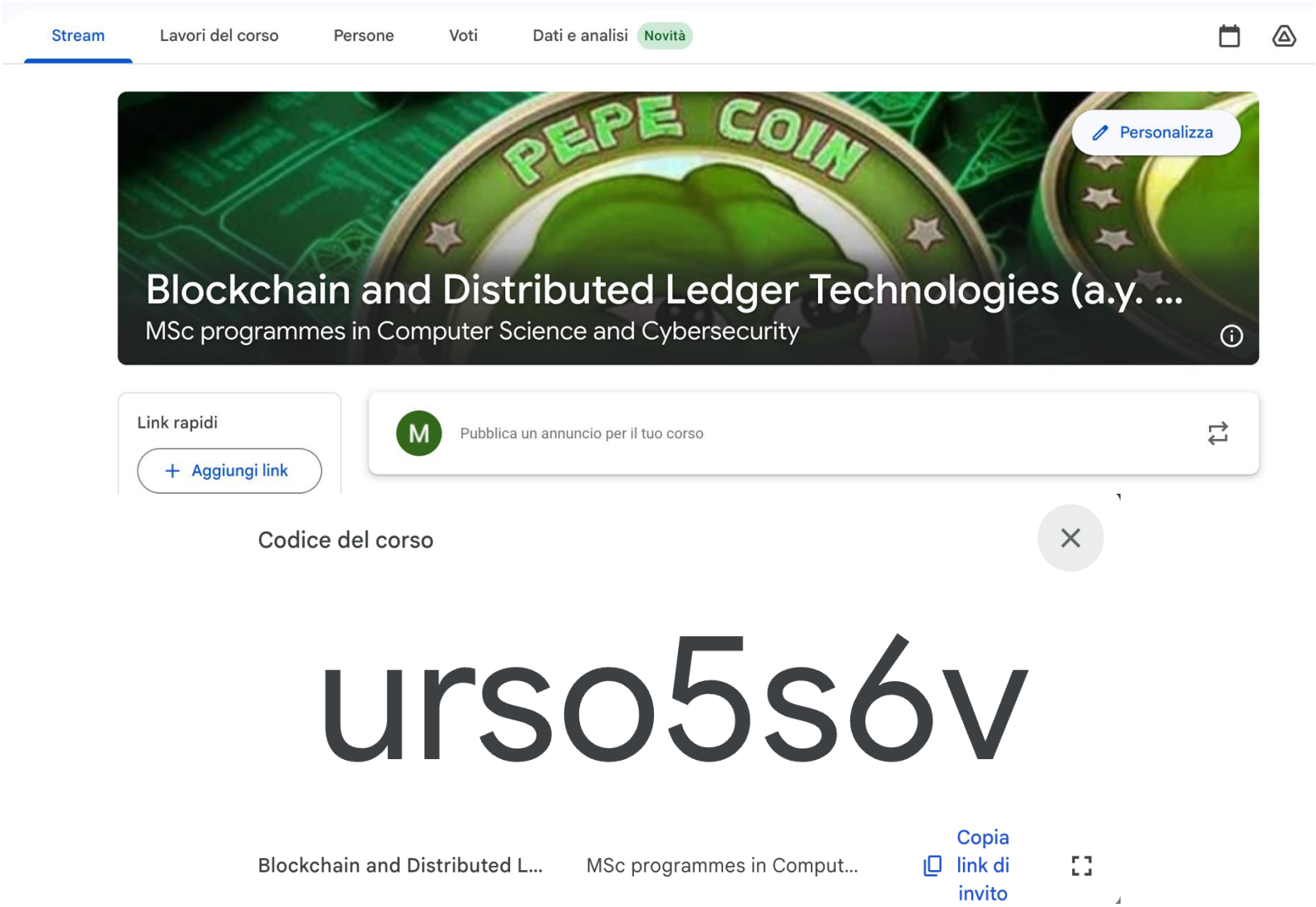
Blockchain and Distributed Ledger technologies

SAPIENZA
UNIVERSITÀ DI ROMA

Massimo La Morgia
massimo.lamorgia@uniroma1.it

Info, materials and announcements about the course



Massimo La Morgia

Assistant professor Tenure Track
Ph.D. in Computer Science

My office:
Room G26, 2nd floor, Building G
Viale Regina Elena 295

Office hours and student reception:
Take appointment via email: ***massimo.lamorgia@uniroma1.it***

2023 Seal of Excellence from the ***European Research Council***

Young researcher 2024 from the ***Italian Ministry of University and Research***

Research interests

SystemsLab

Research interests

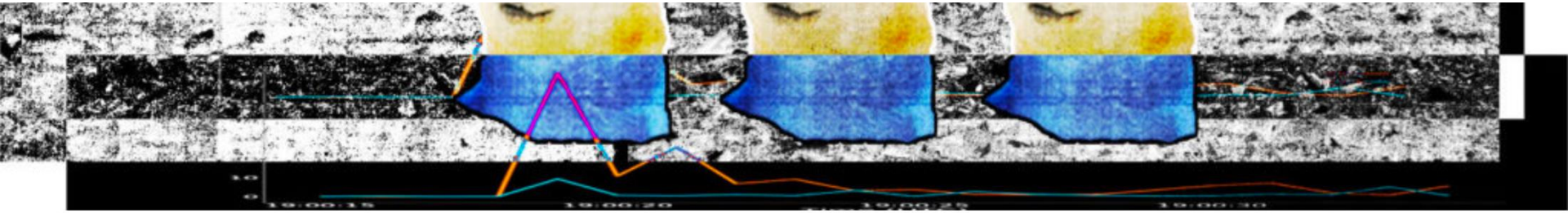
cryptonews All News + Exclusives + Videos + Guides + Exchanges Podcast Tools + Recommended + EN +

Fredrik Vold

Researchers Found a Way to Catch Altcoin Pumpers and Dumpers Early

USD EUR GBP BTC ETH

Bitcoin BTC +2.6%
Buy for 20855.50
Sell for 21151.10



THE WOLVES OF DOGECOIN: INSIDE THE UNDERGROUND CRYPTO HUSTLE

POPULAR

EL PAÍS

Tecnología

TU TECNOLOGÍA · CIBERSEGURIDAD · PRIVACIDAD · INTELIGENCIA ARTIFICIAL · INTERNET · GRANDES TECNOLÓGICAS · ÚLTIMAS NOTICIAS

FAKE NEWS >

De Rafapal a La Quinta Columna: así se financian los canales de conspiraciones en Telegram

Comisiones, donativos y campañas ayudan a sobrevivir a miles de los llamados medios alternativos, según un nuevo estudio que analiza su importancia en español

What will we NOT learn during the course?

