MONEY-LAUNDERING AND CRYPTO-ASSETS

Colonel t.SPEF Giuseppe Lopez

GUARDIA DI FINANZA

THE HISTORY OF BITCOIN

1998: Wei Dai (a Chinese cypherpunk computer scientist) theoretically proposes the B-Money system, a digital currency that uses a *decentralized* "*Ledger*" to manage the record of transactions.

1998: Nick Szabo (an American computer scientist of Hungarian origin) proposes Bitgold, a digital currency (which never came to life) that defines the concept of "Blockchain" for managing trust and consensus, with a clear focus on privacy, use of cryptography and *proof-of-work*.

In 1998, Nick Szabo designed a mechanism for a decentralized digital currency he called "bit gold". Bit gold was never implemented, but its design was a precursor to Bitcoin's architecture.

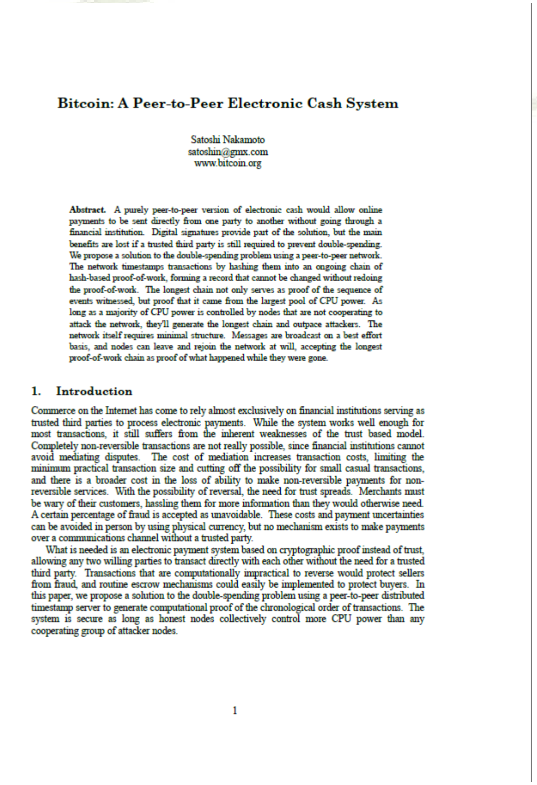
HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

2008

- ❑DIRECT ONLINE PAYMENTS WITH ELECTRONIC MONEY WITHOUT A FINANCIAL INTERMEDIARY (1% TRANSACTION FEES INSTEAD OF 2-4%)

- ❑ELECTRONIC SIGNATURE OF TRANSACTIONS TO GUARANTEE AUTHENTICITY

- ❑TIME-STAMPING TO PREVENT DOUBLE SPENDING GUARANTEED BY THE MAJORITY OF THE NETWORK'S COMPUTING POWER (BLOCKCHAIN)



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

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

There have been many hypotheses about Satoshi's true identity, including Wei Dai, Nick Szabo and several other cypherpunks considered founding fathers, but in fact the mystery has never been revealed.

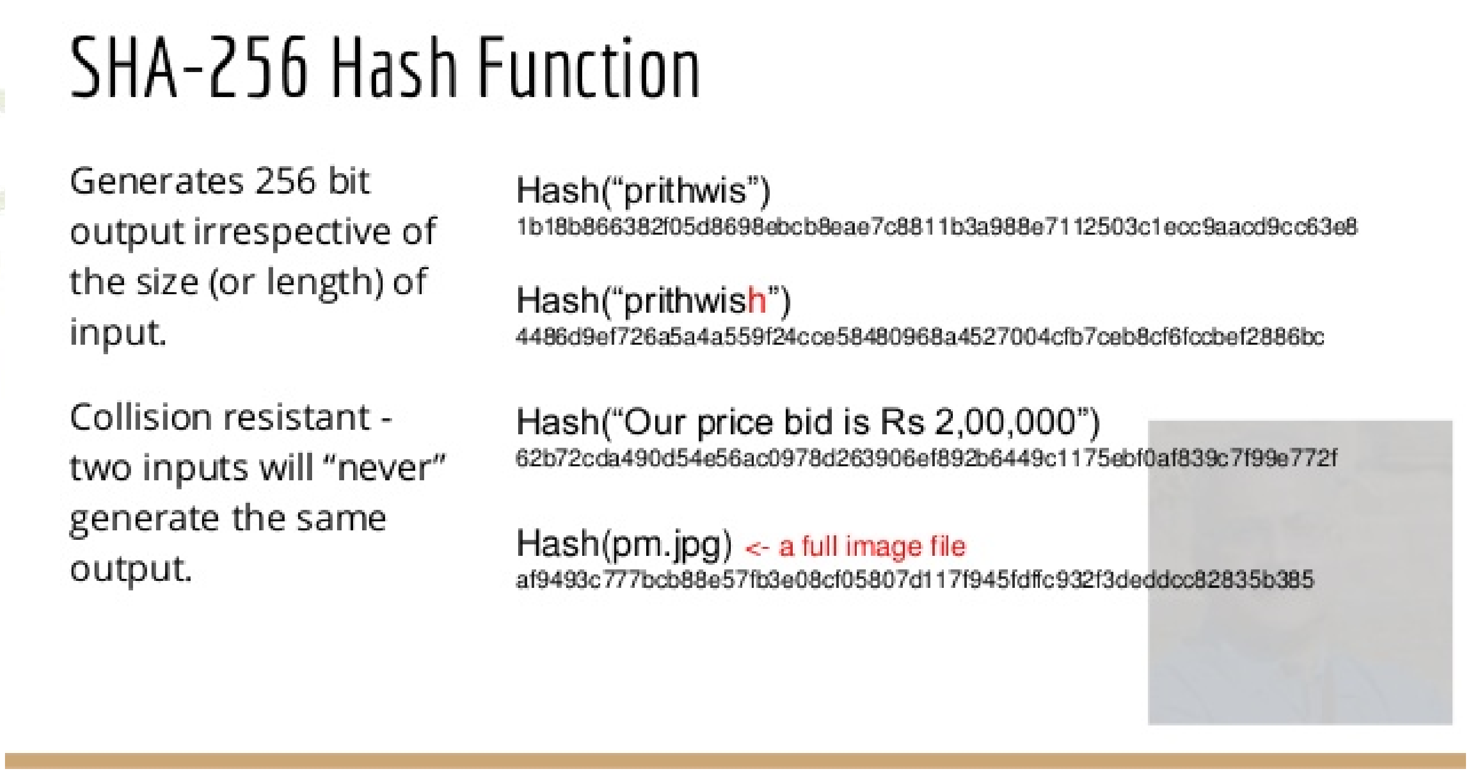
Satoshi's identity is important because there are still 1.1 million unspent bitcoins in his wallet (potentially € 91 billion).

A mysterious figure, likely a group of individuals. He participated in the development of Bitcoin until 2011, but with the first scandals that hit the community (see Wikileaks), he decided to leave and never return.

His last message was: “*I've moved on to other things...*"

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

For encryption, *Bitcoin* uses the **SHA-256 function**, whose name stands for ***secure hash algorithm*** invented by the NSA (National Security Agency) of the USA.



SHA-256 Hash Function

Generates 256 bit output irrespective of the size (or length) of input.

Collision resistant - two inputs will "never" generate the same output.

Hash("prithwis")
1b18b866382f05d8698ebcb8eae7c8811b3a988e7112503c1ecc9aacd9cc63e8

Hash("prithwish")
4486d9ef726a5a4a559f24cce58480968a4527004cfb7ceb8cf6fccbef2886bc

Hash("Our price bid is Rs 2,00,000")
62b72cda490d54e56ac0978d263906ef892b6449c1175ebf0af839c7f99e772f

Hash(pm.jpg) <- a full image file
af9493c777bcb88e57fb3e08cf05807d117f945fdffc932f3deddcc82835b385

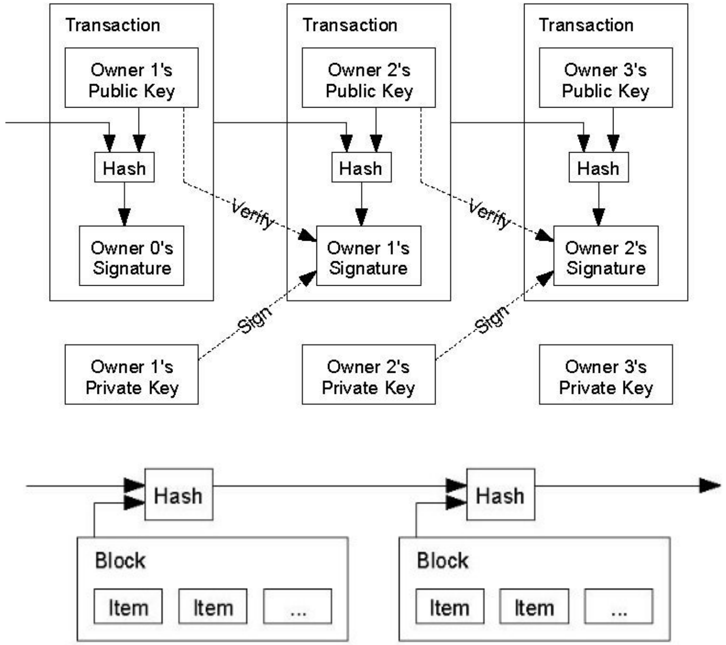
hash fingerprint of a text or computer file is a sequence of letters (a , b, c, d, e, f) and numbers (zero through nine) typically 64 characters long.

