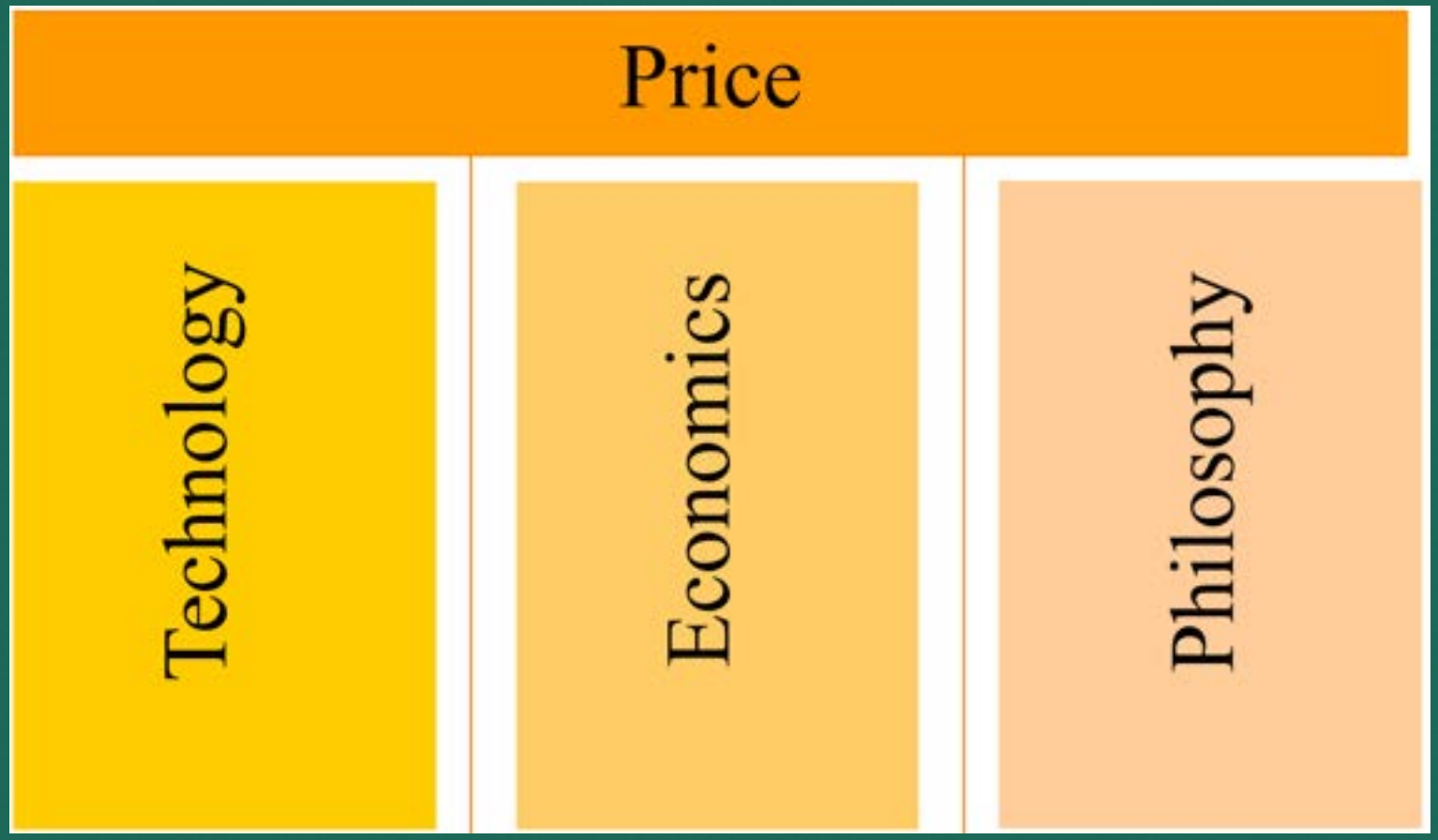
Café numérique

Bitcoin
Stable coins
and
Real World Asset tokens

- Avv. Lars Schlichting, LL.M.
- 5 mars 2026

LEXIFY
MORE THAN LAWYERS

The bitcoin pillars

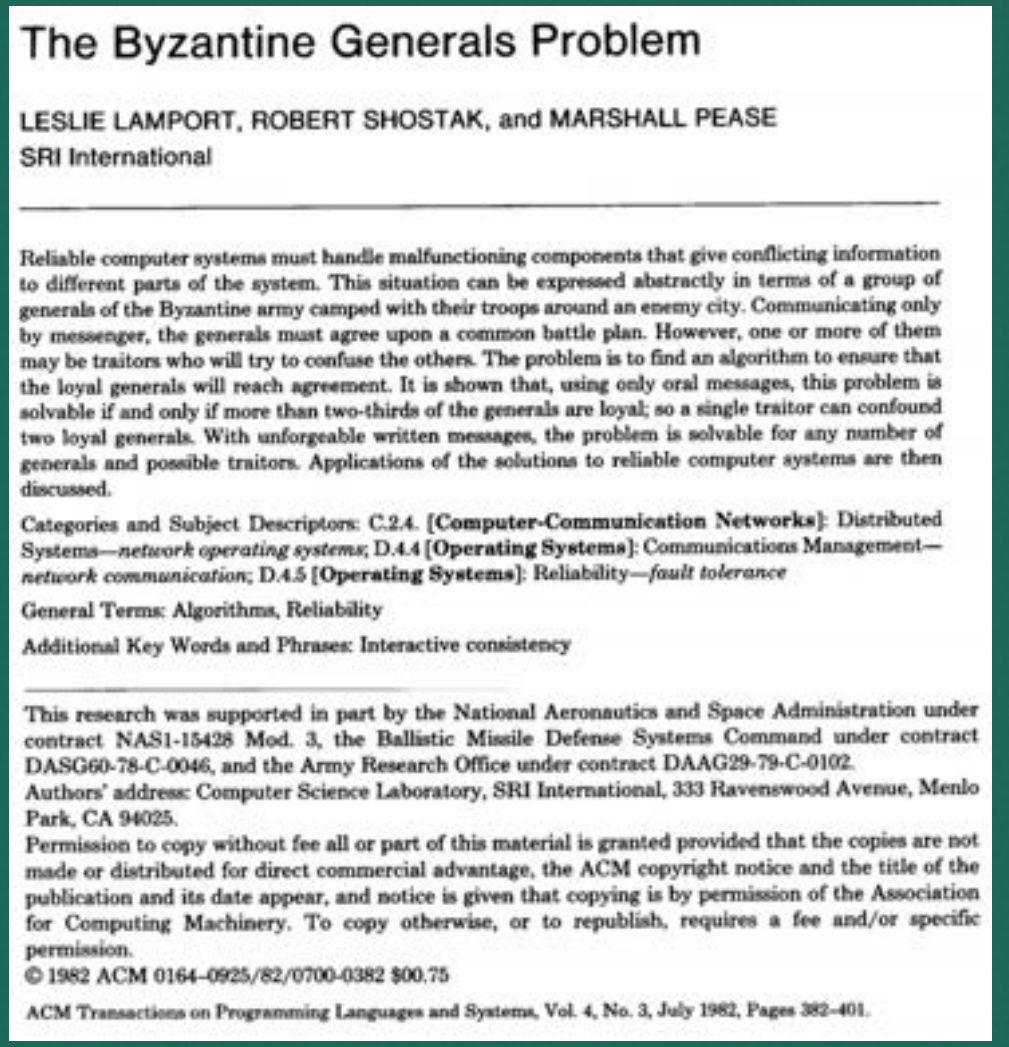


LEXIFY
MORE THAN LAWYERS

Let's beginn with a problem

1982

How can we build trust without a trusted party?



The Byzantine Generals Problem

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International

Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed.

Categories and Subject Descriptors: C.2.4. [**Computer-Communication Networks**]: Distributed Systems—*network operating systems*; D.4.4 [**Operating Systems**]: Communications Management—*network communication*; D.4.5 [**Operating Systems**]: Reliability—*fault tolerance*

General Terms: Algorithms, Reliability

Additional Key Words and Phrases: Interactive consistency

This research was supported in part by the National Aeronautics and Space Administration under contract NAS1-15428 Mod. 3, the Ballistic Missile Defense Systems Command under contract DASG60-78-C-0046, and the Army Research Office under contract DAAG29-79-C-0102.
Authors' address: Computer Science Laboratory, SRI International, 333 Ravenswood Avenue, Menlo Park, CA 94025.

ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, July 1982, Pages 382–401.

LEXIFY
MORE THAN LAWYERS

And start with the solution

2008

trust everybody by trusting nobody

