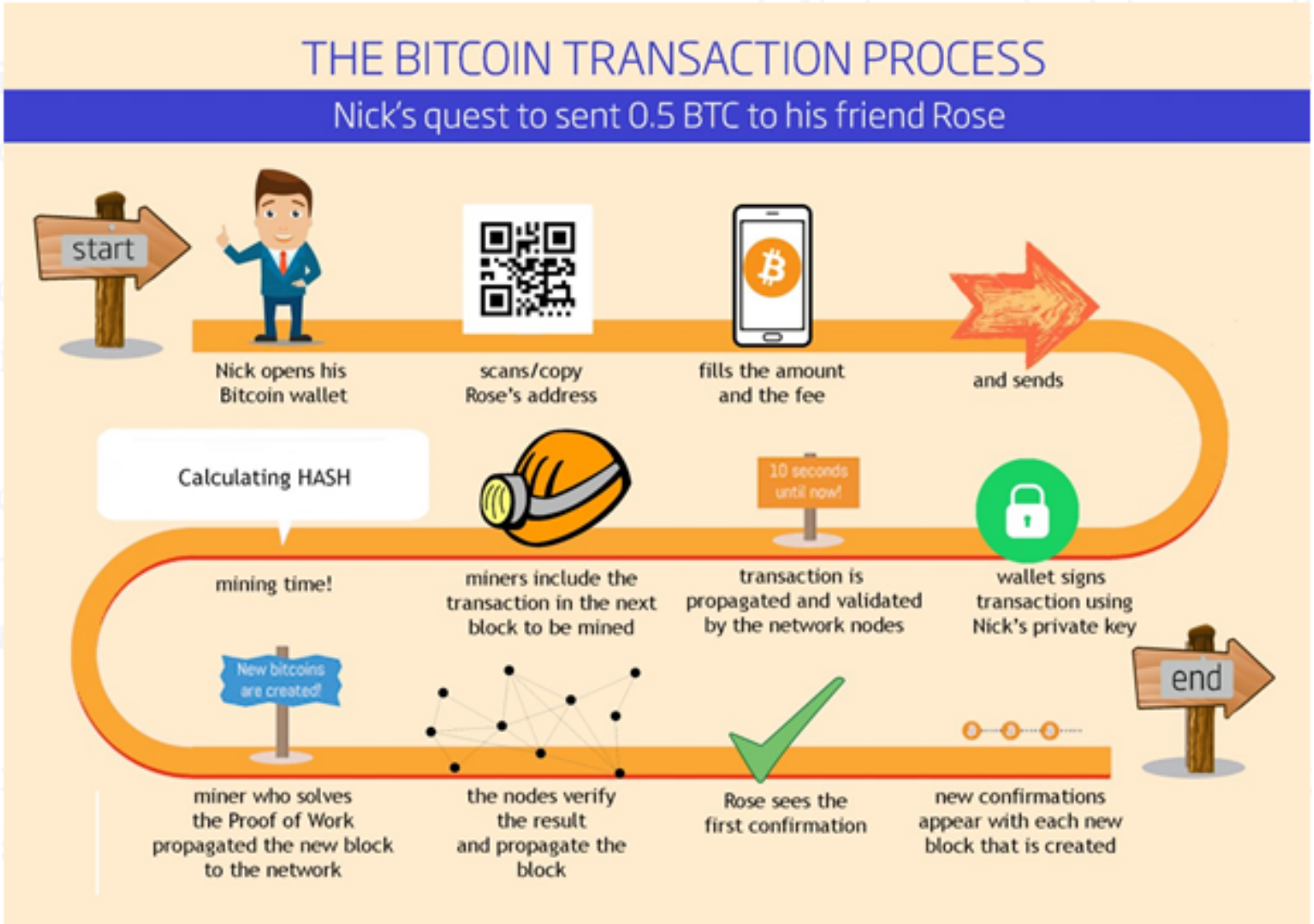
- No intermediary in transactions
- An autonomous (self-executing) system
- No system administrator (no root)
- Everything is recorded (immutable recording system)
- Developers who support the system (Community)
- Preferably open source and "free software"

Crypto Currencies - How Does Blockchain Work? [4]

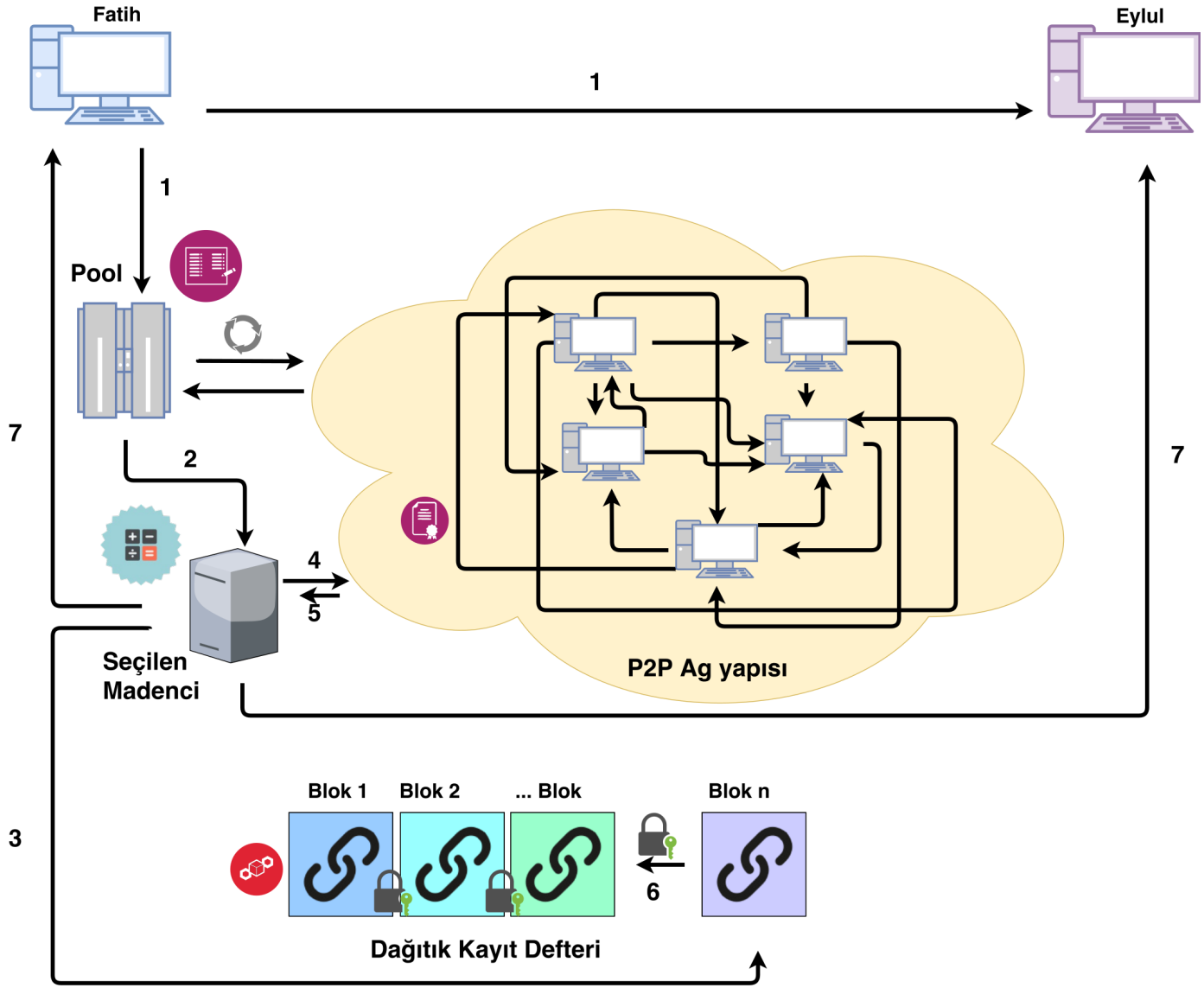


How Blockchain Works

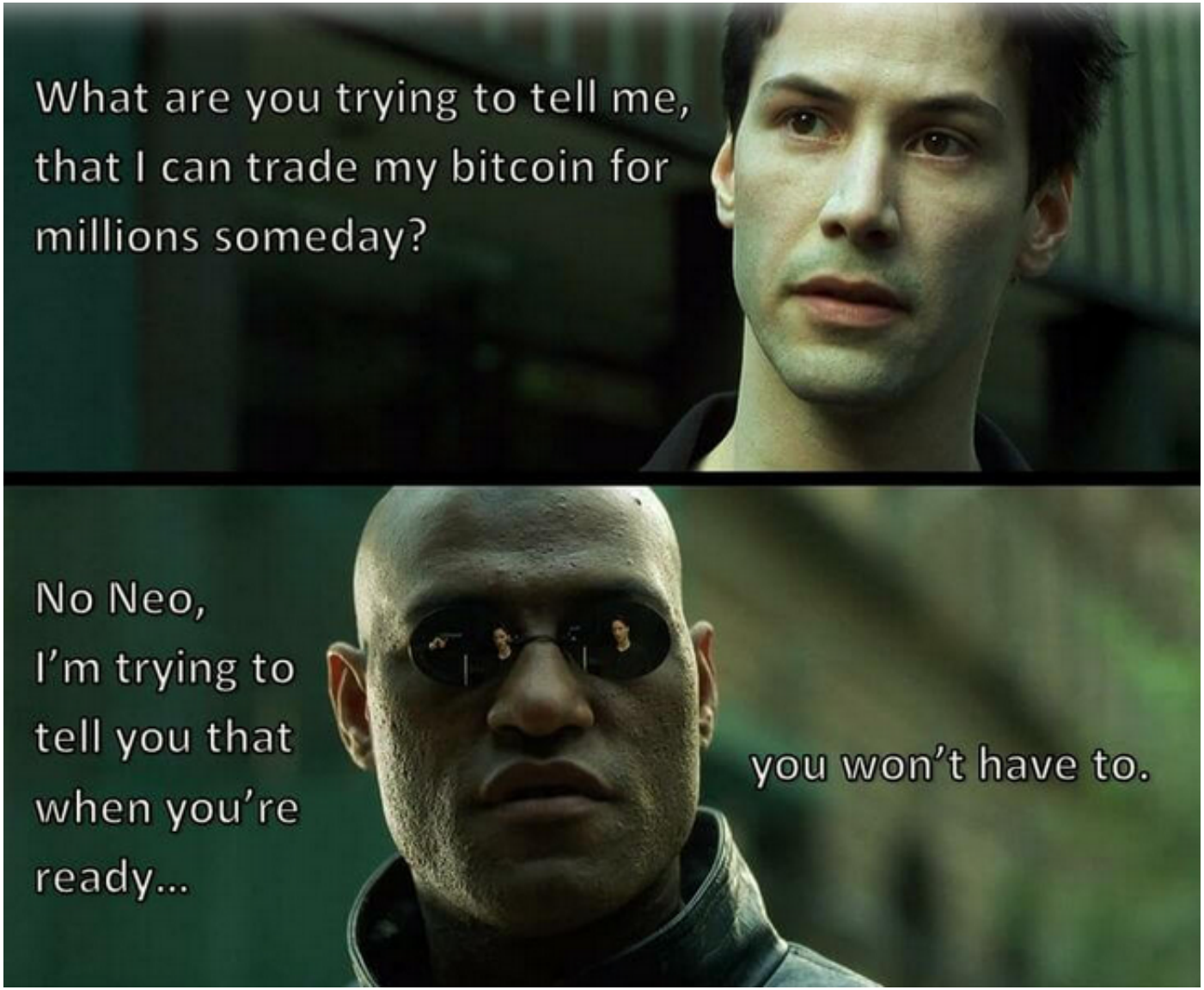
How Does It Work? (Satoshi Style (revised) :))



How Does It Work? (Pool added (revised) :))



Bitcoin :))

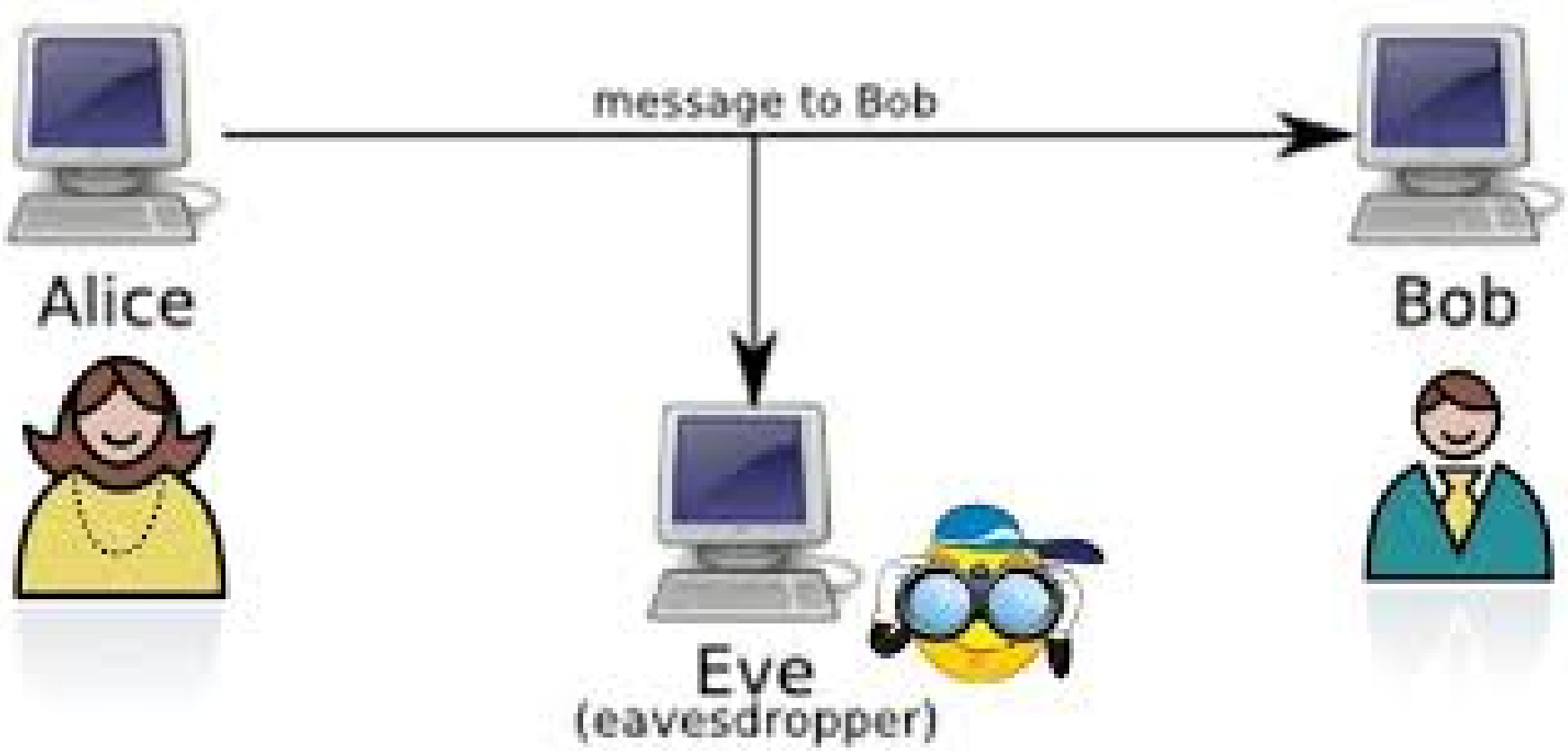

What are you trying to tell me, that I can trade my bitcoin for millions someday?
No Neo, I'm trying to tell you that when you're ready...
you won't have to.