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

OBJECTIVE: TO REPLACE TRUST WITH A CRYPTOGRAPHIC SYSTEM

Each owner transfers currency to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding the same to the end of the coin (TRANSACTION CHAIN)

Timestamping works by hashing a block of objects so that they have a timestamp, and then publishing the hash. The timestamp obviously proves that the data must have existed on that particular date, since it ended up in the hash. Each timestamp includes the previous one in its hash, forming a true chain, and each timestamp obviously strengthens the previous ones (BLOCKCHAIN).



https://blockchaindemo.io/
https://coindemo.io/

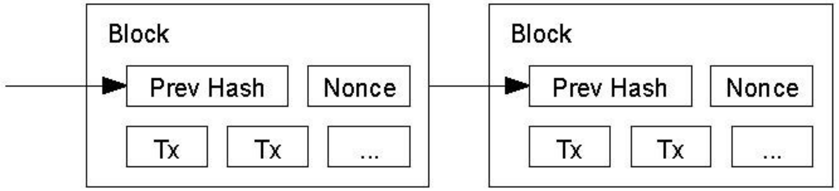
Based on *blockchain,* there is a technology called *permissionless distributed ledger technology* (DLT), which allows consensus to be reached on changes to a distributed ledger in the absence of a central administrator. In this case, the ledger is structured into blocks of validated transactions linked together using cryptographic techniques.

