

bitcoin

philipp machač, 803320

The root problem with conventional currency is all the trust that's required to make it work.

The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.

– Satoshi Nakamoto

THE TIMES

Max SC, min SC
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 £37-billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering 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 guarantees 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

99p

Pub chain cuts the price of a pint from £1.69 to 99p levels Business, page 47



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



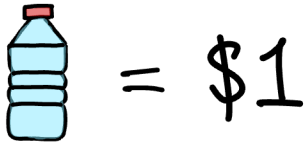
be your own bank

WHAT IS MONEY?

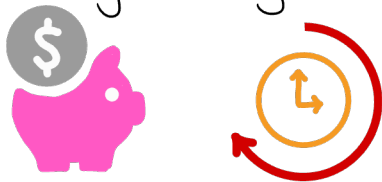
Medium of exchange
(buy things)











Unit of measure
(what is item priced in?)



Store of value
(save money for long term)



6000 BC		Physical Objects
5000 BC		Barter
4000 BC		Gold
600 BC		Coins
900 AD		Paper
1950		Cards
1990		digital money
2009		Bitcoin

~~Scarce~~
~~Durable~~
~~Divisible~~
~~Portable~~
~~Fungible~~
~~Verifiable~~
~~Open to all~~
~~Privacy~~
?

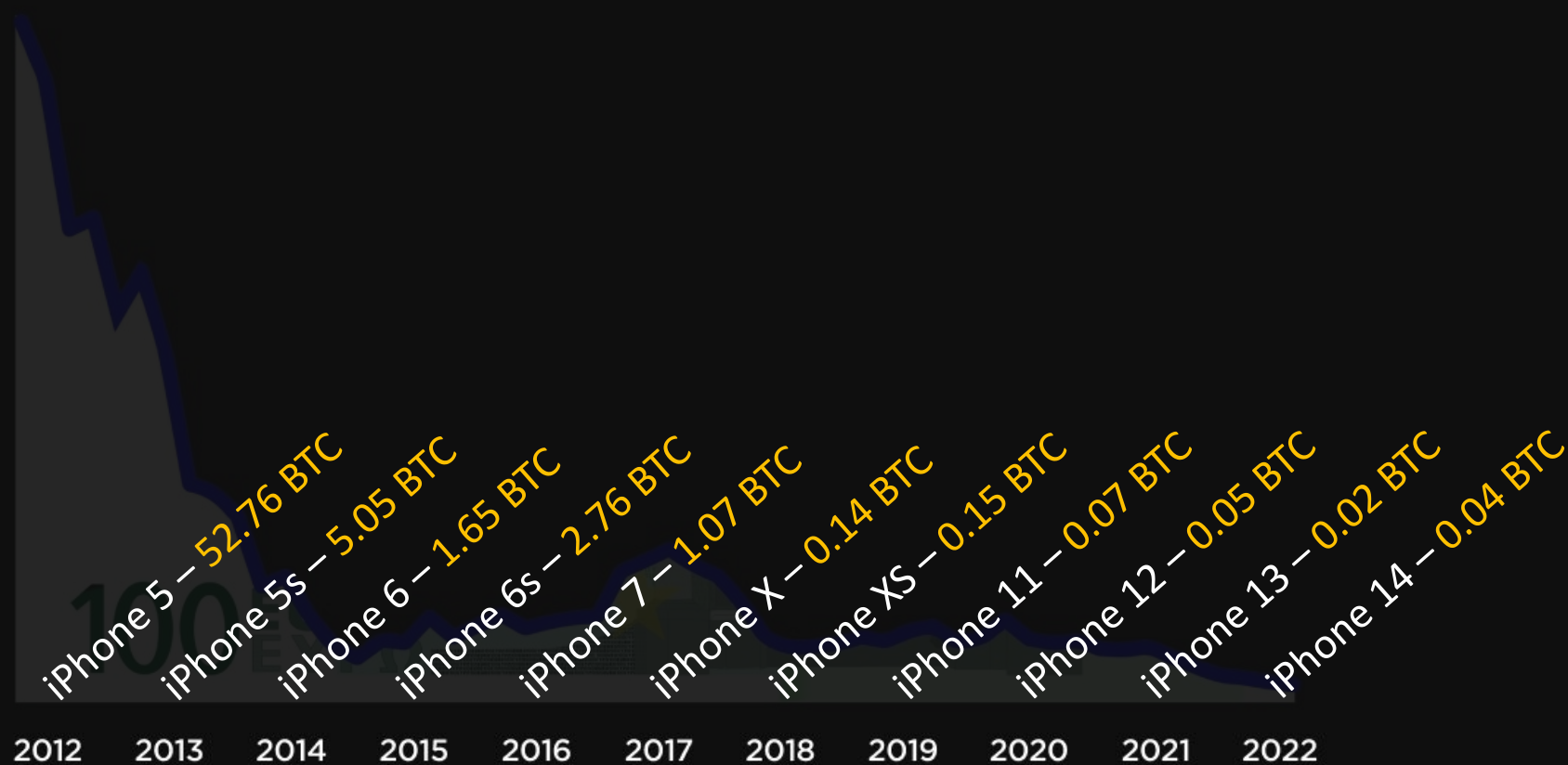
WHAT IS MONEY?

