

CRYPTOCURRENCY, BLOCKCHAIN, AND A NEW ECONOMIC WORLD

OLLI

LATE SUMMER 2021

LECTURE 4

BEBO WHITE - BEBO.WHITE@GMAIL.COM



HOLY BITCOIN, ALL CRYPTO ENTHUSIASTS ABOARD THE NEW RELIGION

CRYPTOCURRENCY LATEST NEWS

by Adilin Beatrice / September 3, 2021



Because of its underlying technology, holy bitcoin is worth becoming a religion

BEGINNING ATTEMPT AT BIBLIOGRAPHY

<https://bit.ly/3BzmjTq>

I will adding to it and hope that you will too

"The currency of this world should be the dollar. And I don't think we should have all of the Bitcoins of the world out there. I think they should regulate them very, very high," Trump told Varney at the time adding, "It takes the edge off of the dollar and the importance of the dollar."

?

In an interview with Fox Business released on Tuesday, former United States President Donald Trump was questioned about his views on the health of the Wall Street markets, the current administration's progress and the potential of Bitcoin (BTC) and the cryptocurrency market.

In response to the latter question, the former president stated: "I like the currency of the United States, but I think the others are potentially a disaster waiting to happen." He continued:

“

"They [cryptocurrencies] may be fake. Who knows what they are? They are certainly something that people don't know very much about."

If you don't believe it or don't get it, I don't have the time to try to convince you, sorry.

Satoshi Nakamoto

© outland

The New York Times

There's a Better Way to Stop Ransomware Attacks

Aug. 31, 2021



The United States can make it harder. By more aggressively regulating cryptocurrencies, the government can limit their use as an anonymous payment system for unlawful purposes.

If greater regulation does not put an end to using cryptocurrency to pay ransoms, the United States can always consider disrupting a cryptocurrency like Bitcoin. Government hackers could disable the servers of cryptocurrency exchanges, block their internet traffic or infect their payment systems with malware. This would be an extreme and highly aggressive solution, one that would jeopardize the many legitimate storehouses of value that cryptocurrencies represent.

BACK TO THE RESOURCE REQUIREMENTS OF POW

“Change takes energy. This is the basic problem at the root of civilization. It’s the reason we have become so dependent on fossil fuels and the reason we continue to release carbon dioxide into the atmosphere - despite knowing full well that it rapidly deteriorates our climate with disastrous consequences. But every crisis has its possible miracle cure.”

-Sabine Hossenfelder, New York Times, 29 August 2021
(review of a book about nuclear fusion)

the resource requirements of the BTC network might ordinarily put an end to the cryptocurrency discussion

likewise for some unexpected implementation issues e.g., the dominance of mining pools, the unchecked volatility, etc.

but Satoshi left open the door to other possibilities and solutions - the discussion was just beginning

BITCOIN/BLOCKCHAIN ARE OPEN SOURCE SOFTWARE

- collaboratively produced, shared freely, published transparently and developed to be a community good
- there isn't a single chokepoint in the development process - no company or individual that makes, owns and sells the software
- software code is maintained in a public software repository
- why did Satoshi do this? (short answer: Satoshi is/was a cypherpunk)
- there is a difference from freeware or shareware

Being open source means anyone can independently review the code. If it was closed source, nobody could verify the security. I think it's essential for a program of this nature to be open source.

Satoshi Nakamoto

quote fancy

SHAREWARE

- no access to the program source code and no ability to modify
- there is no community of support
- it is developed and released by someone who keeps full control of the intellectual property (IP)
- distribution model is “download and try - if you like it, buy it”

OPEN SOURCE VS. FREWARE

- both refer to essentially the same set of licenses and software but different underlying values
- freeware
 - “free” means freedom (Richard Stallman)
 - focusses on what the recipient is allowed to do - run, copy, distribute, study, change, improve, etc.
 - “free software is a social movement”
- open source
 - focusses on practical consequences especially effective collaboration on software development
 - “open source is a development methodology”

OTHER EXAMPLES OF OPEN SOURCE SOFTWARE

- Linux
- Apache
- Android
- Mozilla
- MySQL
- etc., etc.



these softwares “run the world!”

PROBLEMS WITH THE BTC MODEL QUICKLY APPEARED (AND REMAIN)

- unexpected and unpredicted volatility
- a slow “transaction rate” (i.e., how quickly transactions could be verified and added to the blockchain) limits widespread use - the 10 minute window
- the PoW model required extensive computational resources (by design) but
 - restricted the entities that could become *miners*
 - resulted in environmental impact
- the maximum limit on coin in circulation appeared arbitrary
- open source means freedom to address these issues

LET'S TALK ABOUT VOLATILITY (1/3)

- one of the major criticisms/concerns about cryptocurrency
- the connection between cryptocurrency and its volatility certainly shapes its popular perceptions
- are there any precedents? “how many of us have been around at the birth of a totally new financial infrastructure?”
- who has heard the “tulip-mania” meme?
- who remembers “Silver Thursday” (March 27, 1980)?

Tulip mania

From Wikipedia, the free encyclopedia

"Tulip fever" redirects here. For the film set during the period of tulip mania, see [Tulip Fever](#).

Tulip mania, **tulipmania**, or **tulipomania** (Dutch names include: *tulpenmanie*, *tulpomanie*, *tulpenwoede*, *tulpengekte* and *bollengekte*) was a period in the Dutch Golden Age during which contract prices for bulbs of the recently introduced tulip reached extraordinarily high levels and then dramatically collapsed in February 1637.^[2] It is generally considered the first recorded speculative bubble (or economic bubble);^[3] although some researchers have noted that the *Kipper- und Wipperzeit* (literally *Tipper and See-saw*) episode in 1619–1622, a Europe-wide chain of debasement of the metal content of coins to fund warfare, featured mania-like similarities to a bubble.^[4] In many ways, the tulip mania was more of a hitherto unknown socio-economic phenomenon than a significant economic crisis (or financial crisis). And historically, it had no critical influence on the prosperity of the Dutch Republic, the world's leading economic and financial power in the 17th century. The term "tulip mania" is now often used metaphorically to refer to any large economic bubble when asset prices deviate from intrinsic values.^[5]



Extraordinary Popular Delusions and the Madness of Crowds

From Wikipedia, the free encyclopedia

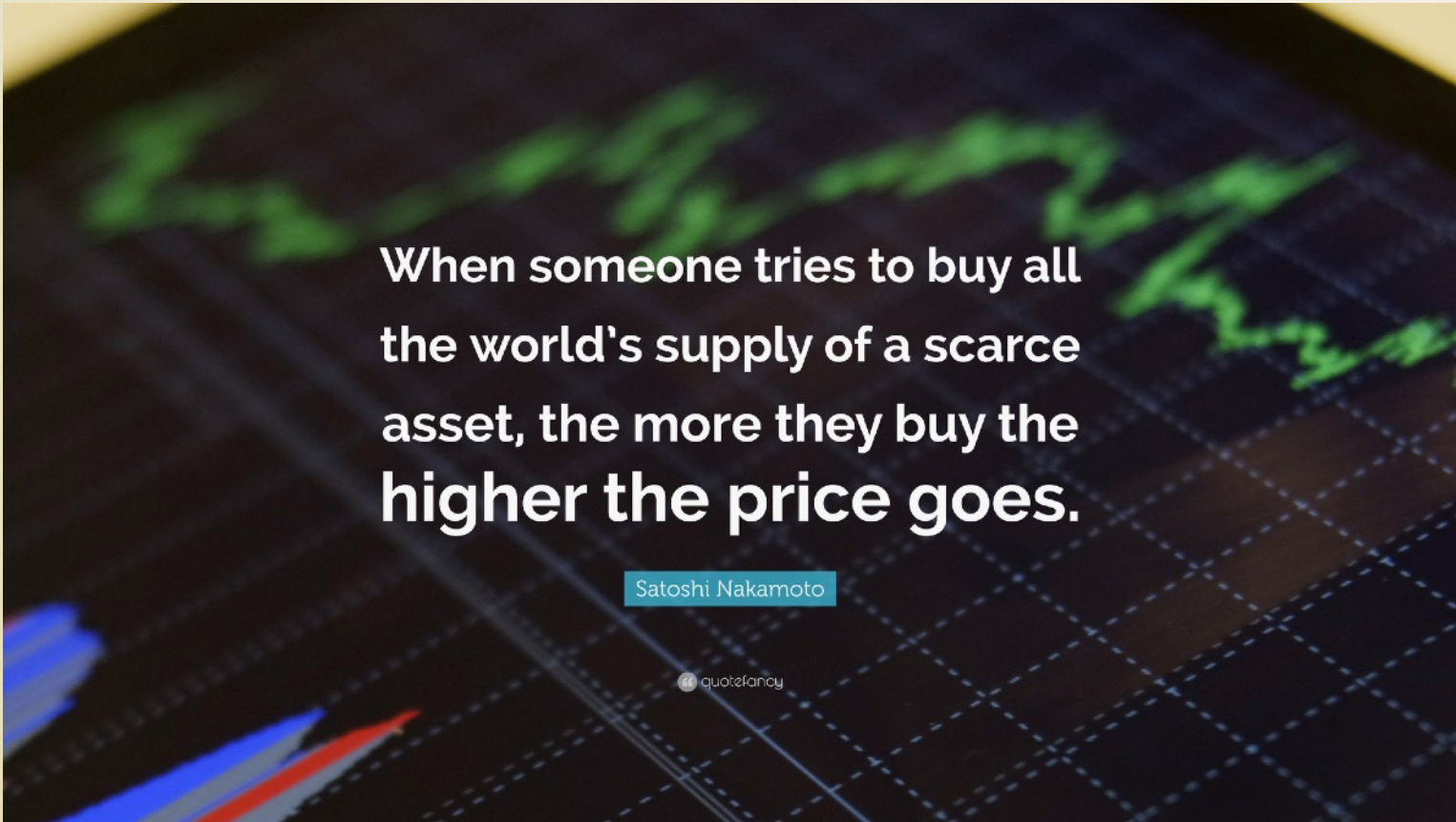
Extraordinary Popular Delusions and the Madness of Crowds is an early study of crowd psychology by Scottish journalist [Charles Mackay](#), first published in 1841.^[1] The book chronicles its subjects in three parts: "National Delusions", "Peculiar Follies", and "Philosophical Delusions". MacKay was an accomplished teller of stories, though he wrote in a journalistic and somewhat sensational style.

There was a total disconnect between the fundamental value of a tulip and the price that a prized specimen could bring

“NoCoiners” love to use the
tulip mania meme



The Hunt brothers try to corner the silver market



When someone tries to buy all the world's supply of a scarce asset, the more they buy the higher the price goes.

Satoshi Nakamoto

quotefancy

.....until

would it be possible for someone to buy all/majority of bitcoin?