https://www.blockchain.com/explorer

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

OBJECTIVE: TO REPLACE TRUST WITH A CRYPTOGRAPHIC SYSTEM

To implement timestamping on a *peer-to- peer network, we will need to use a proof-of-work* system *that involves finding a value that, when hashed (e.g. with SHA-256), returns a hash starting with a number of zero.*



```
"Hello world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello world! 2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello world! 4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world! 4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

To compensate for increasing hardware speeds and the changing interest of operating nodes over time, *proof-of-work* difficulty is determined by a moving average that aims to create an average number of blocks per hour. If blocks are generated too quickly, the difficulty increases.

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

WHY INTRODUCE PROOF OF WORK?

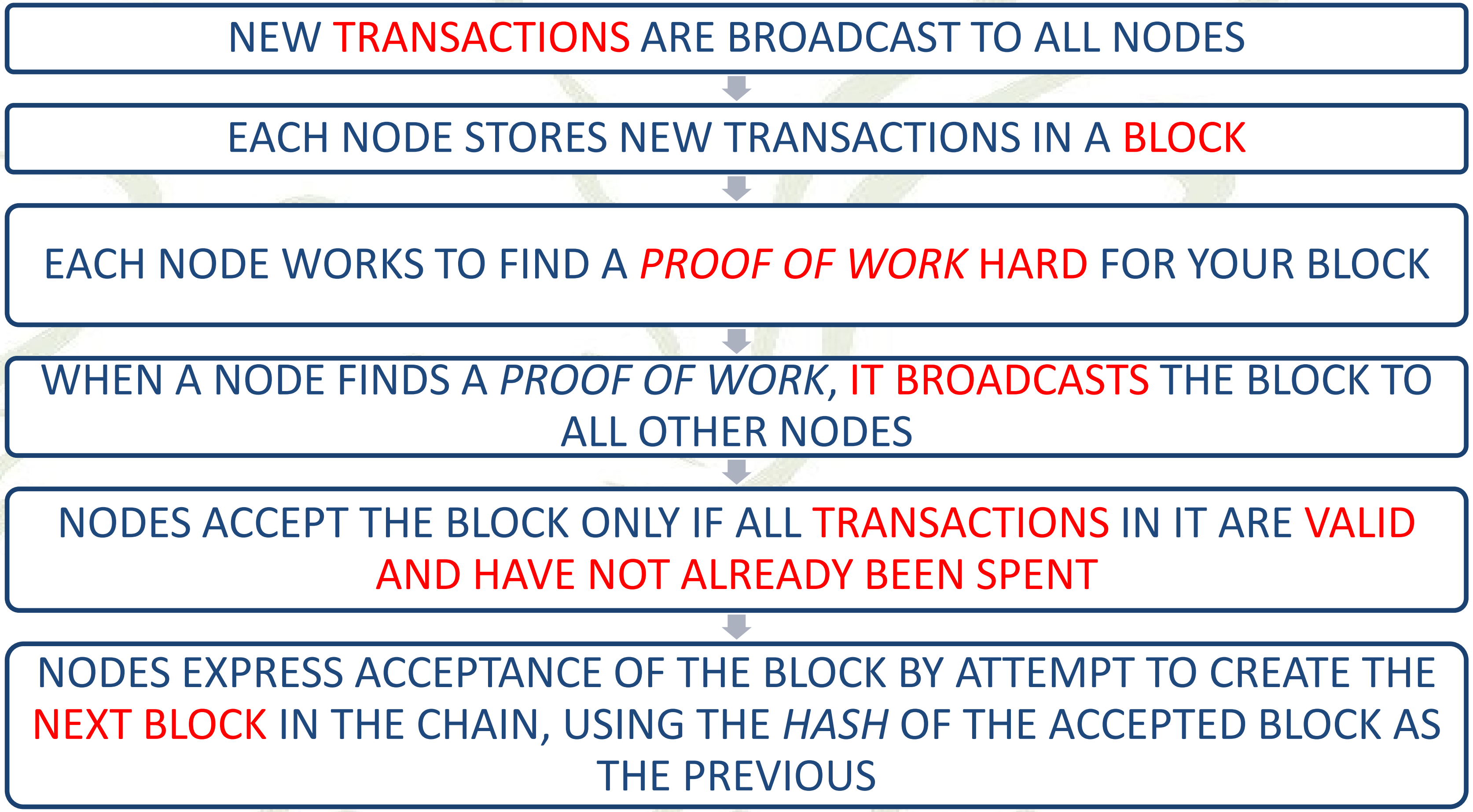
THE MAIN ADVANTAGES ARE
A GREAT DEFENSE AGAINST ATTACKS TWO
AND THE GUARANTEE OF REPRESENTATION IN MAJORITY DECISIONS

Proof *of work* imposes several limits on the actions that can be performed on the network, and an efficient attack would require a huge amount of time and incredible computing power. Although DOS attacks on a blockchain are theoretically possible, in practice the results would be disappointing and the costs extremely high.

In a *proof-of-work system,* the only thing that matters is the computing power used to solve mathematical problems and generate new blocks. Those with large amounts of money, therefore, have little control over the network.

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

HOW THE NETWORK WORKS



NEW TRANSACTIONS ARE BROADCAST TO ALL NODES

EACH NODE STORES NEW TRANSACTIONS IN A BLOCK

EACH NODE WORKS TO FIND A *PROOF OF WORK* HARD FOR YOUR BLOCK

WHEN A NODE FINDS A *PROOF OF WORK*, IT BROADCASTS THE BLOCK TO ALL OTHER NODES

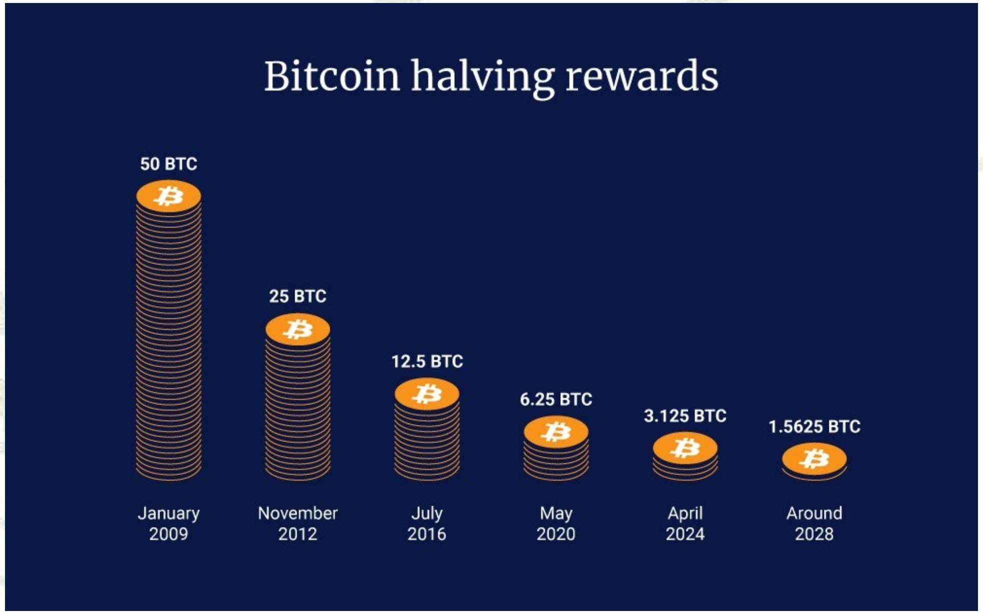
NODES ACCEPT THE BLOCK ONLY IF ALL TRANSACTIONS IN IT ARE VALID AND HAVE NOT ALREADY BEEN SPENT

NODES EXPRESS ACCEPTANCE OF THE BLOCK BY ATTEMPT TO CREATE THE NEXT BLOCK IN THE CHAIN, USING THE *HASH* OF THE ACCEPTED BLOCK AS THE PREVIOUS

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

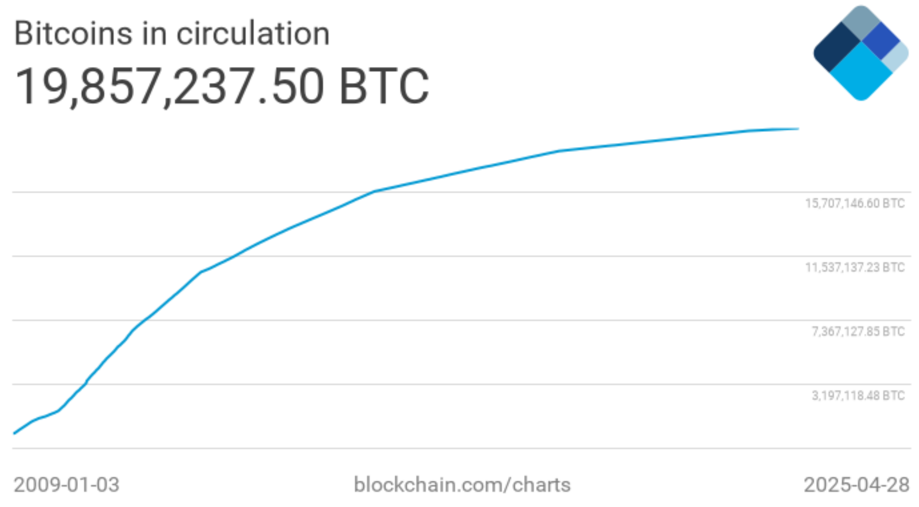
HOW TO PROMOTE NODES: MINING

By convention, the first transaction in a block is a special transaction that “mints” a new coin owned by the block’s creator (Coinbase transaction). This provides an incentive for nodes to support the network and provides a way for the initial distribution of coins into circulation (Block reward). The initial incentive was 50 bitcoins, but it is halved every 210,000 blocks and is currently 3,125 bitcoins. It will reach zero when the maximum number of bitcoins is reached (in 2144).



The incentive can also be funded through transaction costs. Once 21 million bitcoins have entered circulation, the incentive can be fully transferred to transaction costs and will be completely free of inflationary effects.
The incentive can help encourage nodes to remain honest. If an attacker were able to greedily gather more CPU power than all the honest nodes, they would have to choose between fraudulent use or using it to mint new coins. They must necessarily find it more profitable to play by the rules, since they favor them with more new coins than everyone else combined, rather than undermining the security of the system and the validity of their own wealth.

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS



Bitcoins in circulation

19,857,237.50 BTC

blockchain.com/charts

The network is designed to hold a maximum of 21,000,000 bitcoins.

Bitcoin is growing at a rate of 4% per year and 99% will be mined by 2030 (but the last 1% by 2144).

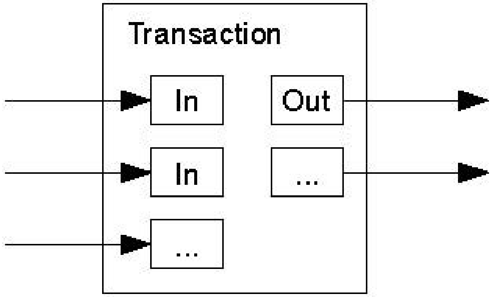
The current reward is 3,125 bitcoins per block.

The “extraction” process is becoming increasingly complex and economically less profitable due to the energy costs for the CPU and cooling.

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

TRANSACTIONS: ADDED AND DIVIDED VALUE

Even if it were possible to move coins individually, it would be unwise to conduct a separate transaction for each cent involved in a transfer.
To ensure that value can be added and divided, transactions contain multiple inputs and outputs.
Typically, there will be a single input from a previous large transaction or multiple inputs grouping smaller amounts, and at most two outputs: one for payment and one to give change to the sender.

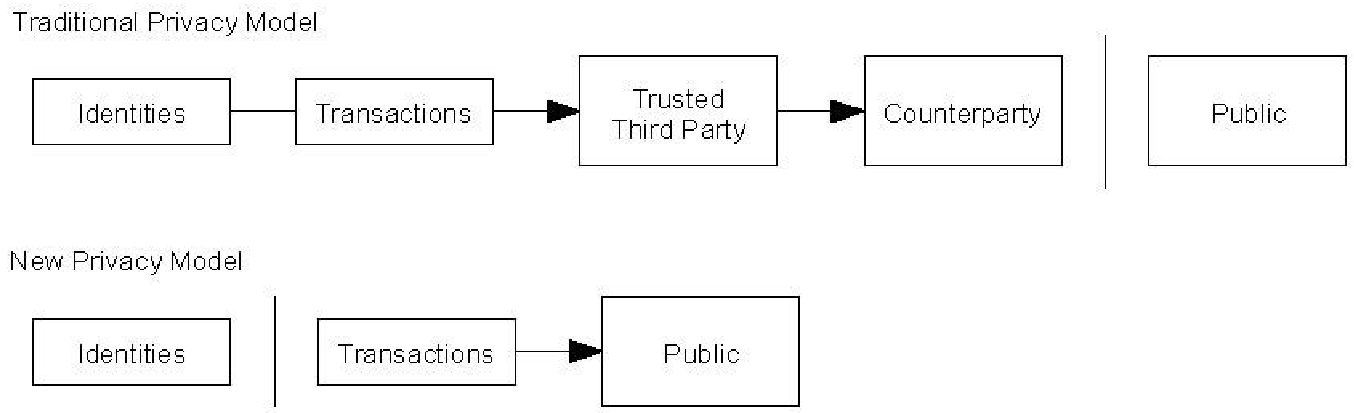


HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

PRIVACY POLICY

The traditional banking model achieves a certain level of privacy by limiting access to information to the parties involved and the trusted third party.

The need to publicly announce all transactions precludes this approach, but privacy can still be maintained by disrupting the flow of information at one additional point: by keeping public keys anonymous. The public can see that someone is sending a certain amount to someone else, but without any information linking the transaction to a specific user.



Traditional Privacy Model

Identities — Transactions → Trusted Third Party → Counterparty | Public

New Privacy Model

Identities | Transactions → Public

As an additional layer of protection, a new key pair must be used for each individual transaction to prevent it from being traced back to a single owner. It's still inevitable that there will be some connection in transactions with multiple inputs, which necessarily reveal that their inputs were owned by the same individual. The risk is that if the owner of a key is revealed, other transactions made by the same person could be traced.

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

THE WALLET

The user must have *client software* capable of managing a *wallet* and accessing the *Bitcoin network.* Alternatively, you can use an *online wallet service*.

A *wallet* is a *software* that allows you to store your *bitcoin* digital credentials. After creating a *wallet* and choosing a *password*, at least one key pair is created (public and private, both with a maximum of 64 alphanumeric characters). For each key pair, a public bitcoin address is also calculated, which being shorter than the keys is also more practical to transmit (a text string of *26-35* characters starting with 1, 3 or bc1 and using upper and lower case letters of the English alphabet except - if it starts with 1 or 3 - lowercase L and uppercase I, uppercase O, more than 10 digits except zero, e.g.: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa).

You can create multiple key pairs, perhaps one for each transaction. The public key is generated from the private key using an irreversible (one-way) function, and the *Bitcoin* address is calculated from this.

It's worth remembering that, unlike traditional wallets, digital wallets do not contain the currency. In fact, digital currencies are not recorded anywhere on your device. To determine our availability of *Bitcoin,* the *wallet* scans all transactions on the *blockchain* to see which ones concern us and totals the amounts that have entered and gone out.

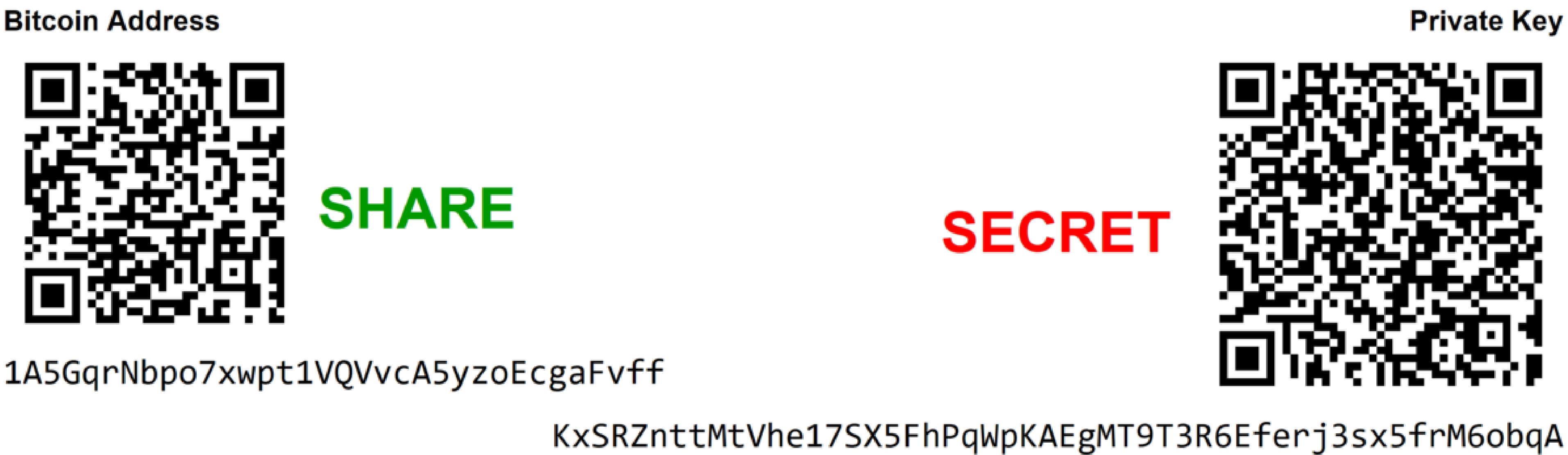
HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

THE WALLET

In short, a cryptocurrency *wallet is a tool that you can use to interact with a blockchain network*, which generates the information needed to send and receive cryptocurrencies over the internet. *blockchain* transactions (*bitcoin address*).