Anything that is a medium of exchange

People need to believe item holds value in order to exchange it

If people believe Bitcoin has value they will use it as a medium of exchange

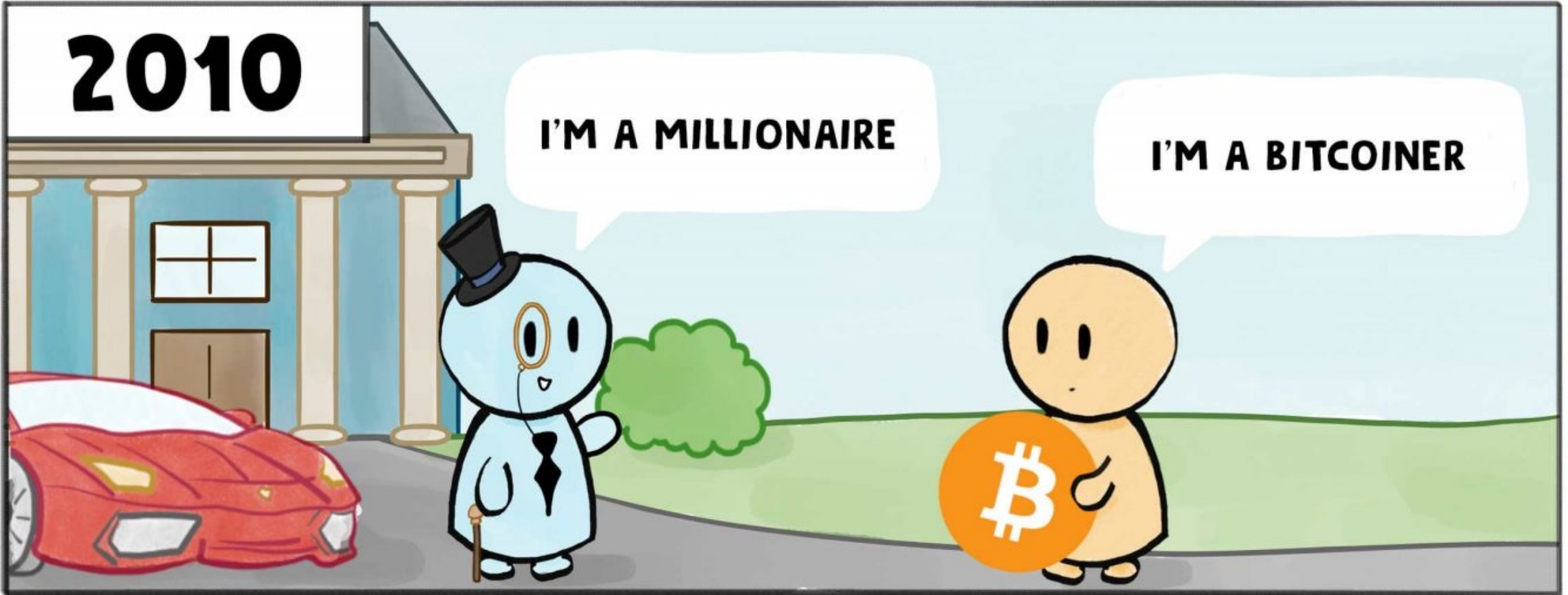
The Euro lost **90% of its Value** against Bitcoin