Fundamentals

Introduction - Blockchain (cryptocurrency) Systems

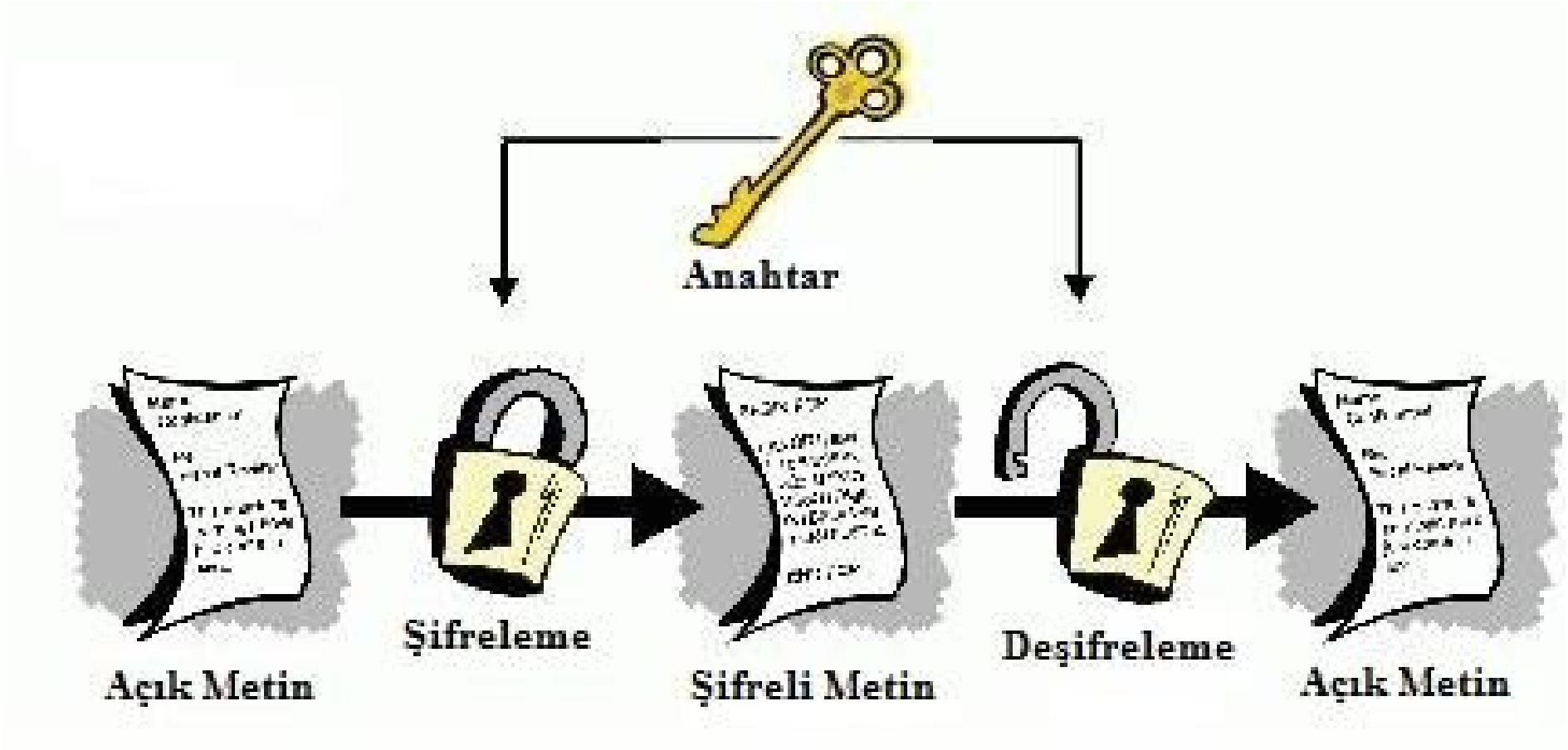
Cryptocurrencies keep the transactions made in the blockchain structure on computers connected to each other with the P2P protocol.

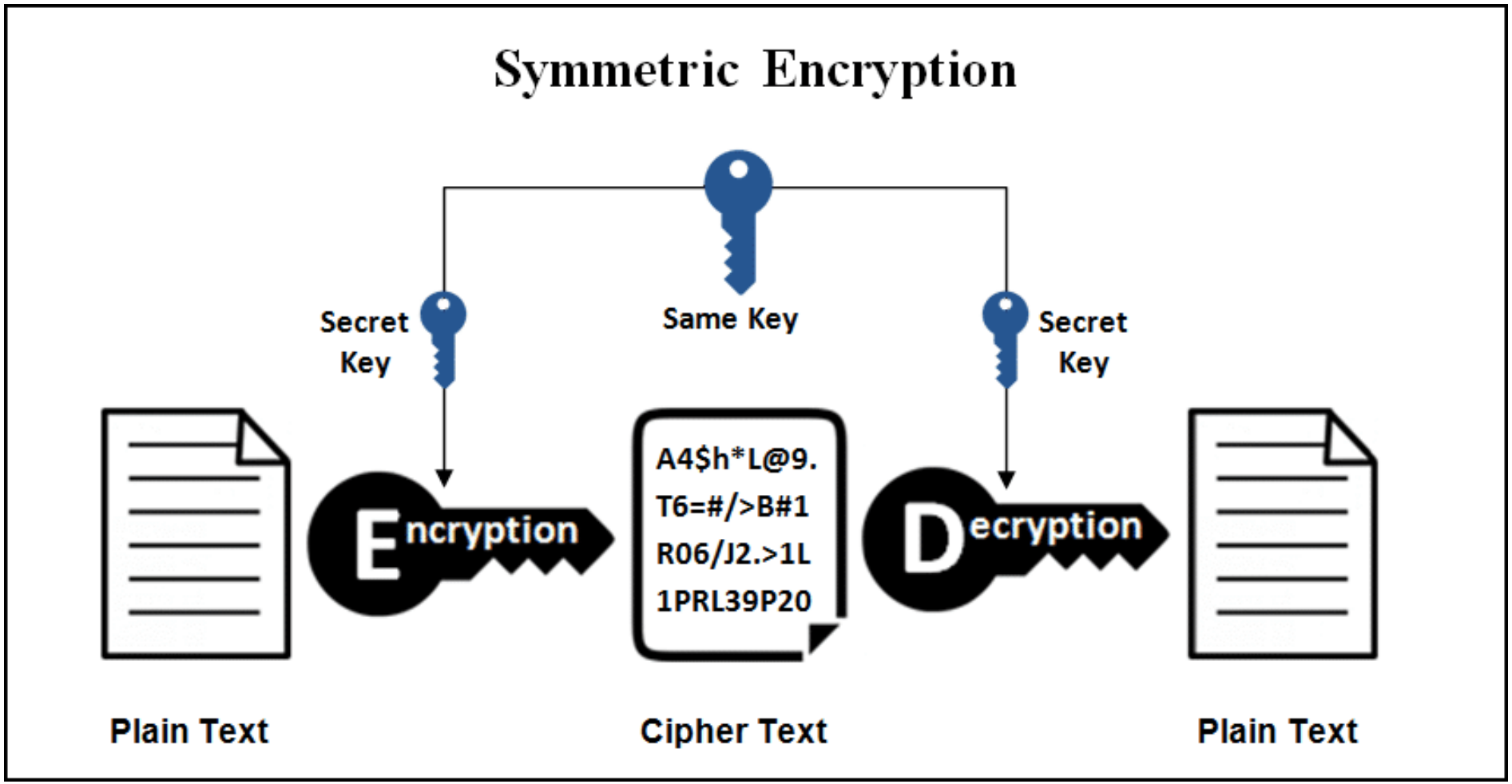
The blockchain technology that Bitcoin introduced to us; the basic concepts and cryptocurrencies will be discussed in this section.


message to Bob
Alice
Bob
Eve
(eavesdropper)

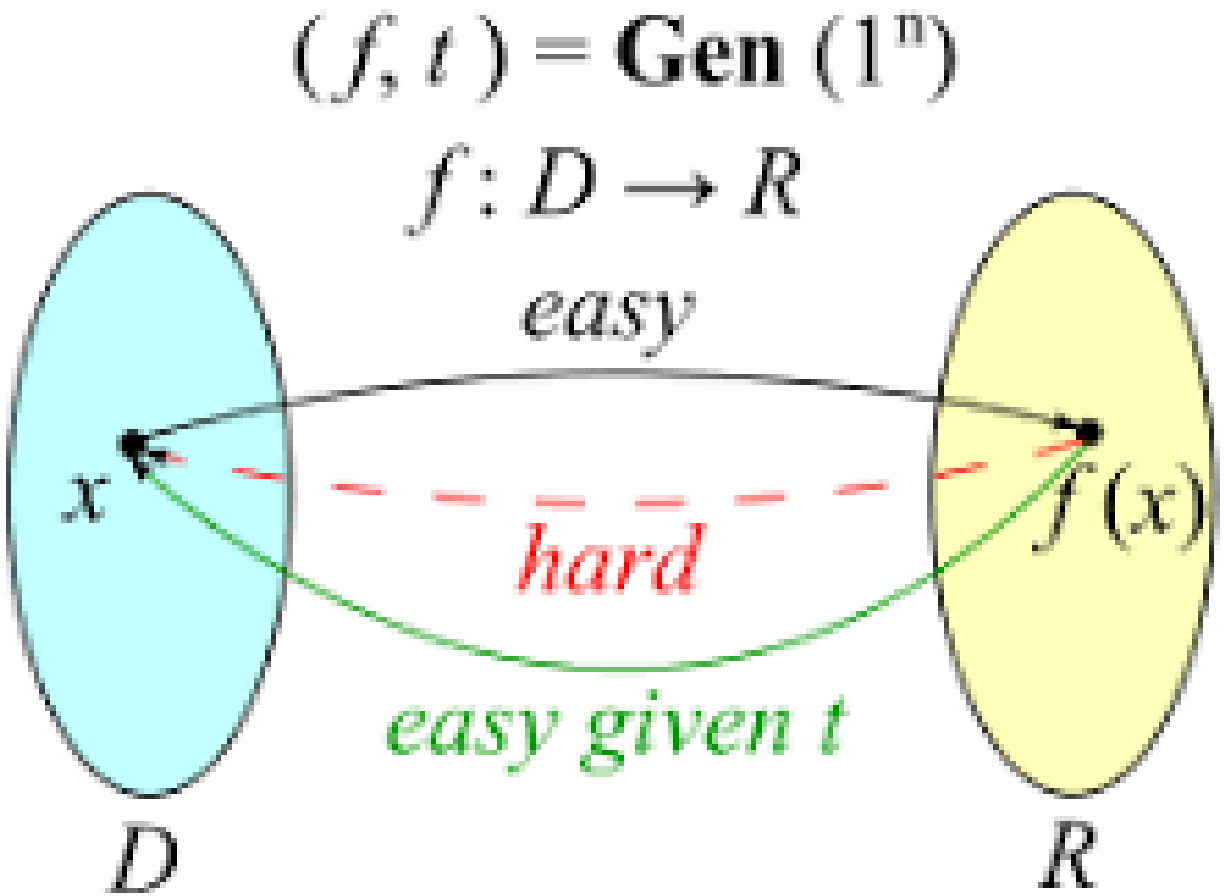
Cryptography

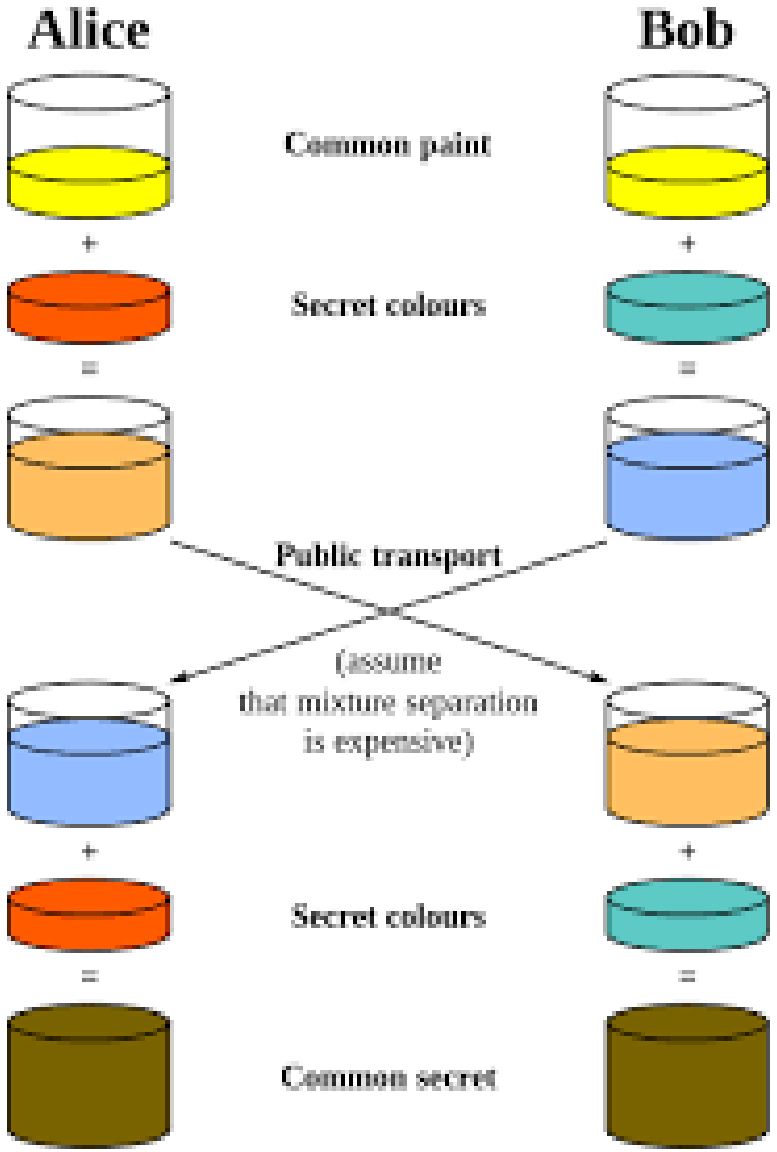
Encryption

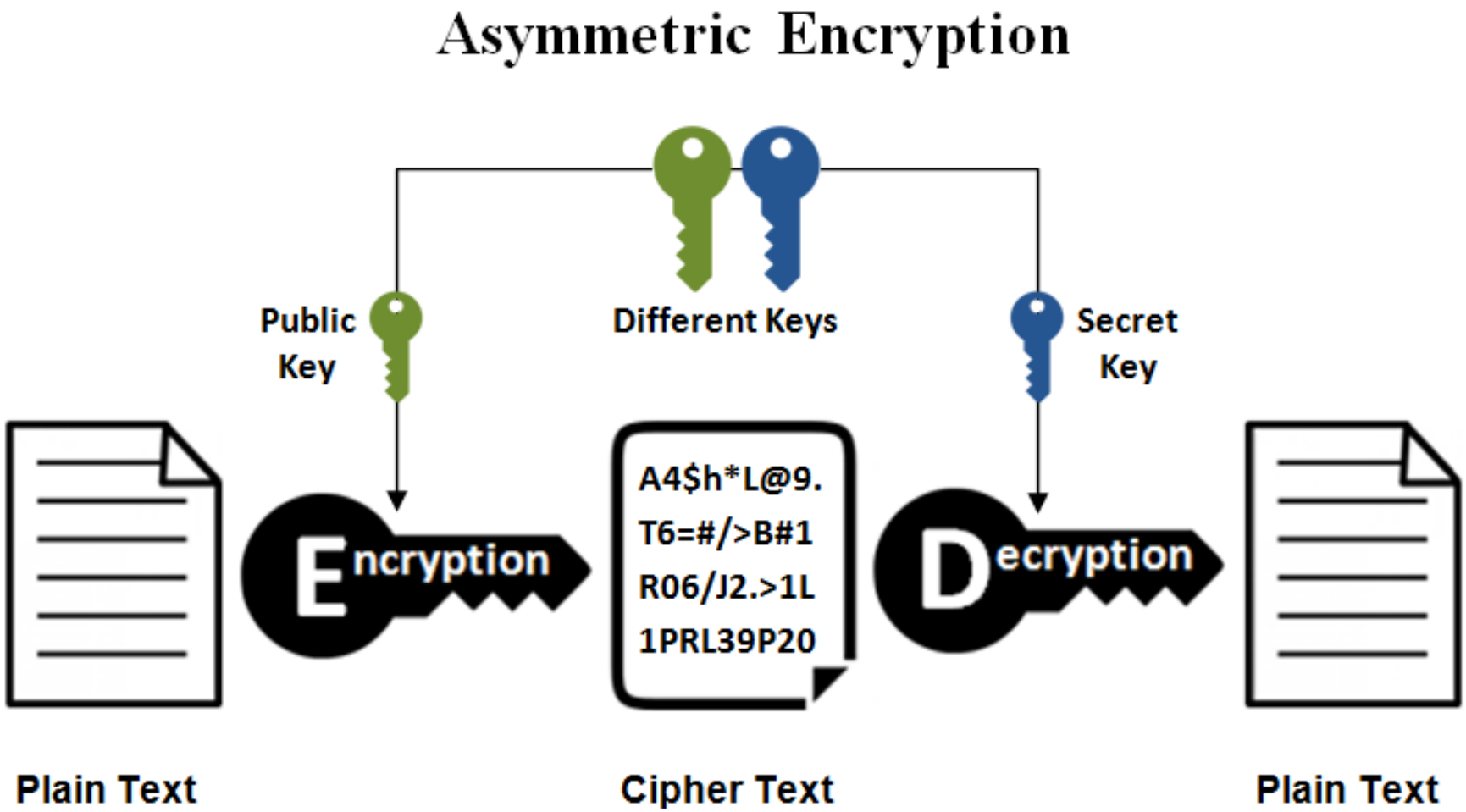



Symmetric Encryption
Secret Key
Same Key
Secret Key
Encryption
A4$h*L@9.
T6=#/>B#1
R06/J2.>1L
1PRL39P20
Decryption
Plain Text
Cipher Text
Plain Text