The private key allows you to access your cryptocurrency regardless of the *wallet* you use. So, even if your computer or smartphone is compromised, you'll still be able to access your funds from another device, as long as you have the corresponding private key. Remember, coins never leave the *blockchain*; they're only recorded from one address to another.

The different types of *wallets* can be divided into three groups: *software wallets, hardware wallets* and *paper wallets*. Depending on their operating mechanisms, they can also be referred to as *hot* wallets or cold wallets.



Bitcoin Address

SHARE

1A5GqrNbpo7xwpt1VQVvcA5yzoEcgaFvff

Private Key

SECRET

KxSRZnttMtVhe17SX5FhPqWpKAEgMT9T3R6Eferj3sx5frM6obqA

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

HOT WALLET VS. COLD WALLET

A *hot wallet* is any *wallet* that's connected to the internet in some way. For example, when you create a Binance account and send funds to your *wallet*, you're depositing into the Binance *hot wallet*. These *wallets* are fairly simple to create, and funds can be accessed quickly, making them useful for *traders* and those who frequently use cryptocurrencies.

The *cold wallets*, on the other hand, do not have an internet connection. Instead, they use a physical medium to store keys offline, making them resistant to online cyberattack attempts . As a result, cold wallets tend to be a much more secure alternative to “warehousing” your coins. This method is also known as the *cold storage* and is especially suitable for long-term investors.

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

SOFTWARE AND HARDWARE WALLET

Software wallets come in several varieties, each with unique features. Most are connected to the internet in some way (*hot wallets*).

WEB WALLET: Used to access *blockchain* networks through a *browser interface* without having to download or install anything. This category includes *exchange wallets*. In most cases, you can create a new *wallet* and set a *personal password* to access it. However, some service providers hold and manage private keys on your behalf (*custodial wallet providers*). While this may be more convenient for inexperienced users, it is a dangerous practice.

DESKTOP WALLET: This is *software* that you download and run locally on your computer, giving you full control over your keys and funds. When you generate a new *desktop wallet*, a file called "wallet.dat" is stored locally on your computer and contains the private key information used to access your addresses. It is essential to back up your wallet. your wallet.dat file and save it somewhere safe. Alternatively, you can export the corresponding private key. This way, you'll be able to access your funds from other devices should your computer crash or become inaccessible in some way. Overall, *desktop wallets* can be considered more secure than most web versions.

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

WALLET SOFTWARE AND HARDWARE

MOBILE WALLETS: These work similarly to their desktop counterparts but are specifically designed as smartphone apps. This type of wallet is quite convenient as it allows you to send and receive cryptocurrencies through the use of QR codes. Therefore, mobile wallets are particularly well - suited for making everyday transactions and payments, making them a viable option for spending cryptocurrency in the real world. However, like computers, mobile devices are vulnerable to malicious apps and malware infections. Therefore, it is recommended to encrypt the mobile wallet with a password and back up the private keys in case the smartphone is lost or broken.

HARDWARE WALLETS: Keys are stored on a device that is not connected to the internet. Therefore, hardware wallets are considered cold wallets and one of the most secure options. Furthermore, hardware wallets tend to be less user-friendly, and funds are more difficult to access than with a hot wallet. Using a hardware wallet is related to the intention to hold cryptocurrency for a long time or in large amounts. Currently, most hardware wallets allow you to set a PIN to protect your device.

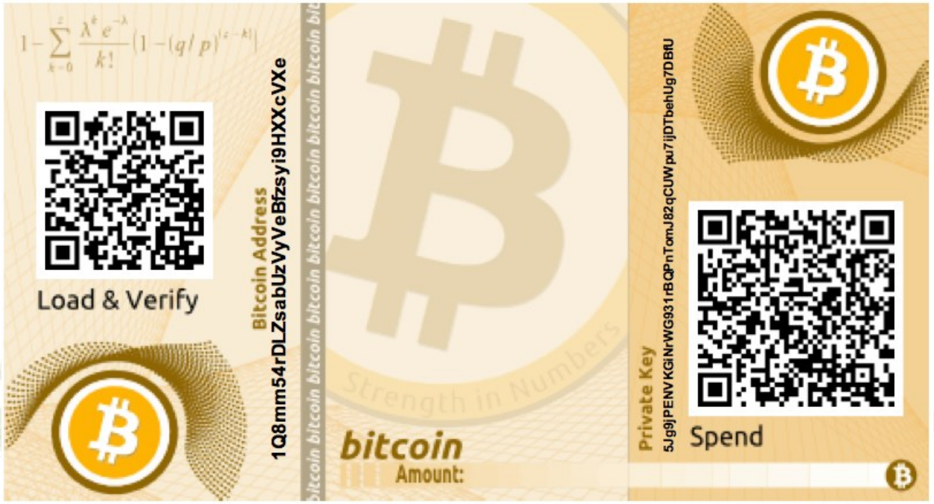
HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

PAPER WALLET

Paper wallet: This is a piece of paper on which an address and its private key are physically printed as a QR code. Scanning these codes allows you to conduct cryptocurrency transactions. These *wallets* are highly resistant to online cyberattacks and can be considered an alternative to *cold storage*.

A major weakness of *paper wallets* is that they don't allow you to send partial funds, only the entire balance at once. For example, imagine you create a *paper wallet* to which you send several transactions, totaling 10 BTC. If you decide to spend 2 BTC, you must first send the 10 coins to another type of *wallet* (e.g., a *desktop wallet*) and spend part of the funds (2 BTC) from there. You can then transfer the 8 BTC to a new *paper wallet*.

However, it's important to remember that your *paper wallet* will be empty after your first outgoing transaction, regardless of the amount, so it cannot be reused.


Load & Verify
Bitcoin Address
1Q8mm54rDLZsabUzVyVeBfzsyi9HXXcVXe
Strength in Numbers
bitcoin
Amount:
Private Key
5Jg9jPENVKGiNrWG931rBQPnTomJ82qCUWpu7ijDTbehUg7DBfU
Spend

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

THE SUBJECTS

***Exchangers*, or online platforms that allow you to buy or sell all the major cryptocurrencies present in the system, in exchange for FIAT currency or other types of crypto assets.**

***Wallet provider*, that is, the person who provides users with the electronic wallet in which to store the keys.**

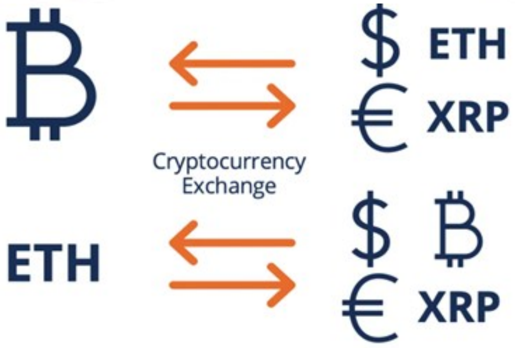
These entities, especially the most reputable and reliable ones, conduct an accurate census of users who register to use the services offered. Therefore, in these cases, it is possible to trace the address of a transaction back to a natural person.

OECD

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

CENTRALIZED EXCHANGE PROVIDER

- subjects that carry out any conversion (*fiat* → crypto, crypto → crypto, crypto → *fiat*) **hold funds** (represented by both *crypto assets* and *fiat currency*) **that are not "theirs"**, that is, third parties, which they may use at any time, or until the conversion operation is carried out;
- if **they also operate** as ***Custodial Exchange Providers*** **hold** the **private keys to the *wallet of those requesting the conversion*** (however, they cannot independently perform any transactions on their behalf).



DECENTRALIZED EXCHANGE PROVIDER

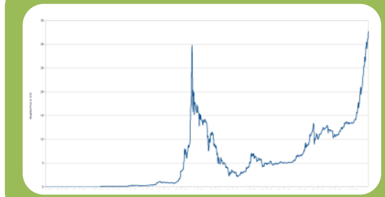
- Entities that **do not hold third-party funds** and simply (allow) trading between users to be managed in a fully automated manner
- Decentralized marketplaces that allow you to manage the **meeting between supply and demand**, automatically

LocalBitcoins.com

HOW BITCOIN WORKS: FUNDAMENTAL CHARACTERISTICS

There is no official value for *Bitcoin:* the reference "price" is taken from the average prices charged by various global exchanges or by the most important exchanges.

Since its creation, the value of a *bitcoin* has grown from a few cents to its current value of over **€ 83,000.**



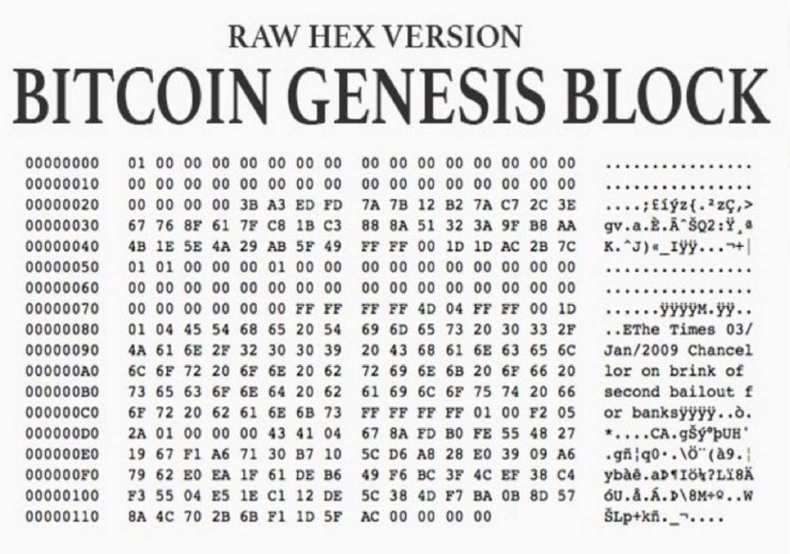
The value is extremely volatile and is influenced by the confidence of the "few" users, their implementation impulses, and current events (exchange failures and thefts).

THE HISTORY OF BITCOIN

- **03.01.2009**: **First block of the blockchain** (*genesis block*). Initially, Bitcoin had no value, but it soon attracted the interest of the computer science community.

- **05.10.2009**: **First market price** corresponding to the cost in terms of electricity for the production of a single bitcoin ($1 = 1,300 BTC)

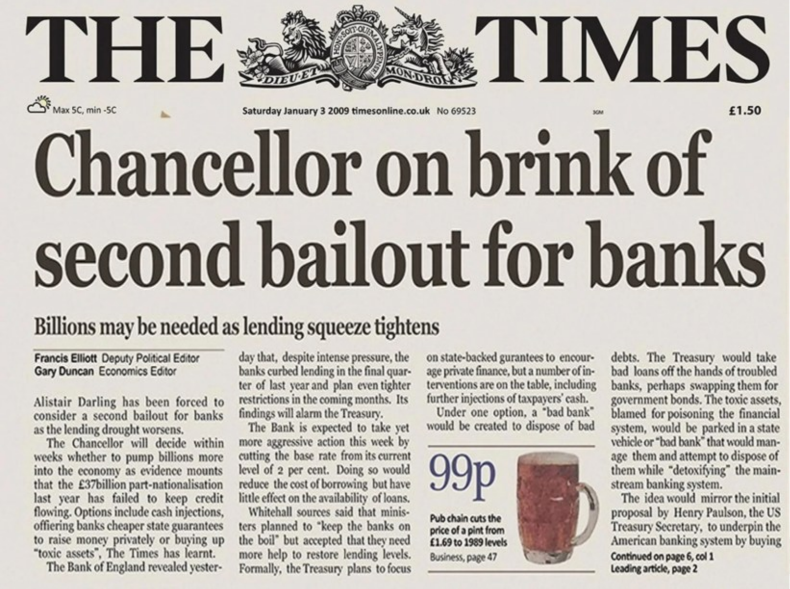
- **06.02.2010**: **bitcoinmarket.org** (first exchange platform for trading bitcoins)



RAW HEX VERSION

BITCOIN GENESIS BLOCK

