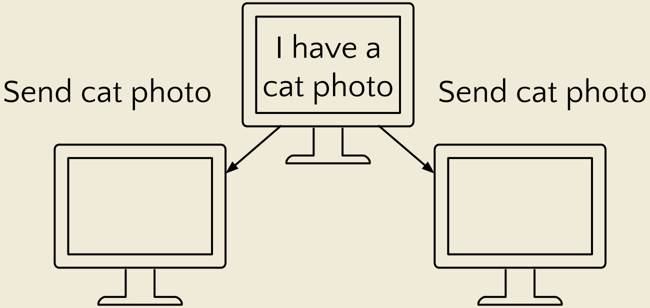
Intro to Blockchain & Defi

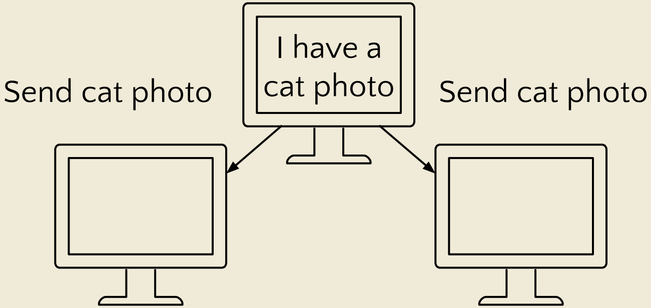
<LEARN/> ALL JUNE . <HACK/> JULY-MID AUGUST . <CELEBRATE/> REST OF AUGUST

A Computer Network

- Computers are really good at sharing information.
  - Text, pictures, videos, websites, etc.
- Can be connected via hardlines, wireless connections, etc.
- You can share the same thing to different people.



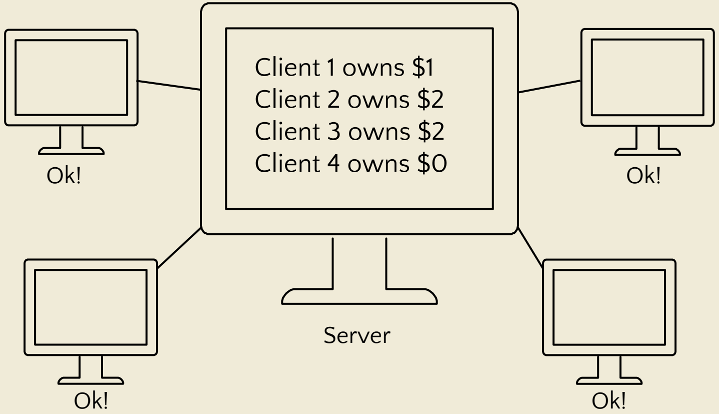
A Computer Network



- Not as good for assets
  - ownership, transactions, money, copyright, licenses
- People can send the same asset to different people.
  - Known as the **“double-spend”** problem
- Can you make it so that you can send something to someone and then **not be able to send it to anyone else?**

The solution until now

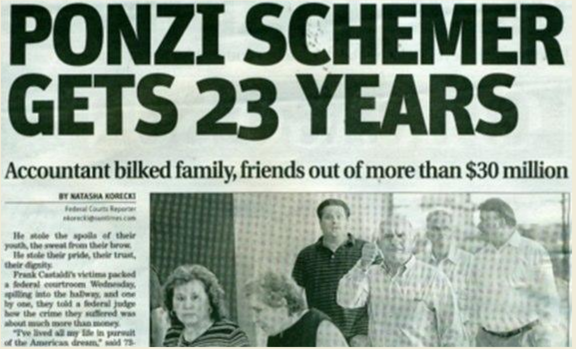
- **Centralized network.** A center server stores the data and keeps track of who owns what.
- Everyone requests the server to update the data.
  - Ex: I want to send $1 to you.
- The server makes sure no one **double-spends**.



Client 1 owns $1
Client 2 owns $2
Client 3 owns $2
Client 4 owns $0

What could go wrong?

- Central point of failure
- High service fees
- Freezing of assets
- Corruption & fraud (illegal, but only if caught)
- Privacy breaches and data hacks



PONZI SCHEMER GETS 23 YEARS

Accountant bilked family, friends out of more than $30 million

BY NATASHA KORECKI

Federal Courts Reporter

nkorecki@suntimes.com

He stole the spoils of their youth, the sweat from their brow.

He stole their pride, their trust, their dignity.

Frank Castaldi's victims packed a federal courtroom Wednesday, spilling into the hallway, and one by one, they told a federal judge how the crime they suffered was about much more than money.

"I've lived all my life in pursuit of the American dream," said 73-

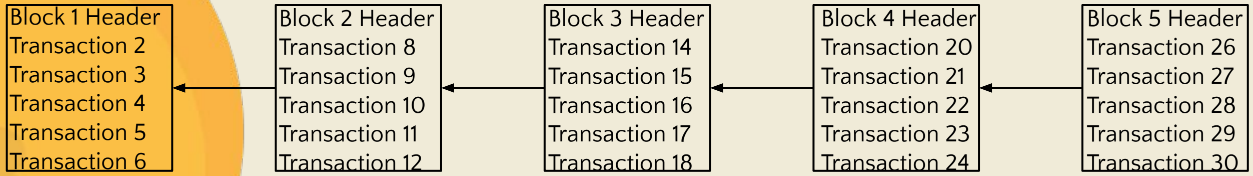
Can we do better?