IT'S MORE LIKE DOT.COM

- displacement
 - boom
 - euphoria
 - profit taking panic
- Hyman Minsky



LET'S TALK ABOUT VOLATILITY (2/3)

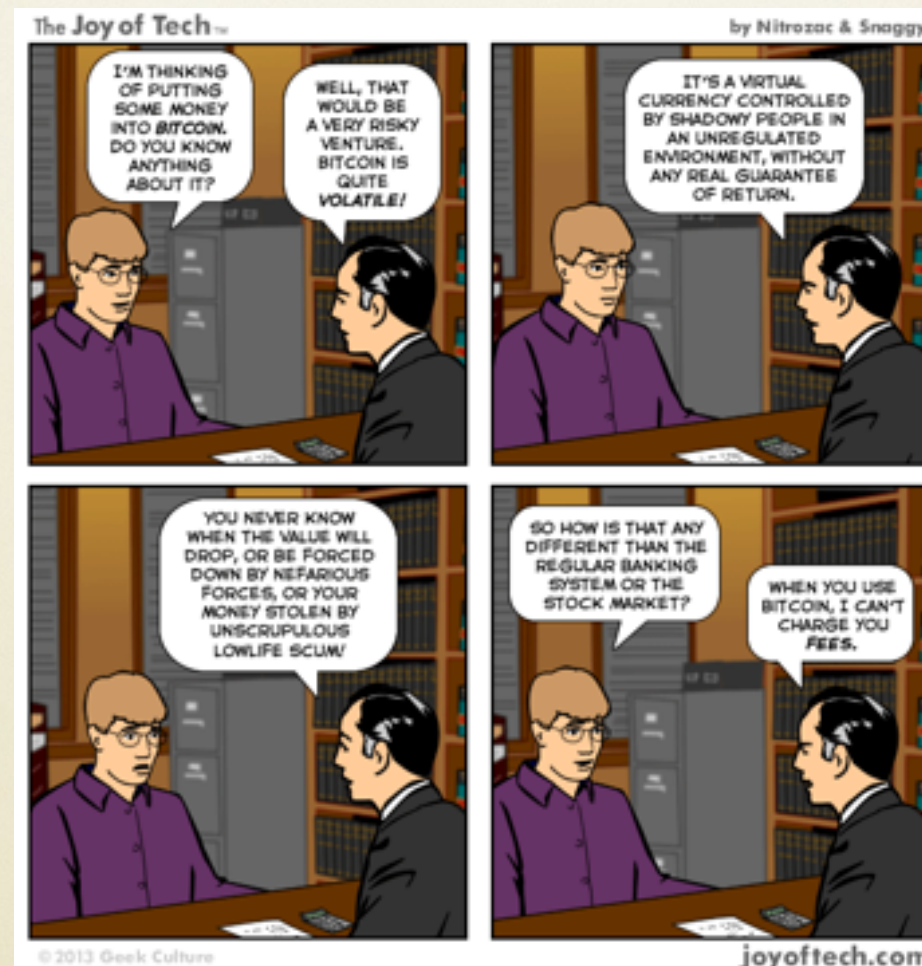
- how much of the volatility is being driven by superficial reasons?
 - media - what's China or Tesla up to?
 - curiosity - the Doge hype
 - “FUD” (fear, uncertainty, and doubt)
 - “FOMO (fear of missing out) has solidly trumped WTHIT (what the hell is this?)” - Paul Singer, Elliott Management
 - speculation - not driven by a true belief in cryptocurrency

LET'S TALK ABOUT VOLATILITY (3/3)

- what might be the non-superficial reasons?
 - scarcity and the maximum number - the supply is perfectly inelastic - a rise in demand cannot result in an increase in the supply or increase the speed of mining
 - the decentralized network - no central authority (bank or government) can step in to support or prop up markets and artificially subdue volatility
- are these potential areas of change to address volatility?
- “Bitcoin’s volatility is a trade-off for a distortion-free market” - Ria Bhutoria, former Director of Research for Fidelity Digital Assets

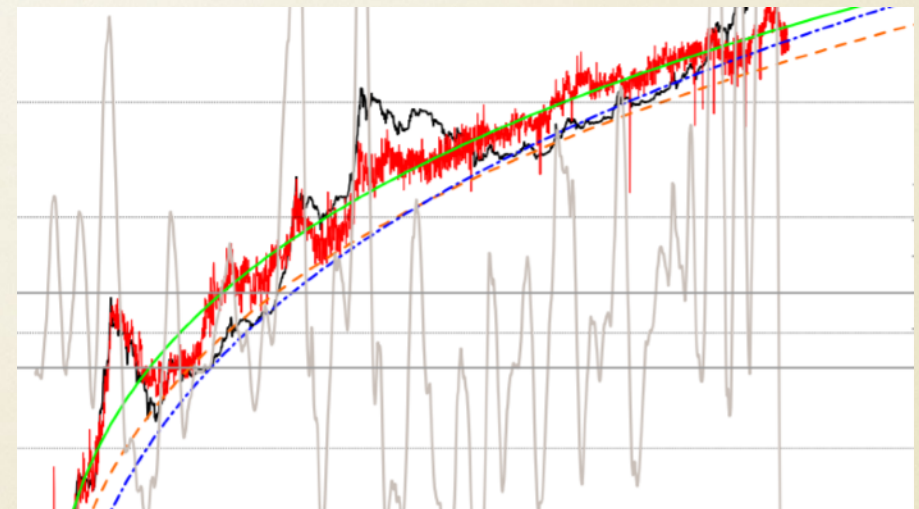
CRYPTOCURRENCY/BITCOIN VOLATILITY MODELS

- should be taken just about as seriously as stock market, bond, commodity, etc. models



METCALF'S LAW

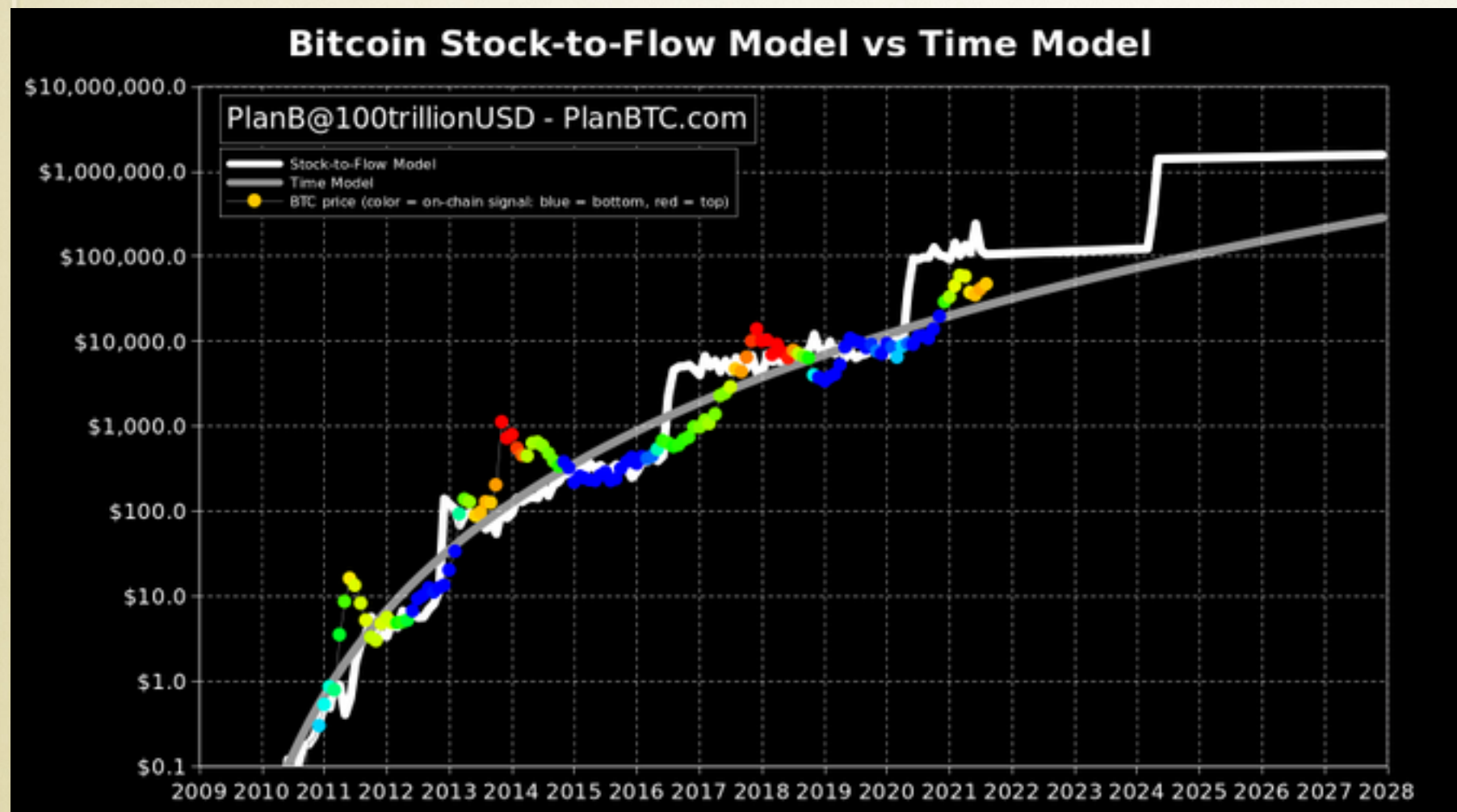
- value of a network is proportional to the square of its number of users
- key measure of cryptocurrency value is the network of people who use them and their connections
- may be used to predict/explain bubbles (ETH Zurich study)
- based on this, bitcoin is overvalued