```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of 
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```



THE TIMES

Max 5C, min -5C   Saturday January 3 2009 timesonline.co.uk No 69523   £1.50

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offiering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed gurantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels

Business, page 47

THE HISTORY OF BITCOIN

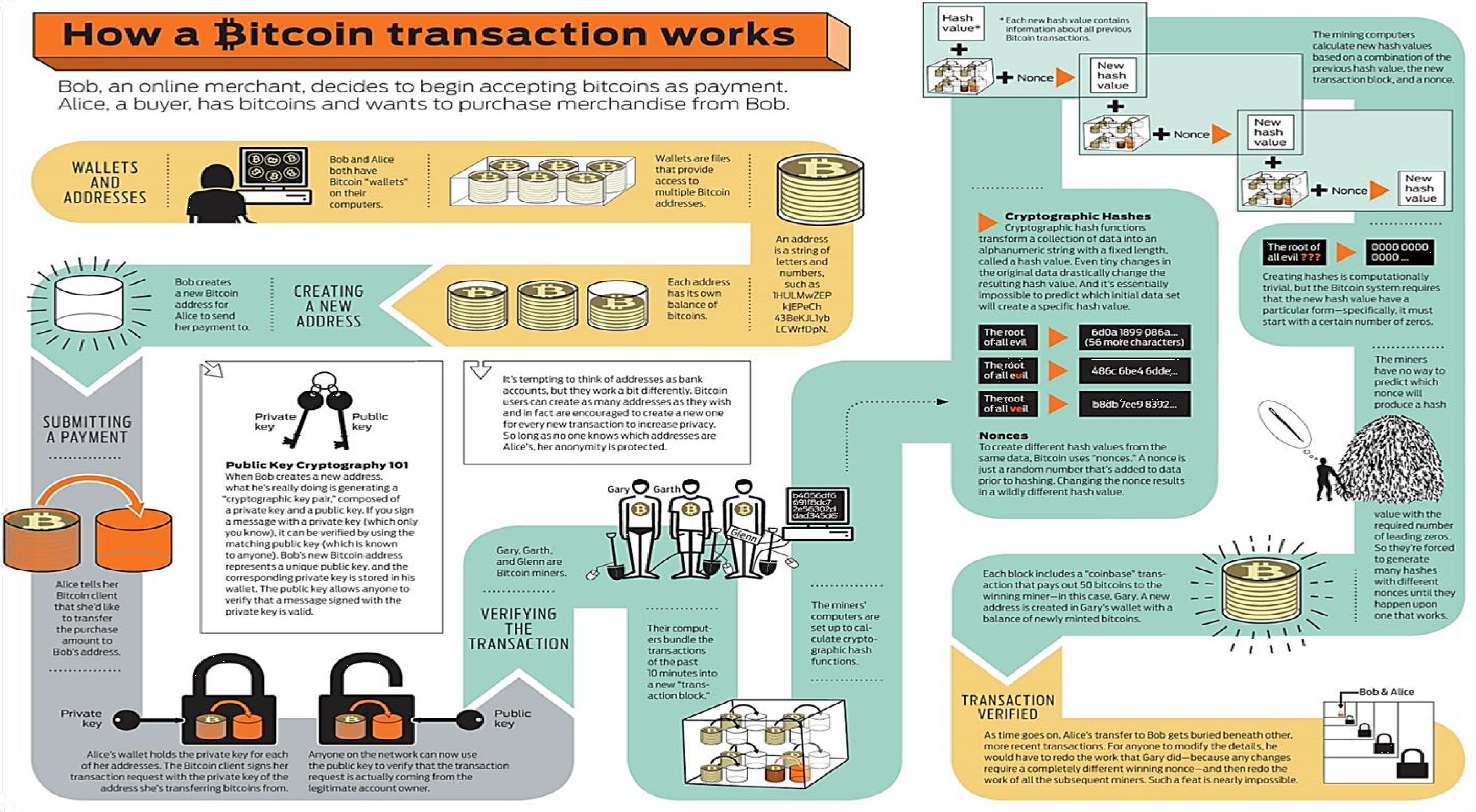
- 22.05.2010: Pizza Day (first transaction establishing a real market price) $25 for 10,000 BTC
- 07.07.2010: Bitcoin version 0.3, according to the well- known computer blog slashdot mention this technology, in the short term hundreds of users develop interest and decide to experiment with the new cryptocurrency.
- 06.08.2010: A vulnerability was discovered in the Bitcoin protocol that allows for the irregular creation of infinite cryptocurrencies. Through a "*soft fork*" the vulnerability is immediately corrected.

Slashdot

*Distinction between **hard forks** and **soft forks**: in the first case the upgrade is not backward compatible because it makes things possible that were not previously allowed (e.g. the coin limit goes from the current 21 million Bitcoin to 42 million), in the second case it is the opposite, i.e. the upgrade is backward compatible because it imposes new restrictions on the rules (e.g. the block size goes from 1 MB to 500 KB). In this second case the new network is compatible with the old one, but not vice versa.*

How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.



WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEPkjEPeCh43BeKJL1ybLCWrfDpN.

Each address has its own balance of bitcoins.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

Public Key Cryptography 101

When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.

Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

* Each new hash value contains information about all previous Bitcoin transactions.

The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

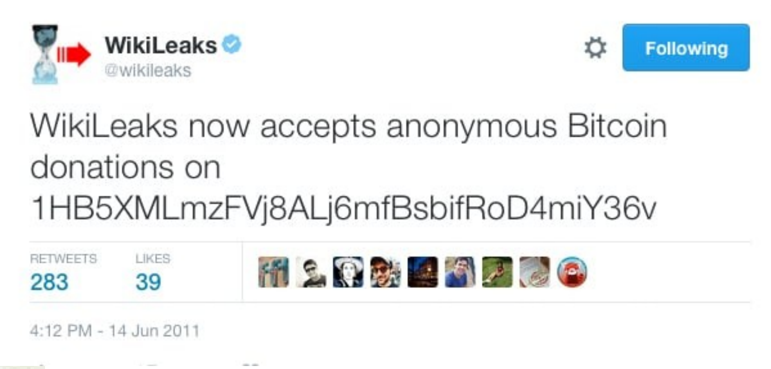
TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

THE HISTORY OF BITCOIN

- **10.12.2010: WikiLeaks scandal - a pirate website attributed to Julian Assange, after having his PayPal account blocked, accepts Bitcoin donations. The first associations between illicit activities and cryptocurrencies emerge. Satoshi abandons the Bitcoin project.**

- **01.02.2011: SilkRoad, the first deep web platform for purchasing narcotics and other illicit goods (1 BTC = 1 $).**



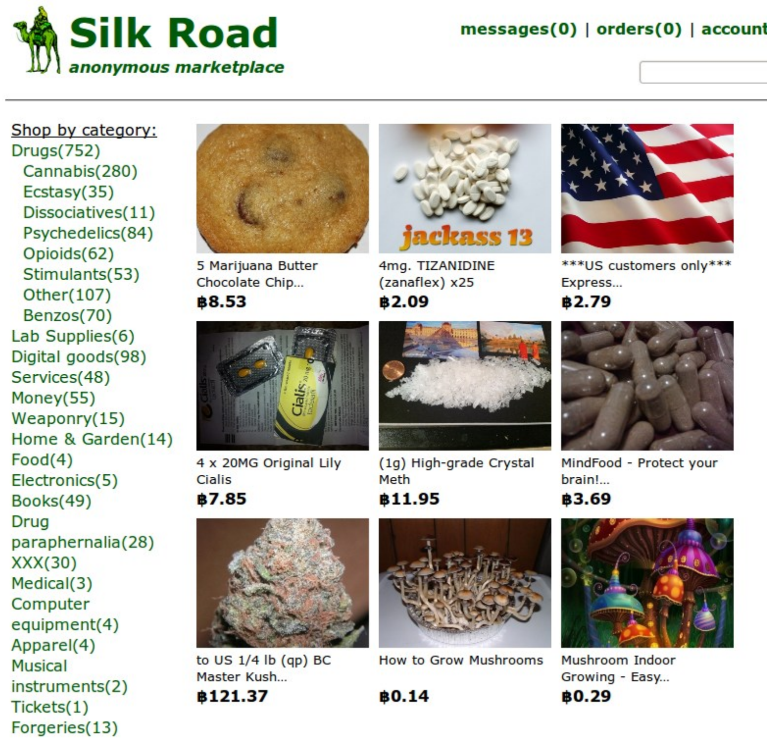
WikiLeaks
@wikileaks

Following

WikiLeaks now accepts anonymous Bitcoin donations on 1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v

RETWEETS 283
LIKES 39

4:12 PM - 14 Jun 2011



Silk Road
anonymous marketplace

messages(0) | orders(0) | account

Shop by category:
Drugs(752)
Cannabis(280)
Ecstasy(35)
Dissociatives(11)
Psychedelics(84)
Opioids(62)
Stimulants(53)
Other(107)
Benzos(70)
Lab Supplies(6)
Digital goods(98)
Services(48)
Money(55)
Weaponry(15)
Home & Garden(14)
Food(4)
Electronics(5)
Books(49)
Drug paraphernalia(28)
XXX(30)
Medical(3)
Computer equipment(4)
Apparel(4)
Musical instruments(2)
Tickets(1)
Forgeries(13)

5 Marijuana Butter Chocolate Chip...
฿8.53

4mg. TIZANIDINE (zanaflex) x25
฿2.09

US customers only Express...
฿2.79

4 x 20MG Original Lily Cialis
฿7.85

(1g) High-grade Crystal Meth
฿11.95

MindFood - Protect your brain!...
฿3.69

to US 1/4 lb (qp) BC Master Kush...
฿121.37

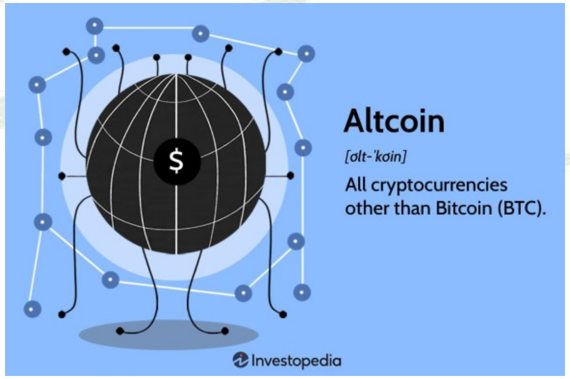
How to Grow Mushrooms
฿0.14

Mushroom Indoor Growing - Easy...
฿0.29

THE HISTORY OF BITCOIN

- **2011: First financial bubble, the first Altcoins emerge on the market at high speed, modified versions of Bitcoin that are presented as an alternative (Litecoin, Namecoin, etc.)**

- **2012: Improvements to the Bitcoin protocol and first “halving” event (reduction of miners ’ fee reward*)***



Altcoin

[ɑlt-ˈkɔin]

All cryptocurrencies other than Bitcoin (BTC).

Investopedia

Bitcoin Halving

[ˈbit-ˌkȯin hävin̩]

An event when the reward for mining Bitcoin transactions is cut in half.

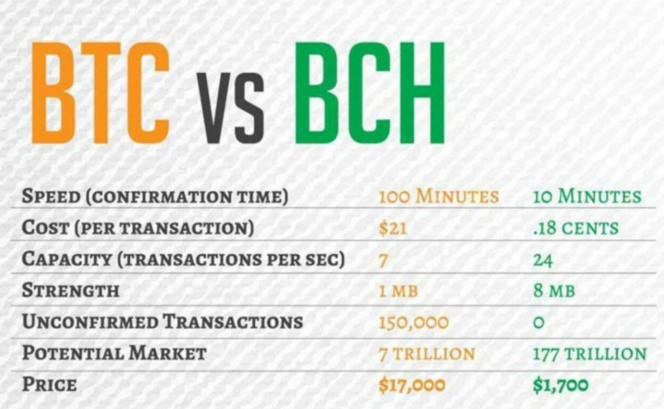
Investopedia

THE HISTORY OF BITCOIN

- **2013-2017**: **Exponential increase in user and market interest, dramatic events determine an unstable and unpredictable price trend**
- **2013**: **The first Bitcoin ATM opens in San Diego, California. SilkRoad is closed and Bitcoin is increasingly associated with criminal activities, going against some public opinion.**
- **2014**: **Microsoft decides to accept payments with bitcoin. The mt.gox exchange platform was hacked, millions of dollars in bitcoins were stolen, and the market price collapsed.**