2010

I'M A MILLIONAIRE

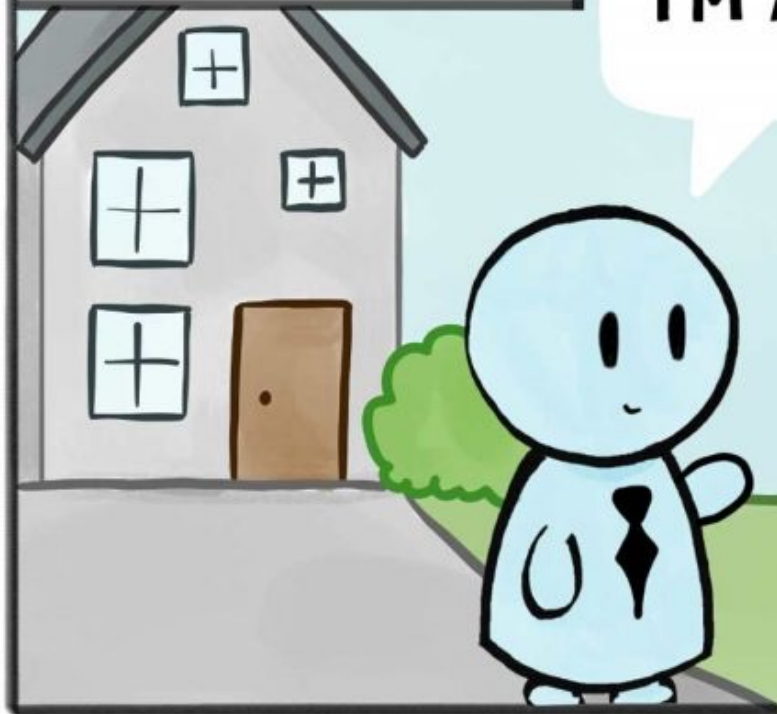
I'M A BITCOINER



2020

I'M A MILLIONAIRE

I'M A BITCOINER



2030

I'M A MILLIONAIRE

I'M A BITCOINER

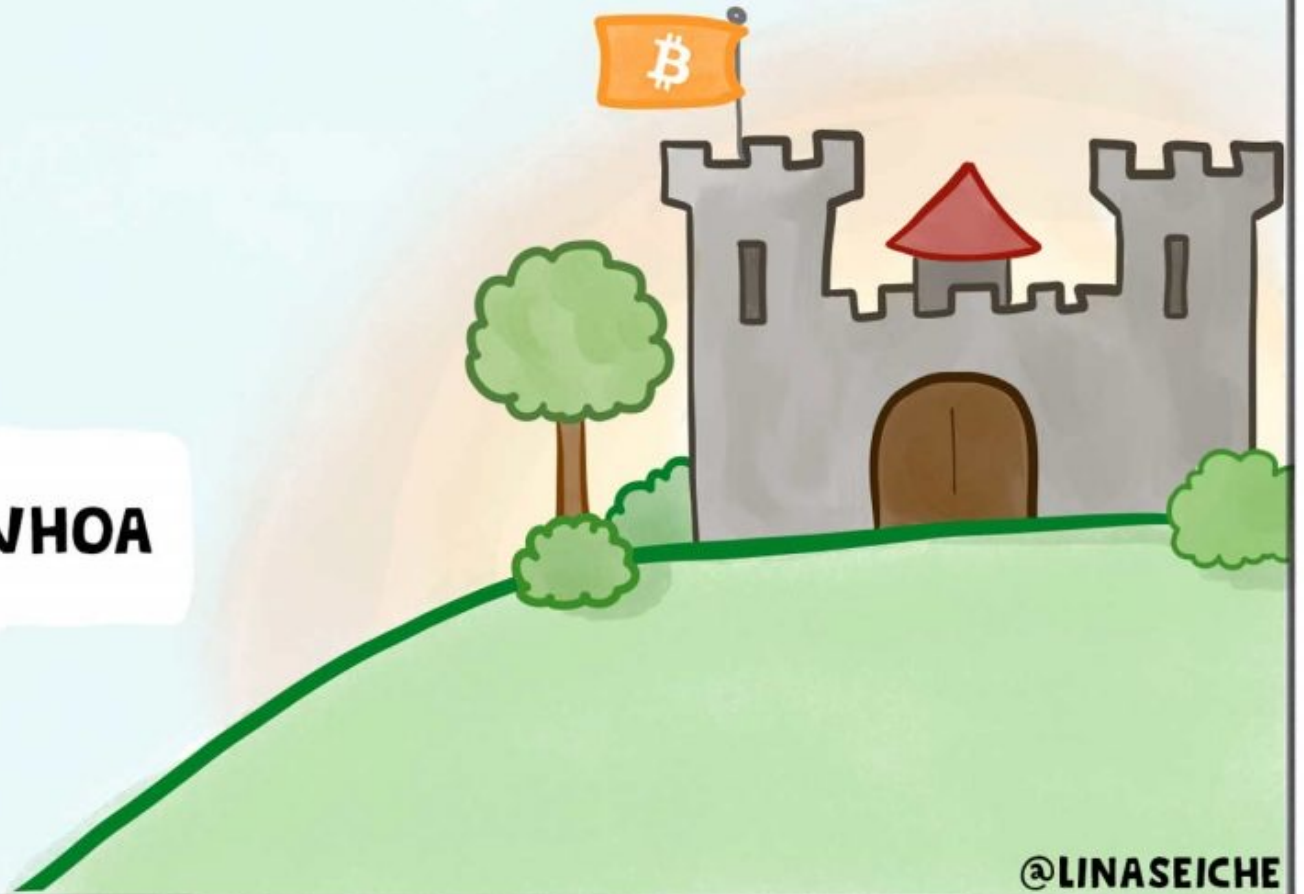


2040

HE'S A
BITCOINER

THEY SAY HE
HAS A WHOLE
COIN

WHOA



@LINASEICHE



take the orange pill

WHAT IS BITCOIN?

Scarce : not easy to obtain

ONLY **21M** Bitcoin
million

Durable : cannot be easily destroyed




Bitcoin ledger stored
in 1000s of computers

Divisible : break into smaller parts

1BTC = 100,000,000 satoshi's

Example:

If water = \$1 

EASIER TO SAY

4000 satoshi's

INSTEAD OF

0.00004 BTC

Portable: easily move it around



cow

vs



gold bars

vs



12 or 24 words
for Bitcoin

Fungible : ability of an item to be interchangeable with another item of the same type



Verifiable: check if its authentic



check public
ledger

Open to all: do not need permission



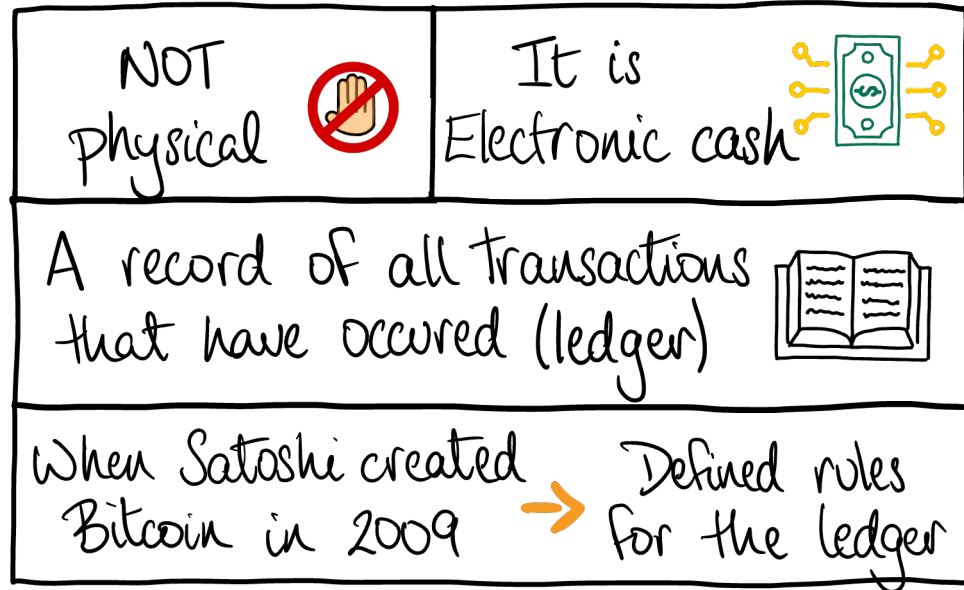
=



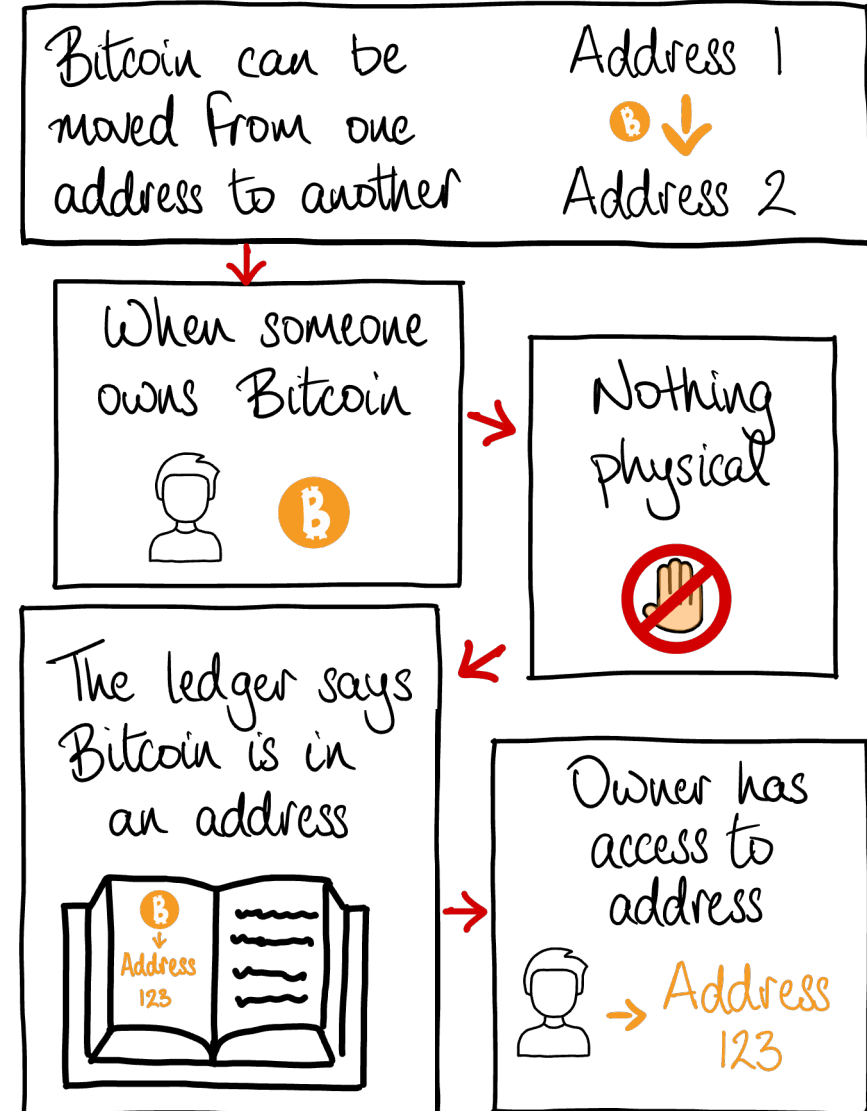
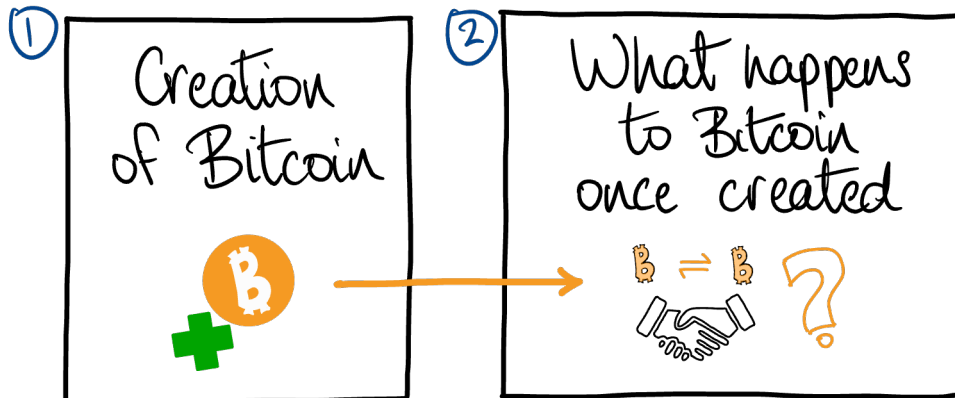
=