....

thanks to mining mechanism

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.

- Source: httphttps://bitcoin.org/bitcoin.pdf

LEXIFY
MORE THAN LAWYERS

Public and private key (asymmetric cryptography)

Figure 4-1. Private key, public key, and bitcoin address

WHY USE ASYMMETRIC CRYPTOGRAPHY (PUBLIC/PRIVATE KEYS)?

Why is asymmetric cryptography used in bitcoin? It's not used to "encrypt" (make secret) the transactions. Rather, the useful property of asymmetric cryptography is the ability to generate *digital signatures*. A private key can be applied to the digital fingerprint of a transaction to produce a numerical signature. This signature can only be produced by someone with knowledge of the private key. However, anyone with access to the public key and the transaction fingerprint can use them to *verify* the signature. This useful property of asymmetric cryptography makes it possible for anyone to verify every signature on every transaction, while ensuring that only the owners of private keys can produce valid signatures.

Source: Antonopoulus, Mastering Bitcoin

LEXIFY
MORE THAN LAWYERS

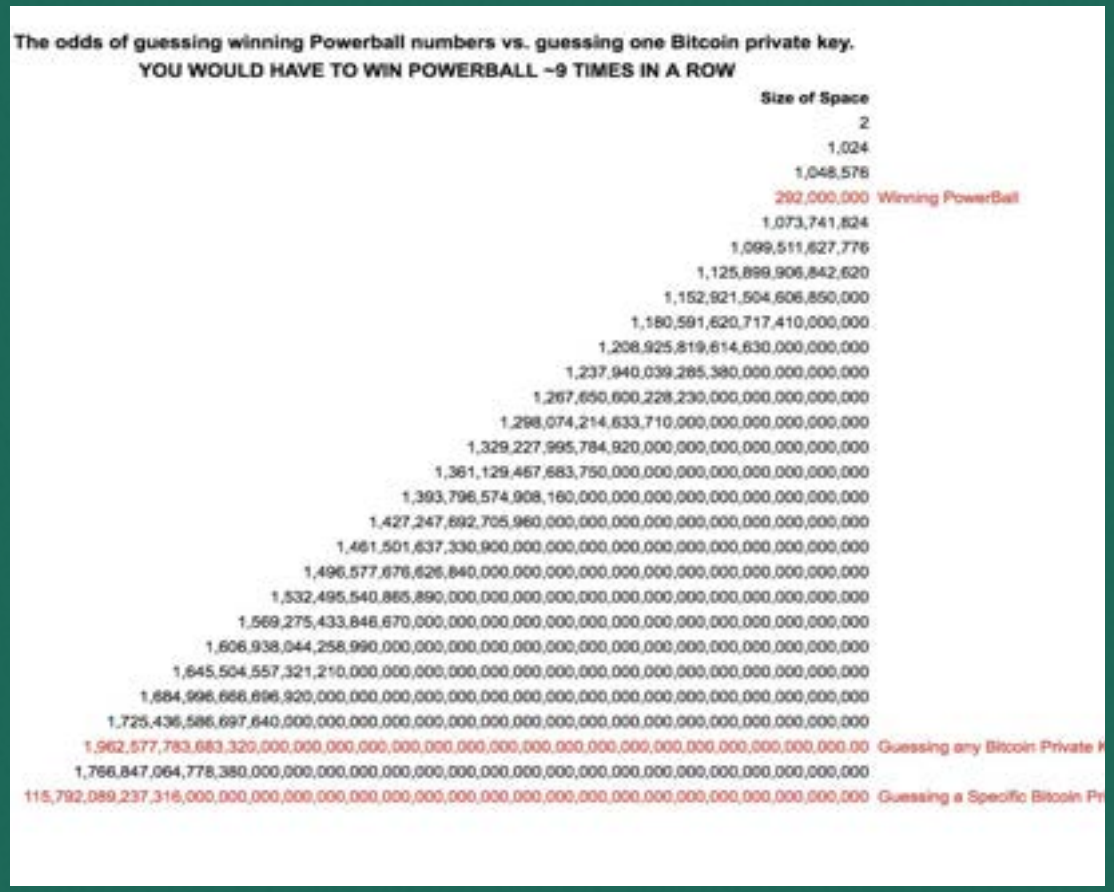
Public and private key (asymmetric cryptography)

- The size of bitcoin's private key space, (SHA256 = 2^{256}) is an unfathomably large number. It is approximately 10^{77} in decimal. For comparison, the visible universe is estimated to contain 10^{80} atoms.