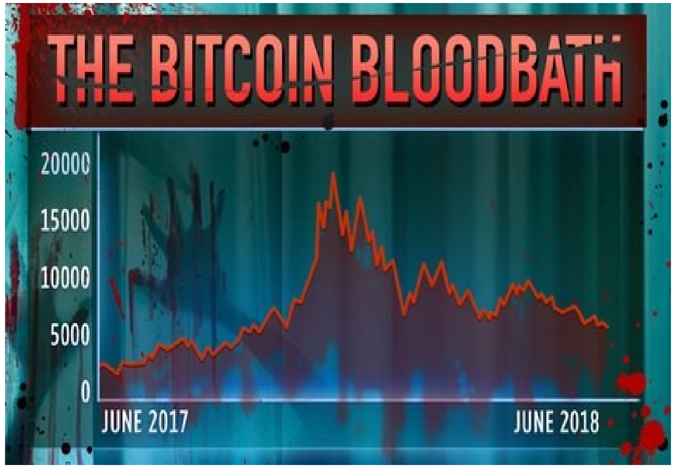
THE HISTORY OF BITCOIN

- **2016**: **Second bitcoin halving**, development of **Ethereum** and **Dapps**, generate the second big bitcoin **bubble** that makes the price skyrocket (period of “**forks**” in themselves and scams based on the **Ponzi scheme**)
- **2017**: Technical change to the Bitcoin protocol. The community splits and the **first big hard fork** occurs, Bitcoin splits into two distinct blockchains: **Bitcoin Classic and Bitcoin Cash**. Following this and other negative news (e.g. China’s ban and strong regularization by Asian countries) the bubble bursts (a **bloodbath**)
- **2020**: **Third halving**, increasingly rapid growth of **Dapps** and **strong investments** by government institutions and the business world
- **2021**: **New bubble** much larger and more marked than the previous ones
- **2024**: **Fourth halving**

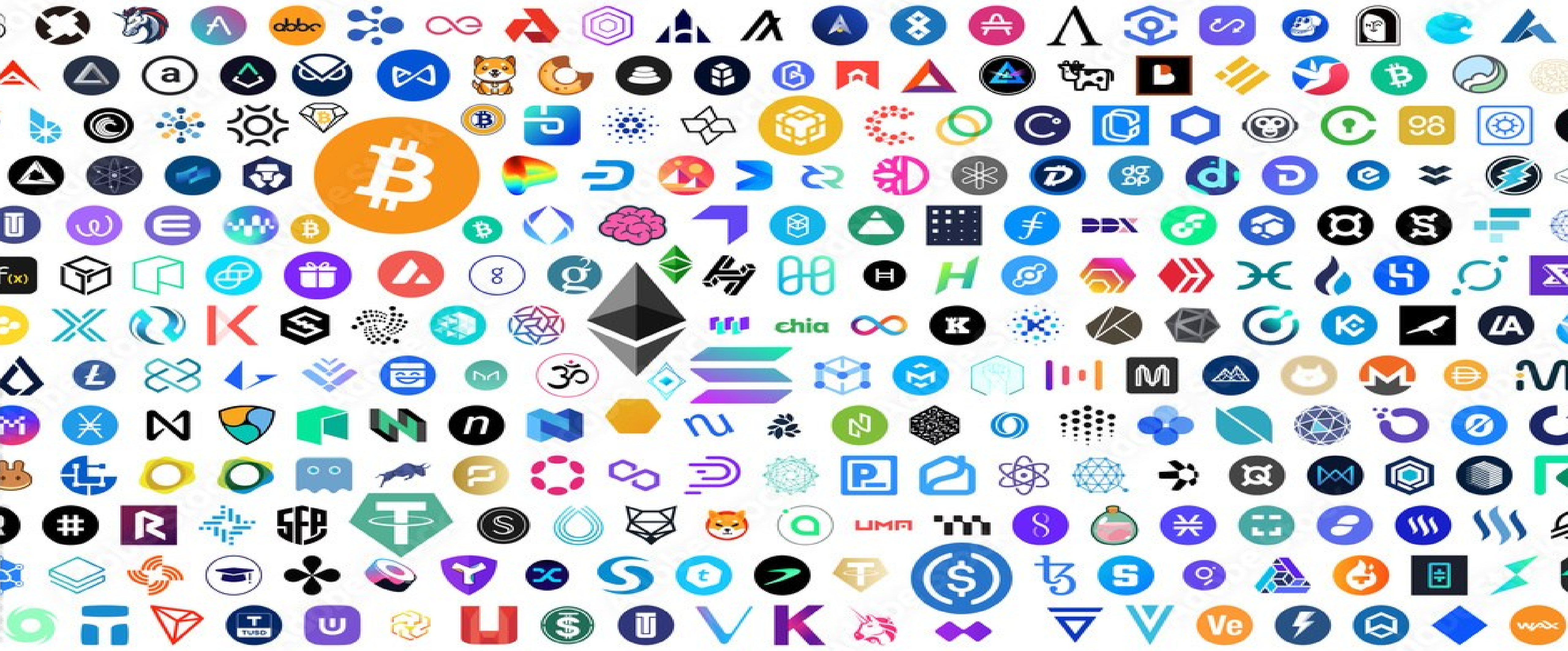


BTC vs BCH

Speed (confirmation time)	100 Minutes	10 Minutes
Cost (per transaction)	$21	.18 cents
Capacity (transactions per sec)	7	24
Strength	1 MB	8 MB
Unconfirmed Transactions	150,000	0
Potential Market	7 trillion	177 trillion
Price	$17,000	$1,700



CRYPTOCURRENCIES



9.826

https://coinmarketcap.com

CRYPTOCURRENCIES

Ethereum: A network dedicated to perfecting contracts. It was created in 2015 by twenty-year-old Russian programmer Vitalik Buterin and leverages the computing power of all nodes on the network to enable the fulfillment and development of *smart contracts,* i.e. traditional contracts whose effects are guaranteed by an algorithm. That is, when certain pre-established conditions are met, contracts are entered into according to the specific conditions previously established by the parties. However, payments are only allowed in Ether (its own cryptocurrency). Ethereum is *account -based*, like a traditional bank. In addition, ethash (not sha-256) is used as the hash function. Since 2022, it has activated its Proof of Stake mechanism because it is more secure, consumes less energy, and is better for implementing new scaling solutions than Proof of Work. In practice, validators must deposit 32 ETH (about € 51,000), thereby putting some value on the network that can be destroyed if they act dishonestly.

Monero: Founded in 2014, Monero focuses on privacy, decentralization, scalability, and fungibility. Compared to Bitcoin, it has significant algorithmic differences in blockchain obfuscation. It effectively prevents the transaction amount from being seen by any third party other than the person who made the transaction.

Tether (USDT): Launched in 2014, it's one of the most popular stablecoins in terms of volume. Unlike other cryptocurrencies, whose price tends to fluctuate more unpredictably, Tether tries to hold its value around a specific asset. As a stablecoin, Tether is pegged or "tethered" to the US dollar at a 1:1 ratio, in order to minimise price volatility. It's a digital token that can be used across blockchains.

SMART CONTRACTS AND NFT

A Token Non-fungible token (NFT) is a special type of token, which represents the title of ownership and certificate of authenticity, written on the Blockchain, of a unique asset (digital or physical). Therefore, NFTs are not mutually interchangeable like cryptocurrencies, which are fungible by their very nature, i.e. they can be duplicated an infinite number of times into exactly identical and interchangeable copies (therefore, it is not possible to uniquely define an identity for a single token that differentiates it from all other ones, thus making all copies equivalent and identical to the original token).

An NFT is a digital asset that represents real-world objects, such as artwork, music, games, and collections of any kind. Whoever buys a work linked to an NFT does not buy the work itself, but simply the ability to prove a right to the work, guaranteed by a smart contract. It all starts with a digital version of the artwork. Typically, a digital photograph or filmed documentation of the artwork is used, stored in digital format, the hash of which is calculated, which is then traded on a blockchain.

USE OF CRYPTOCURRENCY

WAYS TO GET BITCOINS:

1. buying them from other parties in exchange for fiat currencies

To purchase cryptocurrency for legal tender, you need to access an *exchange*. After logging in (through a specific registration on the website), a *wallet is generated indicating the amount of virtual currency corresponding to each* user. Purchases can also be made through ATMs.

2. accept them as consideration for the sale of goods or services

Cryptocurrencies included in the *wallet* can be used to purchase goods and services from entities that accept cryptocurrencies as a means of payment.

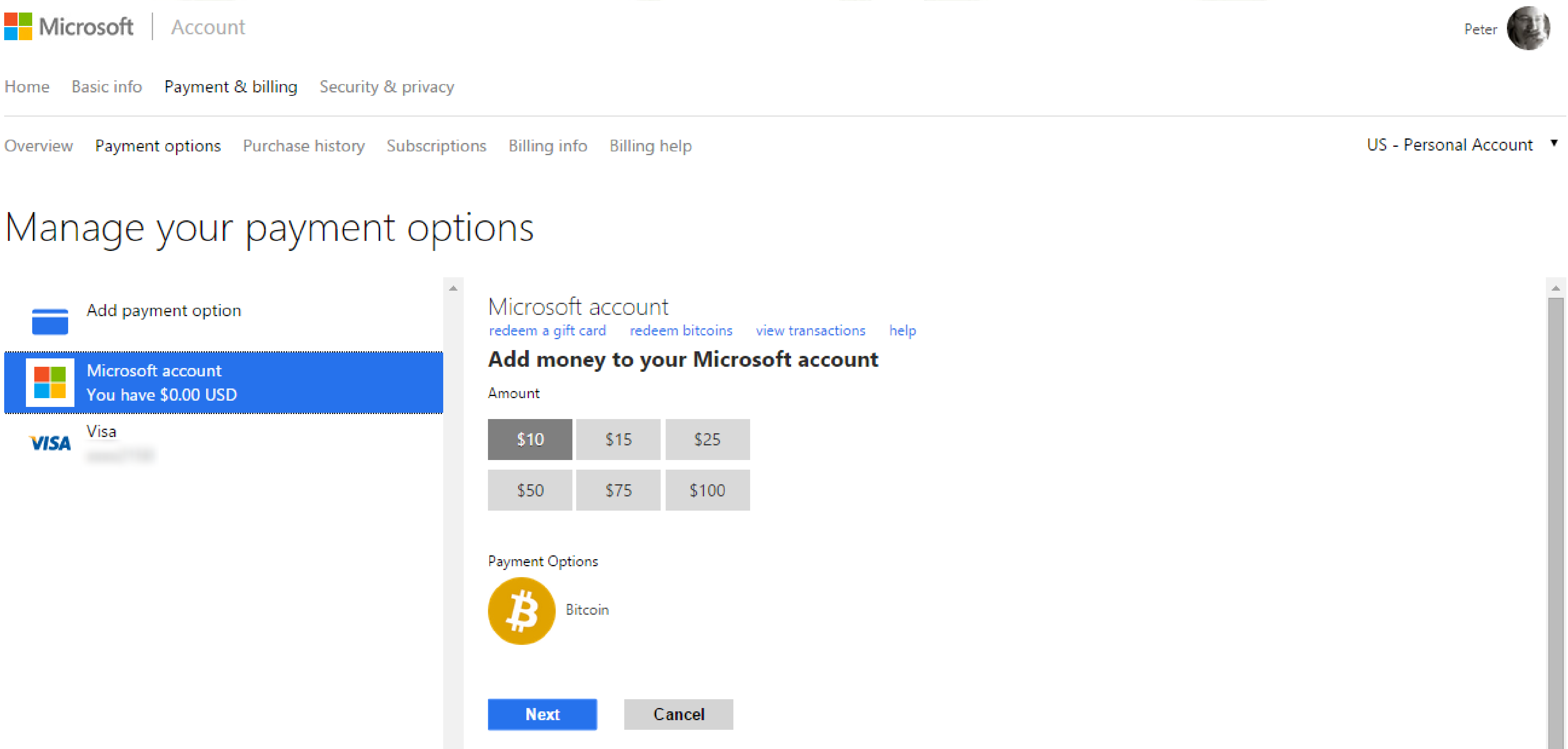
3. Carry out control activities through computer means and, therefore, obtain new virtual currency in exchange (the so-called *mining*)

Mining can be done individually or collectively in so-called *mining pools*.