- Can we replace centralized authorities?
- Can we trust each other to agree on who owns what?
- Can we replace legal protection of our assets with technological protection?

YES!

What is a blockchain?

- The “blocks” - List of records stored in “blocks” of data
  - Each block also contains a header.
- The “chain” - Each block points to the previous block, forming a chain of blocks.
  - If you modify a block, the chain is broken.



Block 1 Header
Transaction 2
Transaction 3
Transaction 4
Transaction 5
Transaction 6

Block 2 Header
Transaction 8
Transaction 9
Transaction 10
Transaction 11
Transaction 12

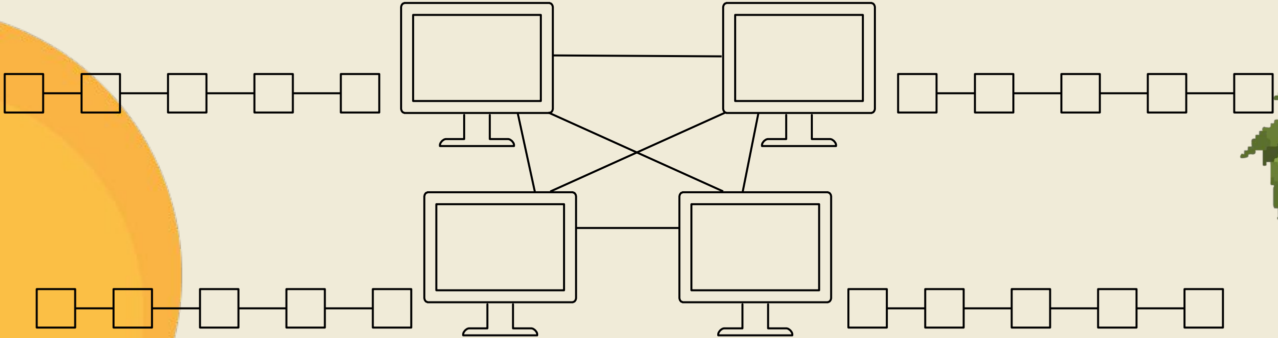
Block 3 Header
Transaction 14
Transaction 15
Transaction 16
Transaction 17
Transaction 18

Block 4 Header
Transaction 20
Transaction 21
Transaction 22
Transaction 23
Transaction 24

Block 5 Header
Transaction 26
Transaction 27
Transaction 28
Transaction 29
Transaction 30

A Blockchain Network

- **Transparent.** Each node in the network has a copy of the blockchain.
- **Secure.** Uses cryptography and digital signatures to prove identity and enforce read/write access.
- **Immutable.** Contains consensus mechanisms that make it hard to change records

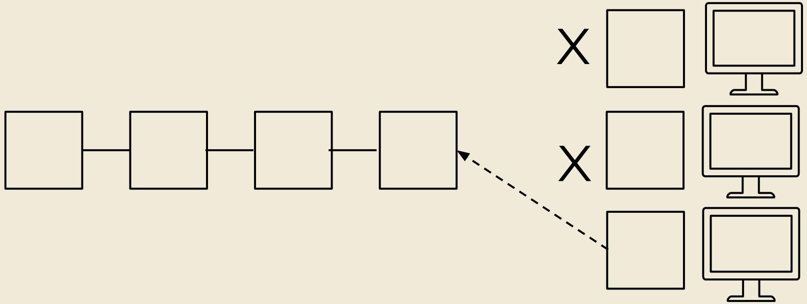


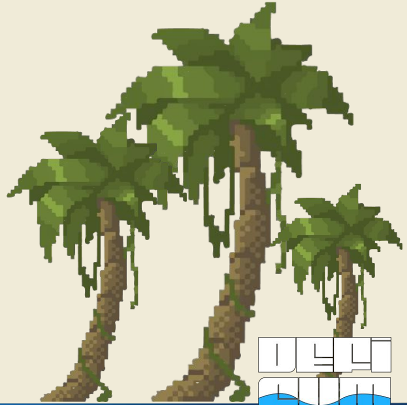
Cryptography & Public/Private Keys

- Blockchain uses asymmetric cryptography
    - A private key (known only to the owner) can generate a public key.
    - The public key (how everyone identifies the owner) cannot reveal the private key
- In Bitcoin, there are 1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,97 addresses
- Practically impossible for anyone to overlap when randomly generating public keys.
    - Every person in the world (7.4 billion) could have 196,385,600,286,334,710,857,791,565,804,391,698,421 addresses.

Reaching Consensus Through Mining

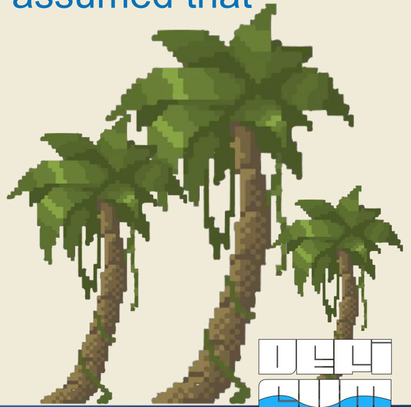
- Each node gets a copy of the blockchain.
- Each node sends their transactions to as many other nodes around them as they can.
- Each mining round, nodes compete in some way (solving a puzzle, random selection, etc).
- The “winner” adds their block to the blockchain, and usually receives a reward.
- The next round begins.