- Movie explanation

LEXIFY
MORE THAN LAWYERS

How difficult it is to find a private key?



The odds of guessing winning Powerball numbers vs. guessing one Bitcoin private key.

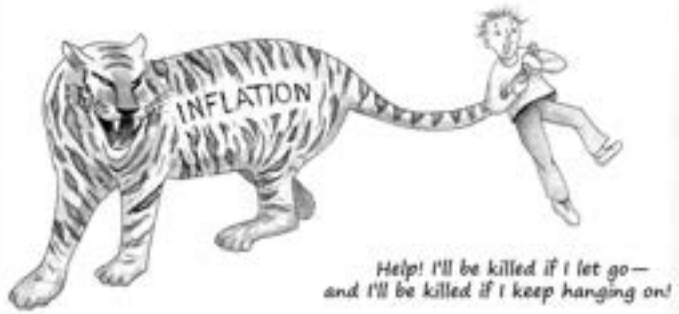
YOU WOULD HAVE TO WIN POWERBALL ~9 TIMES IN A ROW

Size of Space	
2	
1,024	
1,048,576	
292,000,000	Winning PowerBall
1,073,741,824	
1,099,511,627,776	
1,125,899,906,842,620	
1,152,921,504,606,850,000	
1,180,591,620,717,410,000,000	
1,208,925,819,614,630,000,000,000	
1,237,940,039,285,380,000,000,000,000	
1,267,650,600,228,230,000,000,000,000,000	
1,298,074,214,633,710,000,000,000,000,000,000	
1,329,227,995,784,920,000,000,000,000,000,000,000	
1,361,129,467,683,750,000,000,000,000,000,000,000,000	
1,393,796,574,908,160,000,000,000,000,000,000,000,000,000	
1,427,247,692,705,960,000,000,000,000,000,000,000,000,000,000	
1,461,501,637,330,900,000,000,000,000,000,000,000,000,000,000,000	
1,496,577,676,626,840,000,000,000,000,000,000,000,000,000,000,000,000	
1,532,495,540,865,890,000,000,000,000,000,000,000,000,000,000,000,000,000	
1,569,275,433,846,670,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
1,606,938,044,258,990,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
1,645,504,557,321,210,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
1,684,996,666,696,920,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
1,725,436,586,697,640,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
1,962,577,783,683,320,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,00	Guessing any Bitcoin Private K
1,766,847,064,778,380,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
115,792,089,237,316,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	Guessing a Specific Bitcoin Pr

LEXIFY
MORE THAN LAWYERS

Friedrich von Hayeck

- Austrian-British economist and philosopher.
- Shared the 1974 Nobel Memorial Prize in Economic Sciences with Gunnar Myrdal for his pioneering work in the theory of money.
- Inflation Theory.



LEXIFY
MORE THAN LAWYERS

Friedrich von Hayeck

Hayeck Inflation Theory (source https://www.essentialscholars.org/hayek):

- Inflation is a decline in money's purchasing power.
- By far the most common cause of inflation is an increase in the supply of money.
- stopping inflation is easy in principle, but made difficult by politics, not least because it is politics that usually is to blame for starting inflation in the first place.
- Fiat money is money backed by nothing other than faith in the government that issues it.
- Solution: denationalization of money, getting government completely out of the business of issuing money and controlling the money supply.
- Competitive market forces would instead be responsible for supplying sound money.