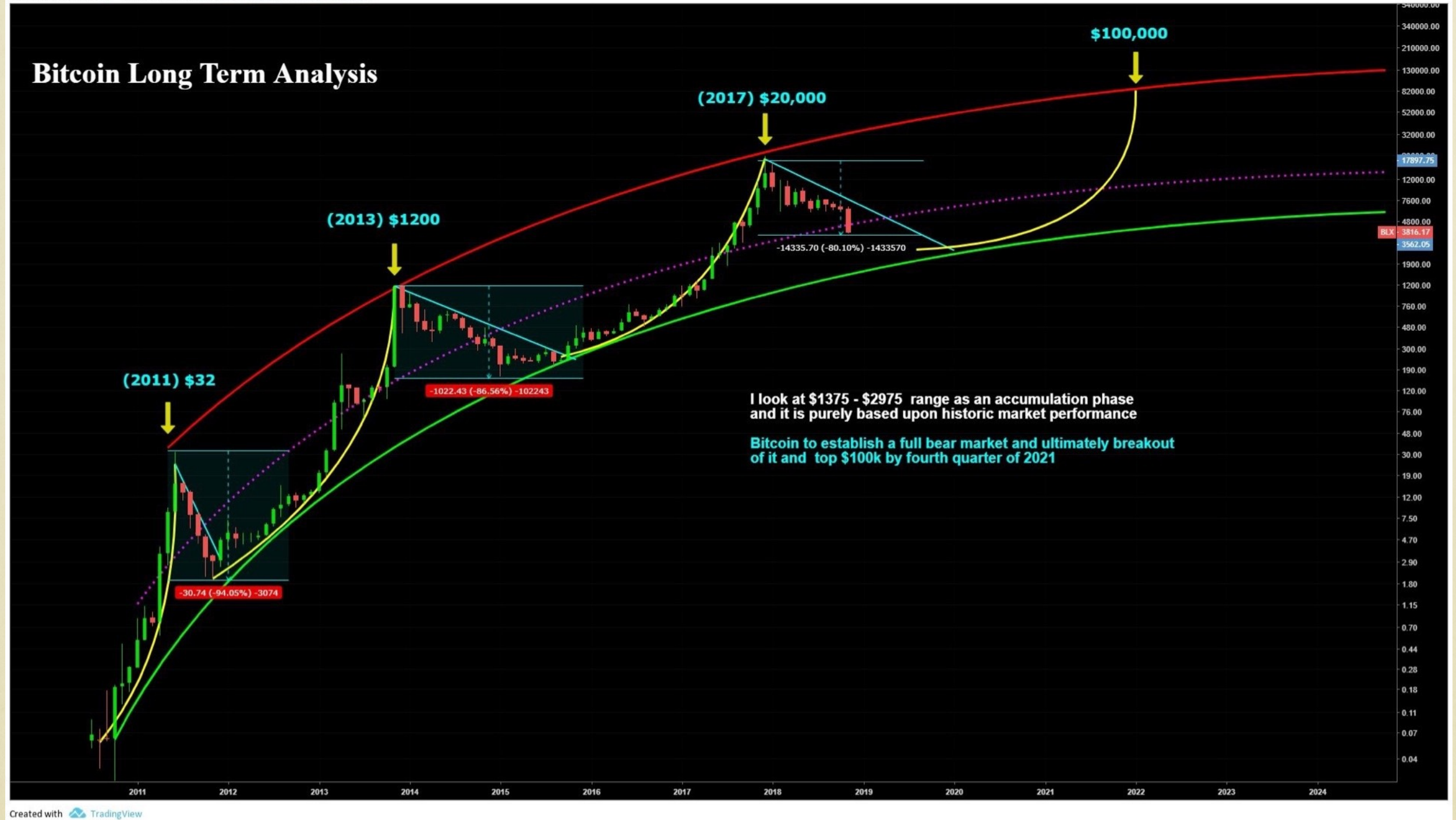


STOCK-TO-FLOW MODEL

Ratio of
stock/supply
and
flow/annual
production

Used for gold
and silver -
who knows if
it works for
bitcoin?





actually agrees with stock-to-flow model...

LET'S TALK ABOUT POW

- PoW was the first consensus algorithm and is in use by the vast majorities of cryptocurrencies
- however, PoW requires extensive computational resources which
 - results in non-sustainable resource and environmental impact
 - severely limits individual mining
 - leads to more BTC network control concentrated in mining pools
- numerous alternatives to PoW have been proposed

PROOF OF STAKE (PoS)

(1/3)

- instead of relying upon miners using terahashes, PoS networks assign voting privileges (on transaction verification) to cryptocurrency owners
- these owners have to “stake” their cryptocurrency holdings to vote on the legitimacy of new transactions
- transaction validators are assumed to be honest due to an active interest in keeping their holdings safe; attacks/corruptions would weaken their personal interests

PROOF OF STAKE (PoS)

(2/3)

- a PoS model would require a user to stake a minimum, non-trivial amount of cryptocurrency to become a validator; this amount is “locked up” and not available
- the user would be assigned blocks to validate periodically
- if a validator’s vote is deemed malicious by other validators, their stake is confiscated; honest validators receive rewards

PROOF OF STAKE (PoS)

(3/3)

- the cryptographic security of the blockchain is affected
- PoS brings down computational requirements - no puzzle solving
- PoS leads to faster block verification and greater throughput
- would the amount of the stake limit the pool of validators?



LET'S LOOK AT THE CURRENT CRYPTOCURRENCY LANDSCAPE (1/2)

- in general, there are four types of cryptocurrency
 - Bitcoin - the grandfather/grandmother of cryptocurrency
 - Altcoin(s) - alternatives to BTC
 - new ideas, new goals, new features - let's do what Satoshi didn't or couldn't
 - different ways of dealing with known BTC issues - PoW, volatility, transaction speed, etc.
 - can come from forks, ICOs (Initial Coin Offerings), etc.

LET'S LOOK AT THE CURRENT CRYPTOCURRENCY LANDSCAPE (2/2)

- Token(s) - crypto assets that are used on decentralized applications
 - usually built on alternative blockchains from altcoins
 - are typically bought and sold by traders
 - more later
- Stablecoin(s)
 - invented because coin exchanges need an easier and quicker way for customers to convert between BTC and USD
 - e.g., Facebook' Diem (originally called Libra) - backed by U.S. Treasury Bills or other dollar-dominated monetary instruments; Tether - originally backed by the dollar, but now??
 - more later

FORKS

- a fork creates a clone of the original software that can then be modified for some specific purpose without altering the original repository
- the Bitcoin Core repository can be forked to:
 - build purpose-specific bitcoin-compatible applications (e.g., a wallet)
 - build a new cryptocurrency that ceases to be compatible with the BTC network and creates a new cryptocurrency network

ALTCOINS

- generically refers to cryptocurrencies that are alternatives to BTC (i.e., “alternative coins”)
- they may be the result of new projects, forks, ICOs (Initial Coin Offerings), etc.
- many attempt to make advancements (e.g., mining PoW, throughput, maximum number of coin), add new features, etc.
- may be supported in wallets, coin exchanges and ATMs
- some convertible to BTC
- many are vanity, scam, etc. and useless

(remember not physical coins)



litecoin,
ripple
and ether
pose for a
family photo

cardano/ada



WHAT ABOUT DOGECOIN? - HYPE OR SERIOUS?

- introduced in 2013
- named for the Doge meme (that I don't really understand)
- the “fun and friendly internet currency”
- started with a supply limit, but was later removed
- uses a different technology in its PoW algorithm dissuading “traditional miners”
- in May 2021, SpaceX announced a rideshare mission to the moon completely funded by Dogecoin



DOGE



DogeCoin



Follow

17.53 k followers



+ Portfolio



Shop with crypto

Sponsored

eToro

You could do the work to be a pro...
or just copy one!

Use CopyTrader™
to automatically
copy the moves of
top-performing

▼
₮ 0.000000604
▲ 0.83%
Buy ▾
Trade ▾
Store ▾
Stake ▾
Bet ▾

Just now

Mkt. Cap. ⓘ

₮ 791.12 k

Vol. 24H

DOGE 293.34 M (₮ 1,783.58)

Open 24h

₮ 0.00000599

Low/High 24h

₮ 0.00000593 - ₮ 0.00000632

Weiss Rating ⓘ

C

OVERVIEW

ANALYSIS

MARKETS

CHARTS

TRADES

ORDERS

FORUM

NEWS

TIMELINE

INFLUENCE

CryptoCompare Index DogeCoin (DOGE) - BTC Historical Price

Line Chart

Logarithmic

Candle Stick

Advanced Chart



1 Hour

1 Day

1 Week

1 Month

3 Months

6 Months

1 Year

3 Years

5 Years

DETAILS

HISTORICAL PRICE

RATING

Max Supply ⓘ	Algorithm	Proof Type	Start Date	Twitter	Website
Not Applicable	Script	PoW	2013-12-06	@dogecoin	DogeCoin
DifficultyAdj.	Mkt. Cap. Penalty ⓘ	BlockNo.	Network H/s	Current Supply ⓘ	Block Reward
240 blocks	0 %	3,880,826.00	392,675,565,926,887.00	130,980,756,383.71	10,000.00

A Bitcoin clone that has reached success through clever marketing. Over the past year well over a hundred new cryptocurrencies have been created but not many have instantly carved out a niche. Dogecoin has sponsored multiple high profile events such as Nascar teams and the winter Olympics - even so, there are few locations to use the coin - and instead, it has become a de facto internet tipping currency. The coin has produced 100 billion units by the end of 2014 and is now producing roughly 5 billion units per year.

Blockchain data provided by: [Blockchair](#) (Main Source), [DogeChain](#) (Backup), and [WhatToMine](#) (Block Reward and Time only)

0.83%

BTC

3.38%

USDT

1.89%

ETH

3.30%

USD

3.01%

EUR

...

INITIAL COIN OFFERINGS (ICO)

- a type of funding based on cryptocurrency rather than shares (i.e., an IPO)
- the cryptocurrency version of Kickstarter or Indiegogo
- a quantity of unique altcoins are sold to speculators or investors in exchange for an established, usable currency
- purchasers have no stake other than these altcoins
- may get some utility of use, e.g., if for products, services, etc.
- the altcoins are promoted for their future value if/when the funding goals are met and the project successfully launches
- can be opportunities or can be scams (just like Kickstarter or Indigogo)

IPO VS. ICO

- buyers get stock, dividends, voting rights vs. buyers get tokens/altcoins with “right of revenue” and service share
- financial statements and performance vs. business plan/ “white paper” (e.g., goals, number of coins, etc.)
- stock offers through intermediaries vs. no intermediaries
- pre- and post-offering governance regulation vs. “smart contracts” (?) regulatory oversight
- etc., etc.








Token Sale Type: ICO

Jurisdiction ▾

Legal Form: -

Token type ▾

✕ Reset filters

#	Coin	Start price	End date ▾				Raised	Funding target	Funding cap	Coins offered
1	 GOPX Token GOPX (ICO)	\$ 1.000	635 DAYS	23 HOURS	23 MINUTES	11 SECONDS	-	-	-	10.00 B (100.00%)
2	 ThinkTank TANK (ICO)	\$ 0.1000	193 DAYS	23 HOURS	23 MINUTES	11 SECONDS	-	5,000,000 USD	9,000,000 USD	90.00 M (60.00%)
3	 Buildin Token BUILDIN (ICO)		120 DAYS	23 HOURS	23 MINUTES	11 SECONDS	-	2,000 ETH	50,000 ETH	50.00 M (50.00%)
4	 MintMe.com Coin MINTME (ICO)	\$ 0.01000	119 DAYS	23 HOURS	23 MINUTES	11 SECONDS	-	200,000 USD	3,000,000 USD	292.58 M (91.43%)
5	 Social Chains SONA (ICO)	\$ 1.000	58 DAYS	23 HOURS	23 MINUTES	11 SECONDS	-	10,000,000 USD	10,000,000 USD	100.00 M (10.00%)
6	 Caizcoin CAIZ (ICO)								JSD	850.00 M (85.00%)
7	 Miningwat MSC (ICO)								JSD	273.00 M (54.60%)

About ThinkTank

Cryptocurrency has become increasingly popular to individuals and businesses. The majority of individuals and corporations have adjusted well to the change of currency. On the other hand, some find themselves daunted by the expertise and budget required to invest. Some find themselves searching for predictions and accurate charts for their favorite asset, only to have to rummage through hundreds of ideas in order to find one decent idea. That's where we want to come in and help. It's a win-win for everyone. Top-level analysts will be rewarded for their contributions, and beginner investors will have reliable analytics to focus on. As the community grows, it will only become better. Bigger rewards and more and more top-notch analysts helping to support the community with their knowledge. Read on to find out how! Our team consists of talented programmers and investors with many years of experience, trading crypto in particular. We're very excited to start this project and help the crypto community abroad. We are consistently looking for talented employees to join and be a part of TANK token/coin.