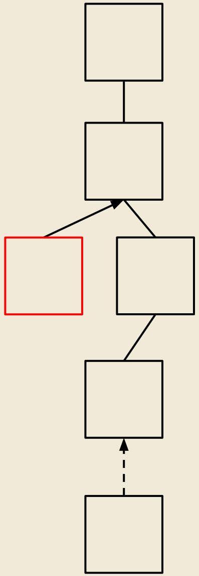
Proof of ___

- Blockchain does not restrict who can mine a block. Instead, blockchain makes it costly for nodes to lie by requiring them to present a proof.
- In Bitcoin, this is a **“proof of work”.**
  - A proof of work is the solution to a cryptographic puzzle that is difficult to produce but easy to check for correctness once you have it.
  - If you find the correct “proof” for a mining round, it can be reasonably assumed that you had to do work (i.e. expending electricity) to find it.



What Proofs Achieve

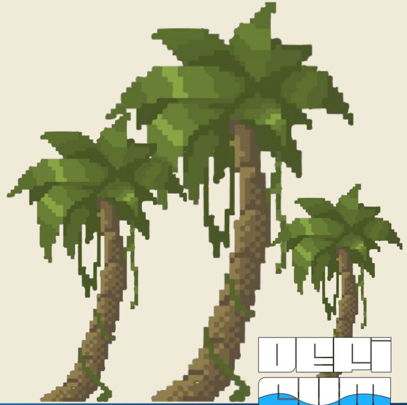
- Protects the blockchain against bad actors.
- For someone to rewrite the chain, they would have to re-mine every block that comes after their transaction.
- However, everyone else is already working on the next block.
- The bad actors would have to work faster than the good actors.
  - They would need 51% of the entire network's processing output.
- The bad blocks end up as dead ends and die out.



Why is Blockchain Important?

1. Data Integrity
2. Distributed Power
3. Value as Incentive
4. Security
5. Privacy
6. Rights Preserved
7. Inclusion

7



Data Integrity

"Acting without integrity costs a lot more time, energy, and reputation."

Problem
Without a central source of truth, what can you trust?

Solution
A peer-to-peer network that's costly to add and change data to.

Distributed Power

“No person or organization has outsized control over the whole.”

Problem
A third party being the source of truth can lie.

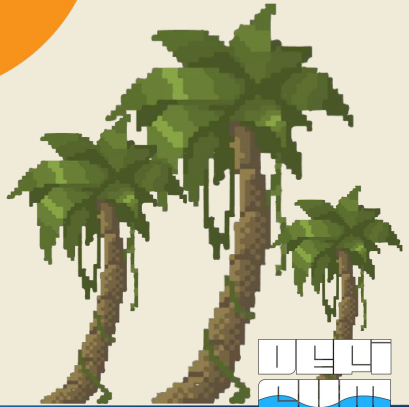
Solution
The users participating in the network maintain the network.

Aligned Incentive

“You can work for your own selfish interests, but that will also benefit the whole.”

Problem
People are driven by different incentives

Solution
Give rewards for providing proof of work. People will have a vested interest in maintaining the network.



Security

“Reckless behavior by one person only damages that person.”

Problem
Hacking, fraud, identity theft etc.

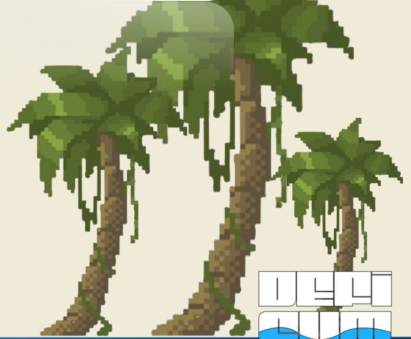
Solution
Public/private key pairs instead of usernames/passwords.

Privacy

“People get to be in complete control of their data.”

Problem
Data exposure to prove your identity.

Solution
Eliminate the need to trust others = eliminate the need to know the true identities of those others in order to interact with them.

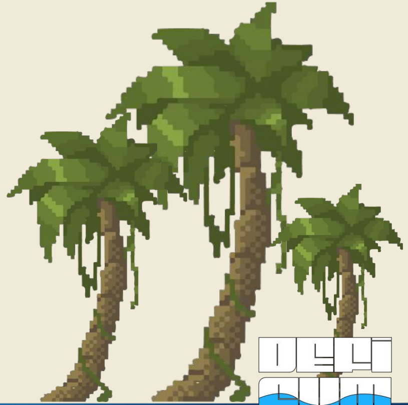


Preserving Rights

“Rights and freedoms are clear and enforceable

Problem
Companies can change terms of service / how their use your data.

Solution
Enforcing rights in code.