LEXIFY
MORE THAN LAWYERS

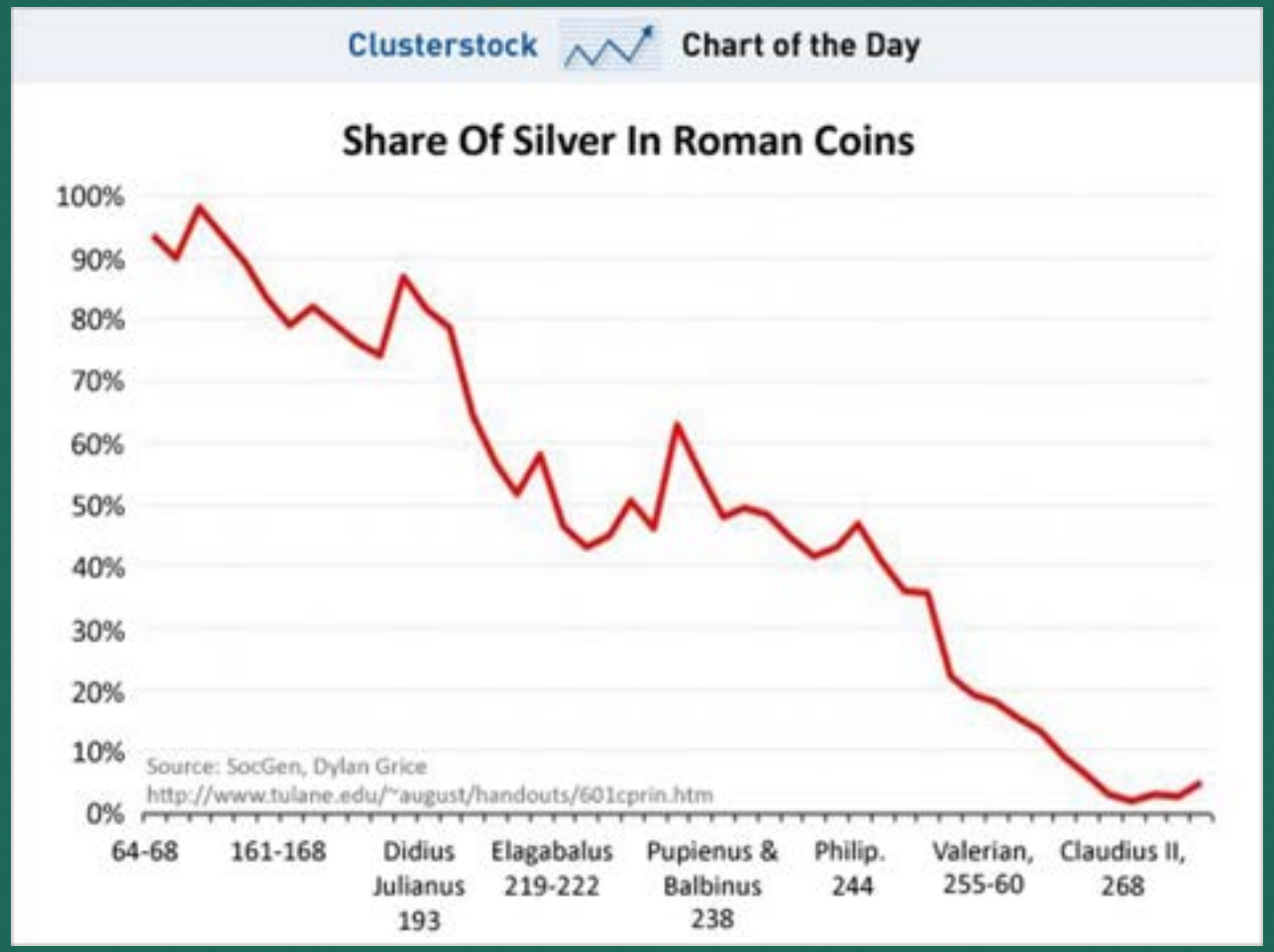
Hayek Interview

"I don't believe we shall ever have a good money again, before we take the thing out of the hands of government, that is, we can't take them violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can't stop." – **Frederick Hayek, 1984**

watch interview

LEXIFY
MORE THAN LAWYERS

Real example of Hayeck's inflation theory



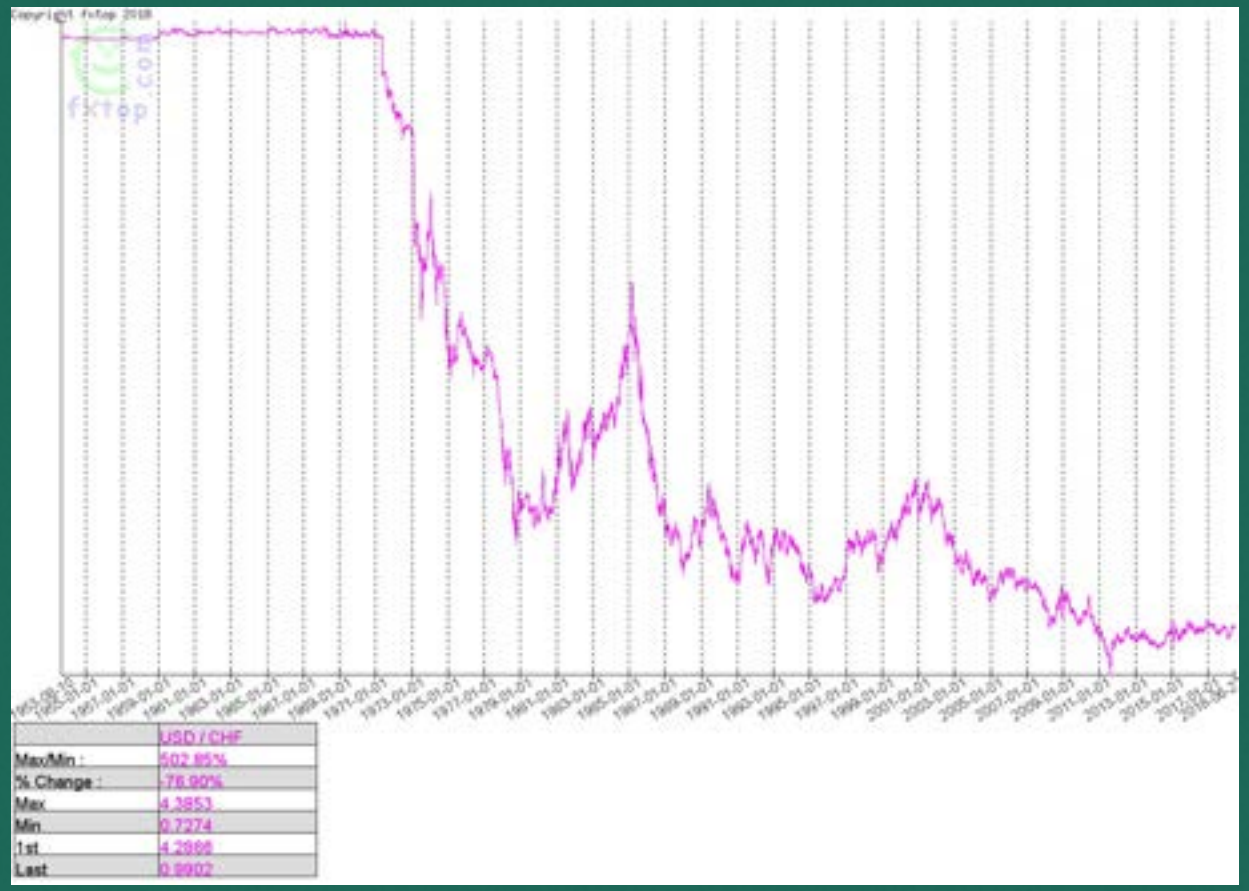
LEXIFY
MORE THAN LAWYERS

Real example of Hayeck's inflation theory

Source:https://en.wikipedia.org/wiki/Hyperinflation_in_the_Weimar_Republic#/media/File:Germany_Hyperinflation.svg