WHAT IS BITCOIN?



LEDGER RECORDS 2 THINGS



ADDRESS

USED TO

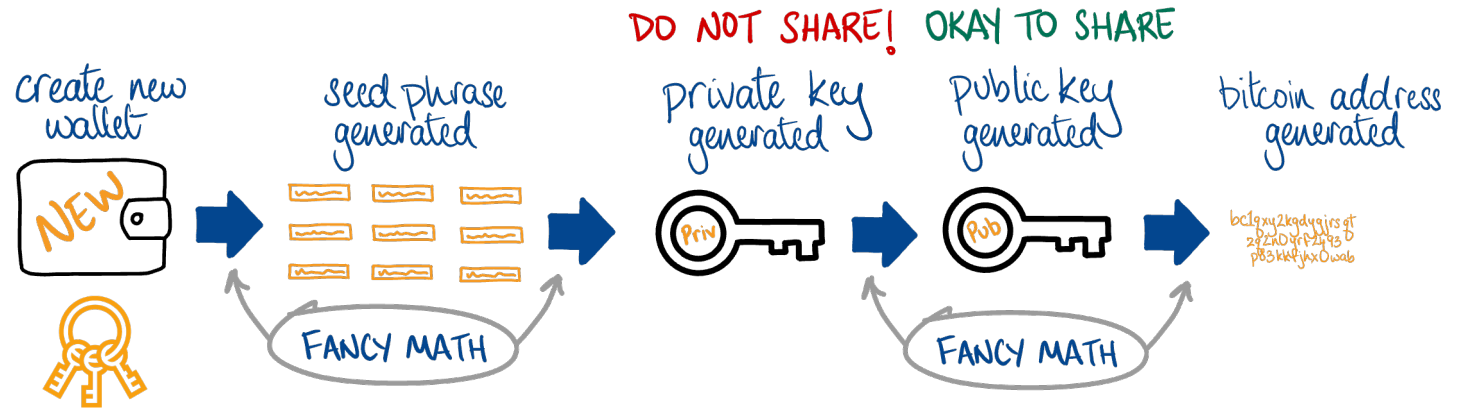


TEXT:

bc1qxy2kgdygjsrztzq2nDyrf2493p83kkfjhx0wab



QR CODE:



NOT YOUR KEYS NOT YOUR COINS

Lose private keys \equiv Lose Bitcoin

WALLET

Desktop
Wallet



Mobile
Wallet



Hardware
Wallet



SEED PHRASE

List of words (12 or 24)
drawn from a list of 2048
English words (BIP39).

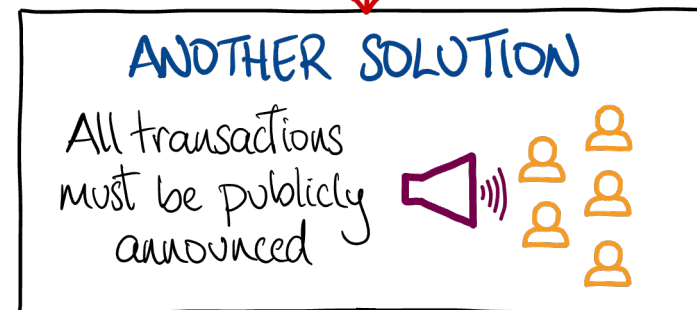
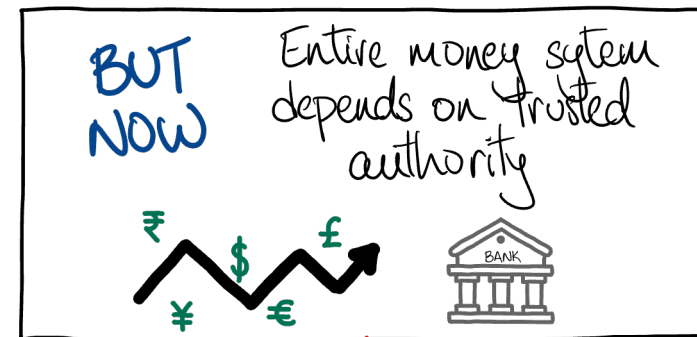
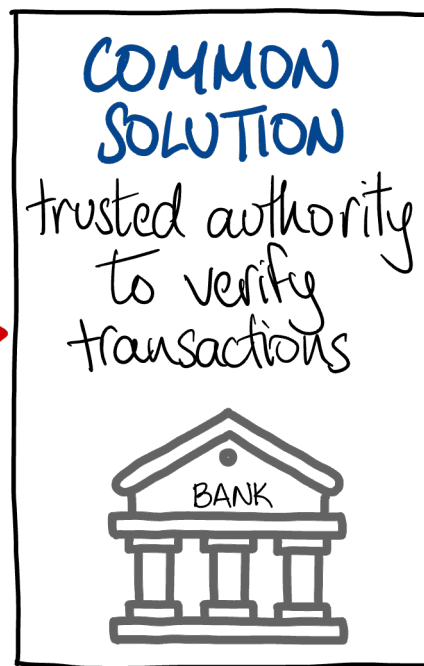
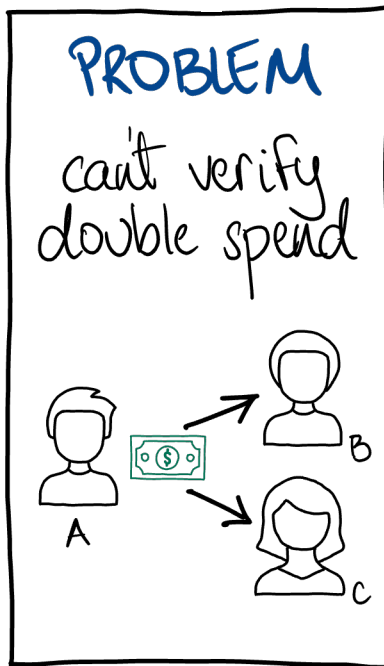
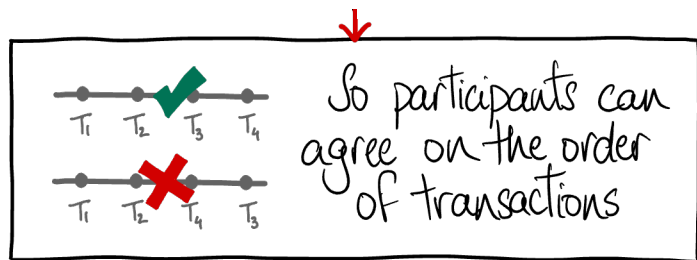
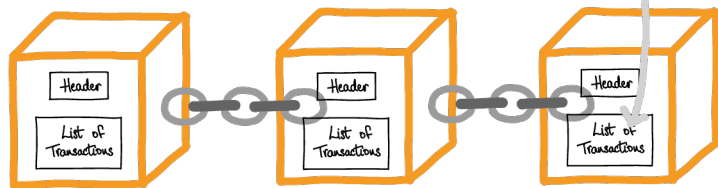
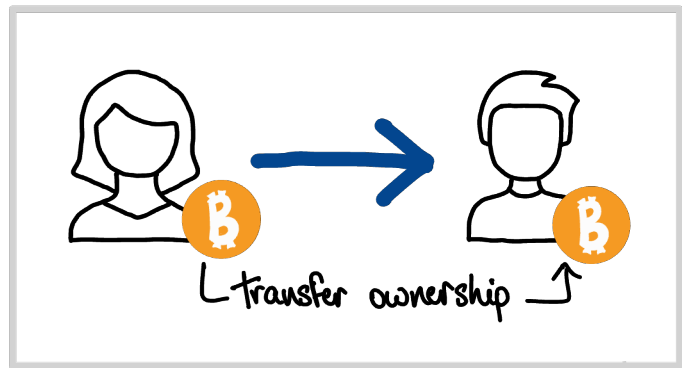
PRIVATE KEY