What will we NOT learn during the course?

What will we learn during the course?

Blockchain definition

Blockchains are **tamper evident** and **tamper resistant** digital ledgers implemented in a **distributed** fashion (i.e., without a central repository) and usually **without a central authority** (i.e., a bank, company, or government).
At their basic level, they enable a community of **users to record transactions** in a **shared ledger** within that community, such that under normal operation of the blockchain network **no transaction can be changed once published**.

In this course, we will understand why the above sentence is true and how the mentioned concepts work.

What will we learn during the course?

Cryptocurrencies, NFT and frauds

Where is it possible to buy and sell cryptocurrencies.

How to store cryptocurrencies.

How to create your own cryptocurrency.*

What is a NFT

How to create your own NFT.*

What is the Decentralized Finance.

Some crypto frauds (Rug pull, wash trading, Pump and dump)

*if we have time

Teaching materials

Bitcoin and general concepts on Blockchain
Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.
Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder.
You can download the PDF version for fre
here: https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf Or buy the printed copy from Amazon.

Ethereum

Eth2Book: https://eth2book.info/capella/part2/incentives/

Advanced topic shared on classroom

All the information are reported on classroom too.

Q&A about course content

Is something not clear?
Do you have questions about a topic or about how something work?

Please fill out this form whenever you need:
https://forms.gle/DSS2VsoYrJ6BQDGz6

Exam

The exam consists of 3 parts

Part 1 : Practical tasks
They are assignment that I will give you during the class. They are hands-on activities on the blockchain, such as: create your own address or send a transaction.

Part2: Group Report and presentation
You will analyze a Blockchain, or a DeFi Protocol, or a blockchain-related event.
You must write a report on the chosen topic and present it (hopefully in class).
The report and presentation will be evaluated separately.

Part 3: Written test
The test may include open-ended questions, multiple-choice questions or exercises.

If there is the suspect that the report was generated using LLMs, or there are doubts about you understanding of course concepts, an additional oral test may be required.

Starting class routine

- **Which is the current Bitcoin price?**

If you do not know, please look for it online and let me know.

- **What is the current Ethereum price?**

If you do not know, please look for it online and let me know.

- **Have you heard any news about blockchain recently?**

I'd really appreciate it if in every class you would answer this questions

Starting class routine

Has anyone ever heard of Bitcoin?

Do you know what a cryptocurrency is?

Has anyone ever interacted with a blockchain?

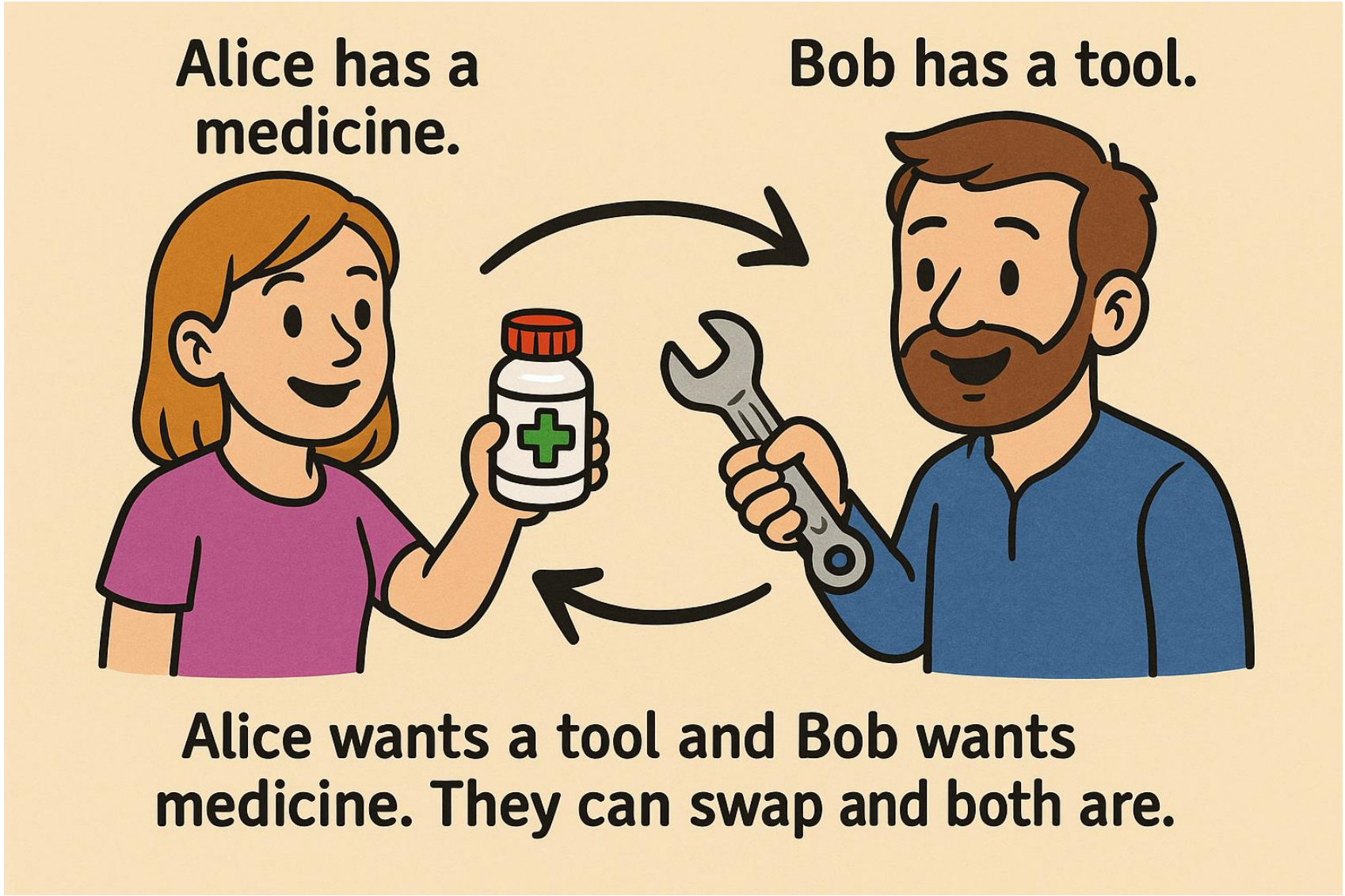
Has anyone ever bought a cryptocurrency? on a CEX or on a DEX?