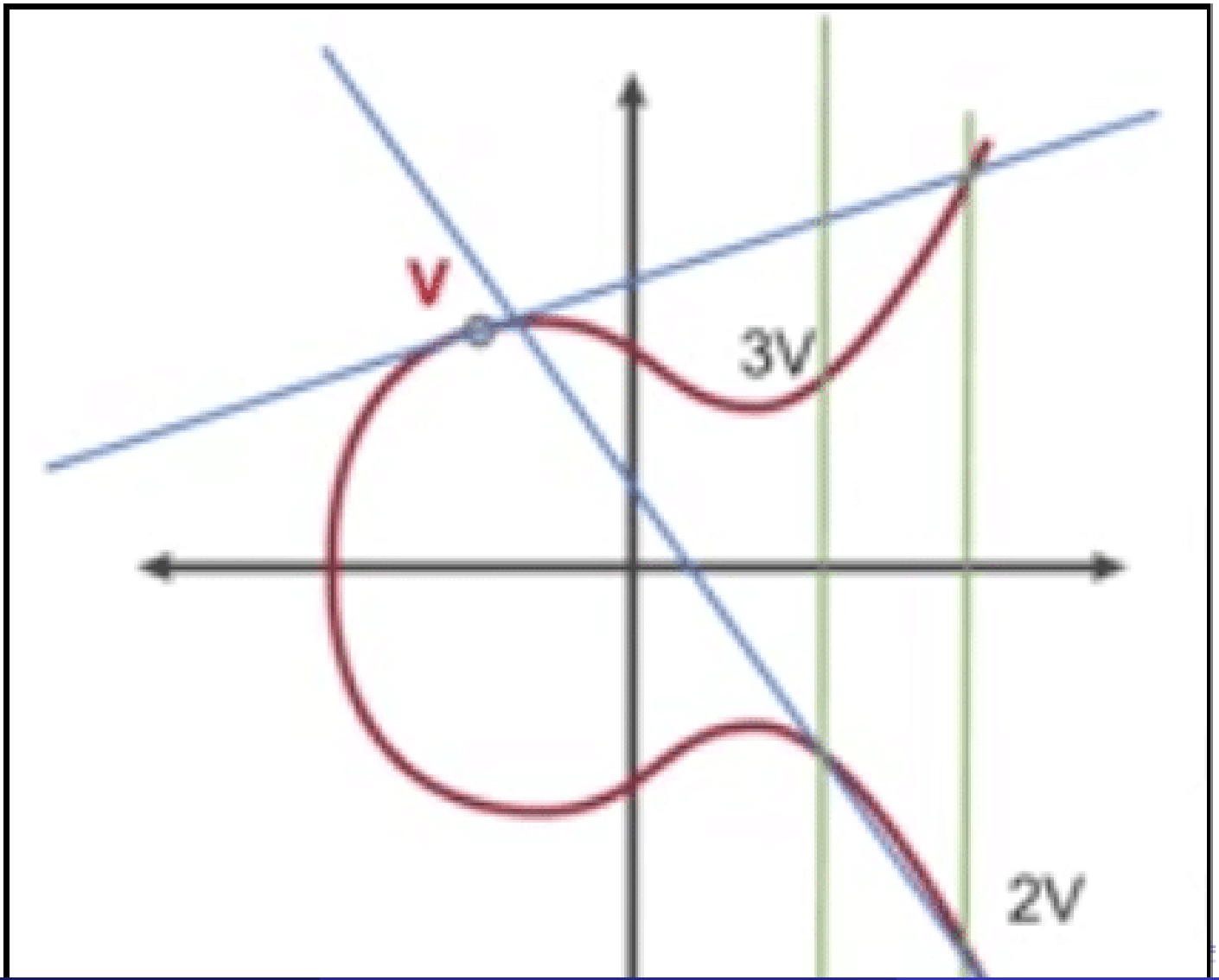
How will the key be safely delivered to the other party?
Key Distribution Problem


$(f, t) = \mathbf{Gen}(1^n)$
$f : D \rightarrow R$
easy
x
hard
f(x)
easy given t
D
R

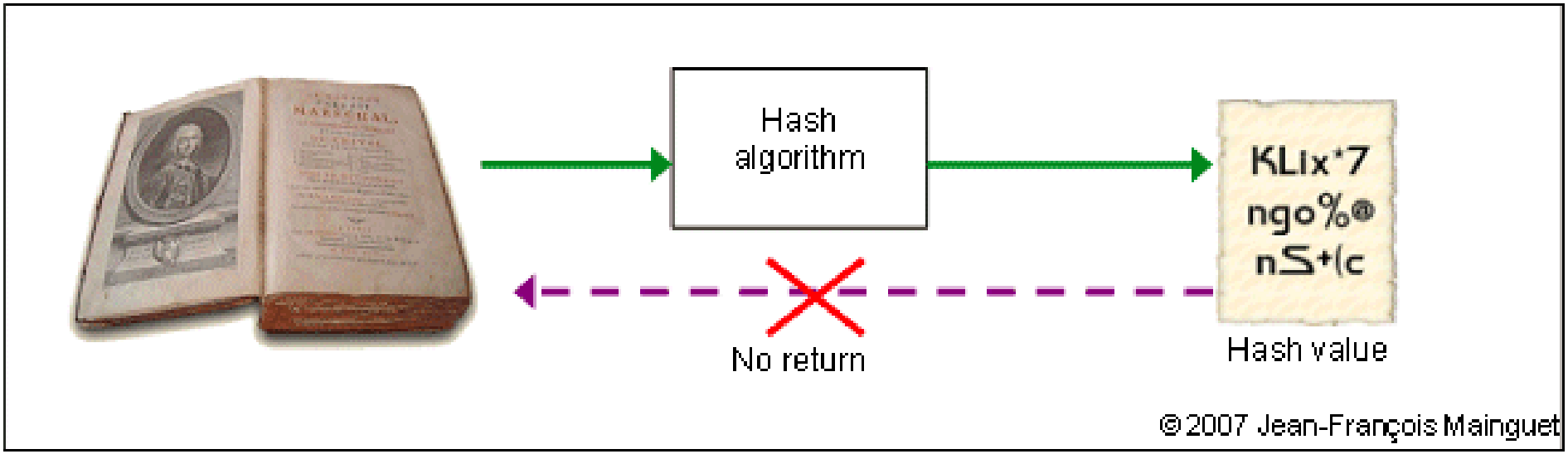

Alice
Bob
Common paint
+
+
Secret colours
=
=
Public transport
(assume
that mixture separation
is expensive)
+
+
Secret colours
=
=
Common secret

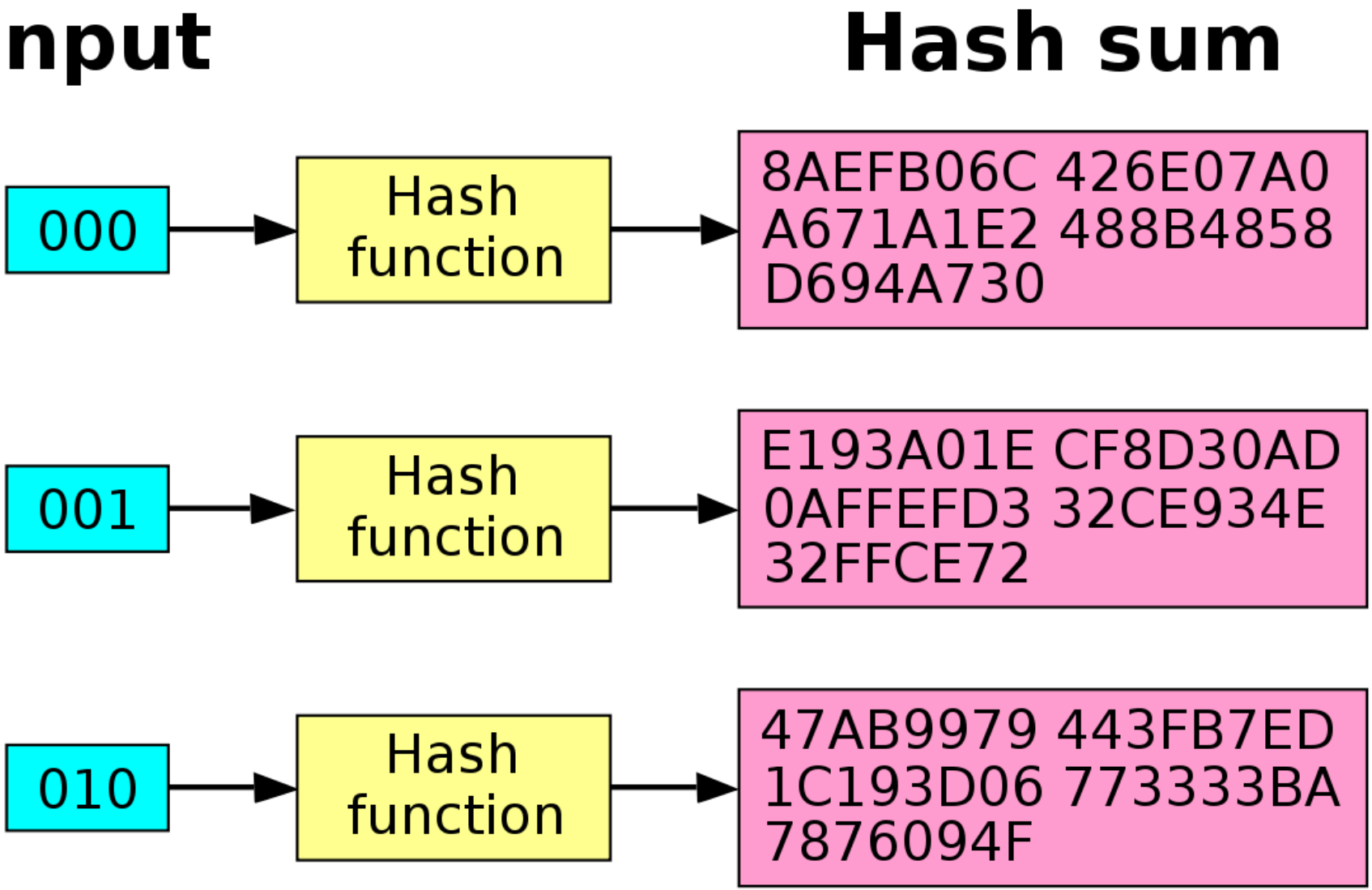

Asymmetric Encryption
Public Key
Different Keys
Secret Key
Encryption
A4$h*L@9.
T6=#/>B#1
R06/J2.>1L
1PRL39P20
Decryption
Plain Text
Cipher Text
Plain Text

Bitcoin and Ethereum use Elliptic Curve encryption



- EEC is much more efficient than RSA. It provides the same level of security as RSA with a smaller (large) key
  - 256-bit key EEC -> 3072-bit key RSA
  - 384-bit key EEC -> 7680-bit key RSA
- NSA recommends 384-bit EEC encryption for highly confidential documents. (Needs an update regularly!)


Hash
algorithm
KLIx*7
ngo%@
n≤+(c
No return
Hash value
©2007 Jean-François Mainguet


Input
Hash sum
000
Hash function
8AEFB06C 426E07A0 A671A1E2 488B4858 D694A730
001
Hash function
E193A01E CF8D30AD 0AFFEFD3 32CE934E 32FFCE72
010
Hash function
47AB9979 443FB7ED 1C193D06 773333BA 7876094F

WIF format

Public key is generated from private key

Cryptography

Cryptocurrency - Bitcoin Wallet - 265 bit private key

WalletGenerator.net

Universal Open Source Client-Side Wallet Generator

Generating new Address...
MOVE your mouse around to add some extra randomness... 258
OR type some random characters into this textbox

5617462b686e534dbd0f847f33b8b92e86f63f0a7dee63c862a0a312e847a0593b15dde2c131e3be5daa101bf67
e8e5b9eb6ba6fc0fd98ca08913764316fbeb96de177ff05a2291db7bbbf2c96d0b5930e30d0622c6d59f3258dba
9ffea15eedc4ca6e287432ecd60d46e9c6876f67b9769259b616d34c54e4eccb6cfa99b627c6a39cb9354026da5
24f1fd5fcadeeb60a6273fd954dfe28892e8efb3dbd25514a63b9a20d909f16ecc188bd20886e4846dff98a8fff
0f25903308dbd175241633794554f68408c81509855af606ec9e9504693d04b74b54734c9b21b6398989b33c733
eaaf25ec2e8caa38255bd4676a3bfa5bd7a2d2ab6865a817d3e052253

Skip »

You may skip this step if you do not plan to use the random key generator.

Step 0. Follow the security checklist recommendation

First step is to **download** this website from Github and open the index.html file directly from your computer. It's just too easy to sneak some evil code in the 6000+ lines of javascript to leak your private key, and you don't want to see your fund stolen. Code version control make it much easier to cross-check what actually run. For extra security, **unplug your Internet access** while generating your wallet.

Step 1. Generate new address

Choose your currency and click on the "Generate new address" button.

Step 2. Print the Paper Wallet

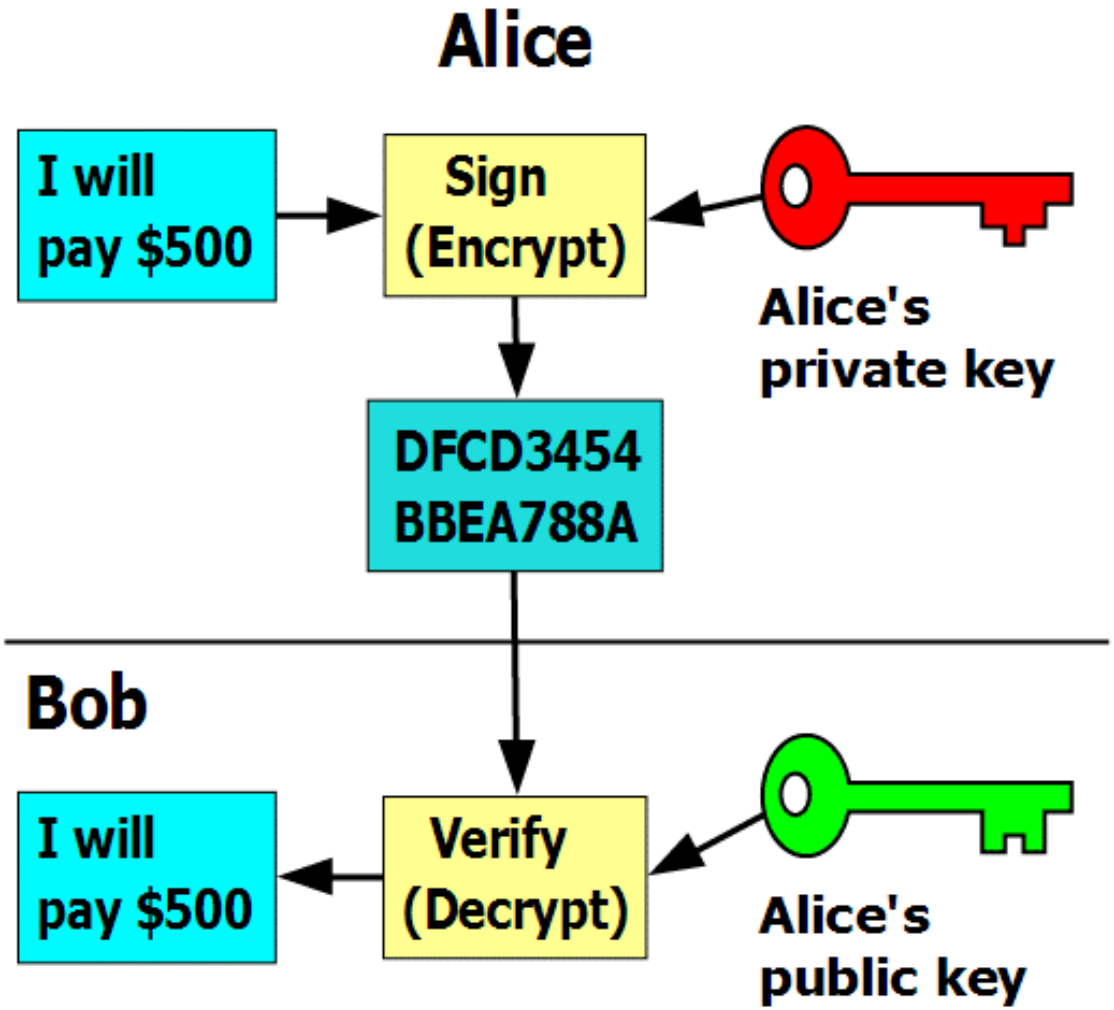
Click the Paper Wallet tab and print the page on high quality setting. **Never save the page as a PDF file to print it later since a file is more likely to be hacked than a piece of paper.**

Step 3. Fold the Paper Wallet

Fold your new Paper wallet following the lines.