Private Key is like
a password
KEEP IT PRIVATE!

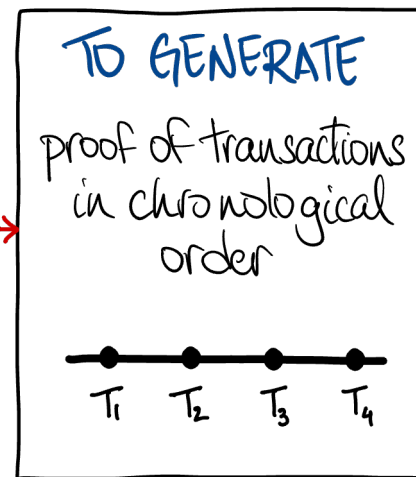
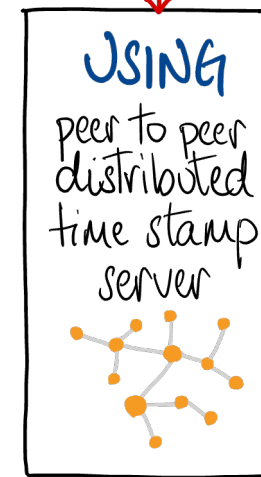
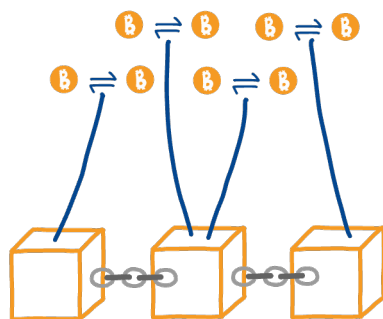
PUBLIC KEY

Public Key is like
an email address
OKAY TO SHARE

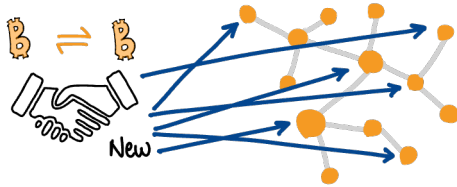
TRANSACTION



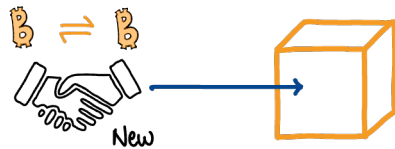
"ON-CHAIN"



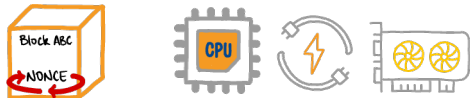
New transactions are broadcasted to all nodes



Each node collects new transactions into a block

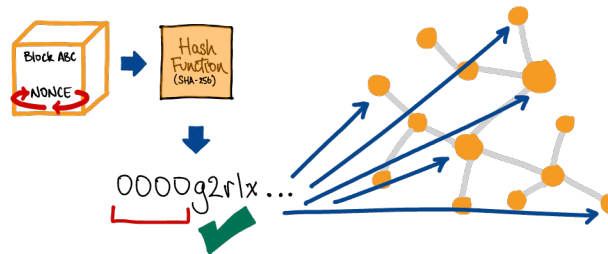


Each node works on finding a proof of work for its block

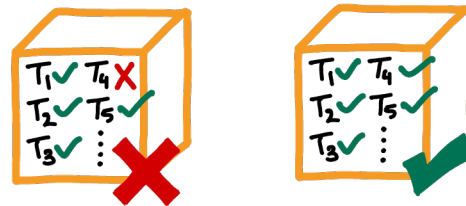


NETWORK

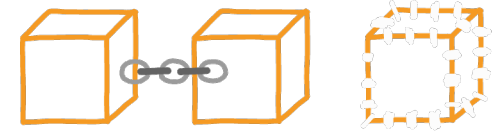
When node finds proof of work it broadcasts the block to all nodes



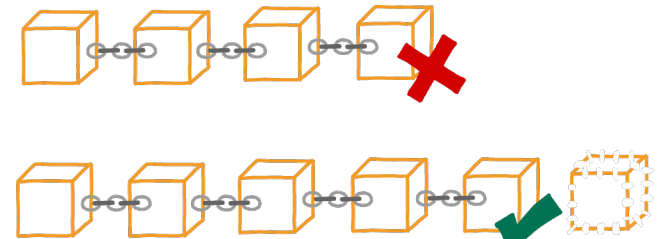
Nodes accept block only if transactions are valid and not spent



Nodes express acceptance by working on the next block on the chain



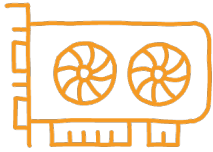
Longest chain = Majority decision = Greatest proof of work



They will keep working on extending it

PROOF OF WORK (POW)

Pow
requires
LOTS of



Computing
power



Electricity



Time



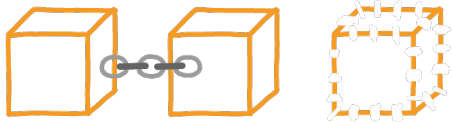
INPUT



0000g2r1x...