Consensus : let's start to think about the problem

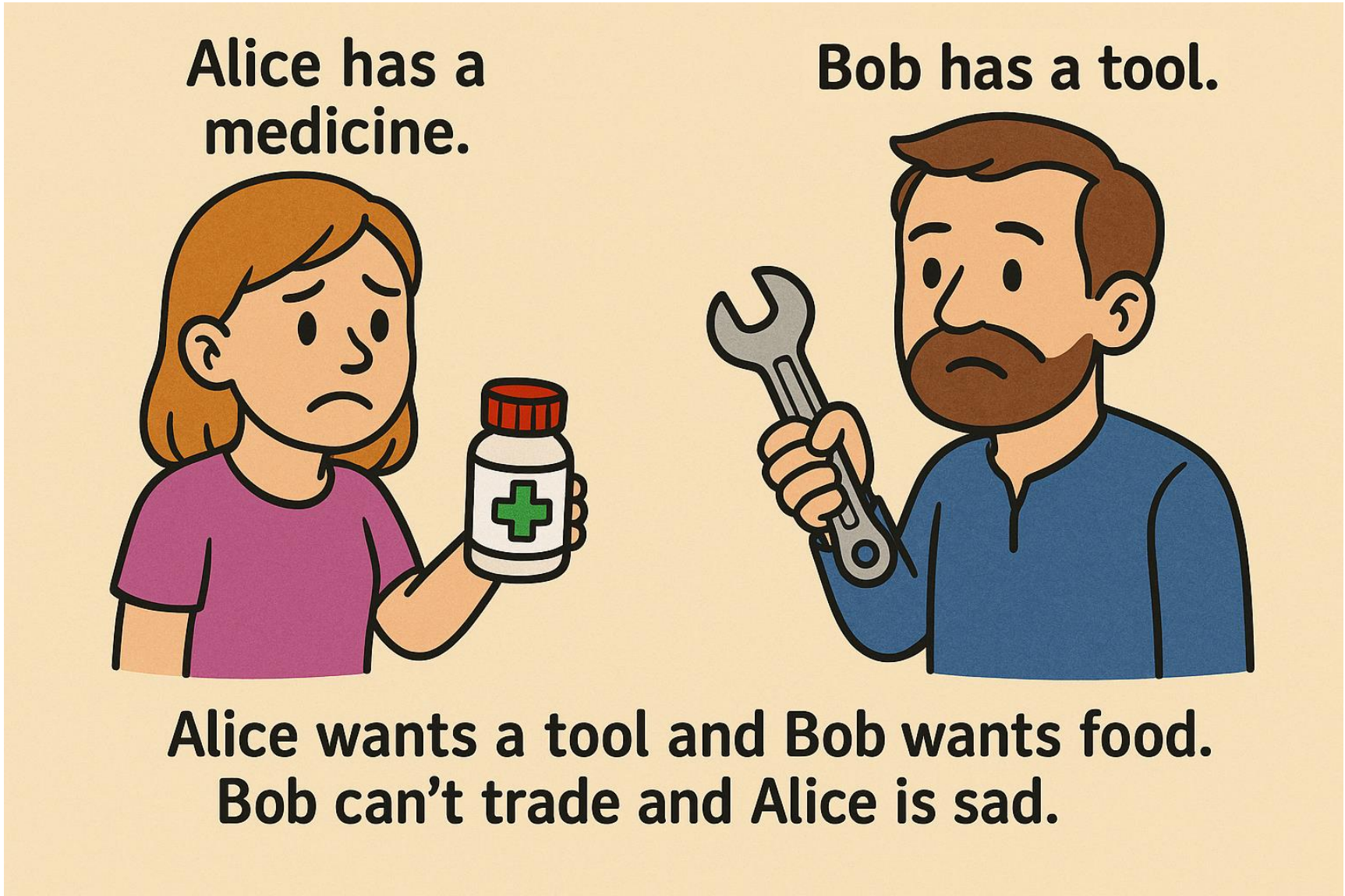
- What price will Bitcoin reach by the end of the course?
- Will Bitcoin remain above 100'000$?
- Will Ethereum surpass 6'000$?

If you win the bet the last class of this course will be a party!

Before currency - Barter



Before currency - Barter



Before currency - Barter

Alice wants a tool, Bob wants food, and Carol wants medicine.
They can trade so that everyone is happy.
They need to coordinate the exchange and meet to swap their items.

Before currency – Credit Base

In a credit-based system.

Alice has a medicine, Bob has a tool, and Carol has food.
Alice wants a tool, Bob wants food and carol wants medicine.

Alice and Bob would be able to trade with each other.
Bob gives Alice the tool, and Alice incurs a debt that she will settle with Bob in the future.

Later, if Alice meets Carol, she can trade her medicine for Carol's food, then return to Bob with the food to settle the debt.

Problems:
- We are assuming that all the items have the same value.
- There is the chance that someone never settle the debt.

Cash System

Cash solves all these problems.

- Trades can happen in any order.
- Items can have different values.
- Higher level of privacy.
- Offline transactions.

Cons:

- Cash-based systems need to be bootstrapped.
- Someone has to guarantee the value backed by cash (typically governments).

Online credit card

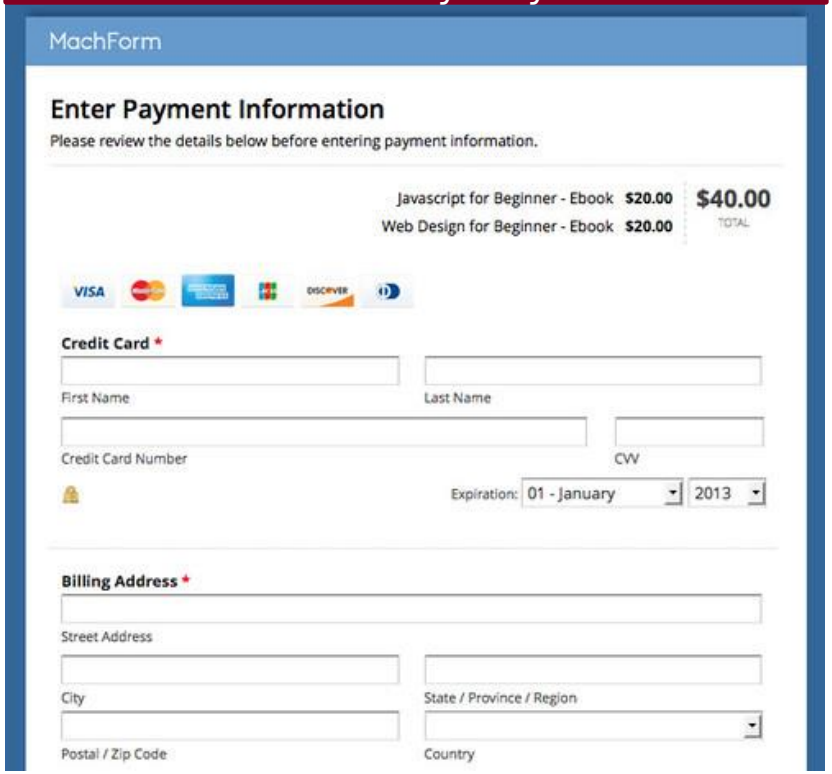
An intermediary is required.