LEXIFY
MORE THAN LAWYERS

Real example of hayeck inflation theory



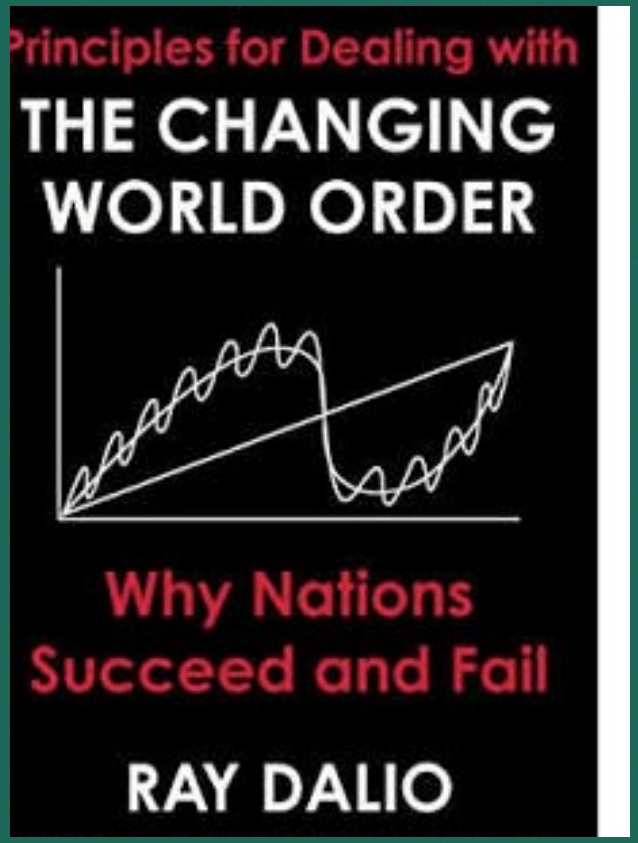
USD/CHF

(1953-2018)

LEXIFY
MORE THAN LAWYERS

Example of countries where politics interfere with central bank

LEXIFY
MORE THAN LAWYERS



"Printing and Devaluing Money Is the Easiest Way out of a Debt Crisis"

LEXIFY
MORE THAN LAWYERS

LEXIFY
MORE THAN LAWYERS

DISE
THE
ANTEED

New York

First to Last—

No. 27,412 (Copyright, 1931, New York Tribune Inc.) SUNDAY, DEC

tist
men
ked
ohn R.
entified
Up by
Matron
Flatly
Guilty

Ford Would Replace Gold With Energy Currency and Stop Wars

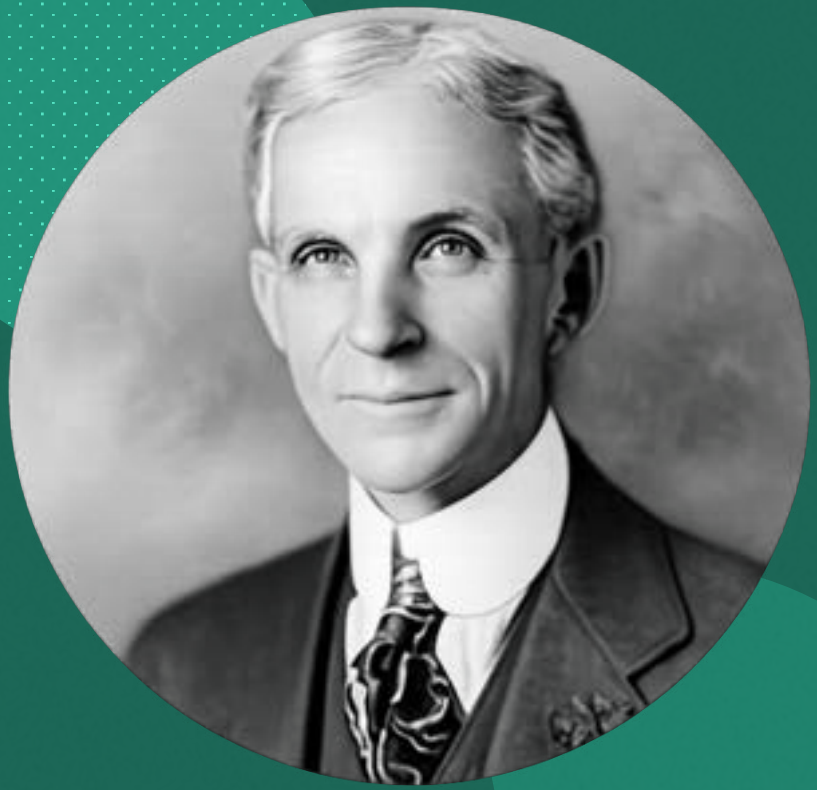
Declares if Government Will Give Him Muscle Shoals Plant He Can Demonstrate Success of Plan to Substitute Natural Wealth as Basis of World's Money

FLORENCE, Ala., Dec. 3.—Henry Ford and Thomas A. Edison arrived here to-day to inspect the Muscle Shoals nitrate plant, which the Detroit automobile manufacturer proposes to take over from the government, and almost immediately Mr. Ford declared the purpose of his vast new project. It is not to make money, or, primarily,

bankers who to-day control the bulk of the world's gold supply. No matter to what country they as individuals claim allegiance, they all play the same game to keep the gold they have in their own hands and to get just as much more as possible.