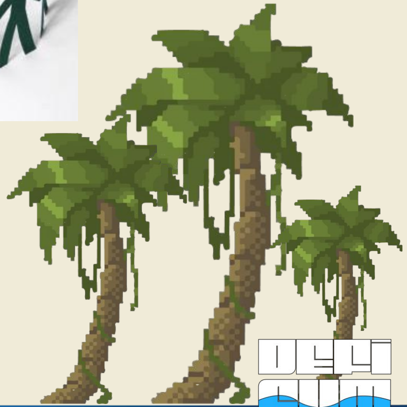


Inclusion

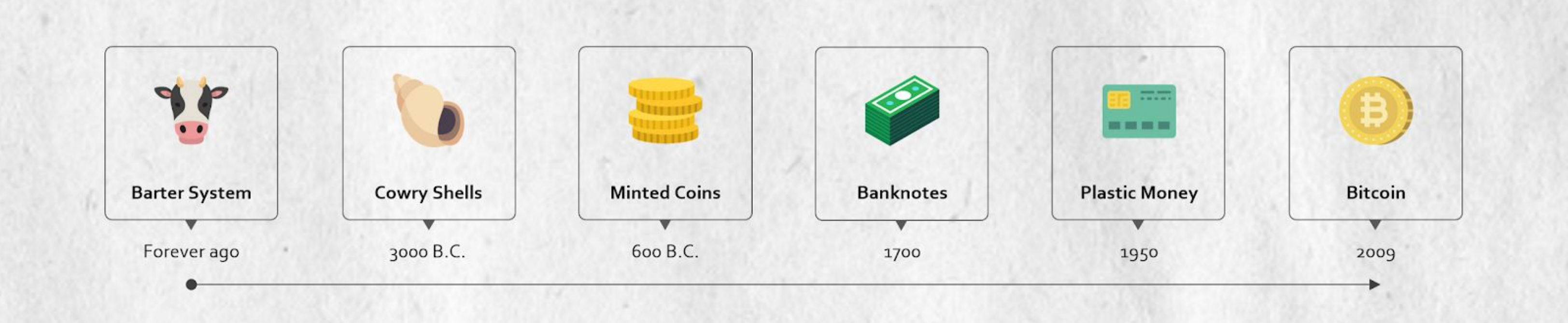
“Everyone in the world should have the ability to participate.”

Problem
Half of the world does not own a bank account

Solution
No need for bank accounts, credit scores, or age requirements to transact on a blockchain.

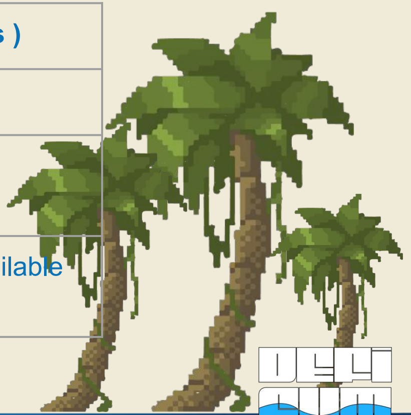


History of Money



Barter System	Cowry Shells	Minted Coins	Banknotes	Plastic Money	Bitcoin
Forever ago	3000 B.C.	600 B.C.	1700	1950	2009

Keynesian (current financial system)	**Austrian (Bitcoin and most Blockchain systems)**
Inflation is Good	Inflation is Bad
Spending drives economic growth, savings decrease it	Savings and production drive economic growth
GDP is the main determining factor in the strength of an economy	Interest rates determine the amount of savings available to grow the economy



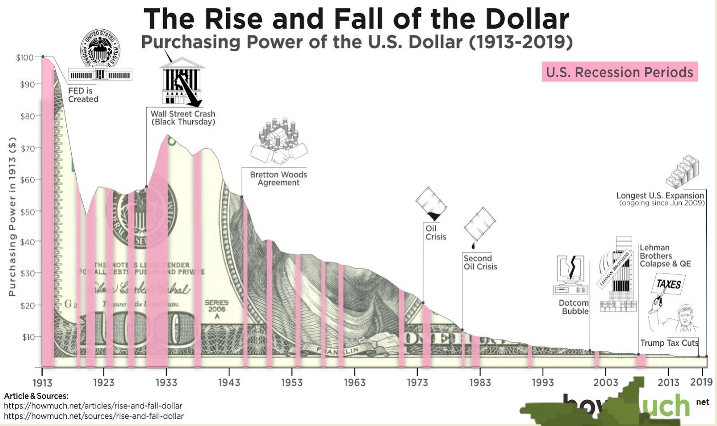
New Store of Value

BITCOIN

- There will be a finite amount of bitcoins. Quantity is 21 million
- Creating new bitcoins is expensive in terms of computing power, electricity consumption
- Instead of “mining” bitcoins you can always buy bitcoins at an exchange

GOLD

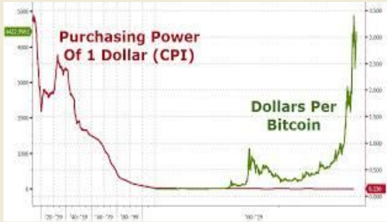
- A finite amount of gold is available in the world. Quantity unknown
- Digging gold out of the ground is complex and expensive exercise
- Instead of mining gold you can also buy gold from a dealer at a commodity exchange



The Rise and Fall of the Dollar

Purchasing Power of the U.S. Dollar (1913-2019)

Article & Sources:
https://howmuch.net/articles/rise-and-fall-dollar
https://howmuch.net/sources/rise-and-fall-dollar