You must provide your card details to the merchant, or add another intermediary such as PayPal.

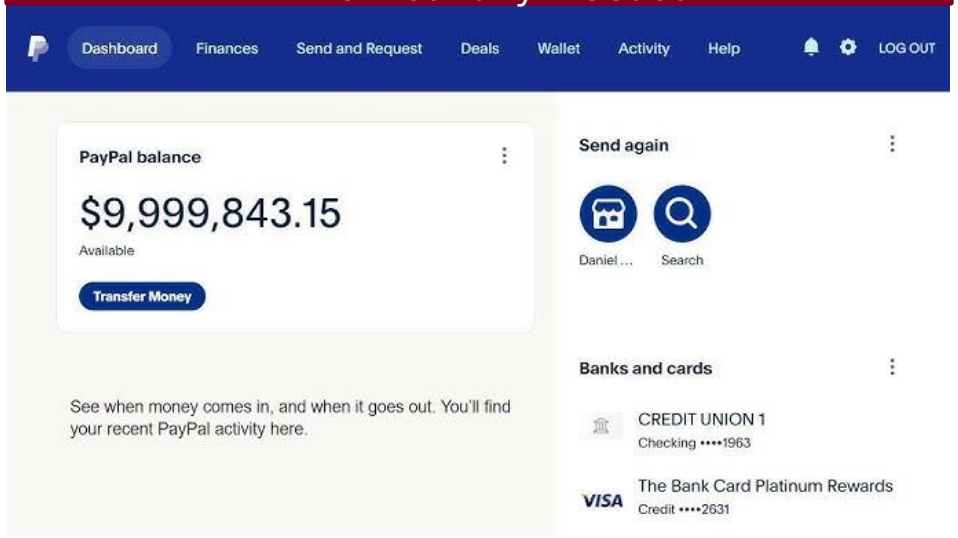
In this case, both the merchant and the customer must use the same intermediary.

The customer can file a chargeback or dispute a credit card statement.

No anonymity



Intermediary needed



Online-cash

The idea is to have a currency that can be spend online with the same benefit of a cash-system.

We can use a virtual note.
So, who has the virtual note can redeem it with who issue it.

But, who create the virtual note?
Well, the creator can sign the note, so now we know we have to pay.
The issuer is no more anonymous.

How hard is to create a perfect copy of the note?
It is very easy in the digital word.

The infinite money machine

Online-cash

The idea is to have a currency that can be spend online with the same benefit of a cash-system.

We can use a virtual note.
So, who has the virtual note can redeem it with who issue it.

But, who create the virtual note?
Well, the creator can sign the note, so now we know we have to pay.
The issuer is no more anonymous.

How hard is to create a perfect copy of the note?
It is very easy in the digital word.
Ok, let's attach an ID to each note, and track it in a ***ledger.***

How can I be sure that the I'm not using a copy of the note?
Let's verify it with the issuer of the note.

Can I trust him, that will eventually pay me or he have the money?
Let's introduce a central authority that guarantee for him.

Problems with centralized authorities

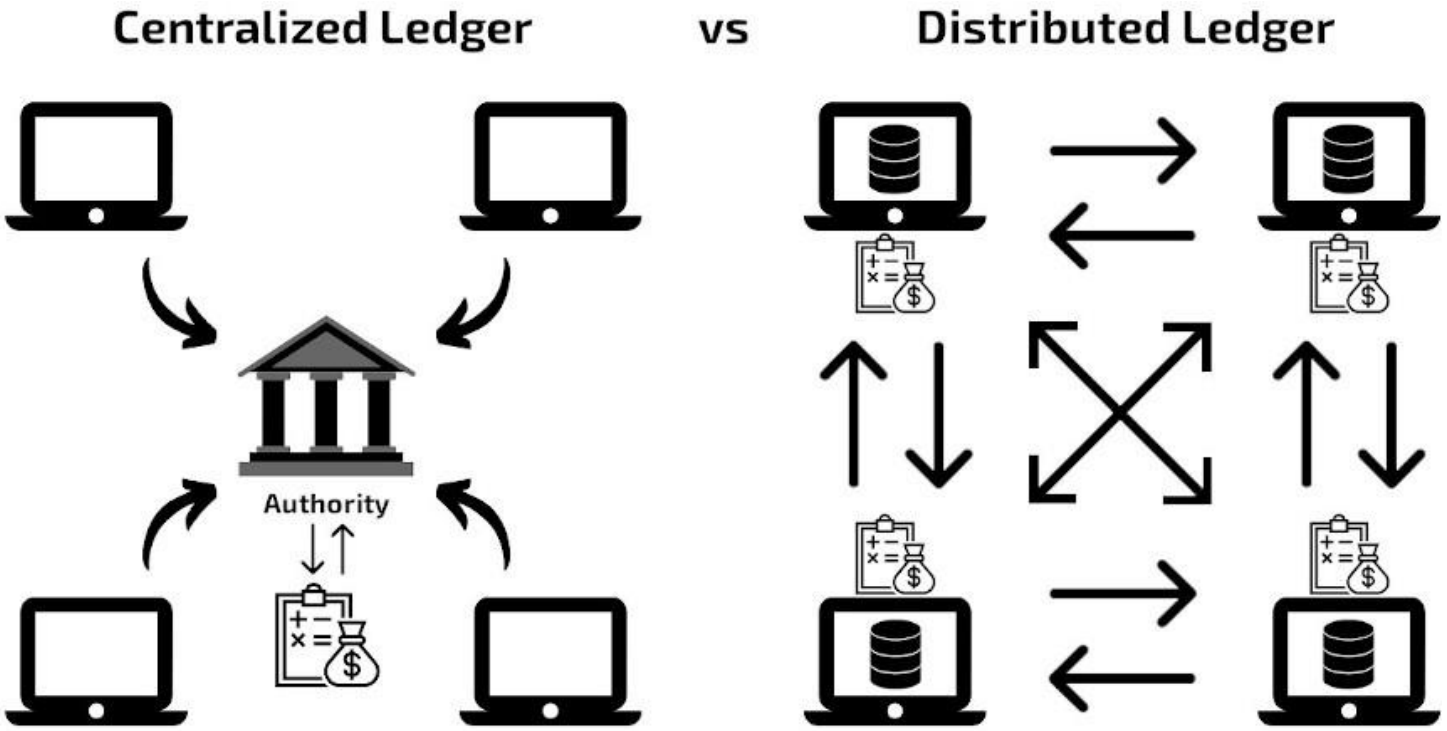
They can censorship transactions.