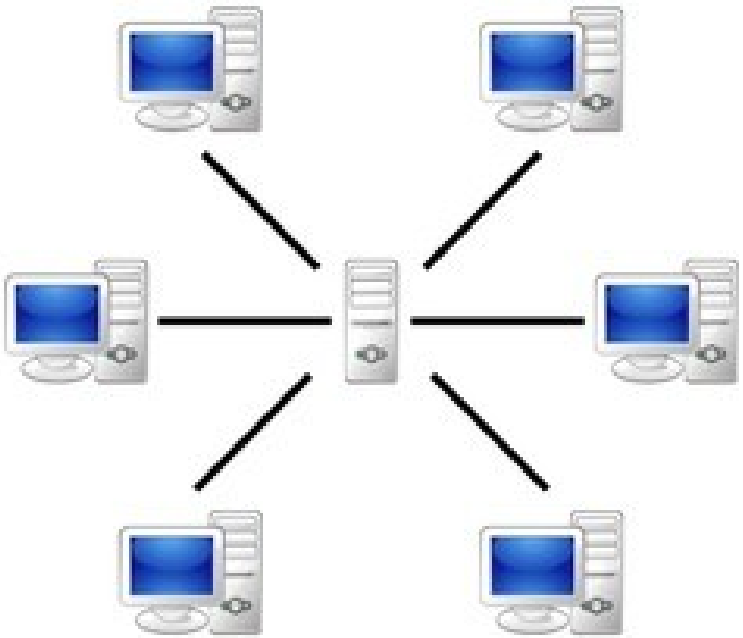
- Hash fn SHA 256 (private key) - > first value
- Hash fn RIPE MD 160 (initial value) -> Part A
- Hash fn SHA 256 (Part A) -> second value
- Hash fn SHA 256 (second value) -> C, First 7 bits (C) -> Part B
- Public key = Part A + Part B

It is claimed that the creation of the private key from the public key will take a very long time (40,000,000,000,000,000,000,000,000,000 years?) with the mathematics and processing power we know.
(Note: Constantly changing with new computers)
Quantum computers and new techniques will shorten this period, for now it is enough for today. However, "Post quantum" cyptography will soon be required.

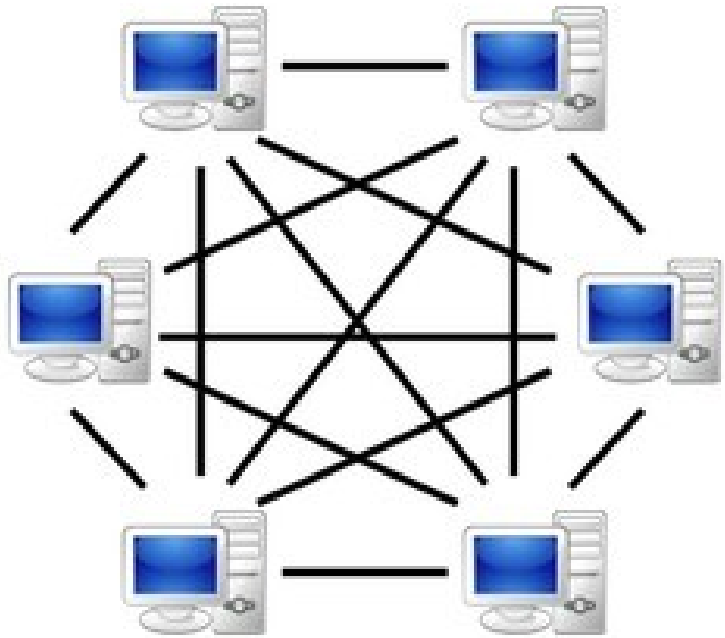

Alice
I will pay $500
Sign (Encrypt)
Alice's private key
DFCD3454 BBEA788A
Bob
I will pay $500
Verify (Decrypt)
Alice's public key

- When connecting Blocks in Blockchain
- Coin mining - creating money (is there really such a process? No.)
  - Not valid for all Cryptocurrency (?)
  - Limited and limited number (?)

P2P



Server-based



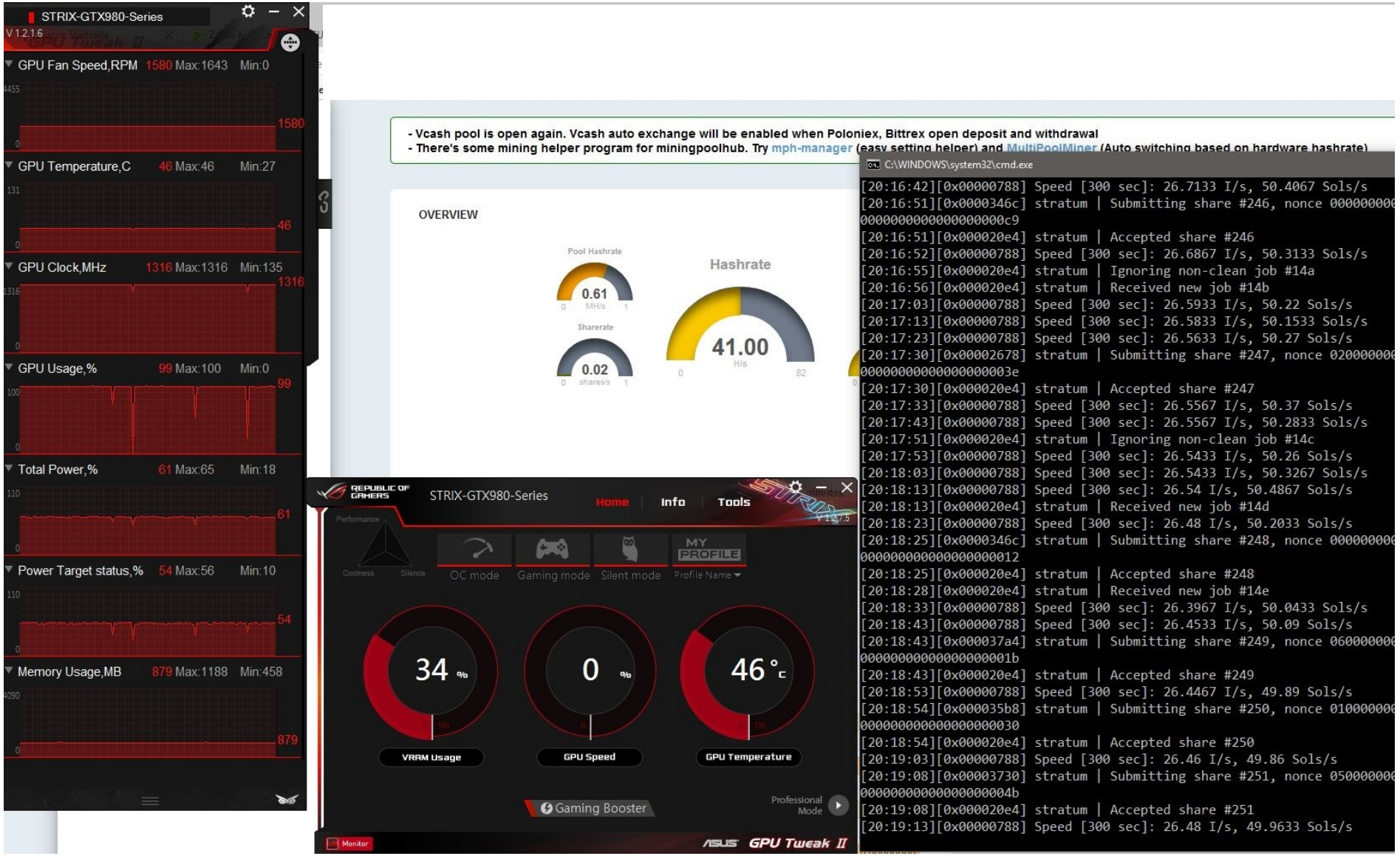
P2P-network

Cryptocurrency Mining Eco System

Miner Node - Machines

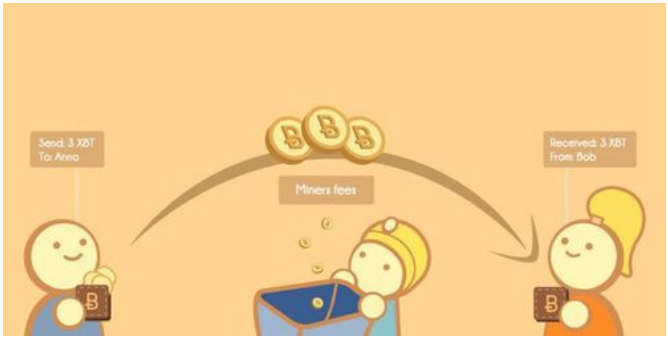
Mining RIG - GPU

Mining Power - GPU H/s



Cryptocurrency Mining

- Share from the money that was put into circulation with the block writing award
- Share from transaction fees




BITCOINERS BE LIKE
I'M IN IT FOR
THE TECHNOLOGY

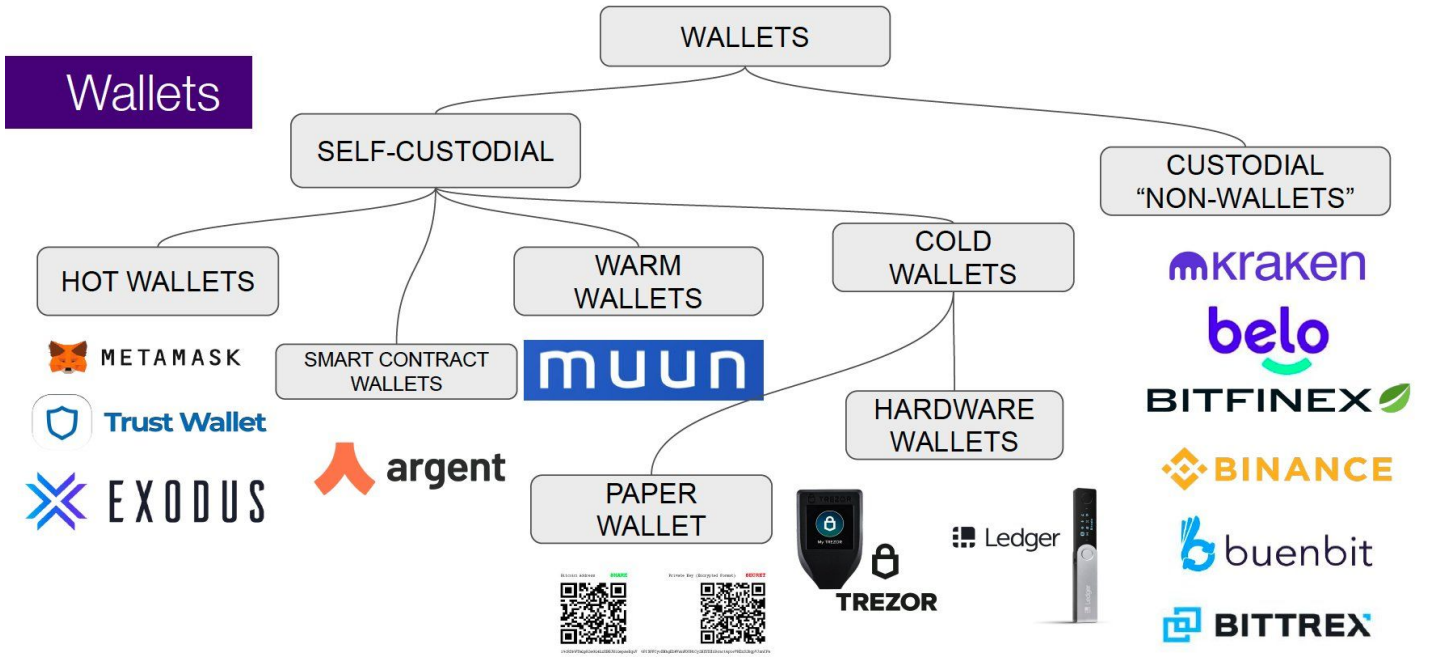
Mining RIG - GPU

Who made the most money during the California gold mine rush?

Cryptocurrency


BTC Wallet Bitcoin Address
16RuRAPTTXYQU8ikWFyGPznpwaeqSRK8RU
Sent bitcoin

Wallets ...


Wallets
WALLETS
SELF-CUSTODIAL
CUSTODIAL
“NON-WALLETS”
HOT WALLETS
WARM
WALLETS
COLD
WALLETS
METAMASK
SMART CONTRACT
WALLETS
muun
Trust Wallet
HARDWARE
WALLETS
argent
EXODUS
PAPER
WALLET
TREZOR
Ledger
kraken
belo
BITFINEX
BINANCE
buenbit
BITTREX
defy
EDUCATION
23