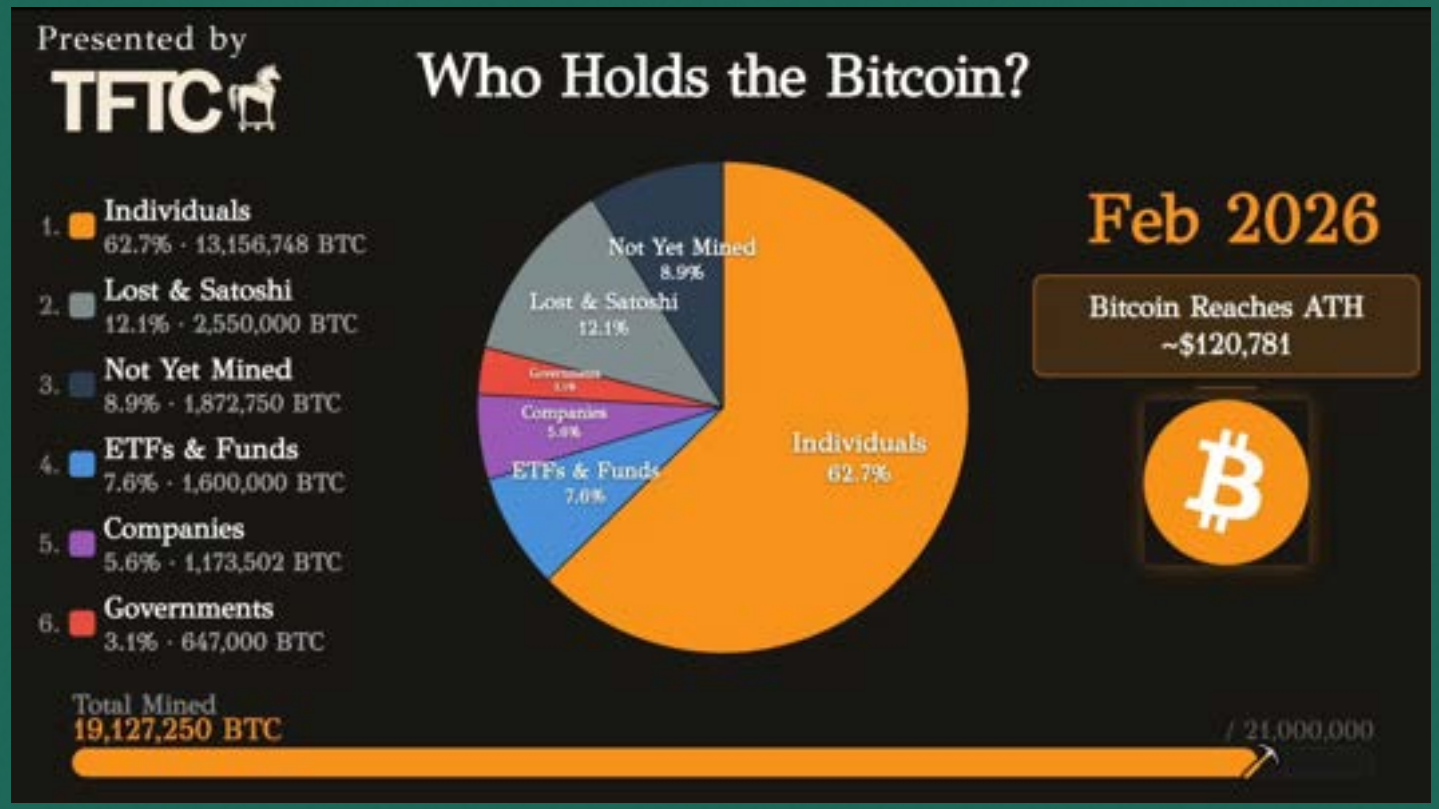
"With the international bankers the festering, starting and fighting of a war is nothing more nor less than creating an active market for money—a

Cra
$10
Edu
Slash I
Sugge
to Ob
$350,
State
To M



LEXIFY
MORE THAN LAWYERS

Bitcoin distribution



https://x.com/TFTC21/status/2023797841089741039

LEXIFY
MORE THAN LAWYERS

Stable coins – Transfer Volume

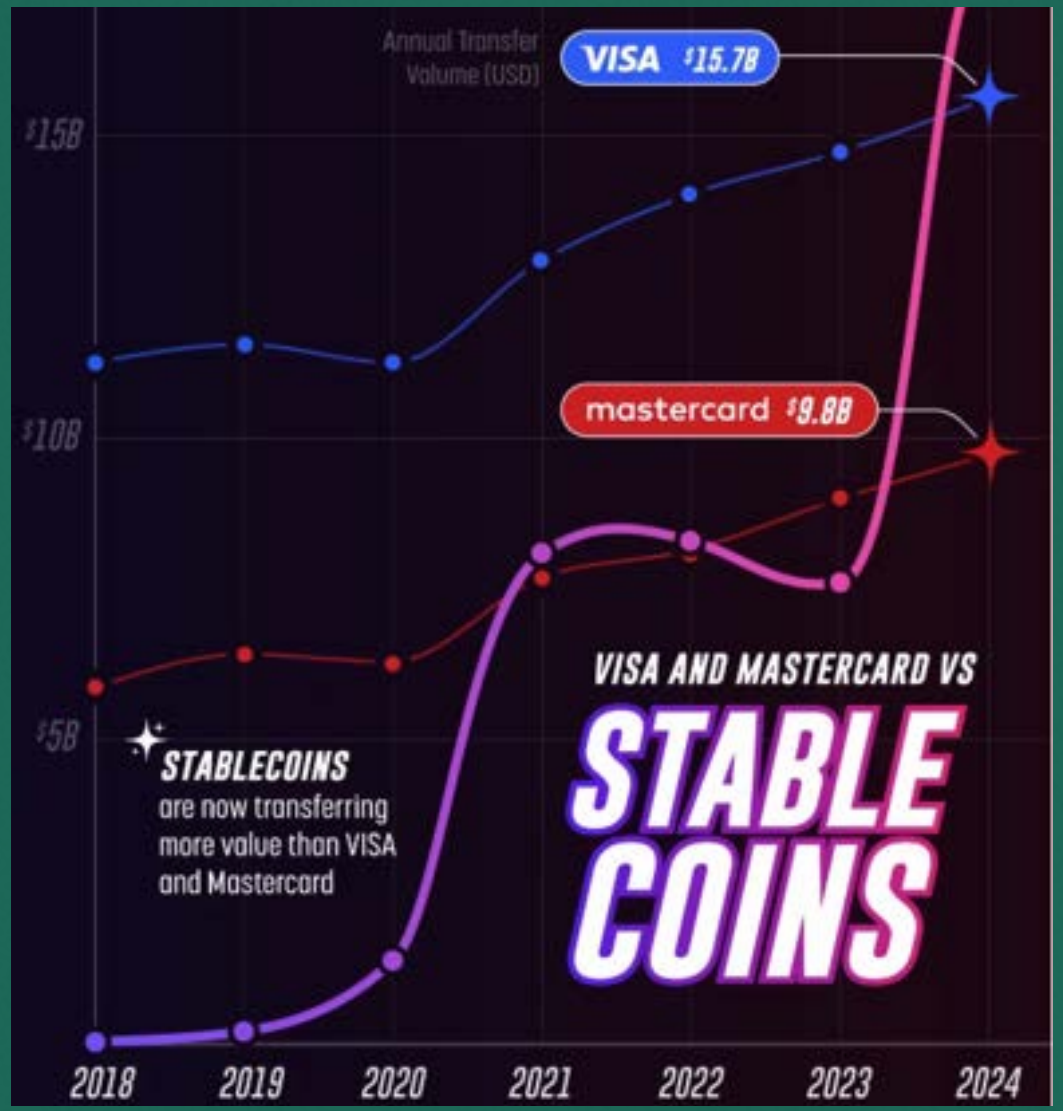
Source: https://hashdex.com/en-EU/insights/crypto-is-getting-more-deeply-ingrained-in-traditional-finance

LEXIFY
MORE THAN LAWYERS

Stable coins transfer volume

Stable coins to beat VISA and Mastercard.
Visa, Mastercard, Paypal are working on introducing payments through blockchain

PayPal issued its own stable coin (PYUSD)



LEXIFY
MORE THAN LAWYERS

Digital Euro

LEXIFY
MORE THAN LAWYERS

Digital Euro

The digital euro is a digital form of cash issued by the European Central Bank (ECB) and available to everyone in the euro area.