Both issuer and customer needs to trust or agree on the same central authority.

Transaction cost. Central authorities make work so they have to be paid.

Transaction can be reverted.

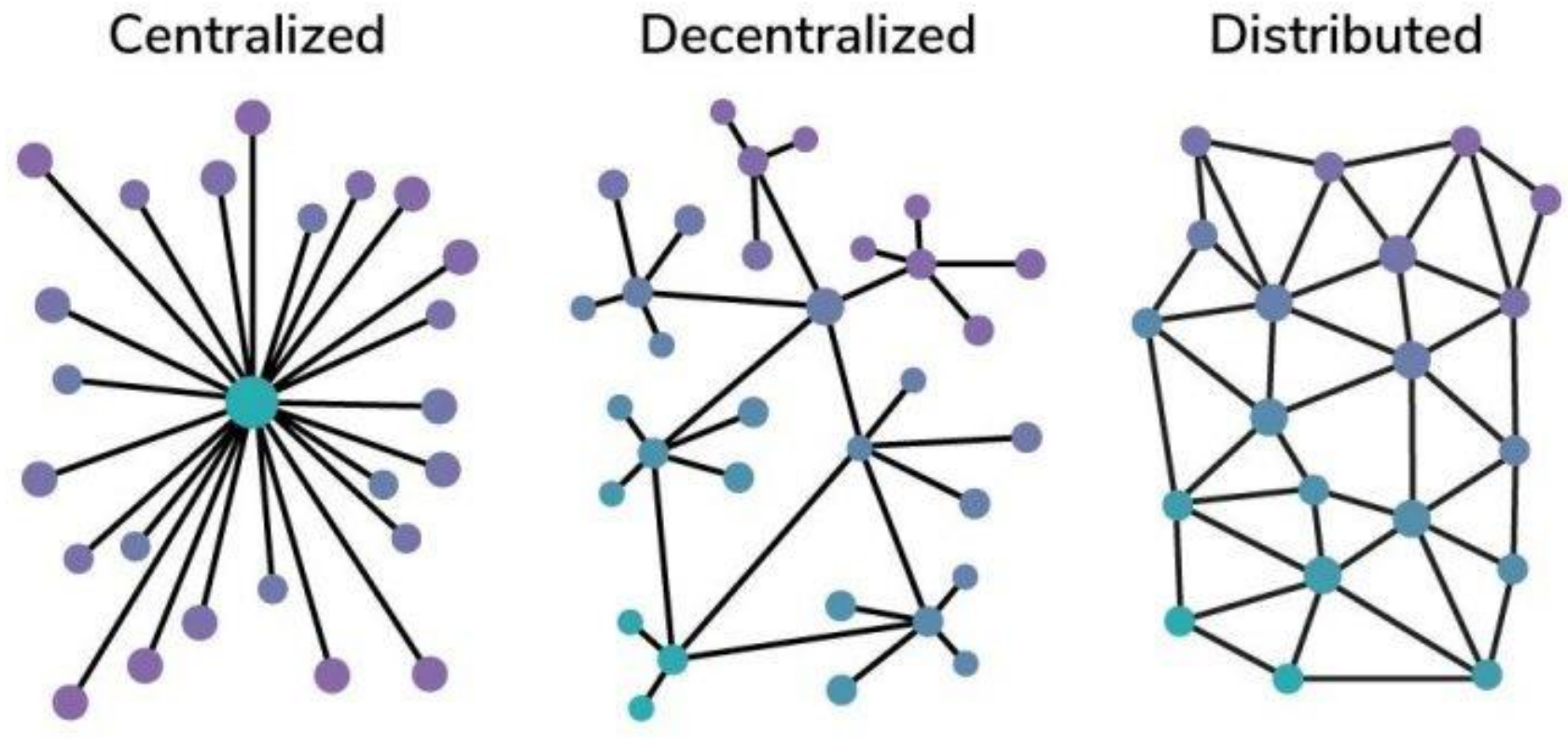
Distributed ledger



- CA can censorship transactions.
- Both issuer and customer needs to trust or agree on the same CA.
- Transactions cost. Central authorities make work so they have to be paid.
- No anonymity.
- Transaction can be reverted.

- No Intermediaries
- Censorship-Trust
- Digital and Borderless
- Pseudonymous Transactions
- Potentially Lower Fees.
- Fast transaction (more or less)

Centralized vs Decentralized vs Distributed



Centralized: A single central authority (server, node, or organization) controls all data processing and decision-making.

Decentralized: Multiple independent nodes make decisions or provide services ***without a single central authority***. Each node can operate on its own while cooperating with others.

Distributed: A collection of independent computers ***that appear to users as a single system***, often sharing tasks and resources.

Blockchains are usually politically decentralized and architecturally distributed

Distributed system

“A distributed system is one in which the failure of a computer you didn't even know existed can render your own computer unusable.” [Laslie Lamport]

In a distributed systems you can make no assumption about:

- **Timing** – messages can be delayed, reordered, or lost.
- **Network reliability** – links can fail or recover unpredictably.
- **Node availability** – any process or machine may crash or restart at any moment.
- **Global state** – no single node ever has a perfectly up-to-date view of the whole system.
- **Clocks** – physical clocks drift; you can’t assume perfectly synchronized time.

Bitcoin - Inception

White paper published on August 18 2008

Bitcoin: A Peer-to-Peer Electronic Cash System

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

1st **transaction** January 12 2009

First **block mined** January 3 2009

THE TIMES

Saturday January 3 2009 timesonline.co.uk No 69523

£1.50

Eat Out from £5

More than 900 great restaurants, including four **Gordon Ramsay** favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

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

99p

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

Business, page 47

Michael Sheen Frost, Nixon and me

Magazine

Working mums So that's how she does it

Body&Soul

Detox in style The best spas on the planet

Travel

Salman Rushdie I won't marry again

Pages 22, 23

Giant killing? Guide to the FA Cup third round

Sport

Bitcoin – Pizza day

On May 22, 2010, the first known **commercial transaction using bitcoin** occurred when programmer Laszlo Hanyecz bought two Papa John's pizzas for ₿10,000, in what would later be celebrated as "Bitcoin Pizza Day".

AltCoin – Not only Bitcoin

Other than Bitcoin exist several (hundreds) other blockchains.