Cryptocurrency - physical(?) wallet

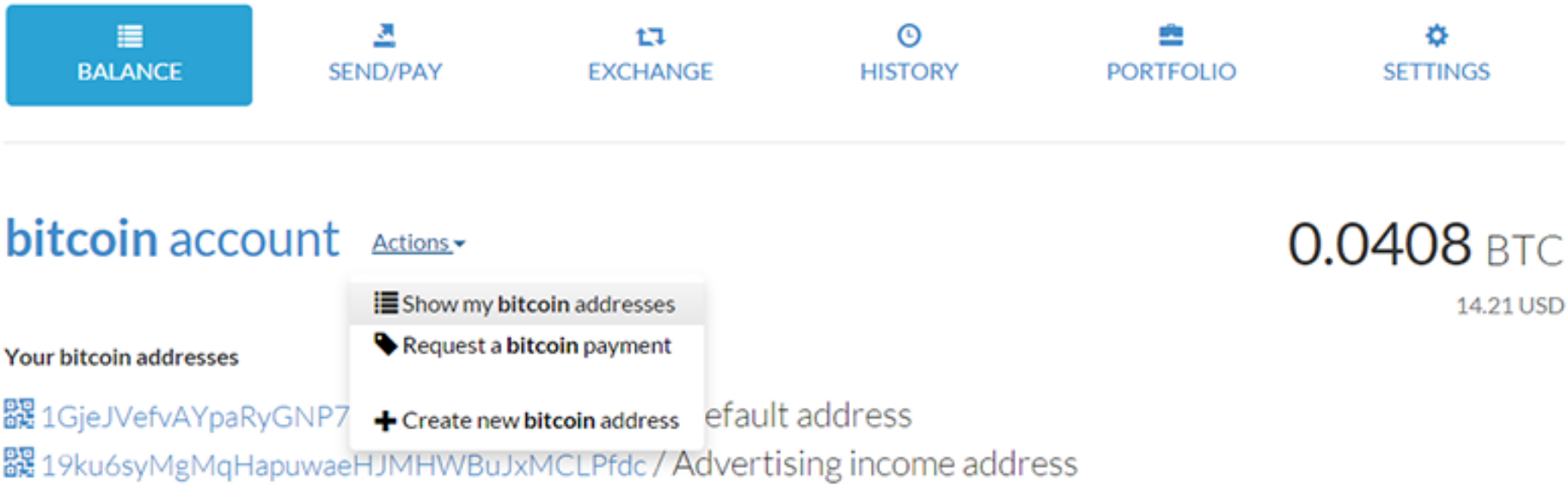
Cryptocurrency - Hardware wallet

Cryptocurrency

Humor

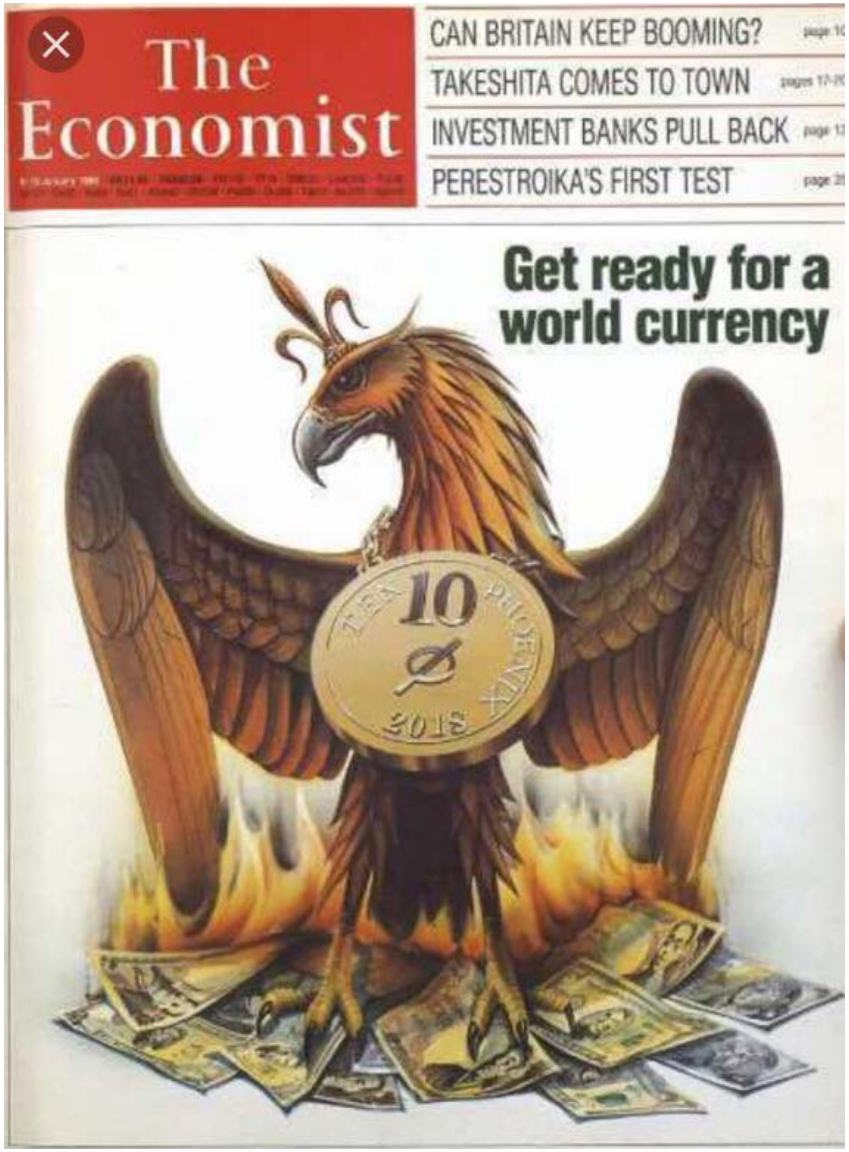
Cryptocurrency
Bitcoin(BTC)

- Bitcoin (BTC),
- using P2P protocol
- decentralized
- Digital (crypto) money
- active since 2009
- Not managed by any financial institution(?)


BALANCE
SEND/PAY
EXCHANGE
HISTORY
PORTFOLIO
SETTINGS
bitcoin account
Actions
Show my bitcoin addresses
Request a bitcoin payment
Create new bitcoin address
0.0408 BTC
14.21 USD
Your bitcoin addresses
1GjeJVefvAYpaRyGNP7
efault address
19ku6syMgMqHapuwaeHJMHWBuJxMCLPfdc / Advertising income address

Cryptocurrency

Bitcoin - The Economist - 1988 - Conspiracy theory?



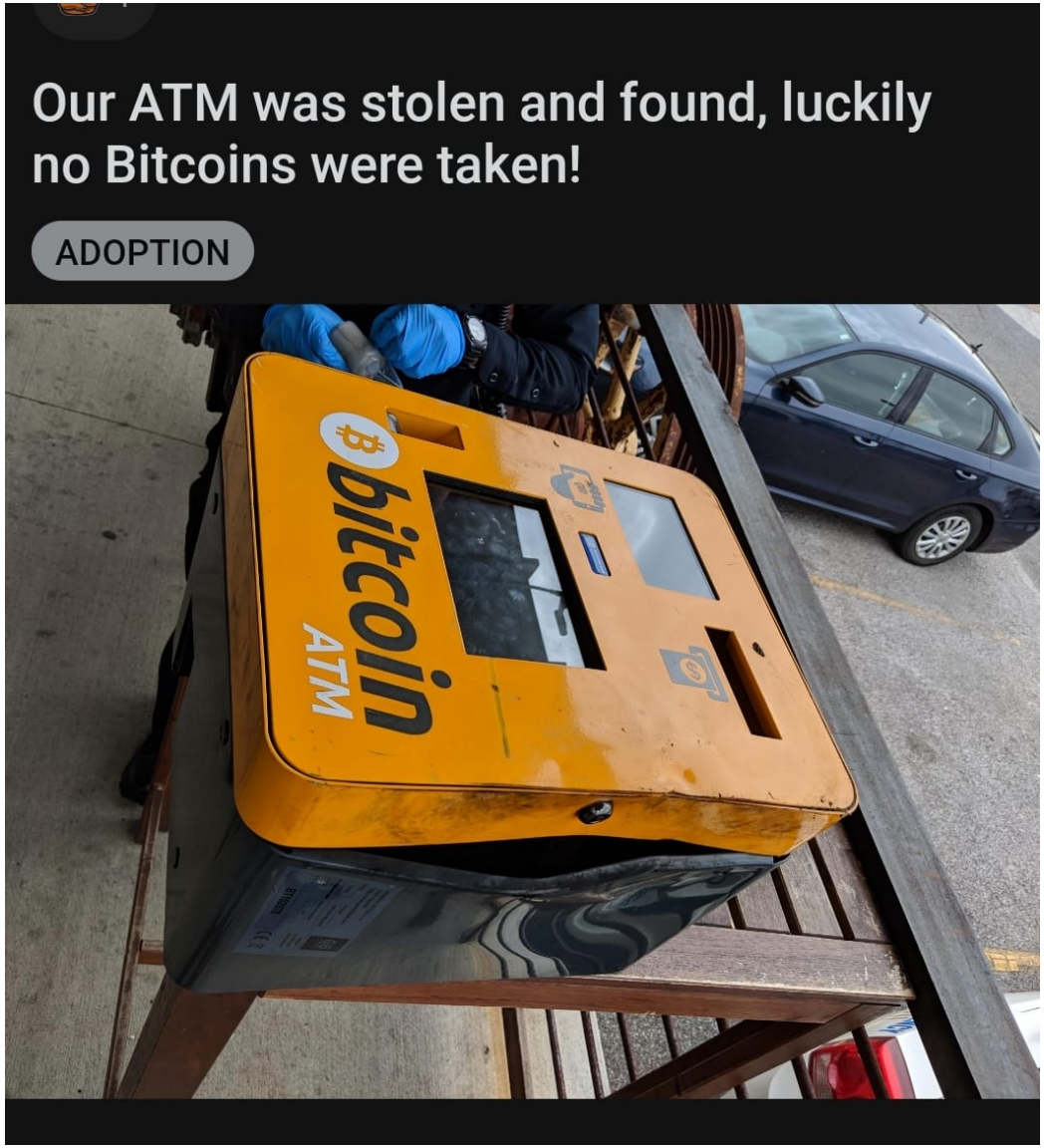
Merkez Bankası'ndan Piyasaları Rahatlatan Açıklama: "Bitcoin'in ne olduğunu biz de tam anlamıyoruz..."

Cryptocurrency

Who uses it

Cryptocurrency

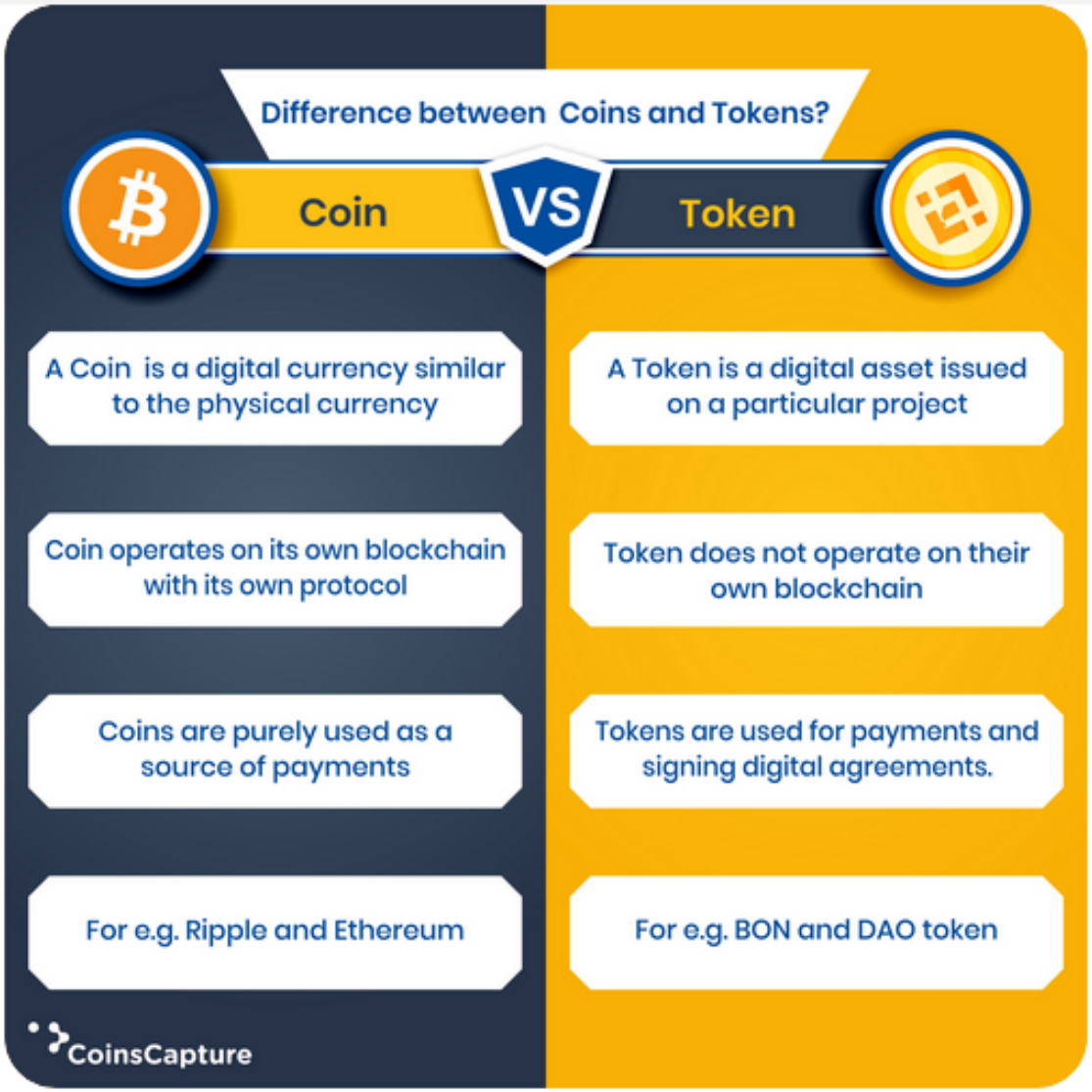
Bitcoin ATM



- Alternative coin (altcoin)
  - Similar to Bitcoin in the way they work (mostly but not always)
  - Need for miner machines (not always for "tokens")
  - Promises a Technology (should but not always as "meme" coins)

Cryptocurrency

Coin versus Token



CRYPTOCURRENCY

COINS

LAYER 1 TECH

01	Unit Of Accounting
02	Medium Of Exchange
03	Store of Value
04	Built INTO the Blockchain
05	Technologically: you are the sole owner of the asset. Your private keys are directed at the asset/storage and you directly own the asset

CRYPTOCURRENCY

TOKENS

LAYER 2 TECH

01	Unit Of Accounting
02	Medium Of Exchange
03	Store of Value
04	Built ON TOP of a Blockchain
05	Technologically: you are given the allowance to spend the asset that you receive, thereby the token is forever owned by the contract creator

Ethereum - It allows running various applications (decentralized app - dapp) on its infrastructures with smart contract. It is possible to develop smart contracts on **Ethereum Virtual Machine** with high-level languages such as **Solidity**.


ethereum
ETHERBROWSER
PEER-TO-PEER MESSAGING
GENERALIZED BLOCKCHAIN
PROGRAM ANYTHING
thereum.org

> *Whereas most technologies tend to automate workers on the periphery doing menial tasks, blockchains automate away the center. Instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly.*
>
> **Vitalik Buterin**

Cryptocurrency

Ethereum - Vitalik Quote

"A smart contract is a mechanism involving digital assets and two or more parties, where some or all of the parties put assets in, and assets are automatically redistributed among those parties according to a formula based on certain data that is not known at the time the contract is initiated."

Vitalik Buterin

Co-Founder And Inventor Of Ethereum

A Next-Generation Smart Contract and Decentralized Application Platform

Satoshi Nakamoto's development of Bitcoin in 2009 has often been hailed as a radical development in money and currency, being the first example of a digital asset which simultaneously has no backing or "intrinsic value ↗ " and no centralized issuer or controller. However, another, arguably more important, part of the Bitcoin experiment is the underlying blockchain technology as a tool of distributed consensus, and attention is rapidly starting to shift to this other aspect of Bitcoin. Commonly cited alternative applications of blockchain technology include using on-blockchain digital assets to represent custom currencies and financial instruments ("colored coins" ↗), the ownership of an underlying physical device ("smart property" ↗), non-fungible assets such as domain names ("Namecoin" ↗), as well as more complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules ("smart contracts" ↗) or even blockchain-based "decentralized autonomous organizations ↗ " (DAOs). What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.

How many Bitcoin nodes?

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Tue Apr 06 2021 07:02:01 GMT+0300 (GMT+03:00).