It is designed as a secure and stable electronic currency that complements physical cash, allowing fast and safe payments in shops, online, and between individuals.

Unlike cryptocurrencies, the digital euro is regulated by the ECB, ensuring trust and stability while providing a digital alternative for everyday payments. It aims to enhance payment options, support financial inclusion, and preserve the euro's role as a public money in a digital economy.

It offers a high level of privacy, without the ECB being able to link personal data to spending habits

LEXIFY
MORE THAN LAWYERS

Digital Euro

LEXIFY
MORE THAN LAWYERS

In the meantime, the market.....

Deka · CaixaBank · KBC · Raiffeisen Bank · SEB
Danske Bank · ING · UniCredit · Sella

PRESS RELEASE

Nine major European banks join forces to issue stablecoin

Amsterdam / Biella / Brussels / Copenhagen / Frankfurt / Milan / Stockholm / Valencia / Vienna – 25 September 2025

ING, Banca Sella, KBC, Danske Bank, DekaBank, UniCredit, SEB, CaixaBank and Raiffeisen Bank International – have joined forces to launch a MiCAR-compliant euro-denominated stablecoin. This digital payment instrument, leveraging blockchain technology, aims to become a trusted European payment standard in the digital ecosystem.

The stablecoin will provide near-instant, low-cost payments and settlements. It will enable 24/7 access to efficient cross-border payments, programmable payments, and improvements in supply chain management and digital asset settlements, which can vary from securities to cryptocurrencies.

The stablecoin will be regulated by EU's "Markets in Crypto-Assets Regulation" (MiCAR), and is expected to be first issued in the second half of 2026. The stablecoin consortium, with the aforementioned banks as founding members, has formed a new company in the Netherlands, aiming to be licensed and supervised by the Dutch Central Bank as an e-money institution. The consortium is open to additional banks joining. A CEO is expected to be appointed in the near future, subject to regulatory approval.

The initiative will provide a real European alternative to the US-dominated stablecoin market, contributing to Europe's strategic autonomy in payments. Individual banks will be able to provide value added services, such as a stablecoin wallet and custody.

"Digital payments are key for new euro-denominated payments and financial market infrastructure. They offer significant efficiency and transparency, thanks to blockchain technology's programmability features and 24/7 instant cross-currency settlement. We believe this development requires an industry-wide approach, and it's imperative that banks adopt the same standards," states Floris Lugt, Digital Assets Lead at ING and joint public representative of the initiative.