Some are: Ethereum, Solana, Tron, Doge, BNB Smart Chain

Coin is the native currency of a blockchain, it is the currency that fuel the blockchain.

Altcoin: Alternative coins to Bitcoin. (Not Bitcoin)

Some blockchain allow users to create piece of codes (smart contract) and run it on the blockchain.

Users can develop and create new currency, commonly called **tokens.**

Market capitalization

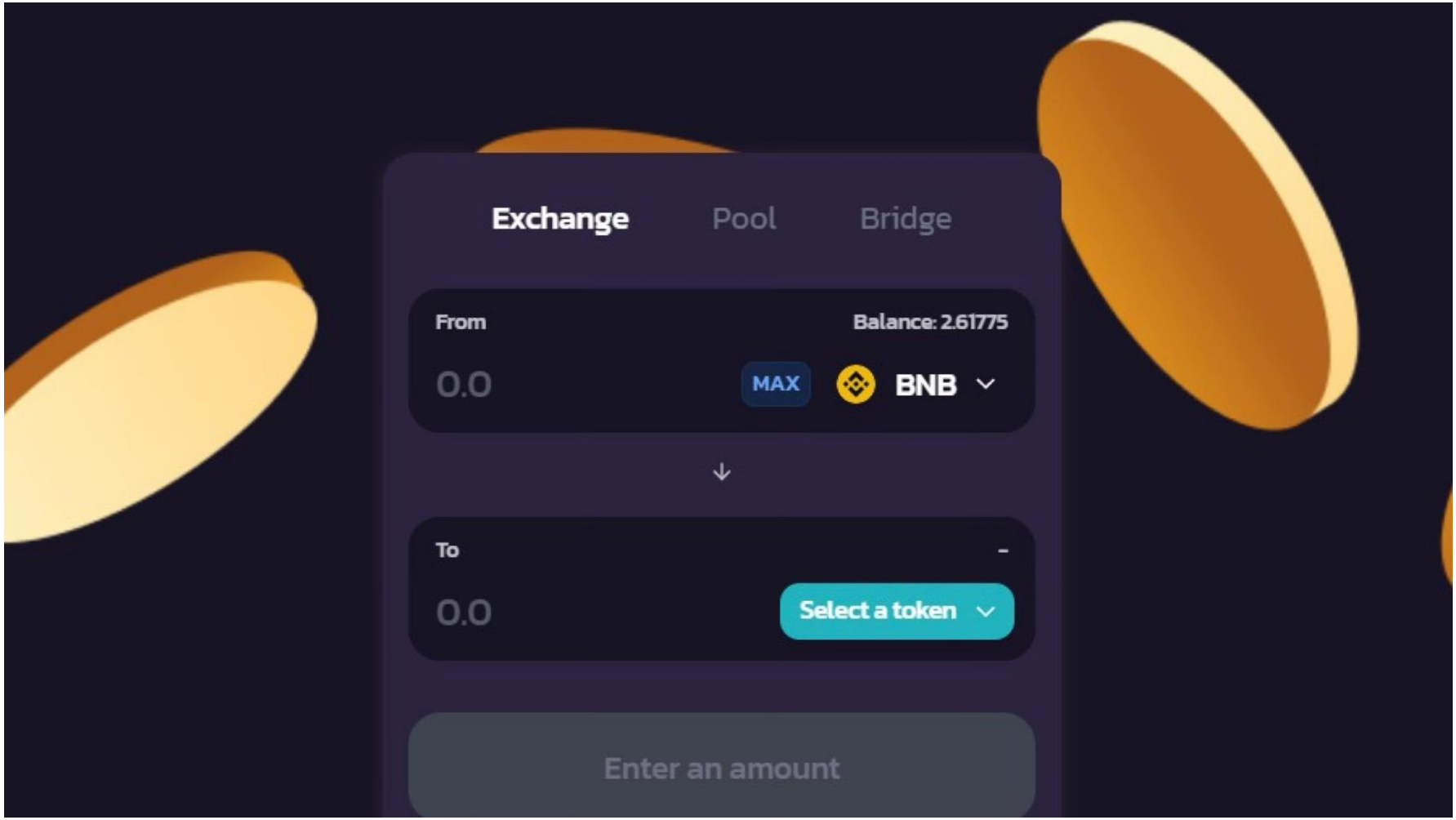
#	Name		Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply
1	Bitcoin BTC	Buy	$112,725.19	0.18%	2.23%	1.74%	$2,245,857,445,296	$62,897,844,842 557.58K	19.92M BTC
2	Ethereum ETH	Buy	$4,172.86	0.03%	6.65%	7.16%	$503,680,255,865	$54,531,120,332 13.06M	120.7M ETH
3	Tether USDT	Buy	$1.00	0.03%	0.06%	0.08%	$172,196,397,314	$179,415,932,673 179.28B	172.01B USDT
4	XRP XRP	Buy	$2.84	0.42%	3.93%	5.37%	$170,307,642,315	$9,290,462,443 3.26B	59.77B XRP
5	BNB BNB	Buy	$994.37	0.52%	4.57%	8.37%	$138,403,764,200	$4,660,585,673 4.68M	139.18M BNB
6	Solana SOL	Buy	$219.84	0.39%	7.18%	5.25%	$119,435,137,985	$10,763,670,008 48.78M	543.27M SOL
7	USDC USDC	Buy	$1.00	0.03%	0.05%	0.04%	$73,929,311,483	$21,786,010,315 21.78B	73.91B USDC
8	Dogecoin DOGE	Buy	$0.2396	0.08%	8.81%	9.30%	$36,202,497,490	$5,414,987,116 22.61B	151.04B DOGE
9	TRON TRX	Buy	$0.3422	0.07%	0.35%	0.23%	$32,397,855,798	$1,222,056,929 3.57B	94.66B TRX
10	Cardano ADA	Buy	$0.8211	0.02%	6.60%	4.22%	$29,399,316,689	$2,333,813,291 2.84B	35.8B ADA
11	Hyperliquid HYPE	Buy	$47.83	1.03%	6.61%	8.81%	$15,974,305,221	$609,696,809 12.69M	333.92M HYPE
12	Chainlink LINK	Buy	$21.27	0.14%	7.44%	8.02%	$14,424,097,949	$1,373,361,463 64.51M	678.09M LINK
13	Ethena USDe USDe	Buy	$1.00	0.01%	0.14%	0.05%	$14,147,503,920	$463,657,705 462.96M	14.12B USDe
14	Avalanche AVAX	Buy	$31.89	0.31%	2.68%	11.65%	$13,469,978,457	$1,624,327,090 50.88M	422.27M AVAX
15	Sui SUI	Buy	$3.35	0.39%	7.18%	3.69%	$11,963,679,482	$1,707,695,925 509.81M	3.56B SUI
16	Stellar XLM	Buy	$0.3641	0.01%	4.31%	3.22%	$11,608,921,617	$371,779,399 1.02B	31.87B XLM
17	Bitcoin Cash BCH	Buy	$567.32	0.27%	4.79%	3.75%	$11,306,279,930	$512,751,118 904.18K	19.92M BCH