THE MOST FAMOUS ICO

- announced by Vitalik Buterin during the North American Bitcoin Conference in Miami in January 2014
- proposal was for an open-source, public, blockchain-based, distributed computing platform and operating system
- ICO opened on 20 July and closed on 2 September after raising US\$18.4 million in bitcoin
- would you have invested in this?

ethereum
ETHERBROWSER
PEER-TO-PEER MESSAGING
GENERALIZED BLOCKCHAIN
PROGRAM ANYTHING



He is 19 years old

ETHEREUM (1/2)



- originally proposed in 2013 by Buterin when he was 19 years old; its initial release was in 2015
- Ethereum is the ledger, ether is the cryptocurrency
- no maximum number of ether in circulation
- mining process is based upon PoW but will be changing to PoS
- supported now in most (all) wallets and on most (all) coin exchanges
- the ICO was probably a huge success since it thought way beyond the scope of BTC



Ethereum White Paper

A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM

By Vitalik Buterin

When Satoshi Nakamoto first set the Bitcoin blockchain into motion in January 2009, he was simultaneously introducing two radical and untested concepts. The first is the "bitcoin", a decentralized peer-to-peer online currency that maintains a value without any backing, intrinsic value or central issuer. So far, the "bitcoin" as a currency unit has taken up the bulk of the public attention, both in terms of the political aspects of a currency without a central bank and its extreme upward and downward volatility in price. However, there is also another, equally important, part to Satoshi's grand experiment: the concept of a proof of work-based blockchain to allow for public agreement on the order of transactions. Bitcoin as an application can be described as a first-to-file system: if one entity has 50 BTC, and simultaneously sends the same 50 BTC to A and to B, only the transaction that gets confirmed first will process. There is no intrinsic way of determining from two transactions which came earlier, and for decades this stymied the development of decentralized digital currency. Satoshi's blockchain was the first credible decentralized solution. And now, attention is rapidly starting to shift toward this second part of Bitcoin's technology, and how the blockchain concept can be



2nd most important paper in cryptocurrency history after Satoshi's?

“Let's make the blockchain programmable - ‘a world computer’”

ETHEREUM NEWS

Vitalik Buterin Compares Bitcoin and Ethereum: BTC is Like a Calculator, ETH is Like a Smartphone



By Jose Antonio Lanz - March 2, 2019

ETHEREUM (2/2)



- immediate differences from BTC
 - block time is 14-15 seconds rather than 10 minutes
 - mining generates Ether new coins at a usually consistent rate
 - different algorithms for PoW and transaction fees
- <https://www.ethereum.org>
- blockchain entries are not simply cryptocurrency transactions! - this is a big deal!

CONSIDER

- the BTC blockchain records financial transactions between 2 parties
- since a financial transaction is a contract, suppose this idea could be extended to any type of contract between parties?
- such contracts are a different type of value
- contracts on a blockchain would possess all the advantages defined for blockchain technology - immutability, non-repudiation, tamper-proof, searchable, distributed, etc.
- if such contracts were programmable, they could be smart contracts
- how might this work?



HOW SMART CONTRACTS WORK (1/3)

- a transaction in a block consists of a contract written in a unique programming language - this is hard
- this contract runs/executes in a contained Turing complete virtual machine, i.e., a small standalone computer - not physical, but in software; embedded scripts in Web pages work like this
- therefore the blockchain becomes a network of computers - that's why Ethereum was defined as a computing platform and operating system
- these “computers” could communicate with other “computers” in other blocks (but not change anything)

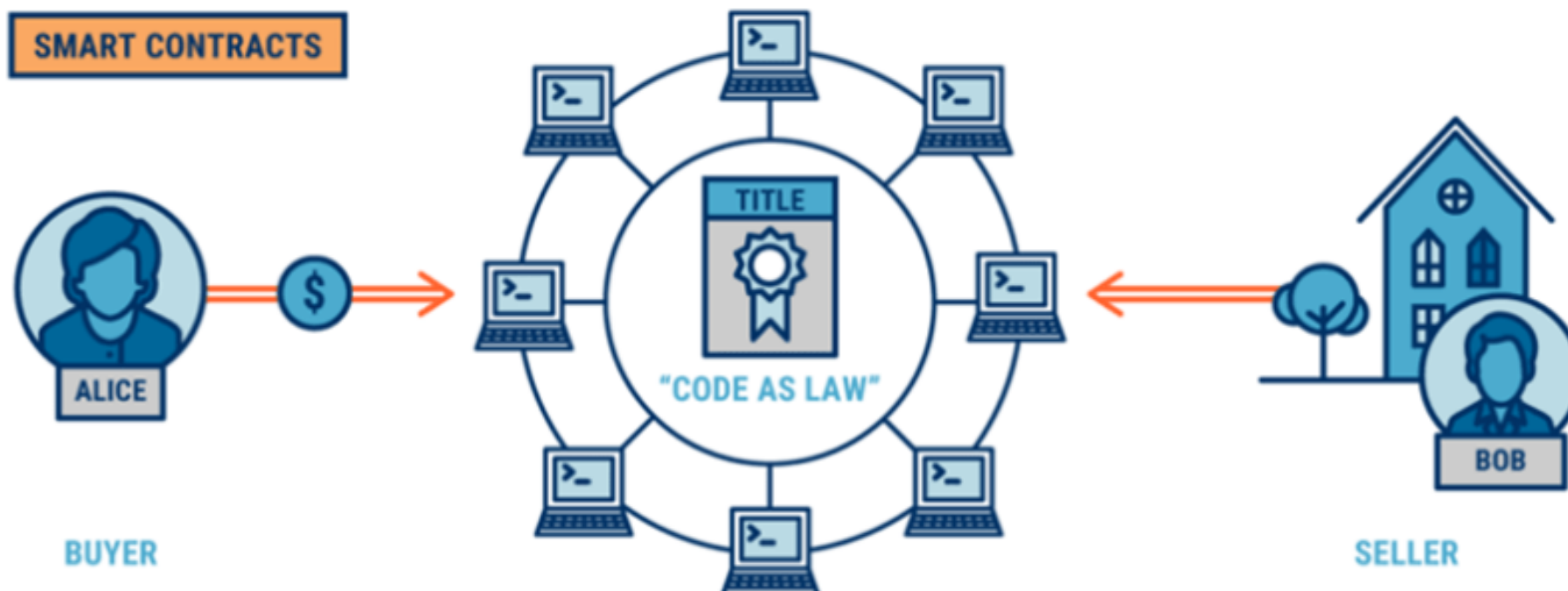


Buying a house on Ethereum

NOW

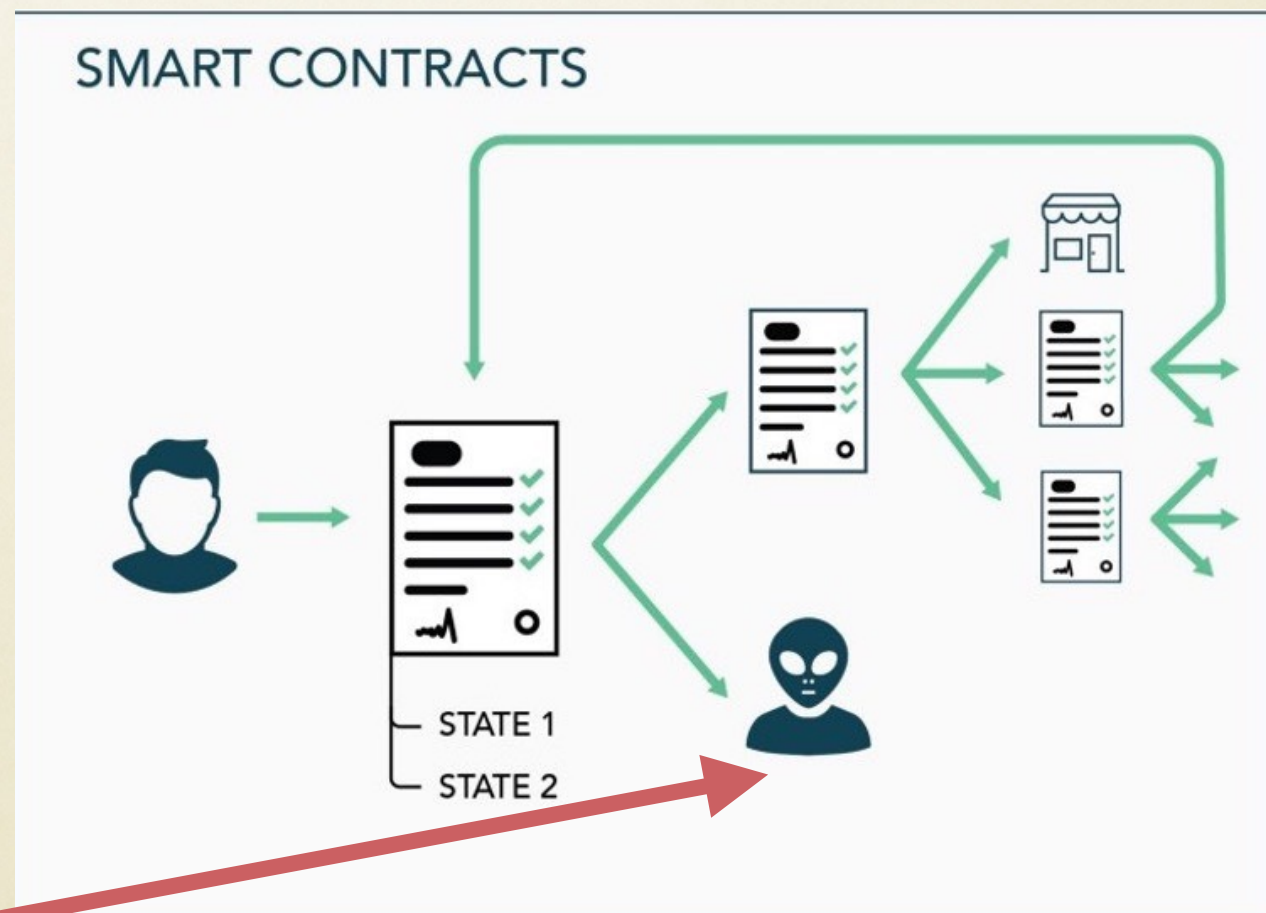


SMART CONTRACTS



HOW SMART CONTRACTS WORK (2/3)

- a smart contract is sometimes called a **DApp** (decentralized application)
- in general, a program running on a decentralized P2P network