###

Press enquiries

Media Relations ING

Daan Wenthold

+31 20 576 63 66

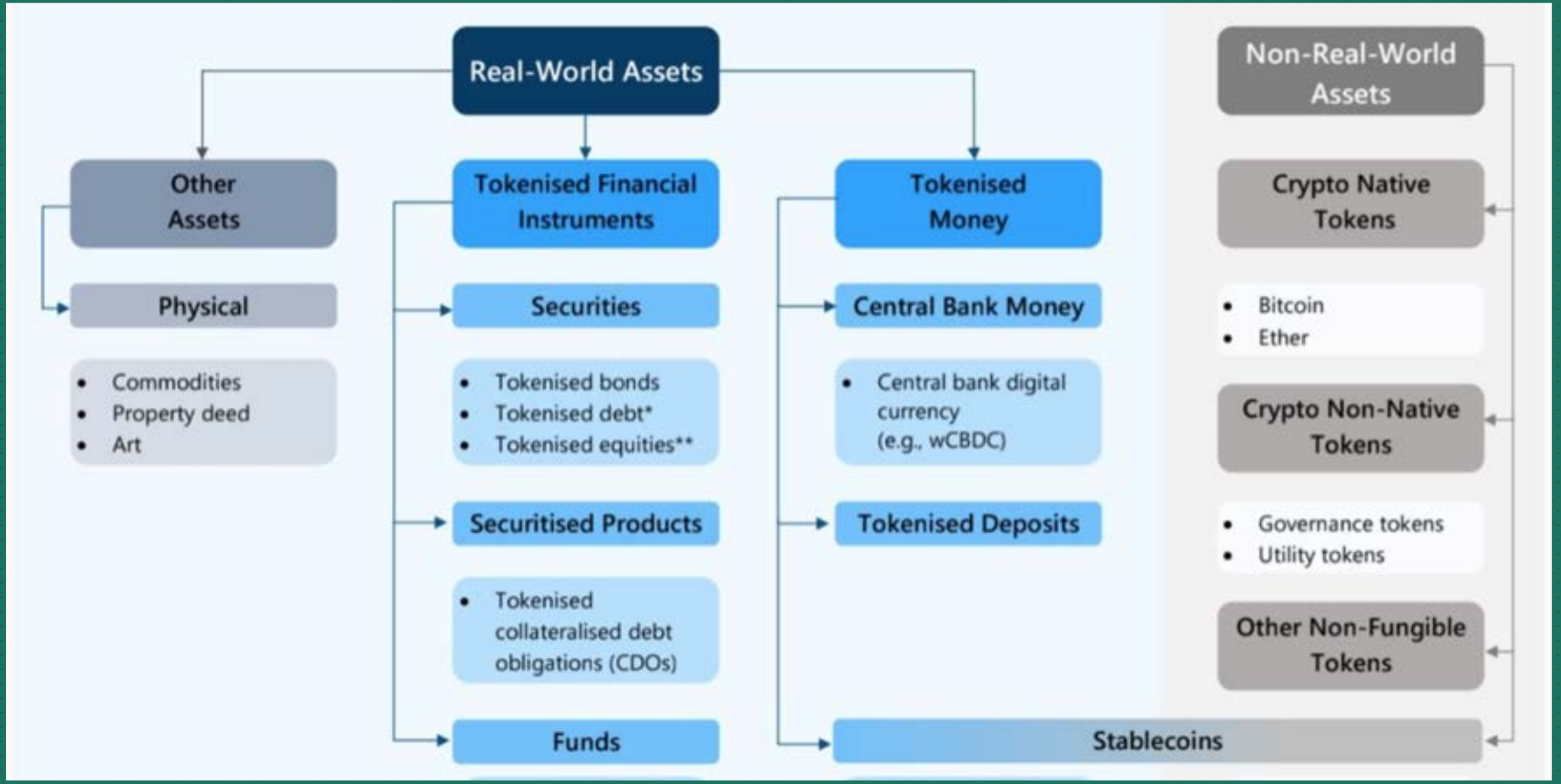
Reuters

Major banks explore issuing stablecoin pegged to G7 currencies

By Elizabeth Howcroft and Tommy Reggiori Wilkes

Deutsche Börse Group and Circle Announce Collaboration to Advance Stablecoin Adoption in Europe

LEXIFY
MORE THAN LAWYERS


Real-World Assets
Other Assets
Physical
Commodities
Property deed
Art
Tokenised Financial Instruments
Securities
Tokenised bonds
Tokenised debt*
Tokenised equities**
Securitised Products
Tokenised collateralised debt obligations (CDOs)
Funds
Tokenised Money
Central Bank Money
Central bank digital currency (e.g., wCBDC)
Tokenised Deposits
Stablecoins
Non-Real-World Assets
Crypto Native Tokens
Bitcoin
Ether
Crypto Non-Native Tokens
Governance tokens
Utility tokens
Other Non-Fungible Tokens

Commodities

- Proof of ownership: token is a proof that client hold gold.
- Tradable: blockchain based platform allow trading on secondary market 24/7
- Redeemable: token vs physical commodity.

LEXIFY
MORE THAN LAWYERS

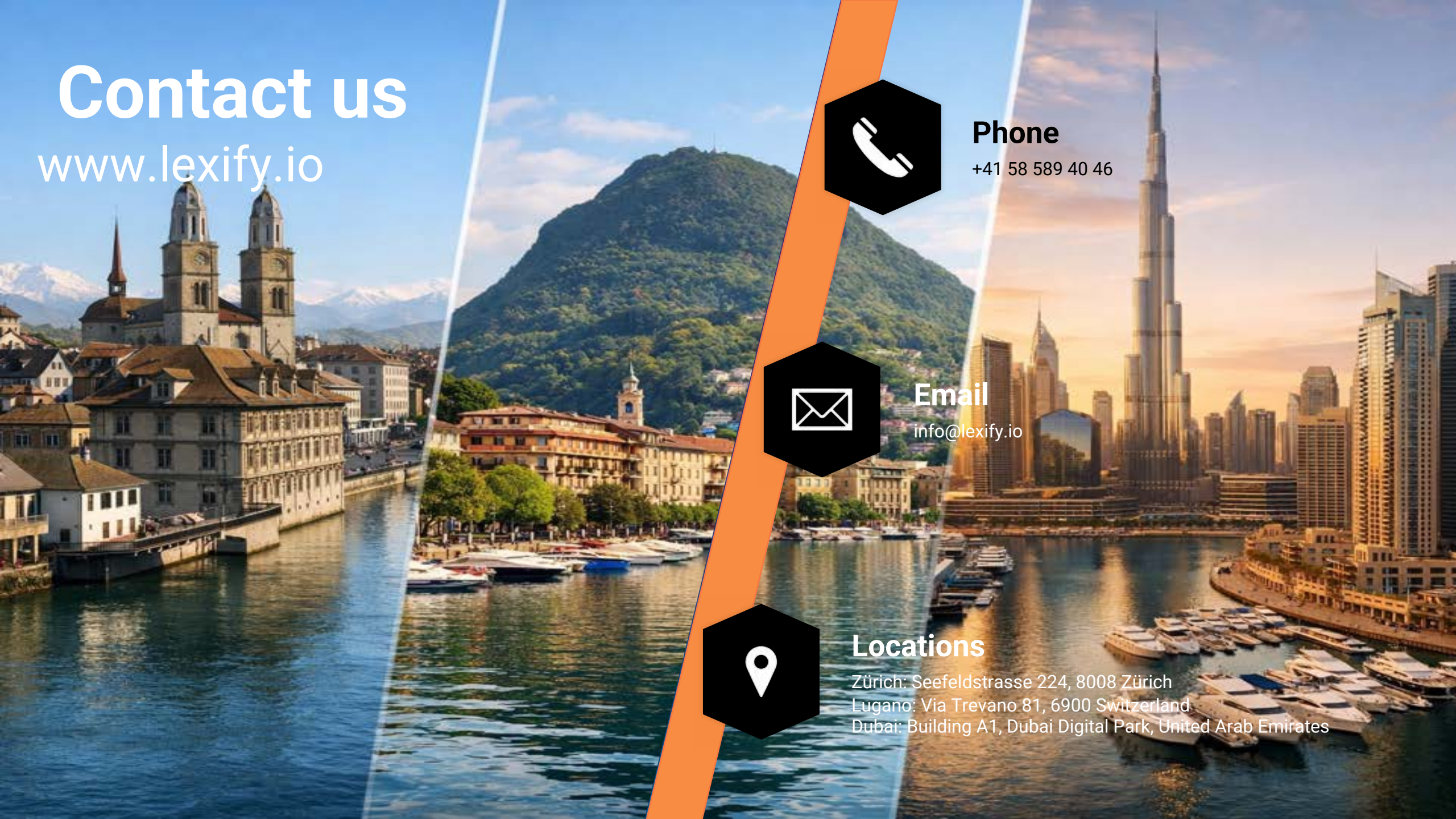
Carbon credits

- Marketplace already active (no authorization required)
- Auditability
- Data Transparency
- Data Accessibility

LEXIFY
MORE THAN LAWYERS

Contact us

www.lexify.io



Phone

+41 58 589 40 46

Email

info@lexify.io

Locations

Zürich: Seefeldstrasse 224, 8008 Zürich
Lugano: Via Trevano 81, 6900 Switzerland
Dubai: Building A1, Dubai Digital Park, United Arab Emirates