Market capitalization

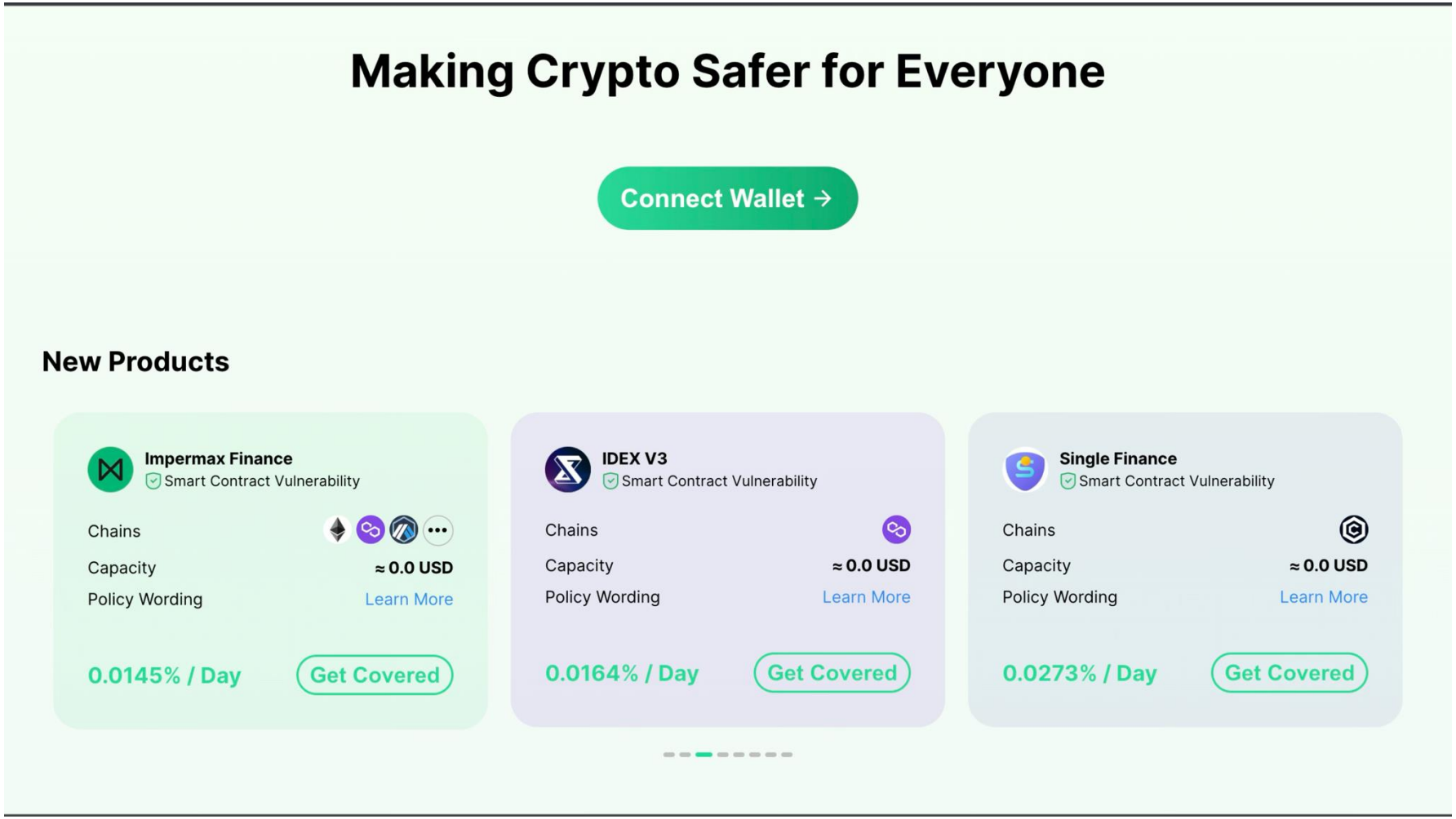
Rank	Name	Market Cap	Price	Today	Price (30 days)	Country
1	Gold GOLD	$25.644 T	$3,819	1.16%		
2	NVIDIA NVDA	$4.470 T	$183.61	3.97%		USA
3	Microsoft MSFT	$3.823 T	$514.45	-0.67%		USA
4	Apple AAPL	$3.800 T	$256.08	4.31%		USA
5	Alphabet (Google) GOOG	$3.055 T	$252.88	-0.92%		USA
6	Silver SILVER	$2.508 T	$44.56	0.78%		
7	Amazon AMZN	$2.427 T	$227.63	-1.66%		USA
8	Bitcoin BTC	$2.249 T	$112,991	0.41%		
9	Meta Platforms (Facebook) META	$1.922 T	$765.16	-1.63%		USA
10	Saudi Aramco 2222.SR	$1.608 T	$6.65	0.08%		S. Arabia
11	Broadcom AVGO	$1.599 T	$338.79	-1.61%		USA
12	Tesla TSLA	$1.443 T	$434.21	1.91%		USA
13	TSMC TSM	$1.414 T	$272.63	2.93%		Taiwan

NFT - Not Fungible token

De-Fi decentralized Finance



De-Fi decentralized Finance



Do I really need a blockchain?

Do I really need a blockchain?