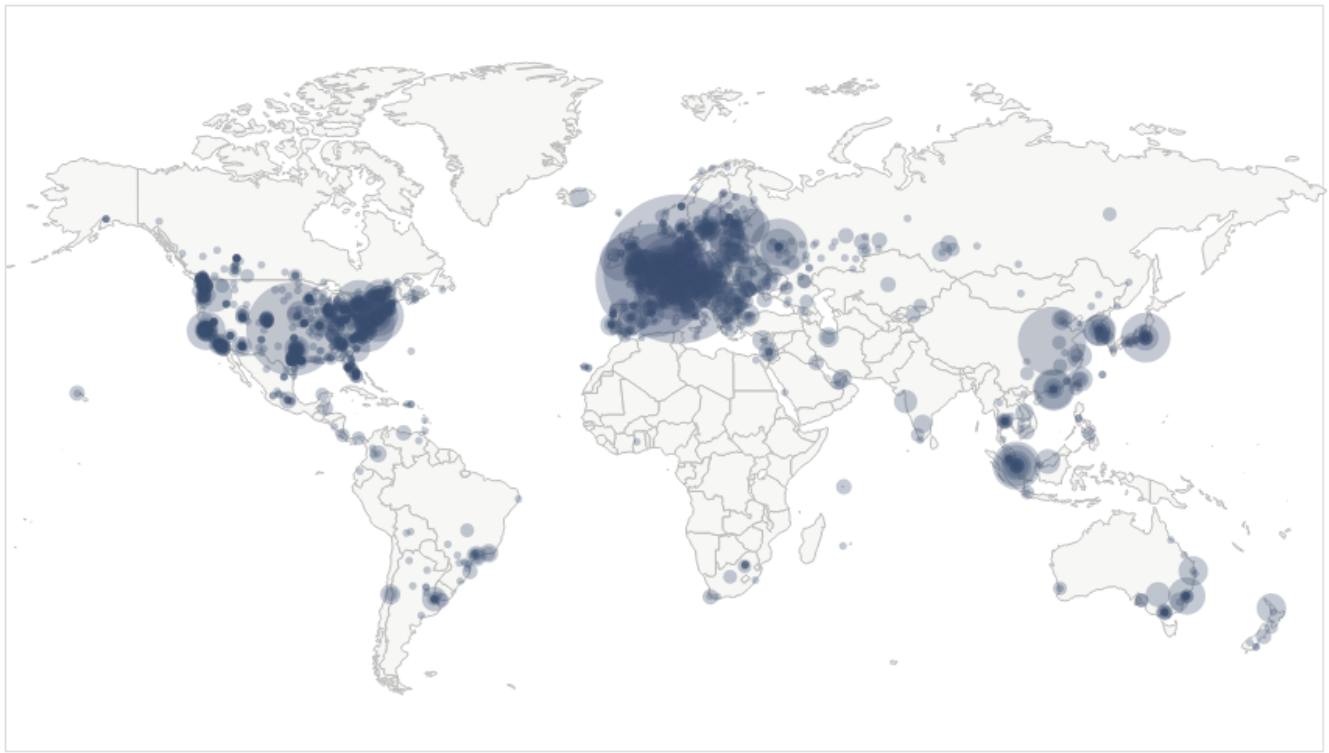
9665 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	1886 (19.51%)
2	Germany	1753 (18.14%)
3	n/a	1746 (18.07%)
4	France	605 (6.26%)
5	Netherlands	414 (4.28%)
6	Canada	322 (3.33%)
7	United Kingdom	285 (2.95%)
8	Russian Federation	239 (2.47%)
9	China	192 (1.99%)
10	Singapore	158 (1.63%)

More (97) »



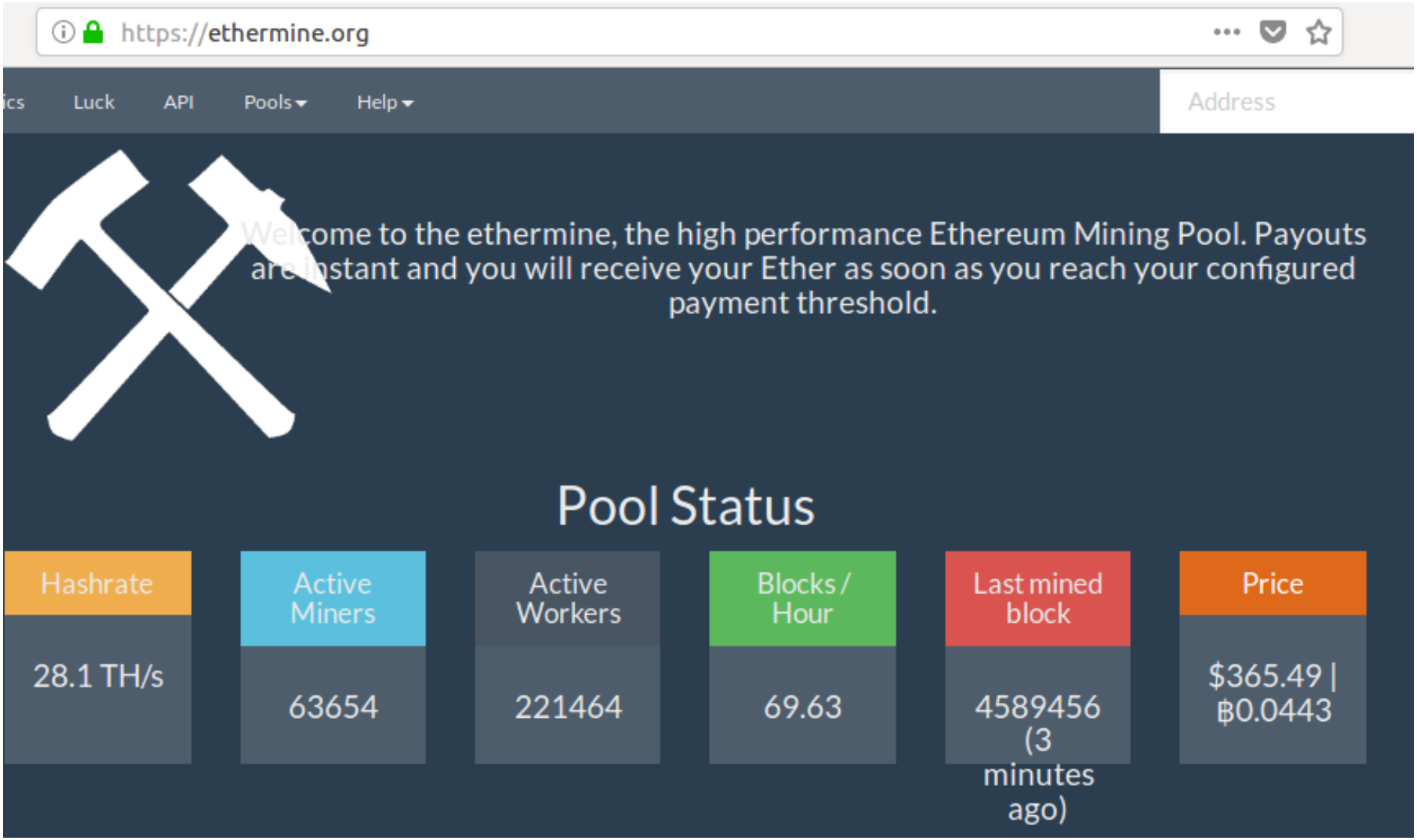
Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

For an updated view: https://bitnodes.io/

Cryptocurrency

Pool - Ethermine



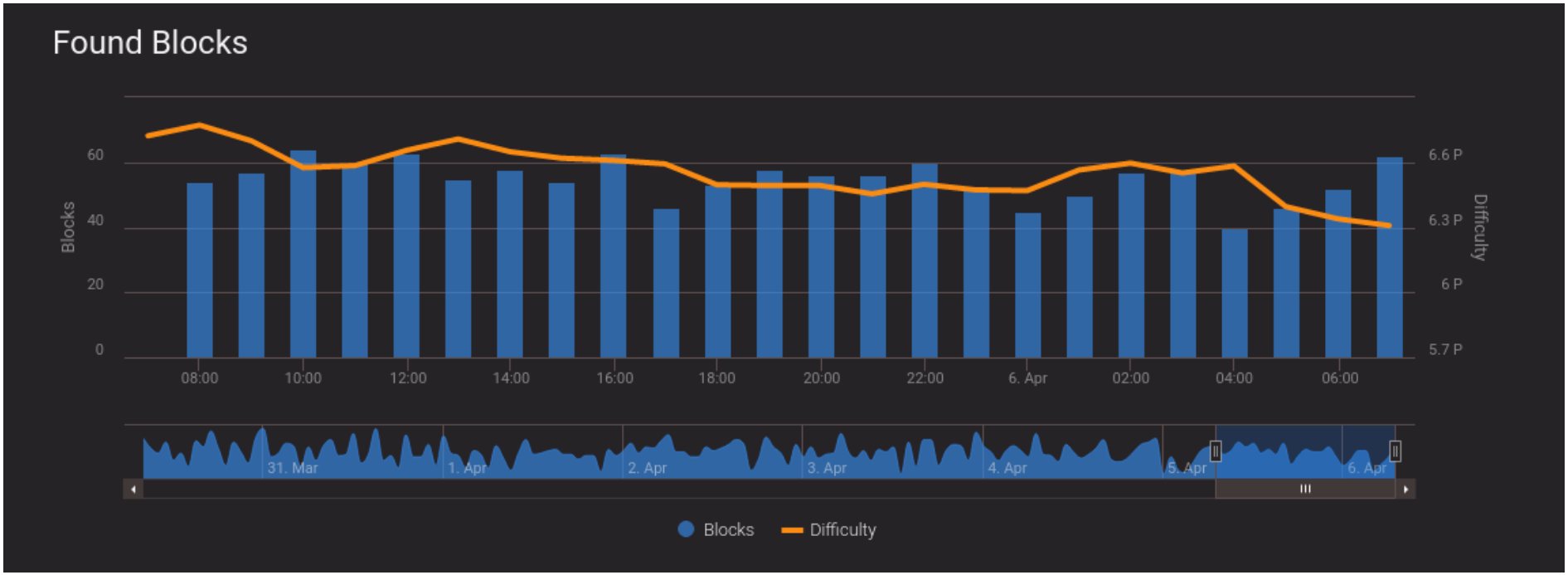
Old graphics, for an updated view: https://ethermine.org