RESULTING IN

①



New blocks being added

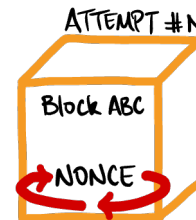
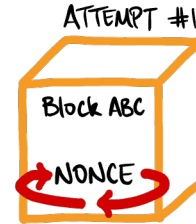
②



new coins
being minted

HOW?

Increment a 'nonce' in the
block until value is found



Proof of work difficulty
changes to maintain
average blocks per hour

time and effort to solve Proof of Work

BITCOIN IS GREEN

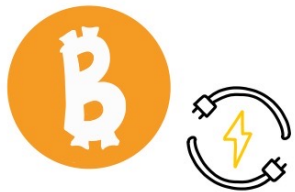


= 165,317 TWh



= 275 TWh

= 0.17% of global consumption



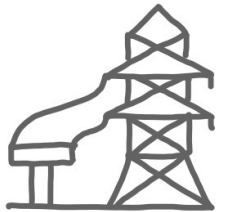
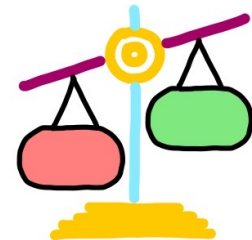
58.9%
Sustainable energy



Consumption is transparent



Balance the grid



INCENTIVES

When nodes expend electricity and CPU time → New coins are created



SIMILAR TO
gold miners
expending resources

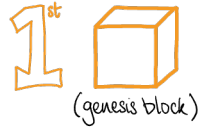


2009 the reward per block was 50 Bitcoin
2023 the reward per block is 6.25 Bitcoin

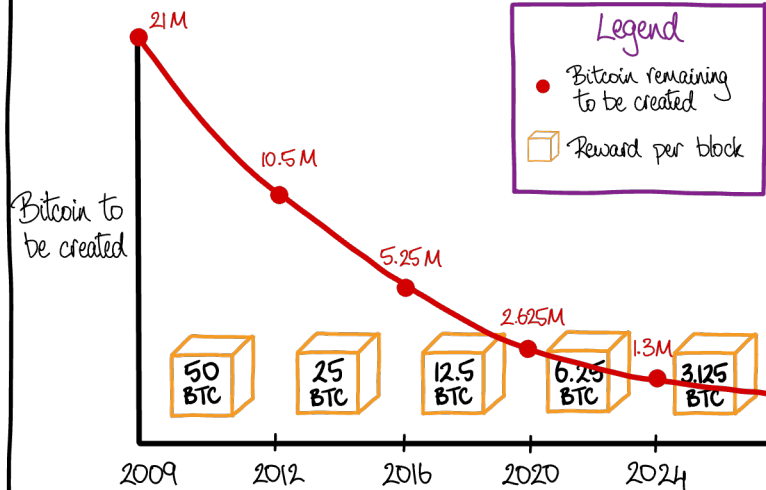
When Satoshi created the
Bitcoin blockchain



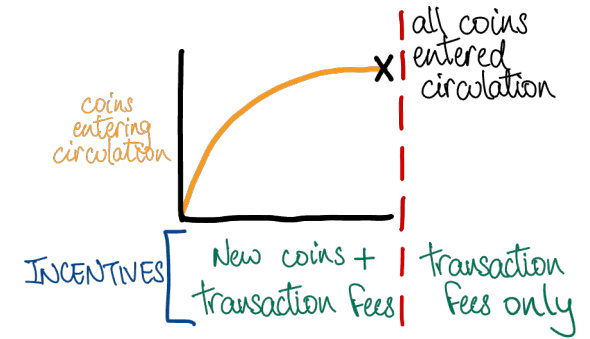
the first block was created + 50 Bitcoin was created
(reward for solving puzzle)



Bitcoin is programmed such that
the reward per block halves
every 210,000 blocks (~4 years)



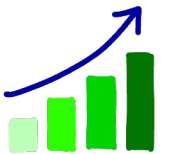
When predetermined
coins enter circulation
INCENTIVE = transaction fees
INFLATION FREE