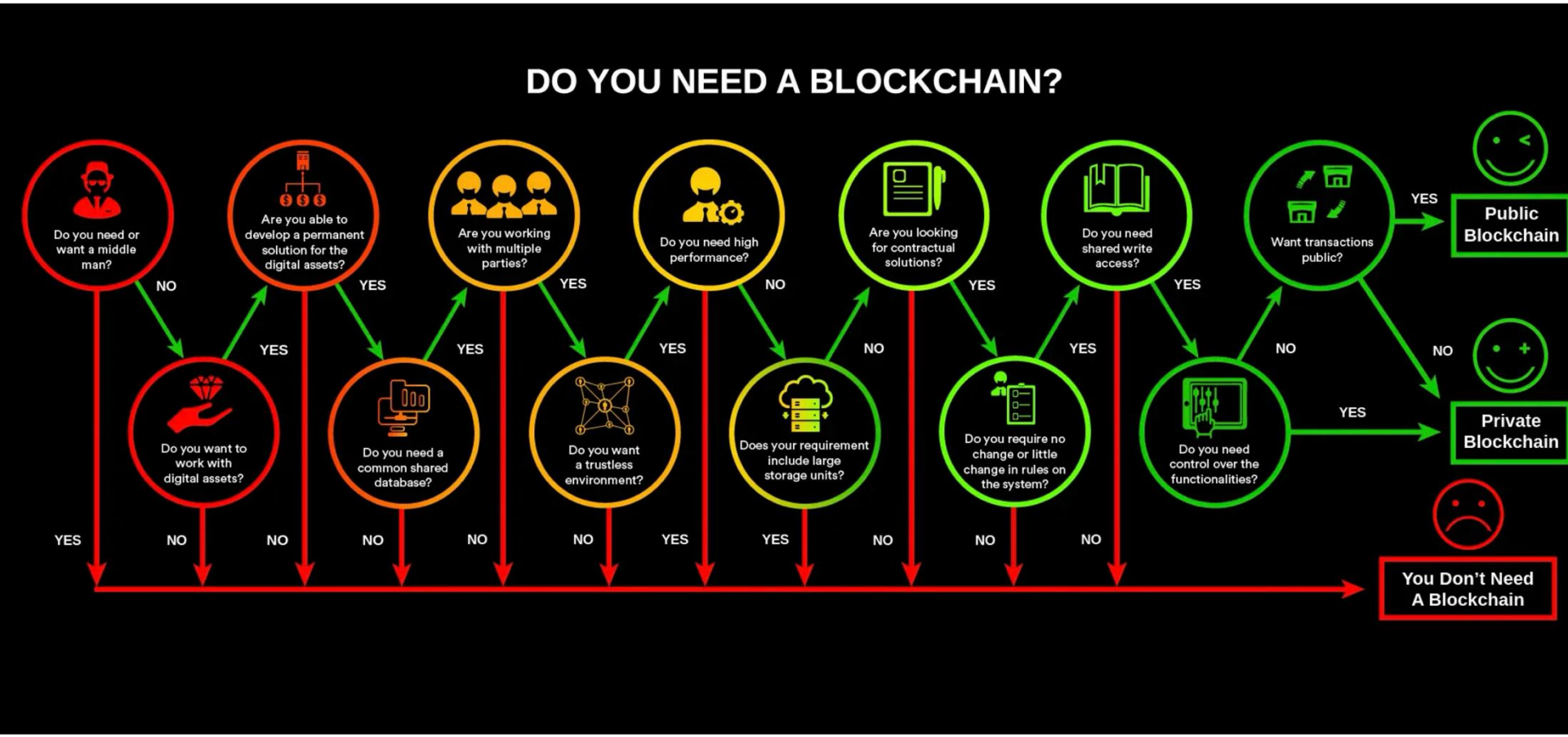


Image from 101blockchains.com

Do I really need a blockchain?

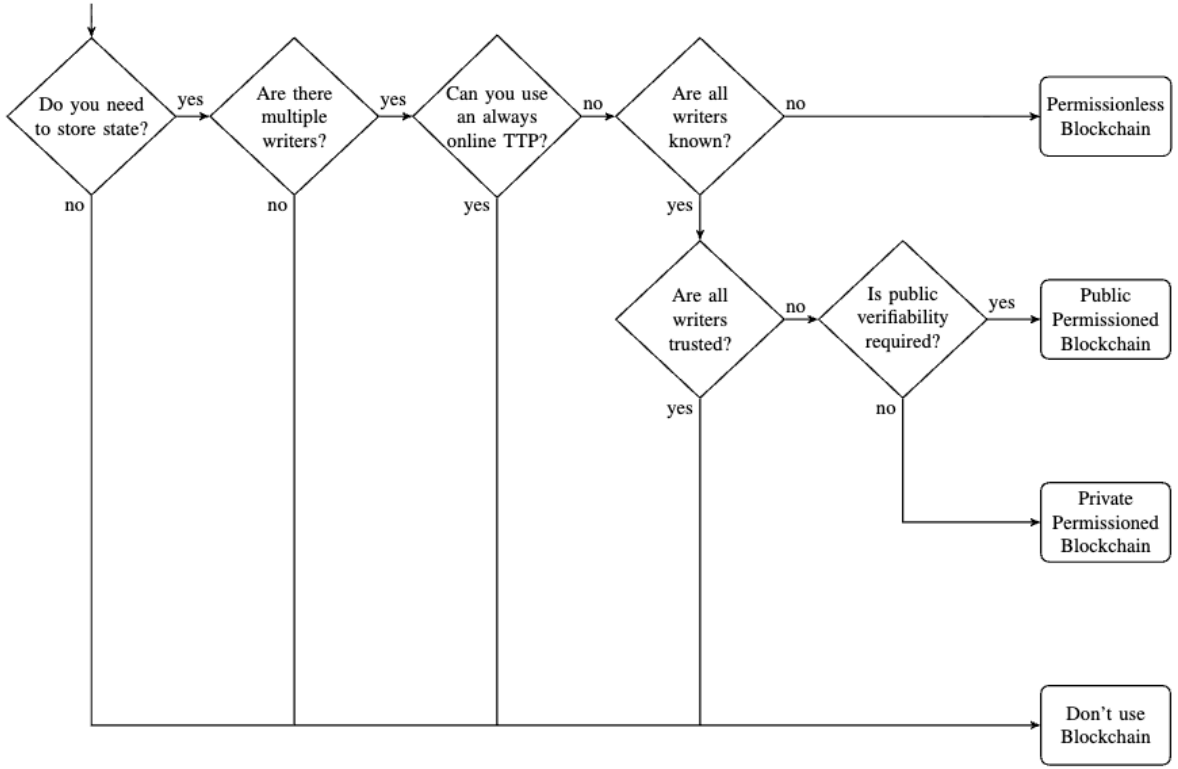


Fig. 1: A flow chart to determine whether a blockchain is the appropriate technical solution to solve a problem (Table I should be considered in the decision making process as well). Writers refer to entities with write access to the database/blockchain, i.e. in a blockchain setting, a writer corresponds to a consensus participant. If a trusted third party (TTP) is available that is not always online, this can be used to establish a known group of writers, i.e. the TTP can function as a certificate authority in such a setting. Public and private permissioned blockchains differ in that a public blockchain allows anyone to read the contents of the chain and thus verify the validity of the stored data, while a private blockchain only allows a limited number of participants to read the chain. Note that for any blockchain based solution it is possible to make use of cryptographic primitives in order to hide privacy-relevant content.

Wüst, K. & Gervais, A. Do you Need a Blockchain? CVCBT, IEEE, 2018