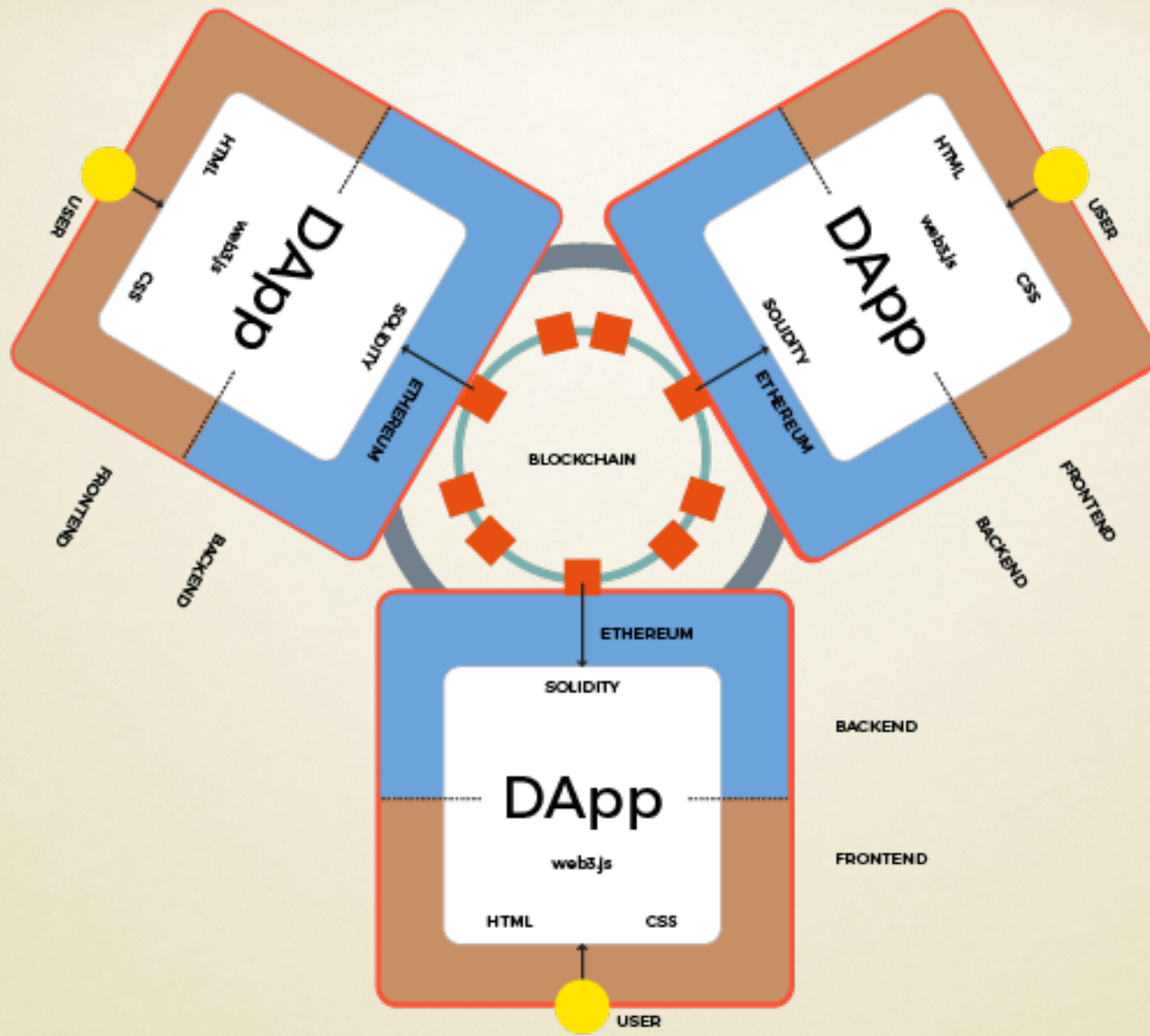
that adversaries
might want to disrupt

HOW SMART CONTRACTS WORK (3/3)

- Turing complete means that these virtual computers can do input, output, processing and communication
- the contracts can do such things as
 - enforce deadlines
 - make payments
 - check security policies
 - maintain records
 - etc., etc. - all under the protection of blockchain primitives
- but being computers and software, they can also have bugs or be vulnerable

ETHEREUM GAS

- gas refers to the cost necessary to perform a transaction/contract
- miners set the price of gas based upon supply and demand for the computational power of the network for processing
- by design the value of gas is distinct from the value of ether (value layer vs. processing layer)
- for example, a contract execution may be worth 50 ETH and the gas price for processing at that particular time is 1/100,000 ETH



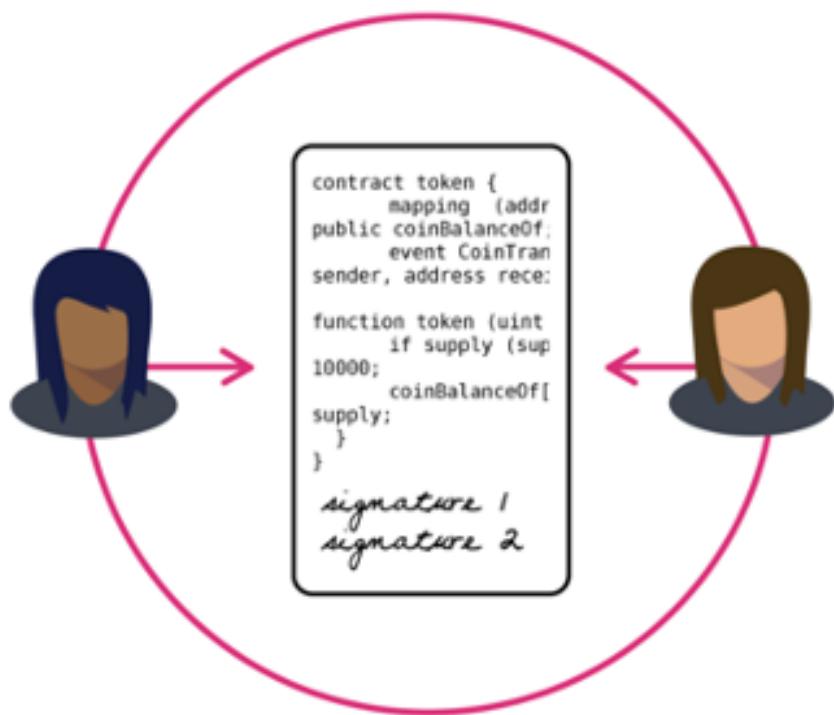
TOKENS

- crypto assets that are used on decentralized applications
- usually built on alternative blockchains from altcoins
- Initial Token Offering (ITOs) - similar in concept to ICOs
- tokens have proven (or unproven) intrinsic utility, e.g., granting investors access to a platform through a subscription, with token holders unlocking the right to use exclusive services with a system, etc.
- tokens are essentially smart contracts that can be bought and sold
- more about tokens later - especially non-fungible tokens (NFTs)

ETHEREUM AND ERC-20

- ERC-20 is a technical standard for tokens/smart contracts on the Ethereum blockchain
- ERC-20 tokens are blockchain based assets that have value and can be sent and received; i.e., they are (like) cryptocurrency
- the big difference is that instead of running on their own blockchain, they are issued on the Ethereum network
- not all wallets support all tokens
- examples include Tron, Bytom, Vechain, Ox, Omisego, Augur, etc.

How to create your own token/ cryptocurrency

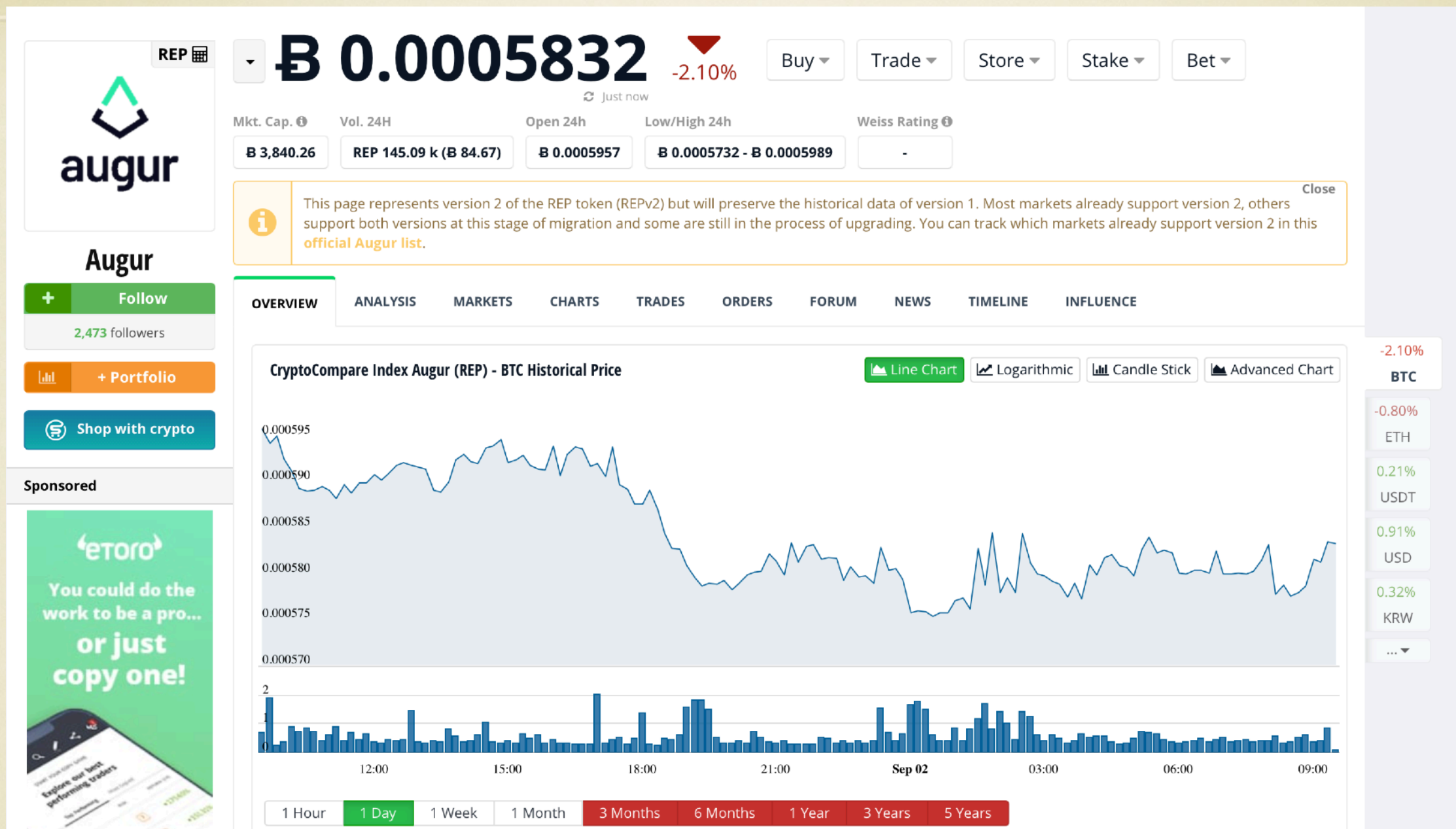


```
contract ClamperCoinTest is StandardToken { // CHANGE THIS. Update the contract name.

    /* Public variables of the token */

    /*
    NOTE:
    The following variables are OPTIONAL vanities. One does not have to include them.
    They allow one to customise the token contract & in no way influences the core functionality.
    Some wallets/interfaces might not even bother to look at this information.
    */
    string public name;                // Token Name
    uint8 public decimals;              // How many decimals to show. To be standard complicant keep it 18
    string public symbol;               // An identifier: eg SBX, XPR etc..
    string public version = 'H1.0';
    uint256 public unitsOneEthCanBuy;   // How many units of your coin can be bought by 1 ETH?
    uint256 public totalEthInWei;      // WEI is the smallest unit of ETH (the equivalent of cent in USD or satoshi in BTC).
    address public fundsWallet;        // Where should the raised ETH go?

    // This is a constructor function
    // which means the following function name has to match the contract name declared above
    function ClamperCoinTest() {
        balances[msg.sender] = 1000000000000000000000000; // Give the creator all initial tokens. This is set to 1000
        totalSupply = 1000000000000000000000000; // Update total supply (1000 for example) (CHANGE THIS)
        name = "ClamperCoinTest"; // Set the name for display purposes (CHANGE THIS)
        decimals = 18; // Amount of decimals for display purposes (CHANGE THIS)
        symbol = "ECV"; // Set the symbol for display purposes (CHANGE THIS)
        unitsOneEthCanBuy = 10; // Set the price of your token for the ICO (CHANGE THIS)
        fundsWallet = msg.sender; // The owner of the contract gets ETH
    }
}
```

Prediction markets are widely considered the best forecasting tool. Augur is an open, global platform where anyone anywhere can create, monitor or trade in prediction markets about any topic. Think of it as an "Early Warning System" with the most accurate event forecasts, a potential "Google Search", "Bloomberg Terminal" or "Reuters Terminal" for crowdsourced event forecasts.