Cryptocurrency

Pool - Ethermine.org

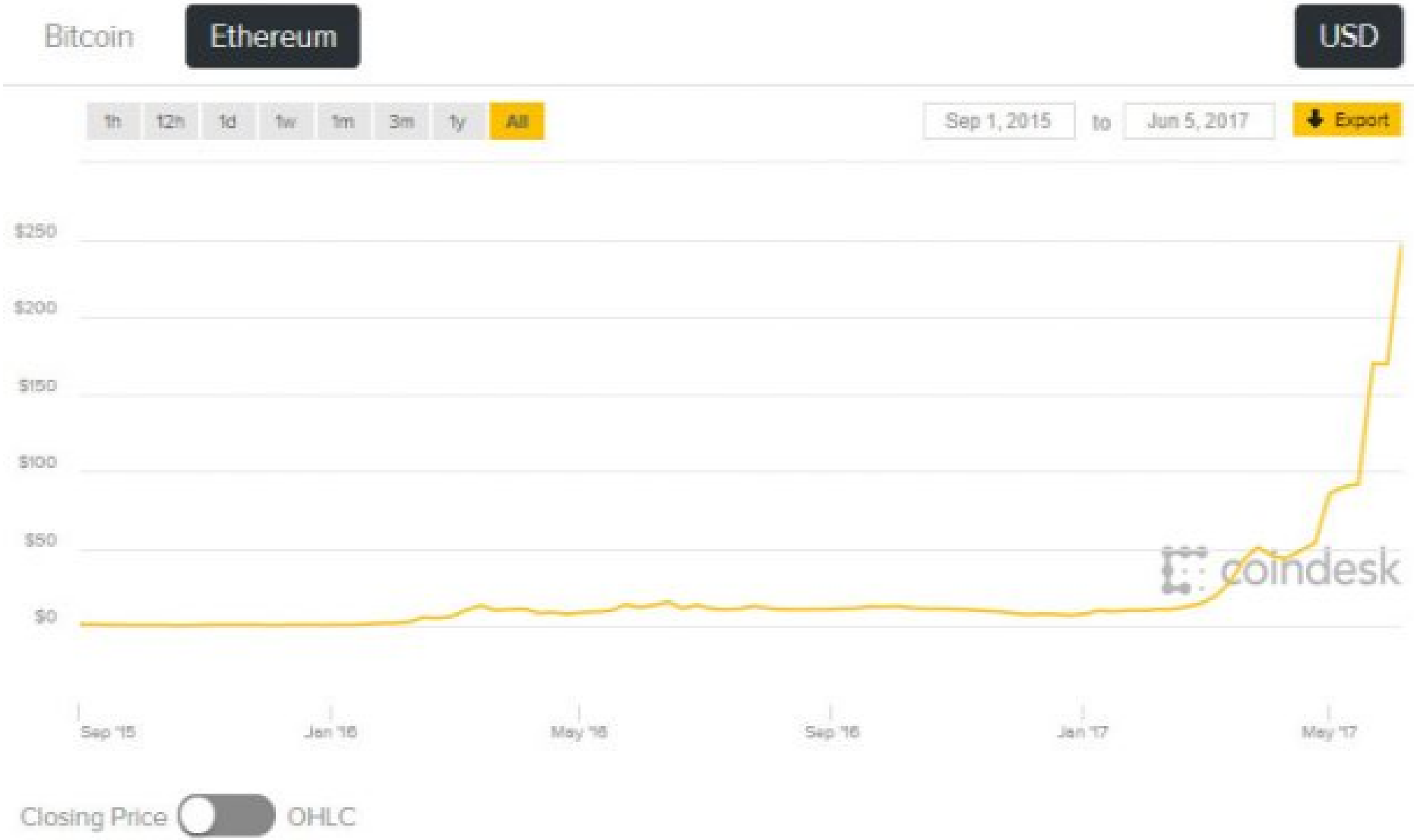
Cryptocurrency

Pool - Ethermine.org



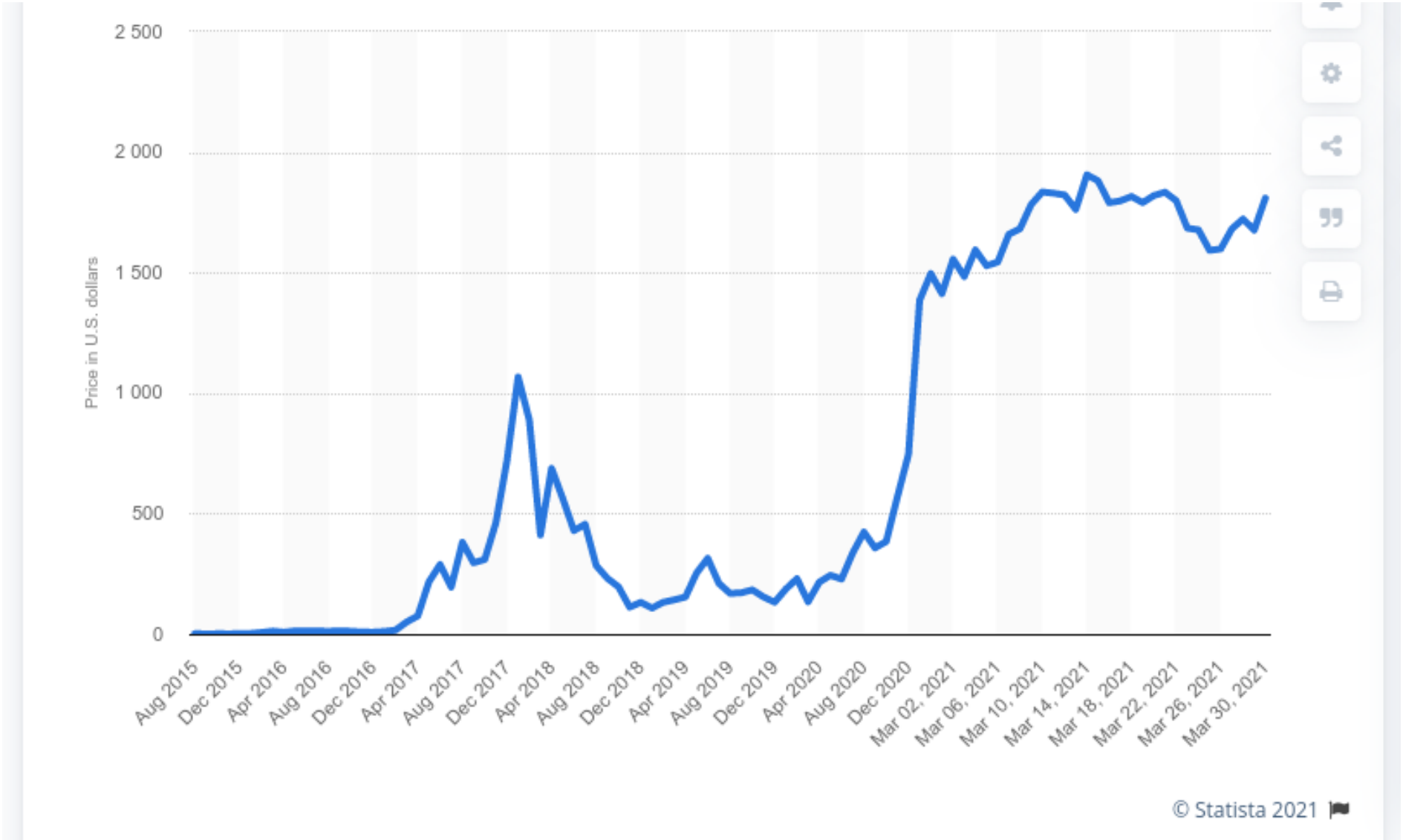
Cryptocurrency

Economy - Value



Cryptocurrency

Economy - Value - Meme Coins

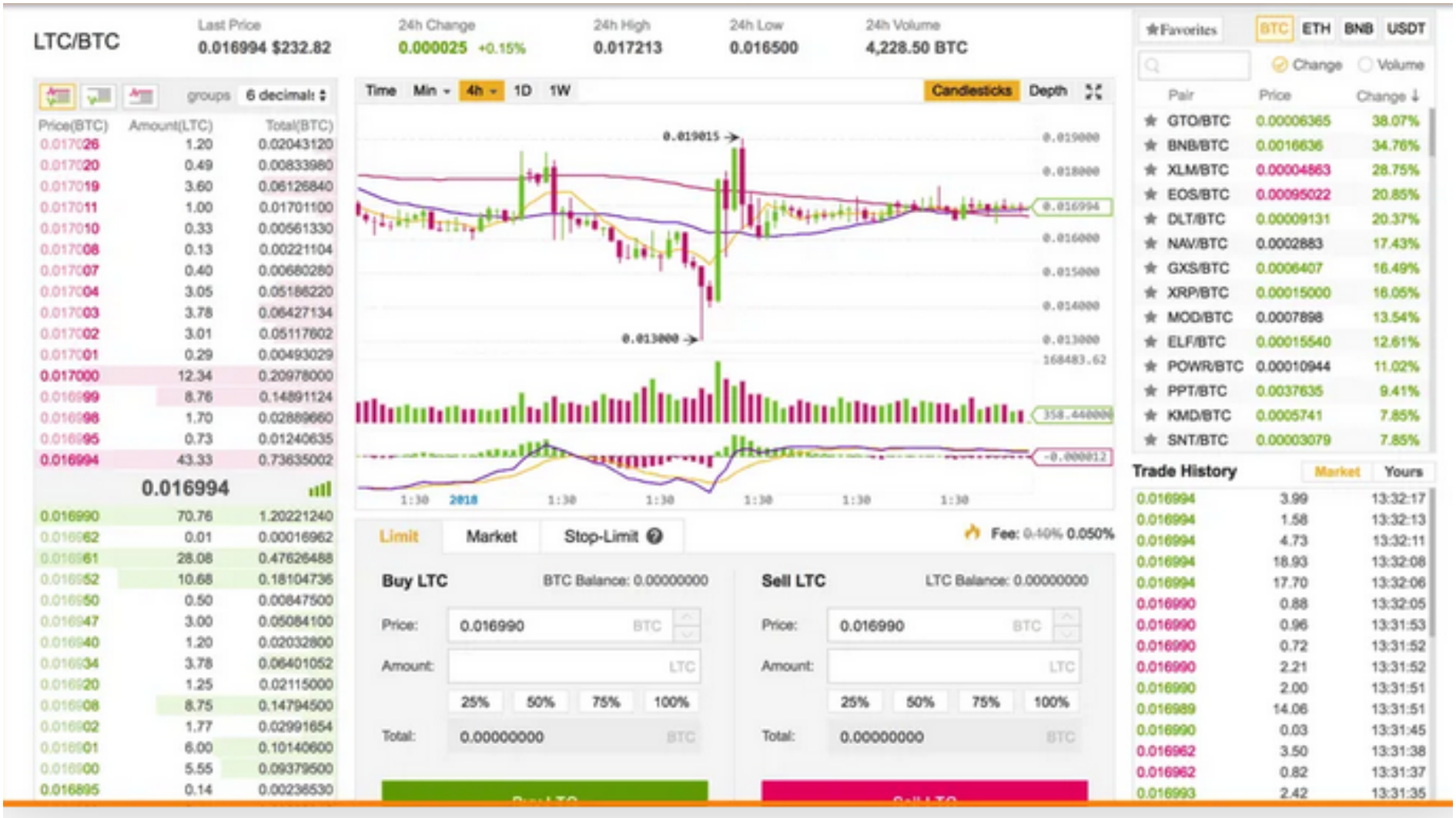


Cryptocurrency

Economy - Value

Cryptocurrency

Exchange



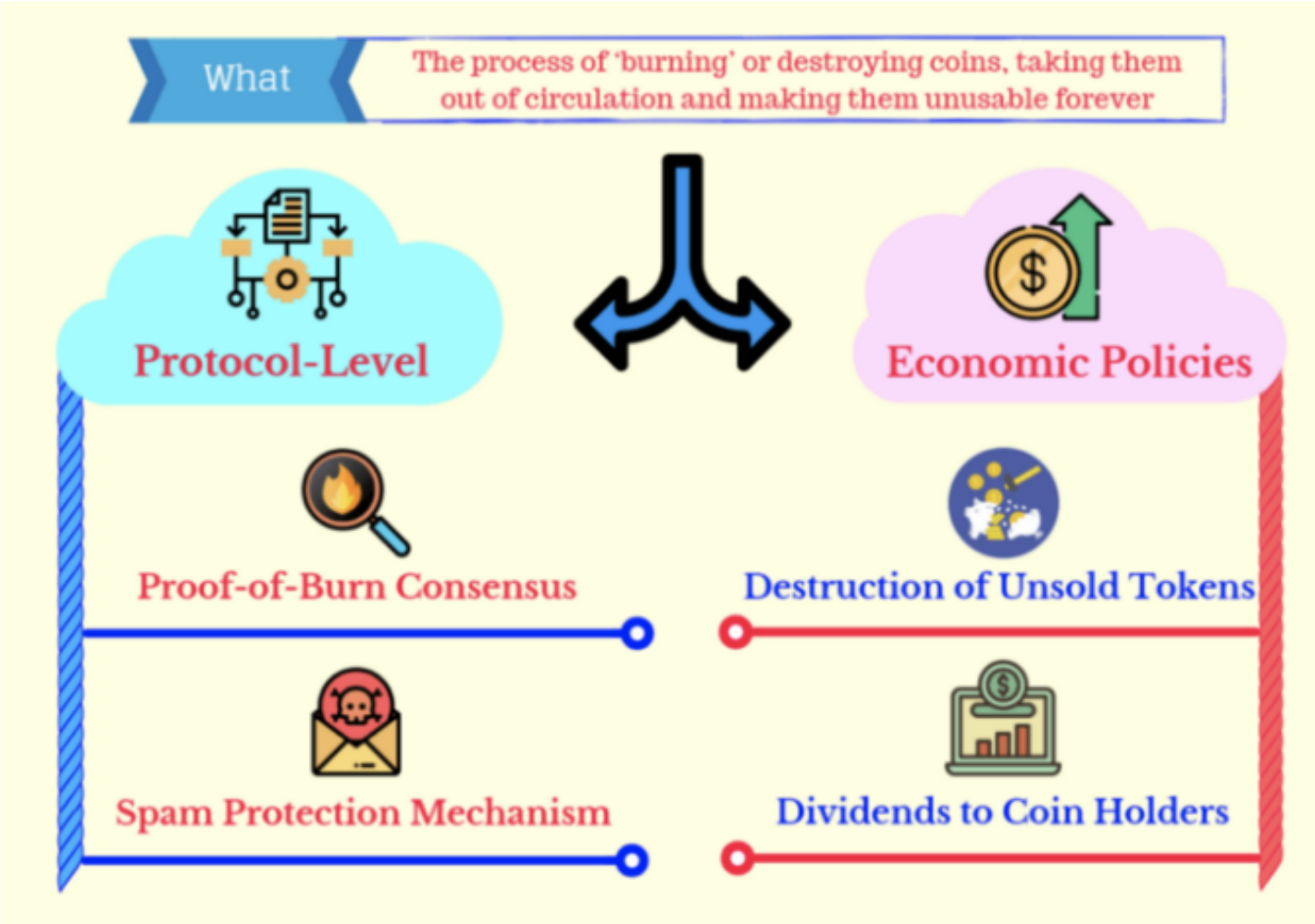

WHO SAID CRYPTO WAS STRESSFUL?
I'M 25 AND I FEEL GREAT!

Staking


WHAT IS STAKING?
Staking means participants hold their cryptocurrency funds in a wallet and thus support the blockchain's functionality. Stakeholders lock their tokens in their wallets. In return, they are rewarded by the network.
Participants become an important part of the network's security infrastructure, acting as validators.
Staking income is offered in the form of interest paid to the holder.

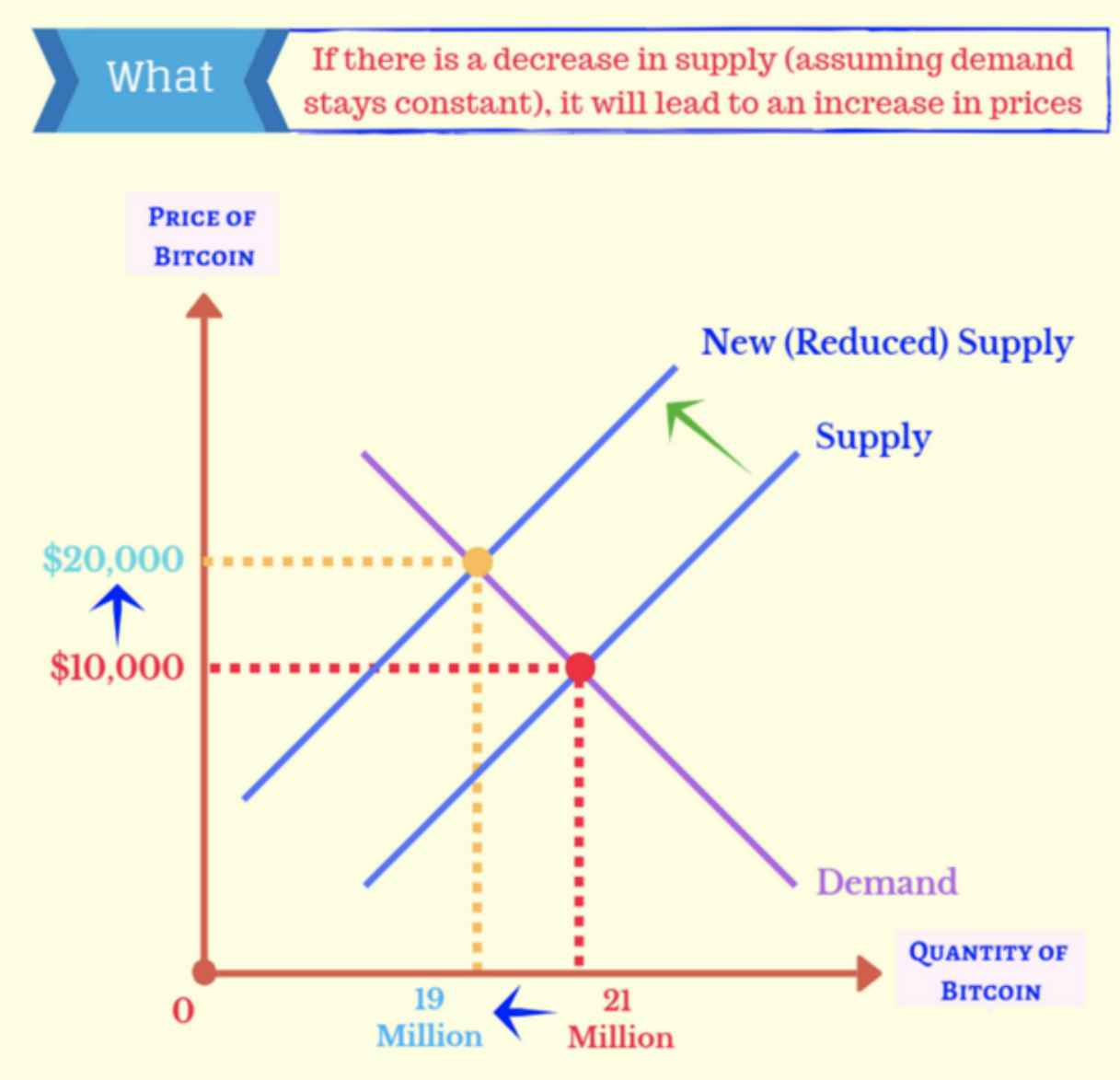
Coin burning[3]

Categories



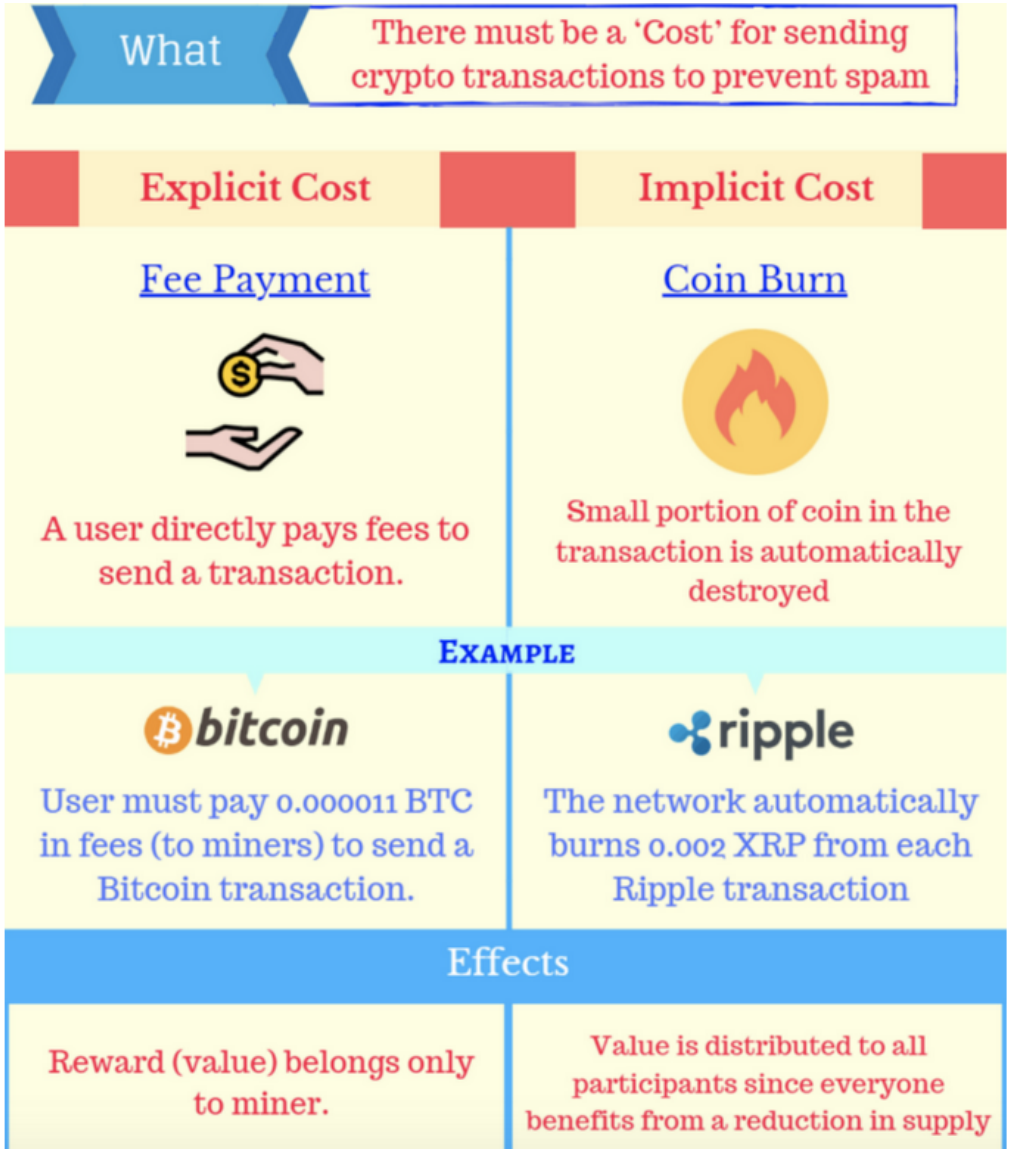
Coin burning to[3]