Incentives encourage
nodes to be honest



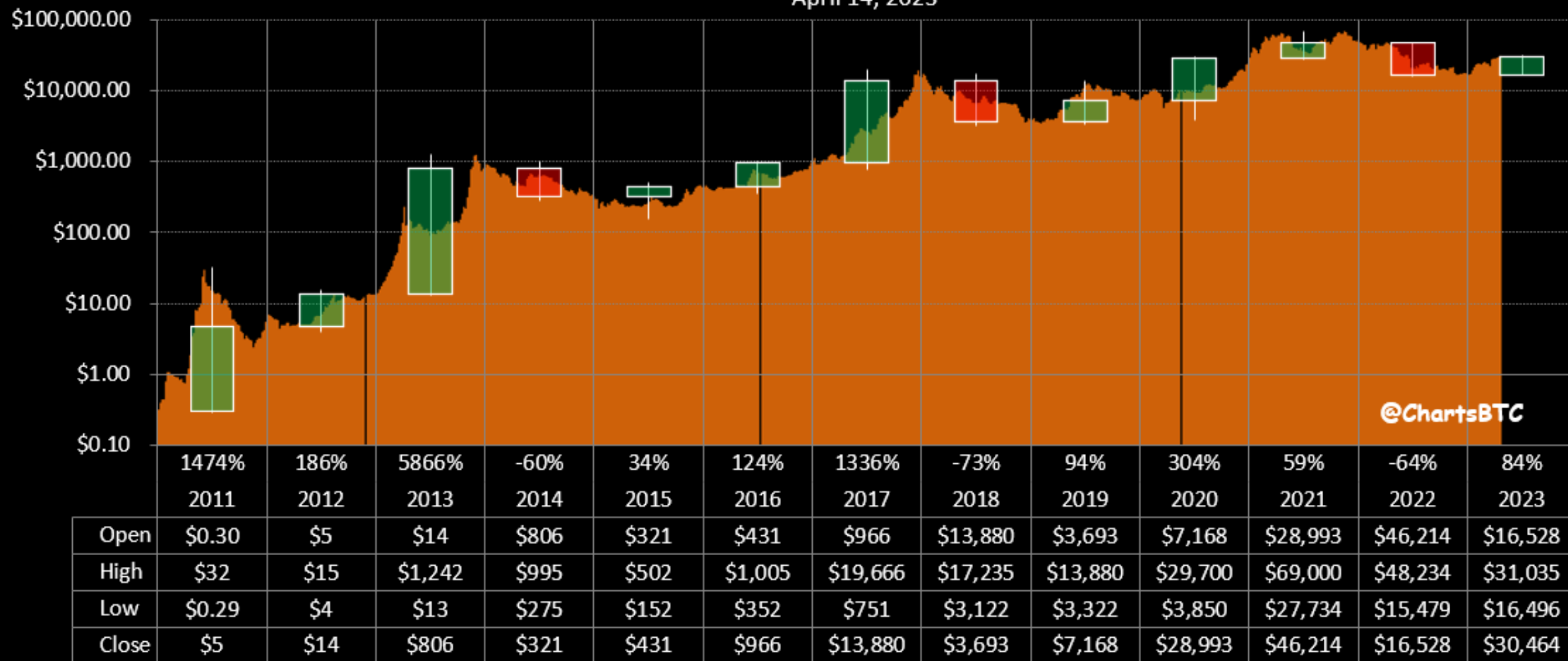
MORE PROFITABLE
to play by the rules





Bitcoin Yearly Candles

April 14, 2023



Source: bitcoincharts.com; ChartsBTC



What are you trying to tell me,
that I can trade my bitcoin for
millions someday?

1 btc = 1 btc

No Neo,
I'm trying to
tell you that
when you're
ready...

you won't have to.

YOU DON'T NEED TO BUY **A WHOLE BITCOIN**

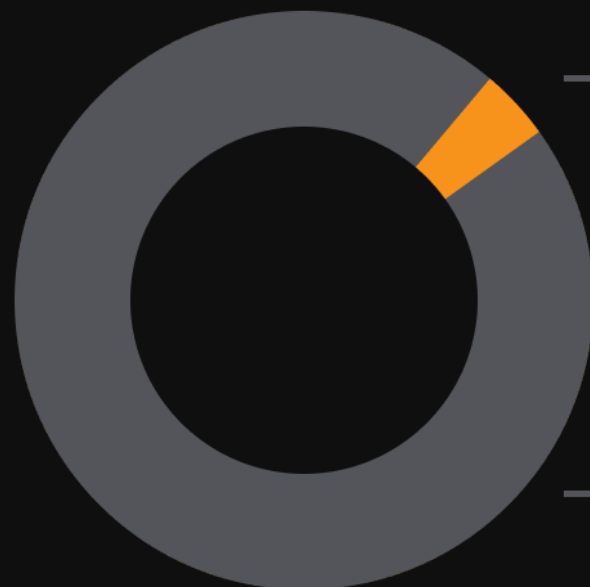


WORLD POPULATION
8.4 BILLION



BITCOIN SUPPLY
21 MILLION

BTC PER PERSON
0.00226 BTC



BITCOIN OWNERS
Just above 100 Million

**"BITCOIN IS CRAZY
INTERNET MONEY"**
More than 7 Billion

YOU ARE STILL **EARLY TO BITCOIN**

**WHEN I GROW UP,
I WANT TO BE A
MILLIONAIRE**



**WHEN I GROW UP,
I WANT TO BE A
WHOLECOINER**



A FEW YEARS LATER

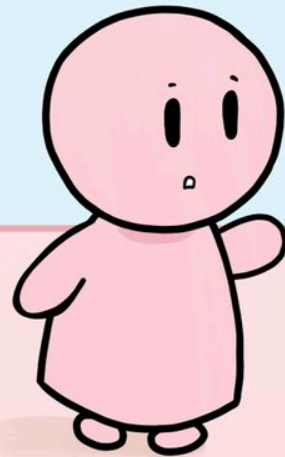
I'M A MILLIONAIRE



DUDE, EVERYONE IS

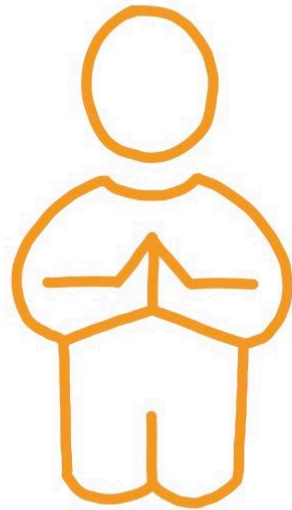


WOAH, IS THAT
A WHOLE BITCOIN?



THANK YOU

Stay Humble



Stack Late





The easiest App to invest in Bitcoin.