STABLECOIN

- the name implies stability - against what? volatility? fear?
- to provide some of the advantages of both fiat currencies (or stable commodities?) and the cryptocurrency worlds
- used mostly as a hedge against volatility of cryptocurrencies
- can also be used as a stable currency that provides increased transparency and decentralization
- may provide faster transaction times and lower fees in some fiat-based activities



A new stablecoin, issued in partnership with Binance

Get BUSD

"Paxos is leading the digital trusts space and we are excited to work with them in developing our native stablecoin."

~CZ, Binance CEO

How to Use BUSD



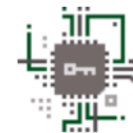
Buy/Sell Direct

Get BUSD 1:1 for U.S. dollars or PAX on the Paxos platform



Trade

Use BUSD to trade crypto on Binance



Hold

Hedge against the volatility of your crypto-assets by holding in BUSD, as stable as the dollar



Transact

Use BUSD wherever ERC-20 tokens are accepted for commerce, loans, payments, etc.

THE REAL COST OF PETRO



100 MILLION PETROS = \$6 BILLION

AT CURRENT VALUE OF \$59.07 PER BARREL



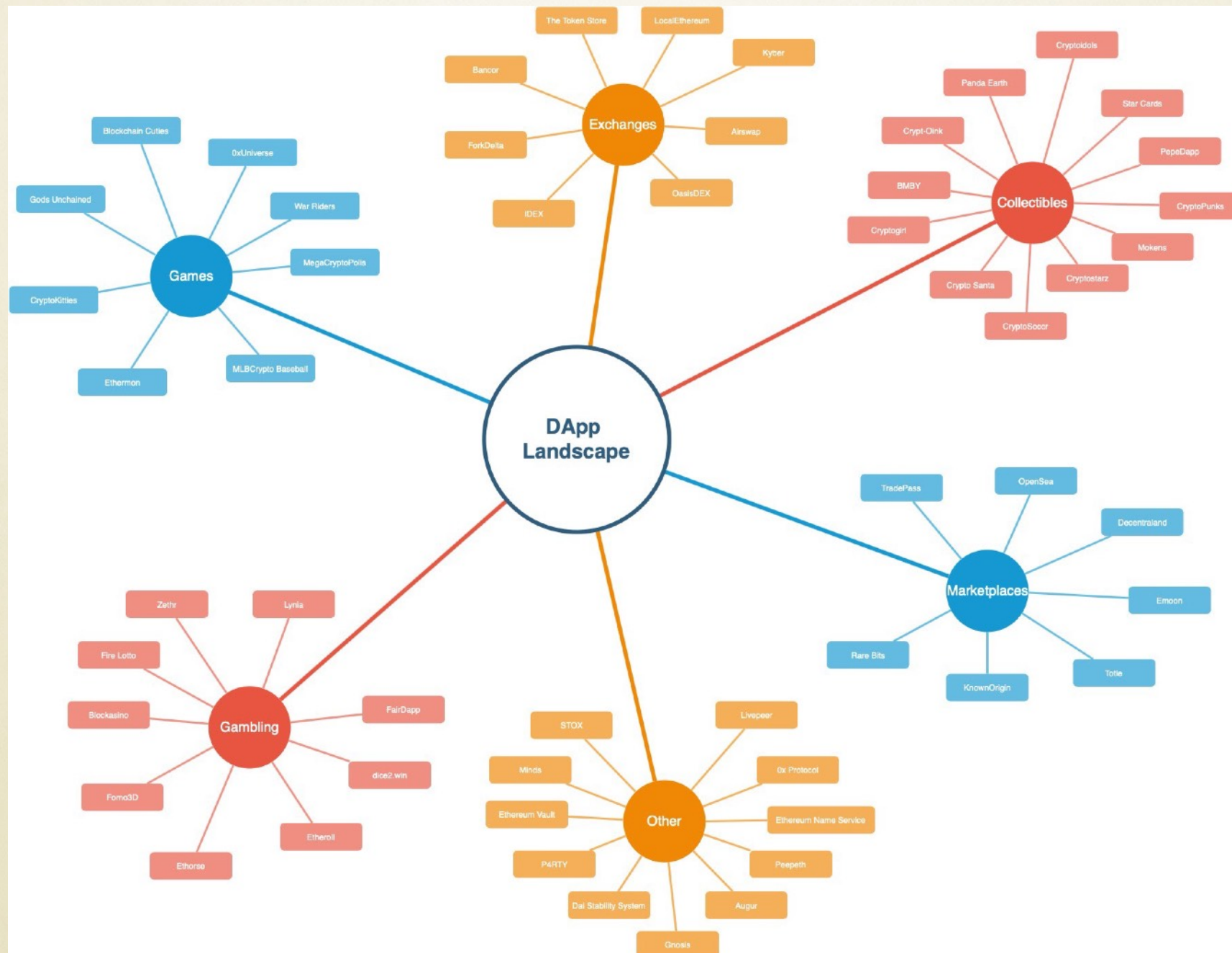
a commodity-based
stablecoin that
became the national
cryptocurrency of
Venezuela in 2018

U.S. citizens are not
supposed to own Petro



Are these stablecoin?

WE NEED TO GO BACK TO DAPPS



DECENTRALIZED APPLICATIONS (DAPPS)

- smart contracts + cryptocurrency + a blockchain + an application
- functions similar to traditional apps but differ in how they incentivize users and store data
- unlike traditional applications, DApps are also controlled by and funded by their users like Ethereum and Bitcoin
- significant because the infrastructure behind the application is on a blockchain meaning that it is public for all users to see

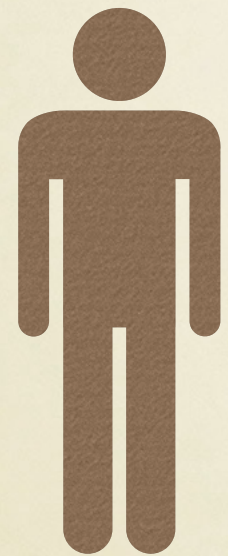
THE SAD STORY OF DAO



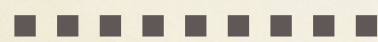
- Decentralized Autonomous Organization
- an investor-directed venture capital fund
- based on the Ethereum blockchain
- no management structure, no board of directors, not tied to any nation
- largest crowdfunding campaign (ICO) in history (May 2016) - raised US\$168 million in ether

- DAO was hit by a smart contract attack attacked in July 2016 when a software bug was identified
- DAO held 15% of all ether in circulation at the time
- hackers stole US\$50 million (3.6 million ether at the time)
- when smart contracts go live, it is impossible(?) to change them (nature of the blockchain)
- controversial solution was a hard fork of Ethereum to Ethereum and Ethereum Classic
- delisted from all major cryptocurrency exchanges by September 2016 - tokens became worthless

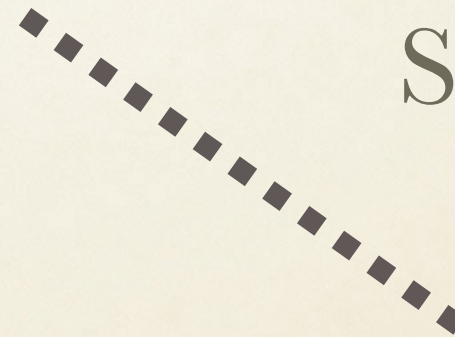
TRADITIONAL(?) APPLICATION, E.G. FACEBOOK



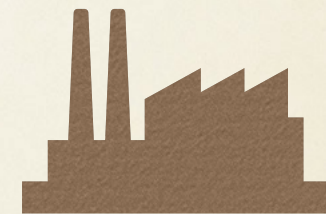
Nick



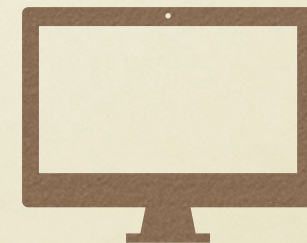
Internet



Facebook

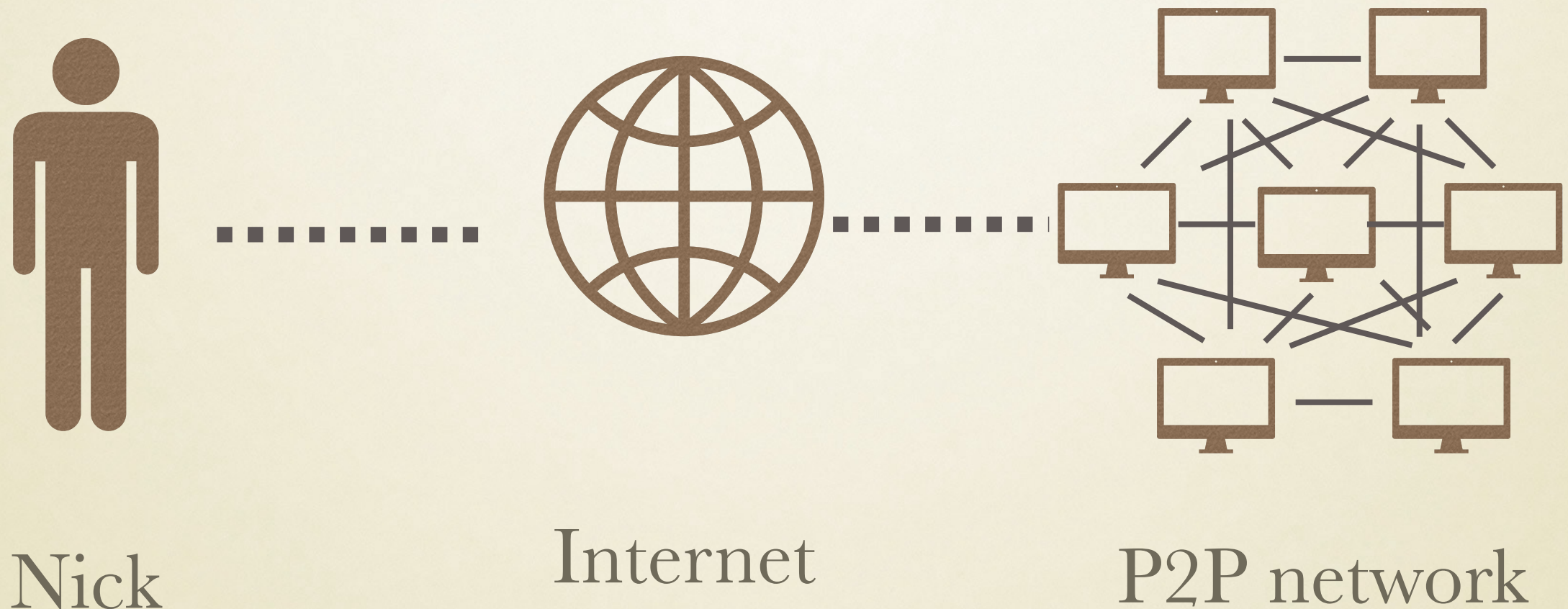


Server farms



Facebook is the provider/owner/developer
of the application

DECENTRALIZED APPLICATION (DAPP)