USE OF CRYPTOCURRENCY

Digital purchases: Several online shopping platforms are starting to support Bitcoin transactions (Microsoft Store, Steam, Twitch, Starbucks…).

Note: The level of diffusion in this area is still modest and is expected to remain so.



Microsoft | Account

Peter

Home · Basic info · Payment & billing · Security & privacy

Overview · Payment options · Purchase history · Subscriptions · Billing info · Billing help

US - Personal Account ▾

Manage your payment options

Add payment option

Microsoft account
You have $0.00 USD

Visa
[redacted]

Microsoft account

redeem a gift card · redeem bitcoins · view transactions · help

Add money to your Microsoft account

Amount

$10	$15	$25
$50	$75	$100

Payment Options

Bitcoin

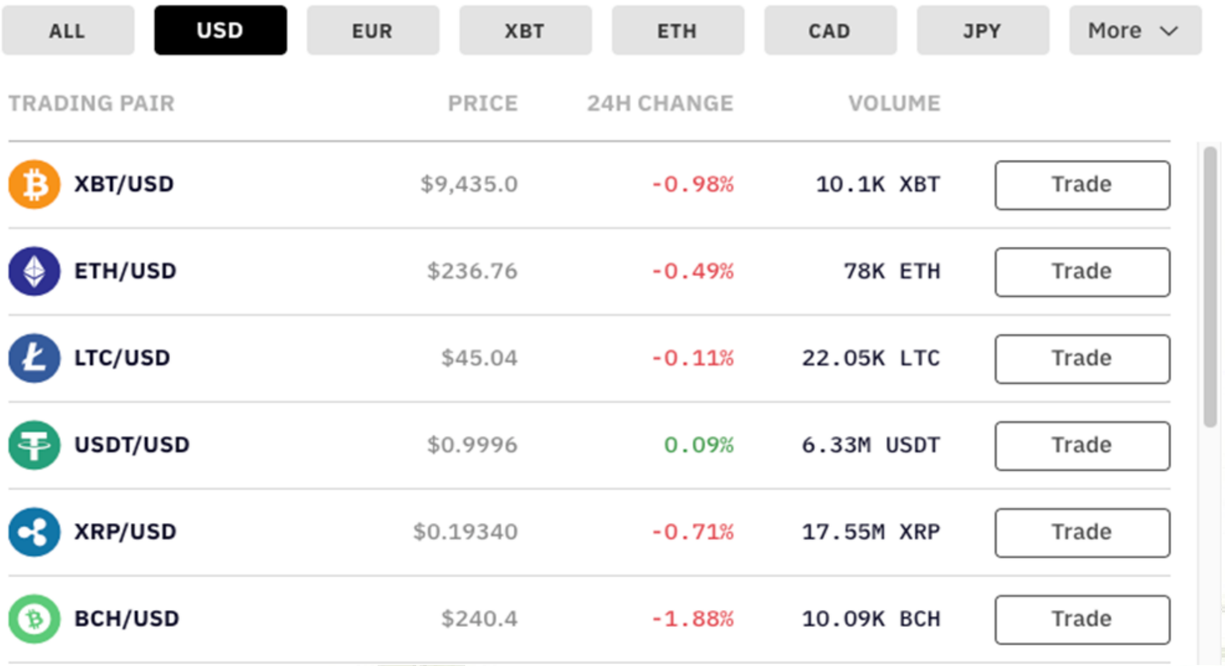
Next · Cancel

USE OF CRYPTOCURRENCY

Withdrawals/Payments: There are ATMs for withdrawing bitcoin and physical POS for making transactions. https://coinatmradar.com/ 204 in Italy

Note: The level of diffusion in this area is still modest, although growing.

USE OF CRYPTOCURRENCY



TRADING PAIR	PRICE	24H CHANGE	VOLUME	
XBT/USD	$9,435.0	-0.98%	10.1K XBT	Trade
ETH/USD	$236.76	-0.49%	78K ETH	Trade
LTC/USD	$45.04	-0.11%	22.05K LTC	Trade
USDT/USD	$0.9996	0.09%	6.33M USDT	Trade
XRP/USD	$0.19340	-0.71%	17.55M XRP	Trade
BCH/USD	$240.4	-1.88%	10.09K BCH	Trade

Buying and selling: There are platforms dedicated to online trading of *crypto assets.*

See: Coinbase, Kraken...

Note: This area is currently the one of greatest interest and diffusion.

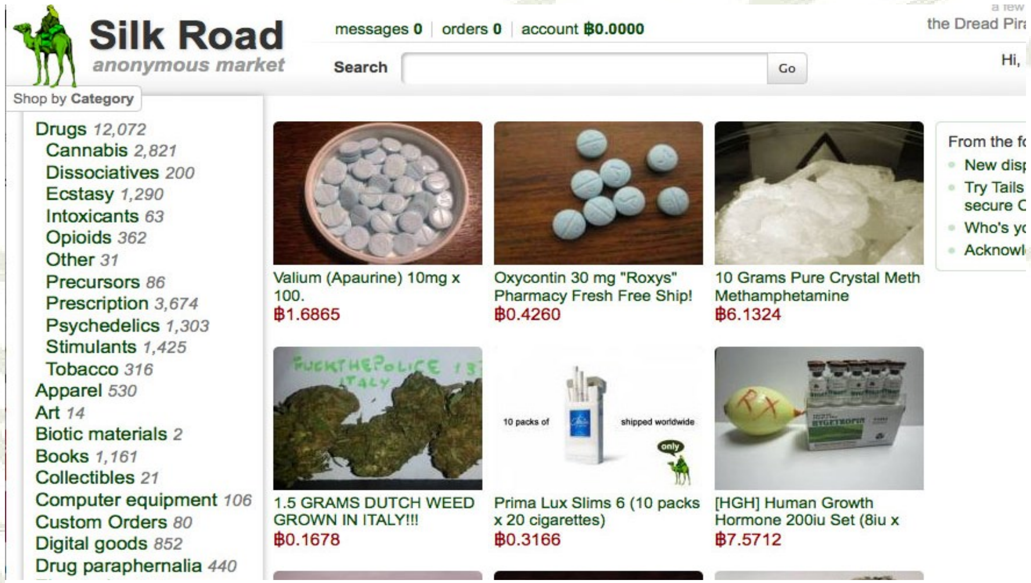
Direct exchange procedures between users are also possible, through:

- *The most common online* trading platforms among individuals (e.g., *eBay*); or the most widely used www.localbitcoins.com
- Transactions carried out with the help of web platforms managed by third parties that operate as de facto intermediaries
- Transactions, carried out on the *deep web*
- The delivery of cash in exchange for account credentials, private keys, or a device such as **Opendime**

USE OF CRYPTOCURRENCY

Purchases: Illegal platforms spread on the black market on the Internet accept transactions exclusively in cryptocurrencies.

Anonymous purchases (mixing): There are widespread illegal platforms on the Internet black market that allow the accumulation and laundering of “black funds”.



Silk Road
anonymous market

messages 0 | orders 0 | account ฿0.0000

a few
the Dread Pir

Search Go

Hi,

Shop by Category

Drugs 12,072
Cannabis 2,821
Dissociatives 200
Ecstasy 1,290
Intoxicants 63
Opioids 362
Other 31
Precursors 86
Prescription 3,674
Psychedelics 1,303
Stimulants 1,425
Tobacco 316
Apparel 530
Art 14
Biotic materials 2
Books 1,161
Collectibles 21
Computer equipment 106
Custom Orders 80
Digital goods 852
Drug paraphernalia 440

Valium (Apaurine) 10mg x 100.
฿1.6865

Oxycontin 30 mg "Roxys" Pharmacy Fresh Free Ship!
฿0.4260

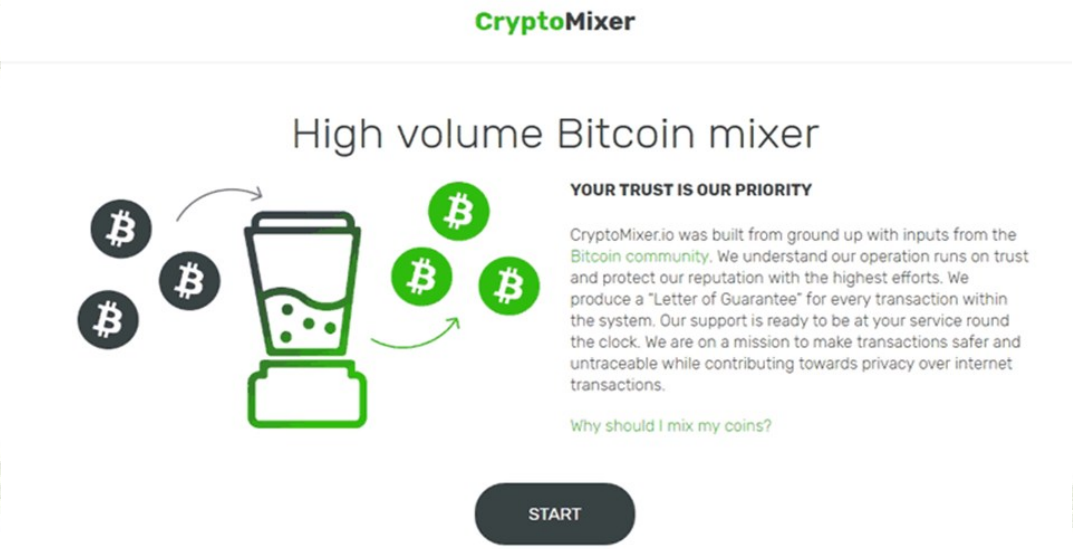
10 Grams Pure Crystal Meth Methamphetamine
฿6.1324