Increase Value of Coins

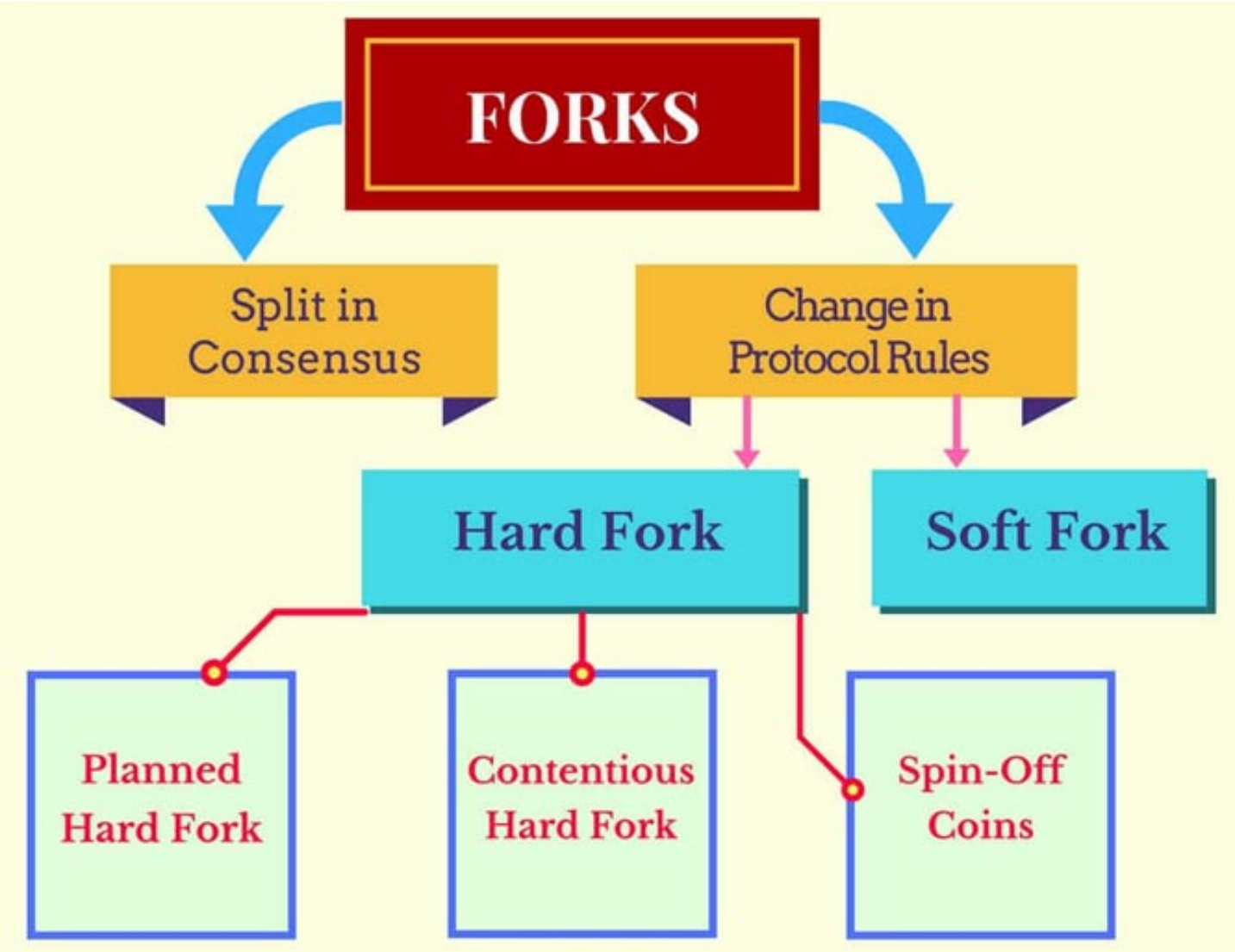


Coin burning to [3]

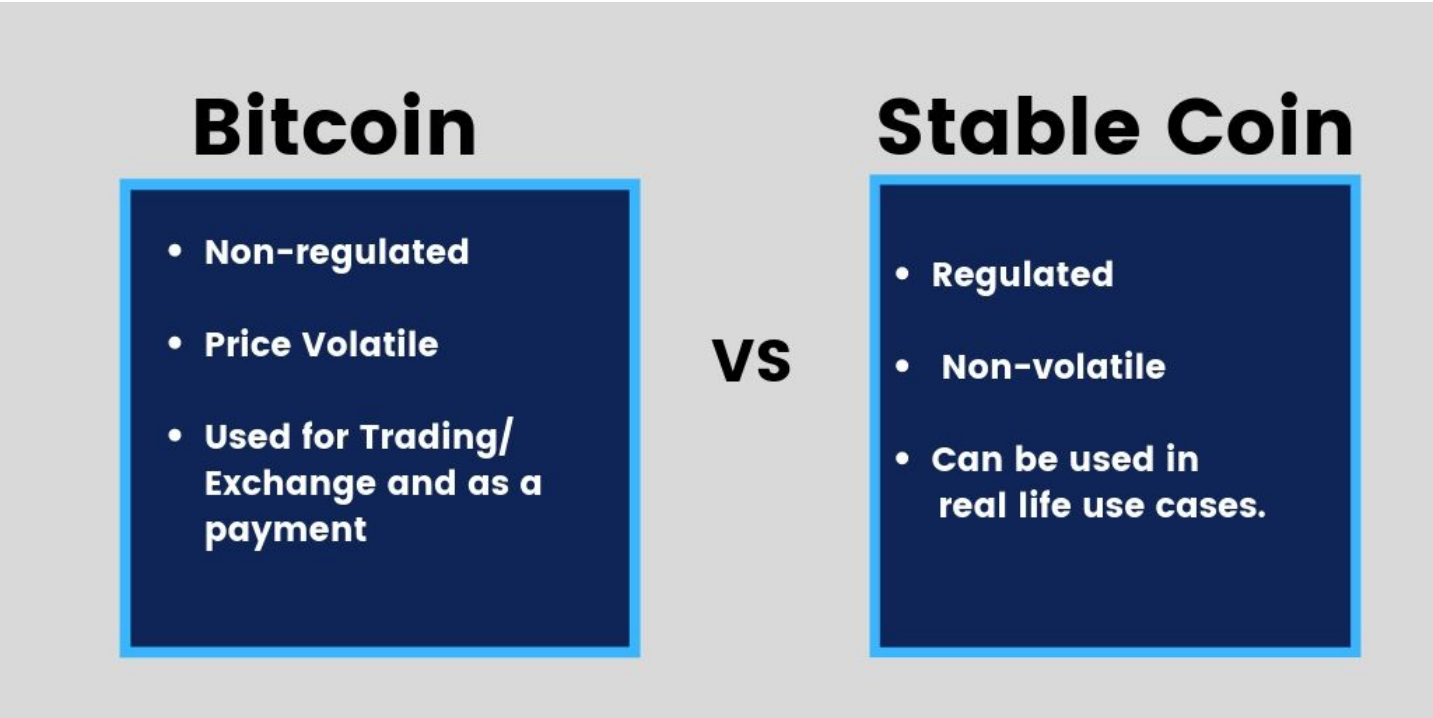
Protection Against Spam



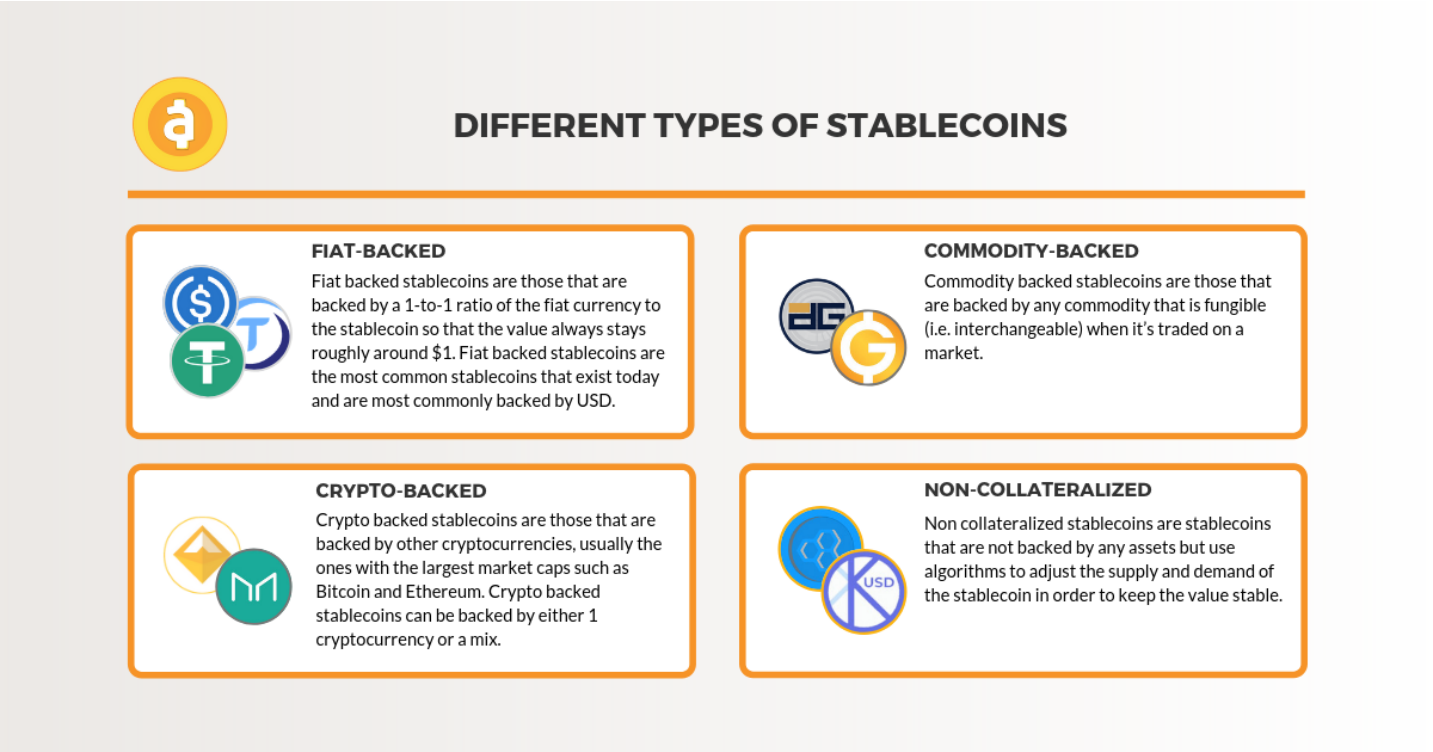
Forks[5]


FORKS
Split in Consensus
Change in Protocol Rules
Hard Fork
Soft Fork
Planned Hard Fork
Contentious Hard Fork
Spin-Off Coins

Stable Coins



Stable Coins



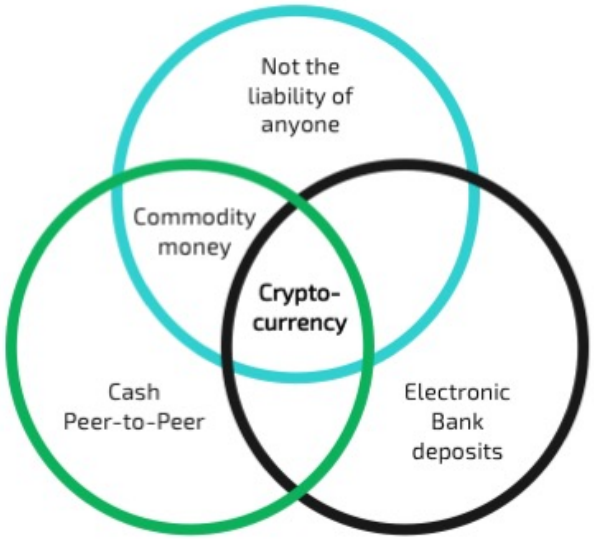
Stable Coins

Types	issue company	issue time	asset-backed by	Issue principle	supervision mechanism
USDT	Tether	Februray 2015	USD	Bitcoin blockchain	Every USDT token issued, they will be backed by a US Dollars in their reserve account. But didn't provide any official documentation or audits.
TUSD	TrustToken	March 2015	USD	Ethereum blockchain	Collateralized, legally protected, and transparently verified by third party Accounting Firm (Cohen & Co)
USDC	Coinbase and Circle	May 2018	USD	Ethereum blockchain	Collateralized by a corresponding USD held in accounts subject to regular public reporting of reserves.
PAX	Paxos	September 2018	USD	Ethereum blockchain	Subject to US government supervision, and audited by Withum. A monthly report on mortgage assets is provided, and PAX also discloses its smart contracts.
EUSD	Epay	January 2019	USD	Ethereum blockchain	Regularly publish third-party audit reports to verify the transparency and legality of it.
DAI	MakerDAO	December 2017	Ether	Ethereum blockchain	Economic incentives ensure that the value is maintained.

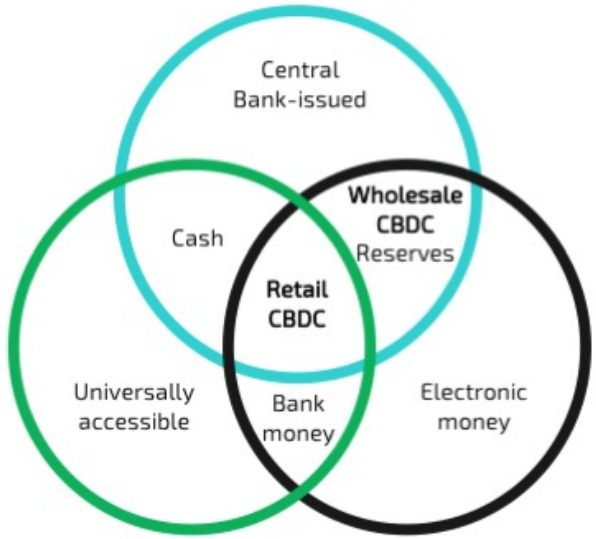
Stable Coins

New Forms of Currency in 2021

Cryptocurrency (CPMI, 2015)



Central Bank Digital Currency (Bjerg, 2017)



Cryptocurrency

Humor - for the many things that we can't cover now


Turkcell LTE
23:20
Tweet
Alphan Manas
@alphanmanas
Emniyet çoğunlukla suça dahil olan silah, mühimmat, uyuşturucu vs'yi yakaldıktan sonra dizerek sergiliyor. Bu kez konu 'Siber Suç' olunca ilginç olmuş.
Translate from Turkish
SİBER SUÇ. MÜC. ŞUBE MÜDÜRLÜĞÜ

Cryptocurrency

The agenda can surprise at any time

- Developments in the World
- Developments in Our Country
  - Regulations?
  - 2020 Presidential Annual Program - cryptocurrency?
  - New bans?
  - New taxes?
  - SWIFT Alternatives (SFPS?)
  - Municipalities
  - civil society ?

Cryptocurrency

The agenda can surprise at any time


I HAVE NO IDEA
WHAT I'M DOING
ME 24 HOURS AGO
ME TODAY

Metaverse Loading ...

Conclusion

Cryptocurrency will be in our lives much more intensely in the future, but first of all,

- should not be seen as just an easy way to make money (Remember every boost is temporary if you can "live without it"...)
- should have more applications - use in our life...
- It should not conflict with the (Decentralized) Philosophy
  - Countries
  - Companies (Facebook etc.)

Conclusion (ctd.)

- Technology should be studied
  - should become easier to use
  - Needs to be faster, scalable
  - Systems that consume less energy should be developed
  - Must offer different "decentralized" services

Conclusion (ctd.)

- Price fluctuations should become more stable
  - Not based on a technological development that will enable its valuation
  - Speculation and manipulations (with the so-called comments of social media phenomena...)
  - So-called sponsorships
  - Pump groups ...
- Legal arrangements should be made

Conclusion (ctd.)

- Should be cleaned of system abusers...
  - Which have no technology behind it
  - Promises high profits and ends the project after raising the money
- In particular, DeFi (decentralized finance); environments should be created where technology can be studied academically.

End of Section One - Waiting for Your Questions...

Dr. Enis Karaarslan : enis.karaarslan@mu.edu.tr

MSKU Blockchain Research Group
http://wiki.netseclab.mu.edu.tr/index.php?title=MSKU_Blockchain_Research_Gr

Document License

- Documentation license of this presentation: by-nc-sa.
- Articles can be reproduced and quoted provided that the source is cited. All photos and pictures except our drawings were obtained from the internet. Permission was not requested as this presentation is non-commercial and for educational purposes. However, in the event of a complaint, the mentioned picture will be removed from the document.

References

1. Bitcoin Whitepaper
2. Ethereum Whitepaper https://ethereum.org/en/whitepaper/
3. Coin Burning: What it is and How Does it Work?, https://medium.com/@cryptoaims/coin-burning-what-is-and-how-does-it-work-f0ade73dcb46
4. How Does Blockchain Work: Guide for Businesses https://web3devs.com/how-does-blockchain-work-guide-for-businesses/
5. What is a cryptocurrency fork? http://www.forex-central.net/Cryptocurrency-fork.php