MAJOR BLOCKCHAIN CONSORTIA AND NETWORKS

R3 CEV

Bank of America
NATIXIS
COMMERZBANK
THOMSON REUTERS
MetLife
中国平安 PING AN
招商银行 CHINA MERCHANTS BANK
TOYOTA FINANCIAL SERVICES
AIA
NOMURA
ING
Westpac
citi
TD Bank
STATE STREET
BNY MELLON
WELLS FARGO
CommonwealthBank
Danske Bank
CREDIT SUISSE
BNP PARIBAS
MACQUARIE
RBS The Royal Bank of Scotland
BBVA
MIZUHO
MUFG
BARCLAYS
SMBC SUMITOMO MITSUI BANKING CORPORATION
UBS
Northern Trust
BMO Financial Group
HSBC
usbank
SEB
SOCIETE GENERALE
Hana Financial Group
J.P.Morgan
CIBC
RBC
UniCredit
Deutsche Bank
INTESA SANPAOLO
Scotiabank
Nordea
SBI Holdings

Digital Asset Holdings (Investors)

ABN·AMRO
accenture
BNP PARIBAS
ASX
citi
Broadridge
CME Group
Goldman Sachs
ICAP
DTCC
IBM
Deutsche Börse Group
J.P.Morgan
PNC
Santander InnoVentures

Hyperledger Project (selected members)

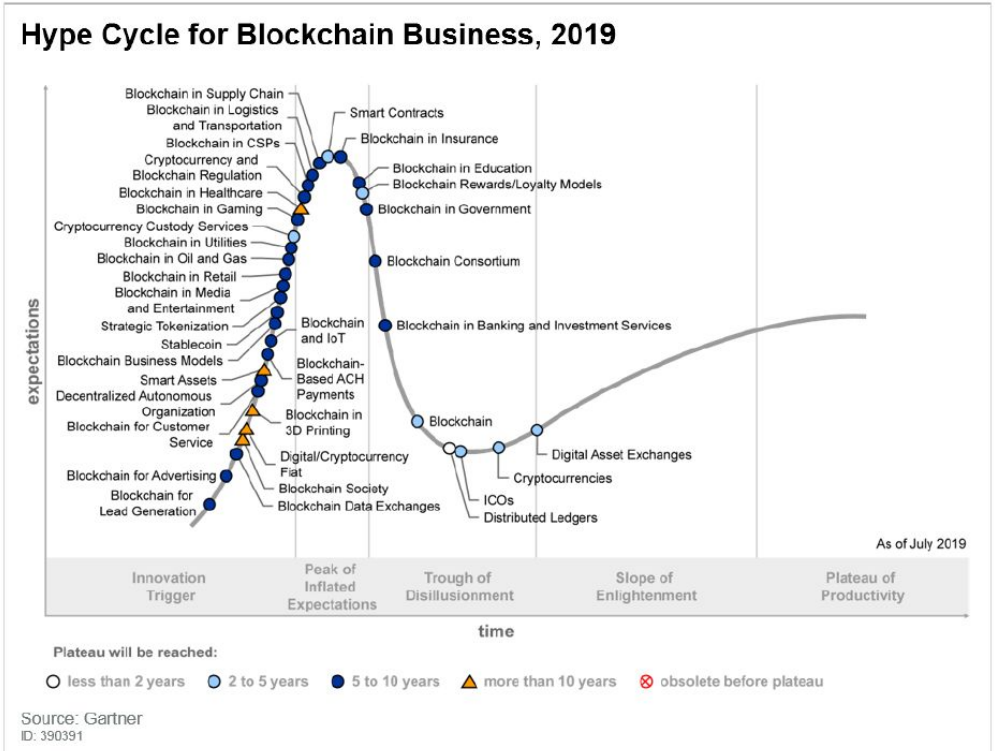
accenture
ANZ
SWIFT
Digital Asset Holdings
STATE STREET
J.P.Morgan
CME Group
WELLS FARGO
DTCC
BNP PARIBAS
IBM
CISCO
SBERBANK
bloq
r3
ABN·AMRO
Deutsche Börse Group
BLOCKCHAIN
Broadridge
BNY MELLON
London Stock Exchange Group

Ripple

Standard Chartered
Westpac
Santander
SHRB 上海华瑞银行
CIBC
ATB Financial
NBAD
UBS
nab
UniCredit Group

BI INTELLIGENCE

The State of Blockchain



Source: Gartner
ID: 390391

Blockchain Ecosystem Today

- Financial Services
- Application
- Exchanges
- Infrastructure
- Mining
- News & Data
- Payments
- Services
- Wallets