application runs on equivalent nodes each
controlled by a different entity



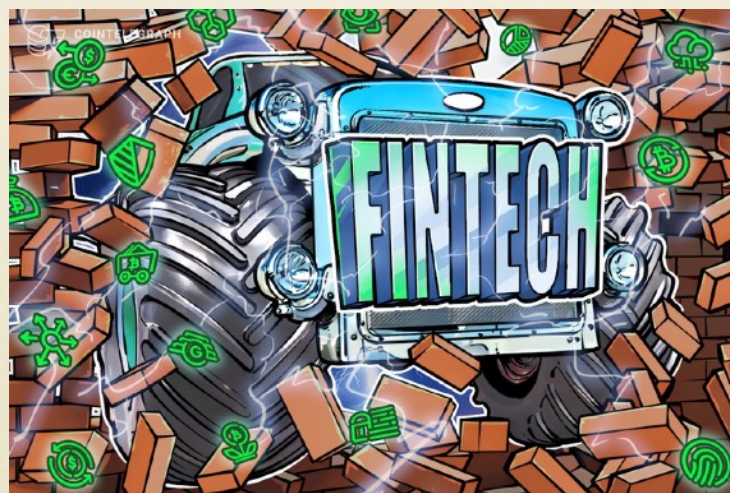
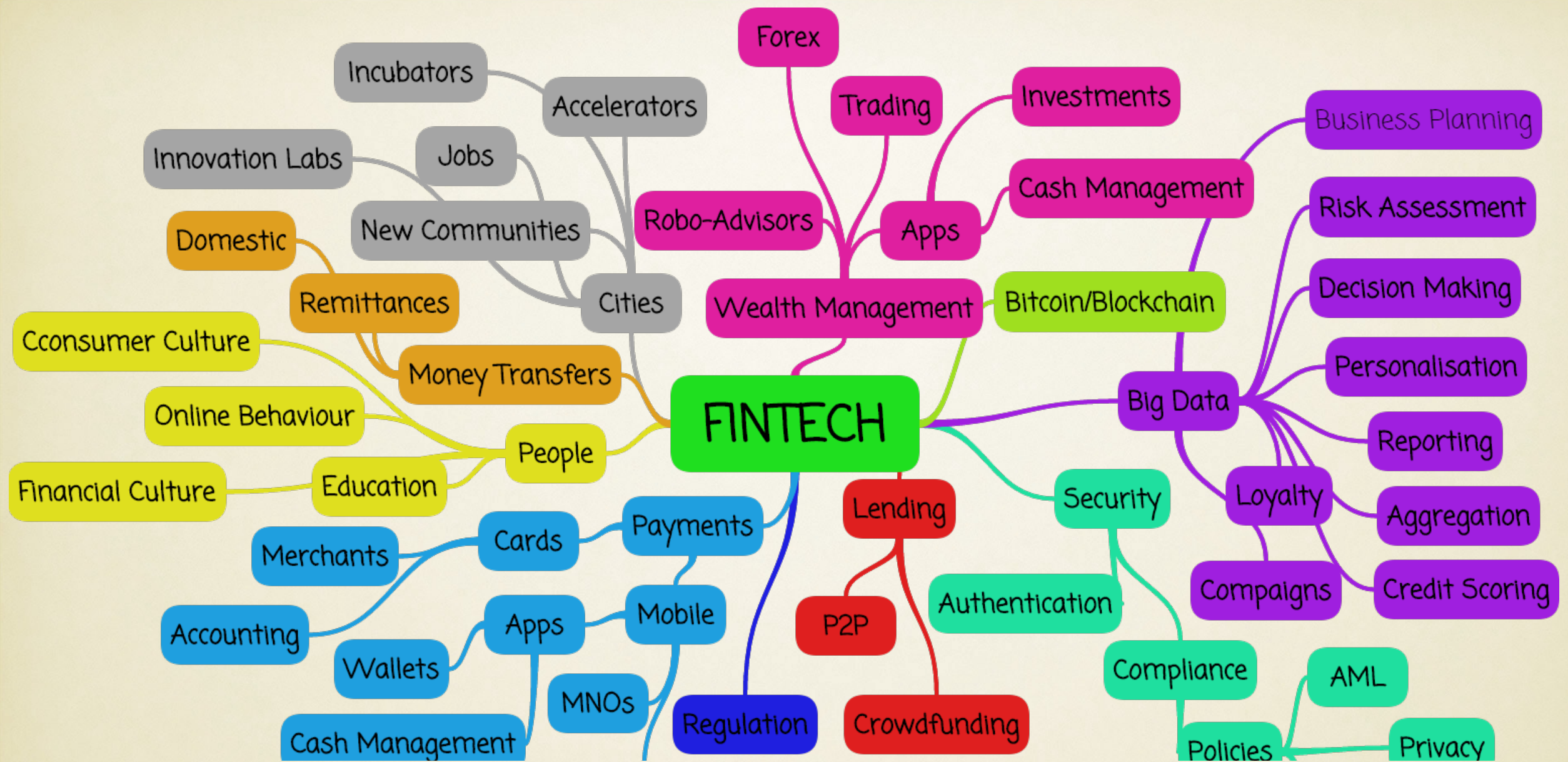
Powering Communities and Opportunities

Steem is a social blockchain that grows communities and makes immediate revenue streams possible for users by rewarding them for sharing content. It's currently the only blockchain that can power real applications via social apps like Steemit.

[Create an account](#)

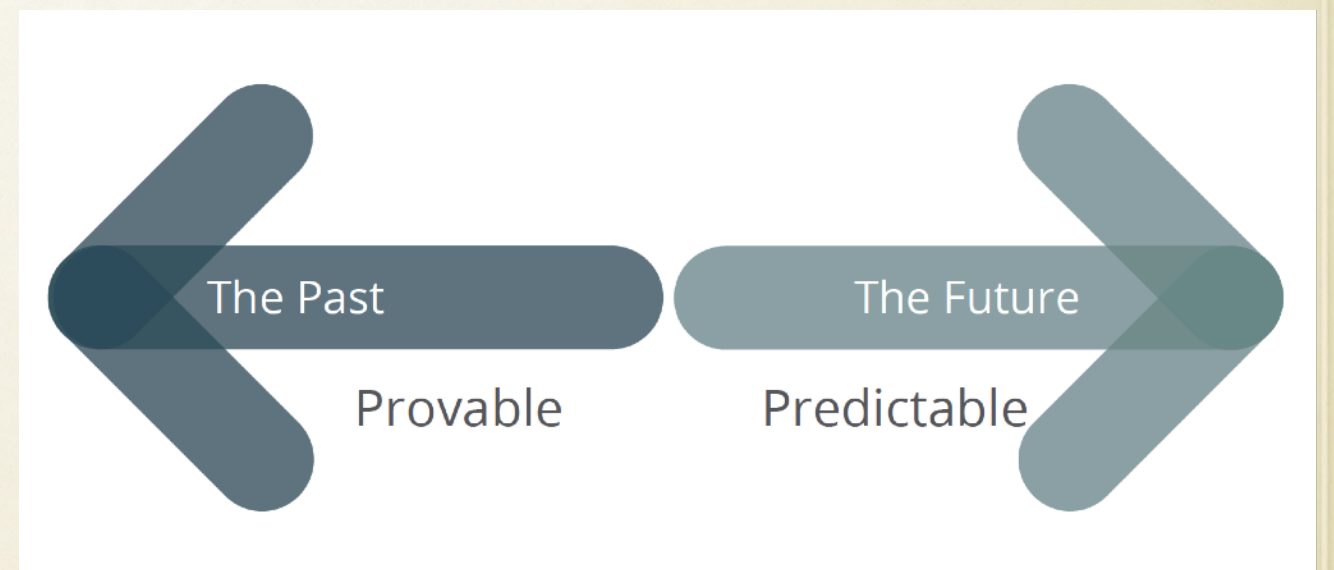
Facebook on the blockchain?

- runs on a dedicated blockchain
- native cryptocurrency (STEEM)
- pays users for posts and interaction
- your data is always encrypted and you're paid for it



CRYPTOECONOMICS

- “past is provable, future is predictable”
- uses cryptography to prove actions occurring in the past
- predicts that economics can ensure that actions occur in the future



CRYPTOECONOMICS - WHY DOES IT WORK?

- works because people trust math and people like money
- establishes trust, even between pseudonymous parties
- makes trust in a person or third party optional (disintermediation)
- reduces the cost of an intermediary to only the actual transaction cost



“A compelling FinTech example is the potential for Blockchain technology to replace legacy post-trade processes that currently require trusted third parties such as clearinghouses and depositories to manage and administer the clearing, settlement, and custody associated with trades and payments.”

-Dhar & Stein, CACM, 10/2017

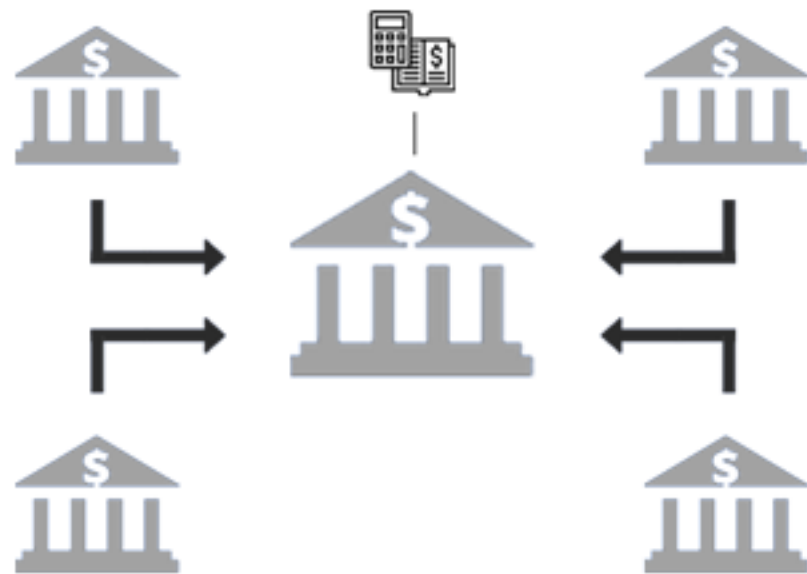
DECENTRALIZED FINANCE (DEFI) (1/2)