🛡 Registered by Financial Market Authority 🇦🇹

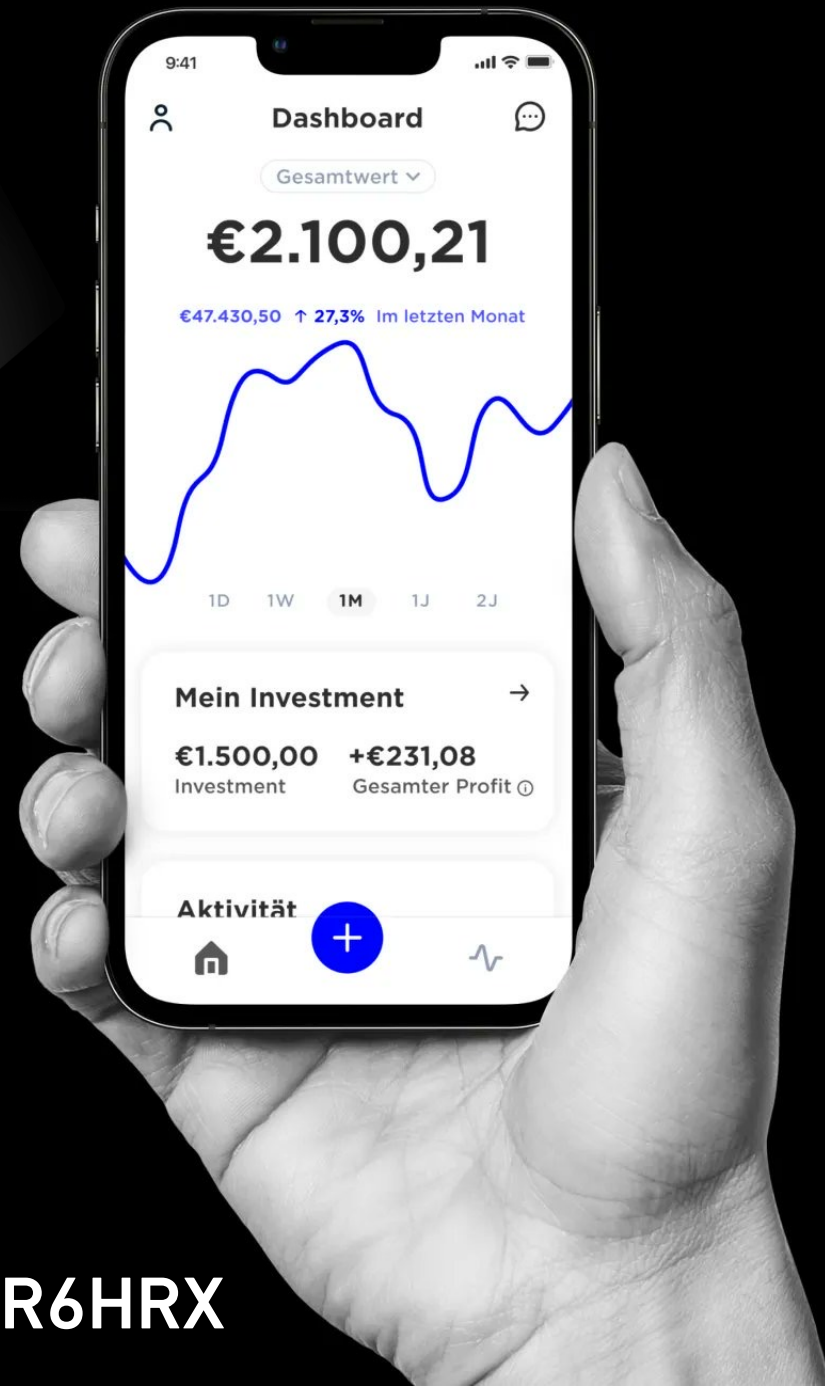
🏦 German Bank Account 🇩🇪

💬 Personal Support

🔒 Highest security standards



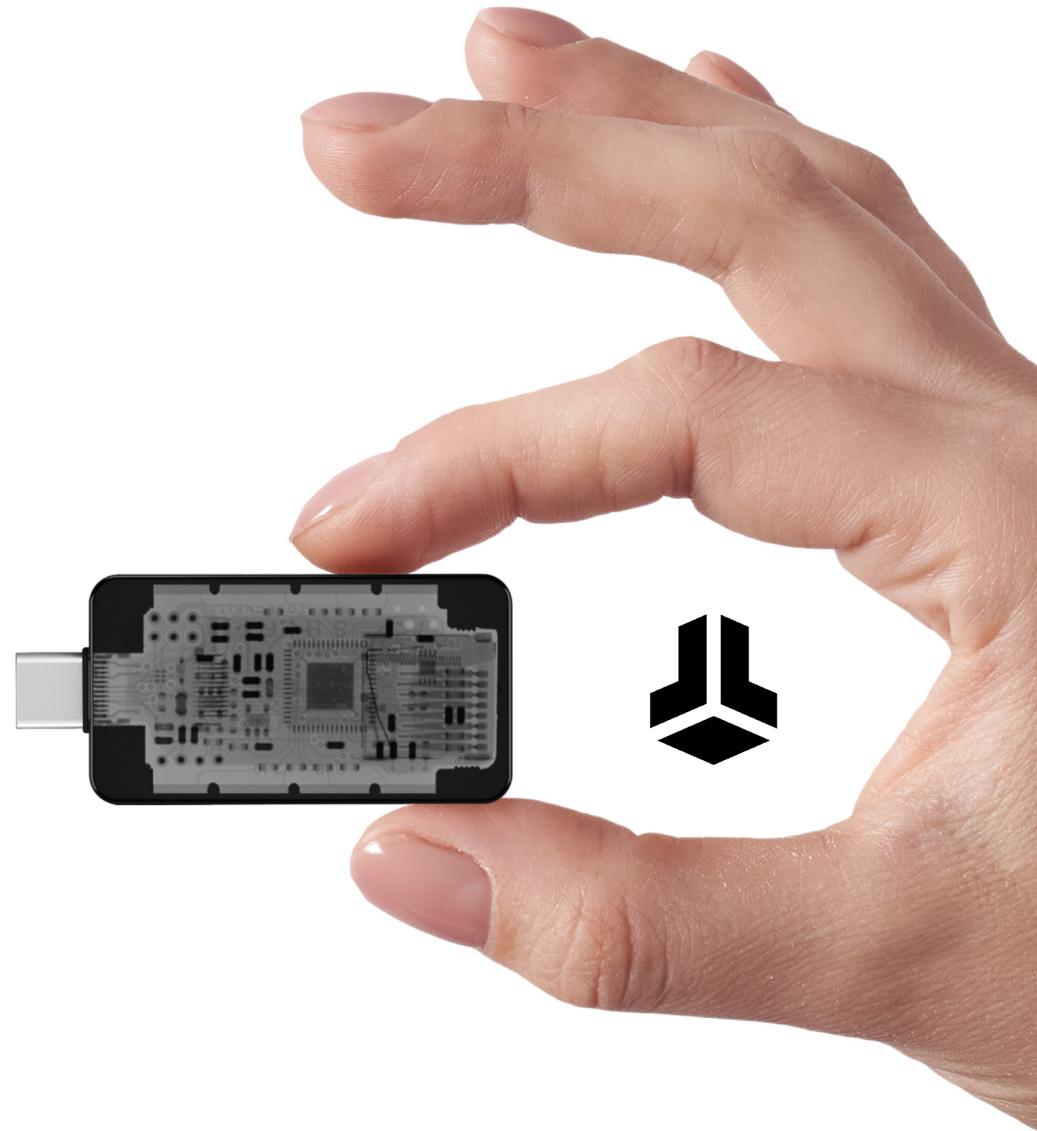
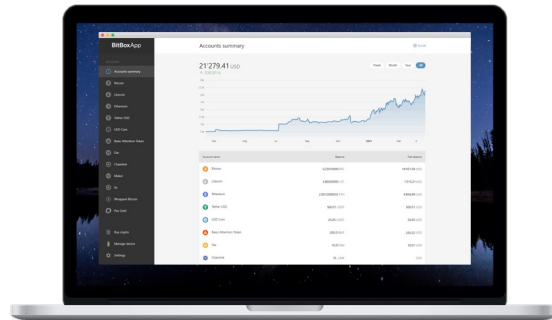
R6HRX



This could be worth 50 billion Dollars.

BitBox02
Bitcoin-only edition

Swiss made 





bücher

podcasts

live



INNSBRUCK
BTC
SEPTEMBER
14-17 2023

#BITCOINKONFERENZ #BTC23