BITMAIN
BTC.com
BINANCE
coinbase
BTCC
WageCan
2018
BITCOIN & THE BLOCKCHAIN
WANXIANG BLOCKCHAIN 万向区块链
HSBC
AMD
Microsoft
Deloitte
Nasdaq
IBM
kik
ANDREESSEN HOROWITZ
Genesis Mining
SLUSH POOL
BITSTAMP
bithumb
OKCoin
KRAKEN
GEMINI
MINING
Coinify
bitpay
PLUTUS
status
Filecoin
BANKEX
po.et
ENTERPRISE
MOBILEGO
zencash
EOS
Tezos
GIFTO
MAD
TenX
SIRIN LABS
VERADX
BINARY FINANCIAL
BLOCKCHAIN CAPITAL
FENBUSHI CAPITAL
TALLYCAPITAL
bitwage
BitPagos
PROCESSORS
coindesk
BlockSocial
MONERO
ZEN
golem
brave
GNOSIS
NETKI
ZCASH
peercoin
BTC
askfm
COINTELEGRAPH
CHAMBER OF DIGITAL COMMERCE
yBitcoin
LTB NETWORK
BLOCKCHAIN
Bitcoin.com
ABRA
TREZOR
Ledger
keepkey
xapo
airbitz
ben
Blockstream
bloq
ripple
consensys
Purse
symbiont
Rubix
BitGo
ZAP
MONAX
ANX
Gem
AlphaPoint
FACTOM
CAPASITY

Blockchain Ecosystem Today

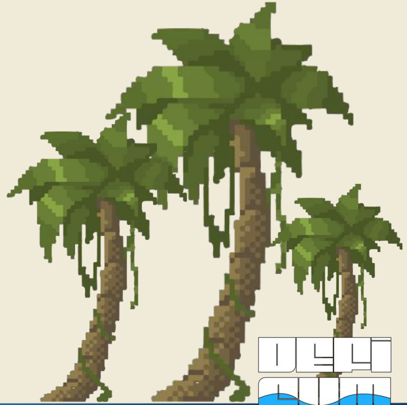
- Decentralized Finance(MakerDAO, Compound, Dharma) and Banking
- Supply chains and logistics (Walmart, IBM)
- Healthcare (MediBloc)
- Government (U.S Navy, Air Force, China Blockchain Network Service)
- Energy grids and sharing (PowerLedger, SunContract)
- Real estate (RealT, Harbor)
- Digital Identity (Civic, Sovrin)
- Law (OpenLaw)
- Voting(Horizon State)
- Many other sectors(Gaming, Gambling, etc)

Blockchain is Interdisciplinary

Blockchain combines elements from economics, math, computer science, and philosophy

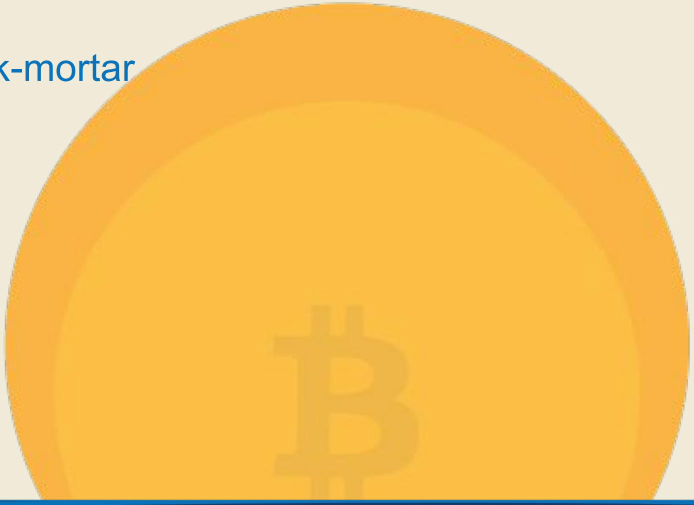
- Computer Science – cryptography, SHA-256 mining algorithm
- Math – probability, elliptic curve cryptography
- Economics – monetary policy, inflation rate, game theory
- Law - regulations, foreign policy
- Philosophy – Cypherpunk Movement, privacy, freedom

Everyone can be part of the conversation.



The Unbanked

- **1.7 billion people in the unbanked population**.
- Why?
  - Lack of money
  - Barriers to entry
  - Lack of trust
  - No access to brick-mortar