- blockchain-based finance that does not rely on central financial intermediaries such as brokerages, exchanges or banks to offer traditional financial instruments
- uses smart contracts on blockchains
- allows customers to lend or borrow funds from others, speculate on price movements on a range of assets using derivatives, trade cryptocurrencies, insure against risks and earn interest in savings-like accounts

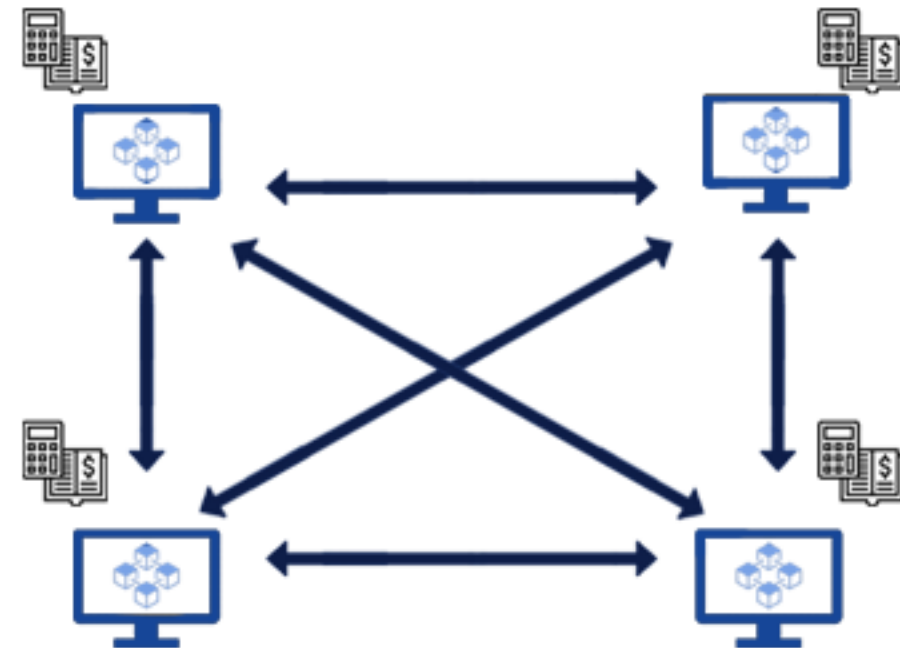
DECENTRALIZED FINANCE (DEFI) (2/2)

- customers maintain control over their private keys
(a non-custodial wallet)
- transactions are searchable on the blockchain

TRADITIONAL FINANCIAL SYSTEM



DECENTRALIZED FINANCIAL SYSTEM




Typical DApp configuration

The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System

Abstract

The Maker Protocol, also known as the Multi-Collateral Dai (MCD) system, allows users to generate Dai by leveraging collateral assets approved by “Maker Governance.” Maker Governance is the community organized and operated process of managing the various aspects of the Maker Protocol. Dai is a decentralized, unbiased, collateral-backed cryptocurrency soft-pegged to the US Dollar. Resistant to hyperinflation due to its low volatility, Dai offers economic freedom and opportunity to anyone, anywhere.

DAI



Dai

+Follow

164 followers

+Portfolio

Shop with crypto

Sponsored

etoro

You could do the work to be a pro... or just copy one!

₹ 1.000

0.00%

1 min ago

BuyTradeStoreStakeBet

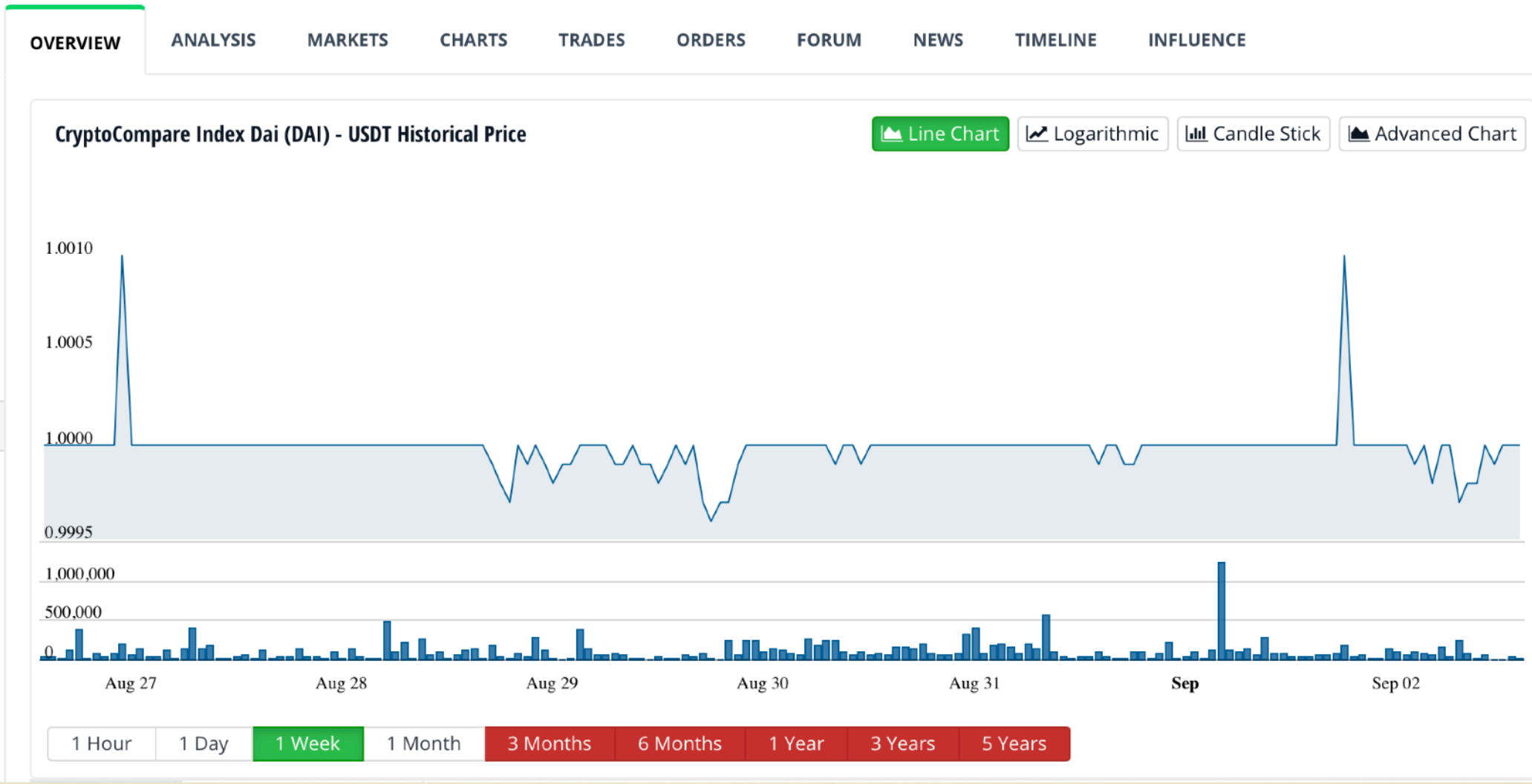
Mkt. Cap.₹ 6.06 B

Vol. 24HDAI 1.77 M (₹ 1.77 M)

Open 24h₹ 1.000

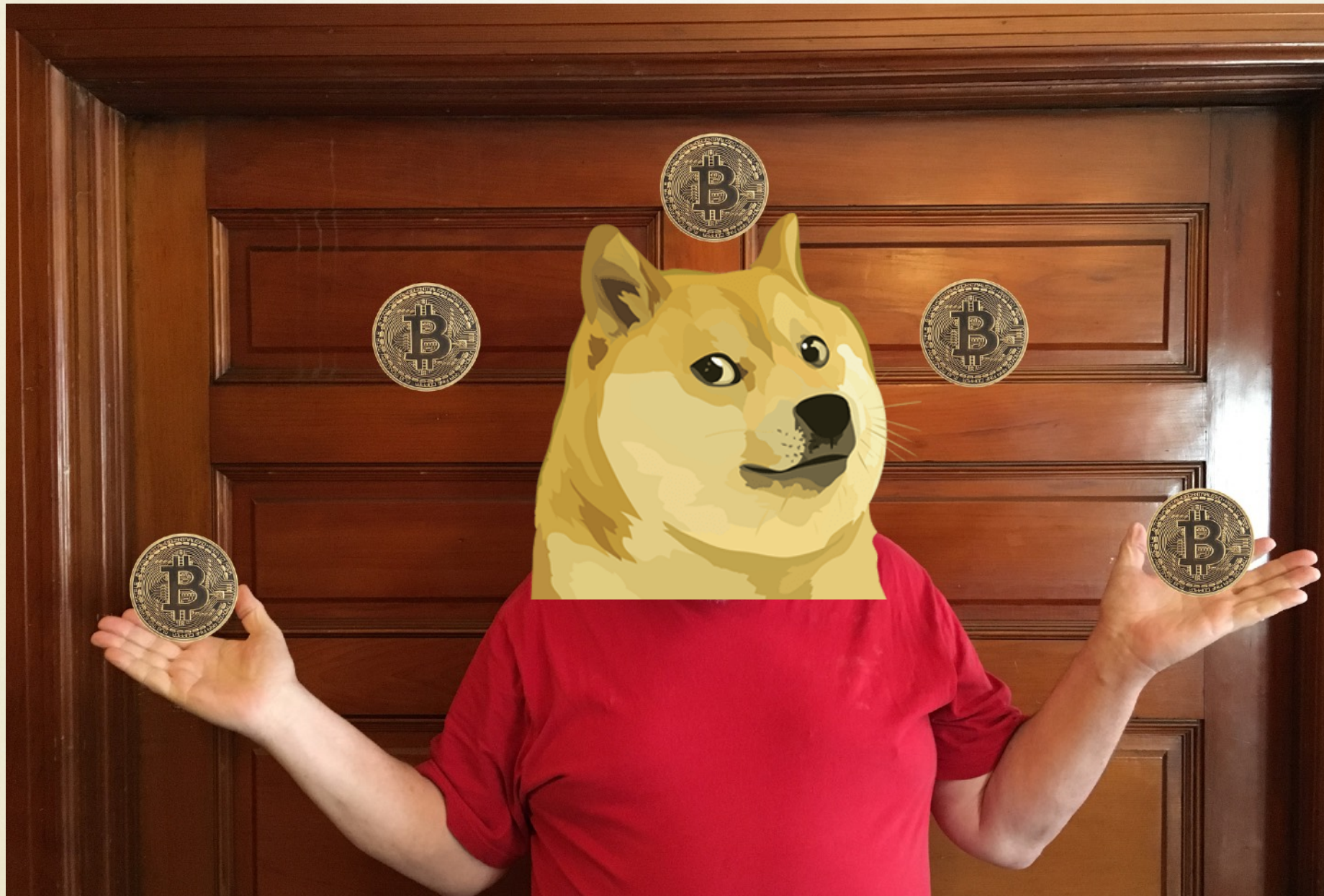
Low/High 24h₹ 0.9946 - ₹ 1.001

Weiss Rating-



- 0.00%USDT
- 0.10%USD
- 1.58%ETH
- 1.79%BTC
- 0.00%USDC
- ...





Questions? Comments?
bebo.white@gmail.com