1.5 GRAMS DUTCH WEED GROWN IN ITALY!!!
฿0.1678

Prima Lux Slims 6 (10 packs x 20 cigarettes)
฿0.3166

[HGH] Human Growth Hormone 200iu Set (8iu x
฿7.5712

From the f
- New disp
- Try Tails secure C
- Who's yo
- Acknowl



CryptoMixer

High volume Bitcoin mixer

YOUR TRUST IS OUR PRIORITY

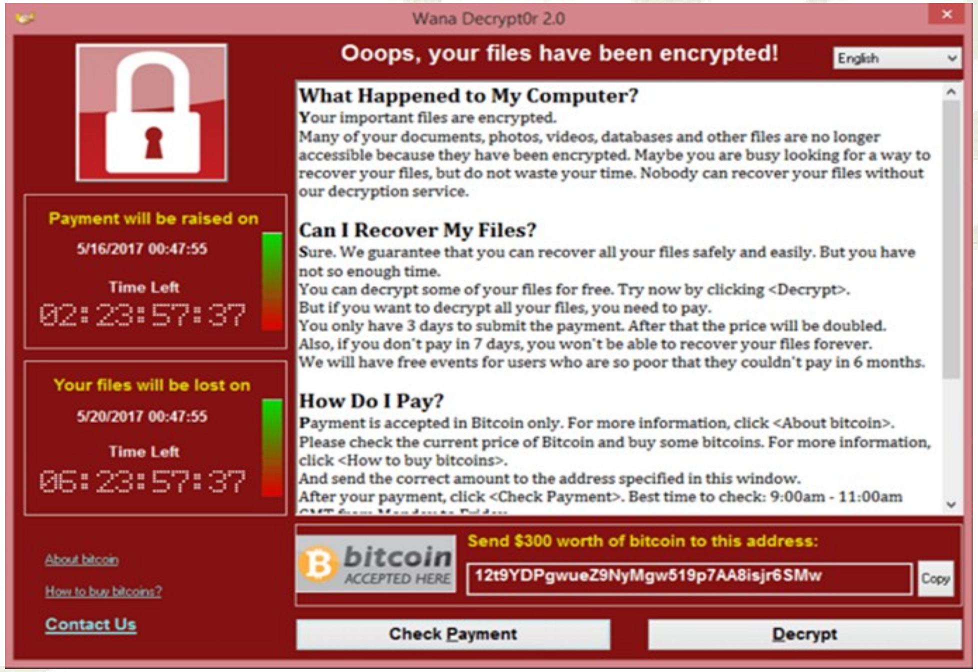
CryptoMixer.io was built from ground up with inputs from the Bitcoin community. We understand our operation runs on trust and protect our reputation with the highest efforts. We produce a “Letter of Guarantee” for every transaction within the system. Our support is ready to be at your service round the clock. We are on a mission to make transactions safer and untraceable while contributing towards privacy over internet transactions.

Why should I mix my coins?

USE OF CRYPTOCURRENCY

Online Extortion: There are ransomware programs that make all your data unreadable and demand a ransom to regain access to it.

Today, these and other types of *online extortion* require payments to be made in cryptocurrency.



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

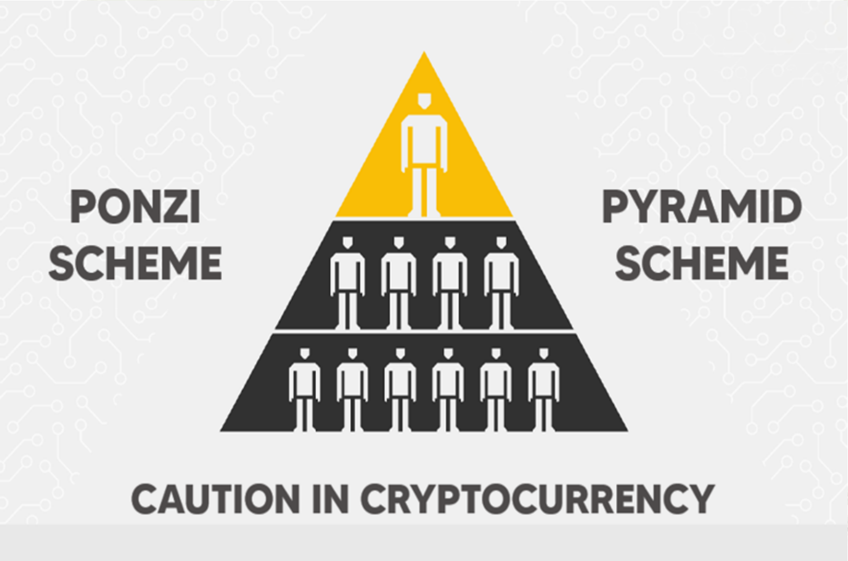
Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have 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.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw



Online Scams: Taking advantage of the market frenzy, several alternative cryptocurrencies have emerged that offer huge returns, but are based on the well-known “Ponzi” fraud scheme.

THE LEGAL CLASSIFICATION OF CRYPTOASSETS

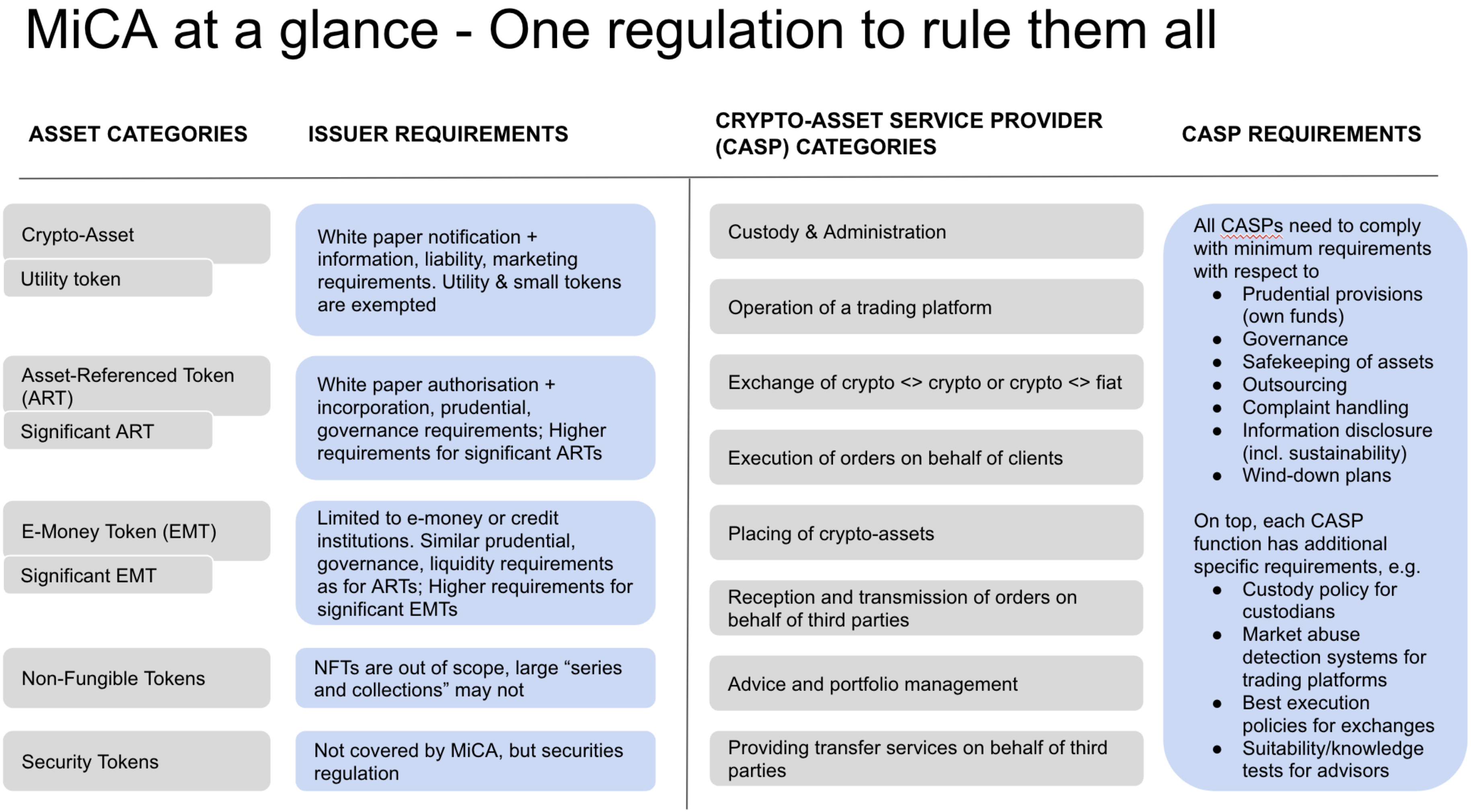
Directive (EU) 2018/843 (Fifth Anti-Money Laundering Directive) by which the European Parliament amended Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing:

a ***digital representation of value*** *that* ***is not issued or guaranteed by a central bank or public body, is not*** *necessarily linked to a legally established currency, it has the legal status of* ***currency or money*** *, but is accepted by individuals and legal entities as* ***a means of exchange*** *and can be transferred, stored and exchanged* ***electronically***.

MiCA (Markets in Crypto-Assets) REGULATION

Regulation (EU) 2023/1114

"cryptoasset": a digital representation of a security or right that can be transferred and stored electronically, using distributed ledger technology or similar technology



MiCA at a glance - One regulation to rule them all

ASSET CATEGORIES	ISSUER REQUIREMENTS
Crypto-Asset Utility token	White paper notification + information, liability, marketing requirements. Utility & small tokens are exempted
Asset-Referenced Token (ART) Significant ART	White paper authorisation + incorporation, prudential, governance requirements; Higher requirements for significant ARTs
E-Money Token (EMT) Significant EMT	Limited to e-money or credit institutions. Similar prudential, governance, liquidity requirements as for ARTs; Higher requirements for significant EMTs
Non-Fungible Tokens	NFTs are out of scope, large “series and collections” may not
Security Tokens	Not covered by MiCA, but securities regulation

CRYPTO-ASSET SERVICE PROVIDER (CASP) CATEGORIES	CASP REQUIREMENTS
Custody & Administration Operation of a trading platform Exchange of crypto <> crypto or crypto <> fiat Execution of orders on behalf of clients Placing of crypto-assets Reception and transmission of orders on behalf of third parties Advice and portfolio management Providing transfer services on behalf of third parties	All CASPs need to comply with minimum requirements with respect to ● Prudential provisions (own funds) ● Governance ● Safekeeping of assets ● Outsourcing ● Complaint handling ● Information disclosure (incl. sustainability) ● Wind-down plans On top, each CASP function has additional specific requirements, e.g. ● Custody policy for custodians ● Market abuse detection systems for trading platforms ● Best execution policies for exchanges ● Suitability/knowledge tests for advisors

Thanks for your attention

Col. t.SPEF Giuseppe Lopez