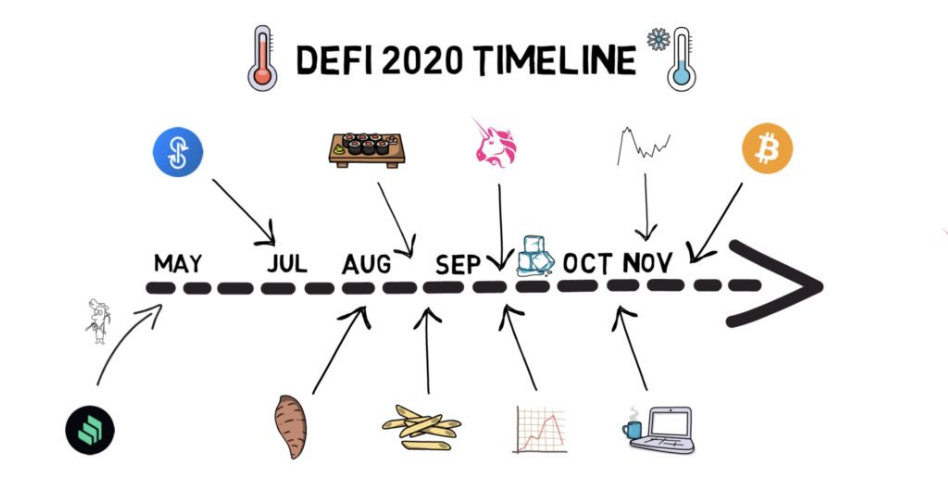
What is Defi

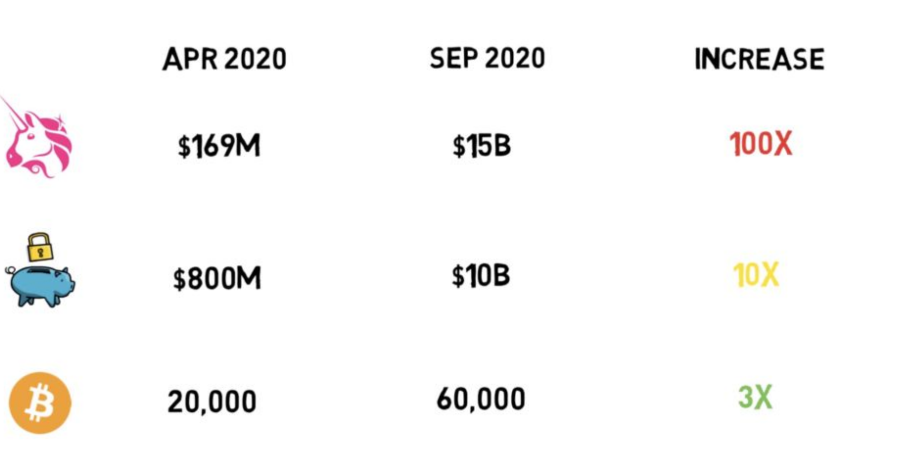
Decentralized finance is a revolutionary form of finance that frees individuals from the dependence of traditional financial intermediaries, utilizing smart contracts on blockchains enabling for complex transactions like lending, speculation, trading, insurance, and interest. The DeFI world is built on DApps (decentralized applications) that modify digital ledgers with smart contract protocols typically integrated through a Web3 wallet. Smart contracts and DeFI protocols are usually open-source and are contributed to by a community of developers like the one we have at DeFi summer.

History of DeFi

- Bitcoin enable p2p payment in 2009, and Ethereum in 2015, allowed for building smart contracts and developing ERC-20 tokens
- DeFi’s beginning is often traced to MakerDAO, a platform that launched in 2015 that allowed users to use cryptocurrency as collateral for loans.
- ICO boom in 2017 funding ethereum projects (Aave, Ren, Kyber, Synthetix, 0rx, Bancor) - popularizing “user-to-contract” model
- Uniswap in 2018 funded by Ethereum Foundation grant
- In July 2019, Synthetix launched first liquidity incentive program
- Liquidity mining program by Compound in May 2020, gaining COMP tokens for lending & borrowing on Compound platform, also with governance protocols
- Yearn Finance aggregator with YFI gov token awarded for providing liquidity

History of DeFi





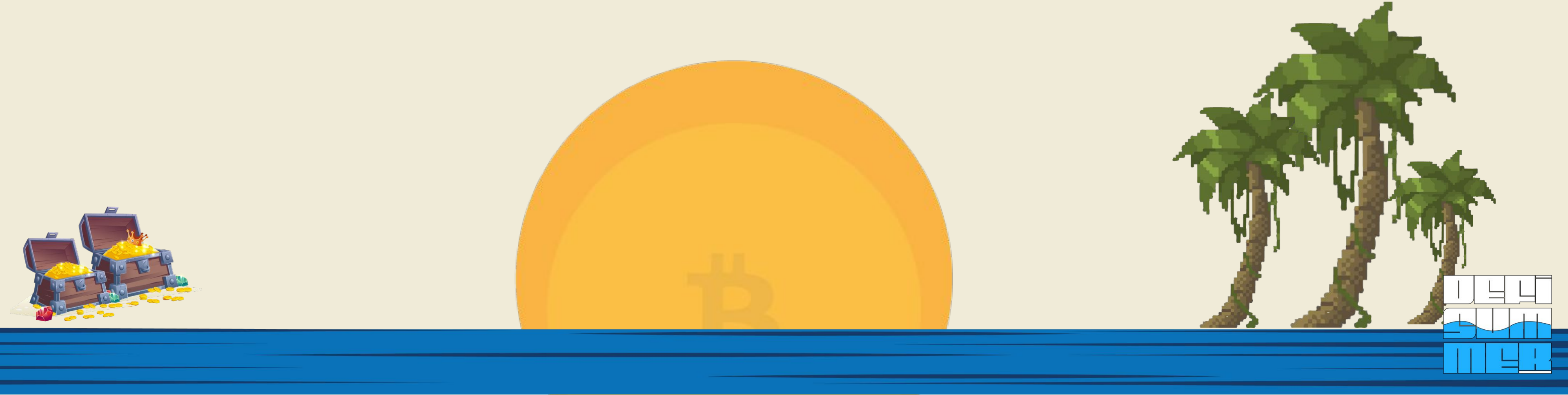
	APR 2020	SEP 2020	INCREASE
🦄	$169M	$15B	100X
🐷	$800M	$10B	10X
₿	20,000	60,000	3X

Advantages of Defi

- Sending and receiving money from anywhere around the world within seconds.
- Access to global funds, not being limited to the funds in the custody of your bank
- Stablecoins/Wrapped coins - are pegged to another asset, like the US Dollar, so the value stays within a few cents of the dollar, full exposure to all asset types.
- Borrowing without credit checks or personal information (NO KYC)
- Transparency - anyone can look at the product data, inspect how the system works and see where the money is
- Ability to plug and play different DeFi apps/protocols
- Gaining fees for being a liquidity providing or being a market maker

Automated Market Makers

Automated market makers (AMMs) are part of the decentralized finance (DeFi) ecosystem. They allow digital assets to be traded in a permissionless and automatic way by using liquidity pools rather than a traditional market of buyers and sellers. AMM users supply liquidity pools with crypto tokens, whose prices are determined by a constant mathematical formula. Liquidity pools can be optimized for different purposes, and are proving to be an important instrument in the DeFi ecosystem.



Constant Product Formula

tokenA_balance(p) * tokenB_balance(p) = k

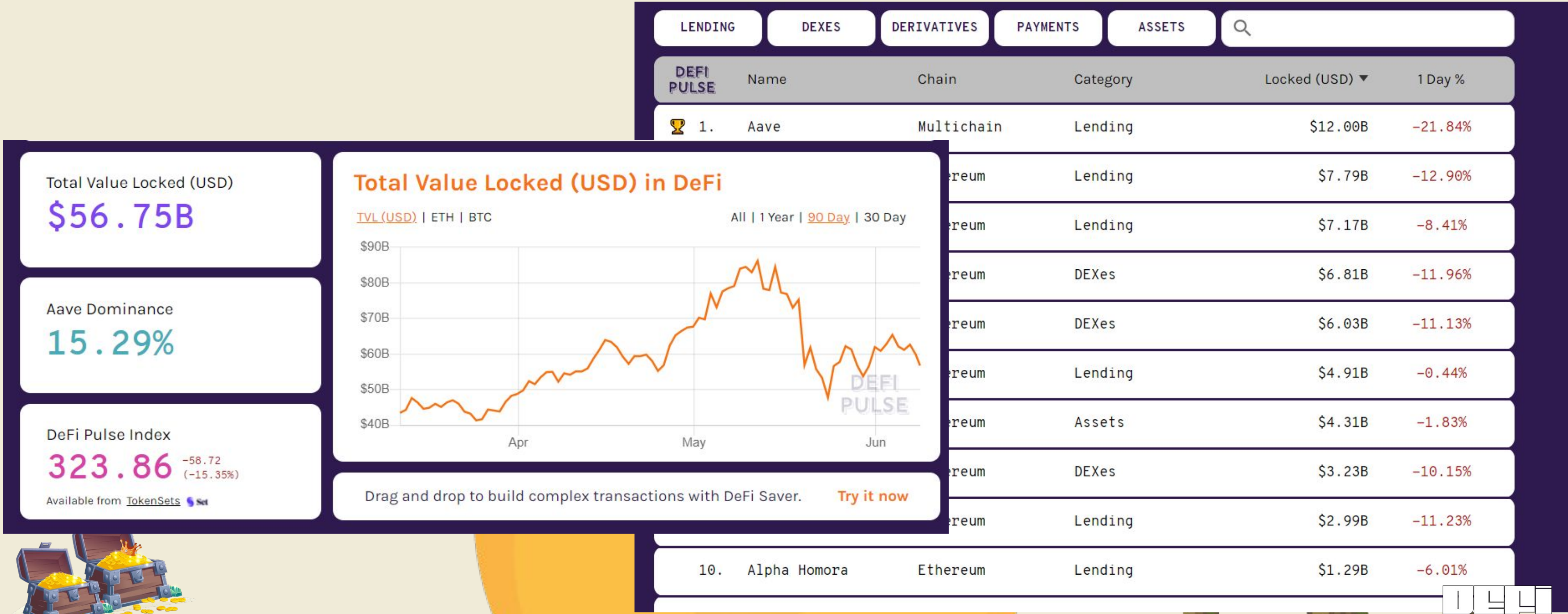
and popularized by Uniswap as:

$x * y = k$

Defi Stack

- Settlement Layer - public blockchain, native currency, Ex; eth blockchain and eth used to record financial transactions on blockchain
- Protocol Layer - Standards/rules written on blockchain that provides liquidity
- Application Layer - consumer facing application abstracting protocol layer
- Aggregation Layer - collecting from various applications (leding, borrowing), analyzing different instruments to maximize returns

Top DeFi Protocols



DEFI PULSE	Name	Chain	Category	Locked (USD) ▼	1 Day %
🏆 1.	Aave	Multichain	Lending	$12.00B	-21.84%
		ereum	Lending	$7.79B	-12.90%
		ereum	Lending	$7.17B	-8.41%
		ereum	DEXes	$6.81B	-11.96%
		ereum	DEXes	$6.03B	-11.13%
		ereum	Lending	$4.91B	-0.44%
		ereum	Assets	$4.31B	-1.83%
		ereum	DEXes	$3.23B	-10.15%
		ereum	Lending	$2.99B	-11.23%
10.	Alpha Homora	Ethereum	Lending	$1.29B	-6.01%

Total Value Locked (USD)

$56.75B

Aave Dominance

15.29%

DeFi Pulse Index

323.86 -58.72 (-15.35%)

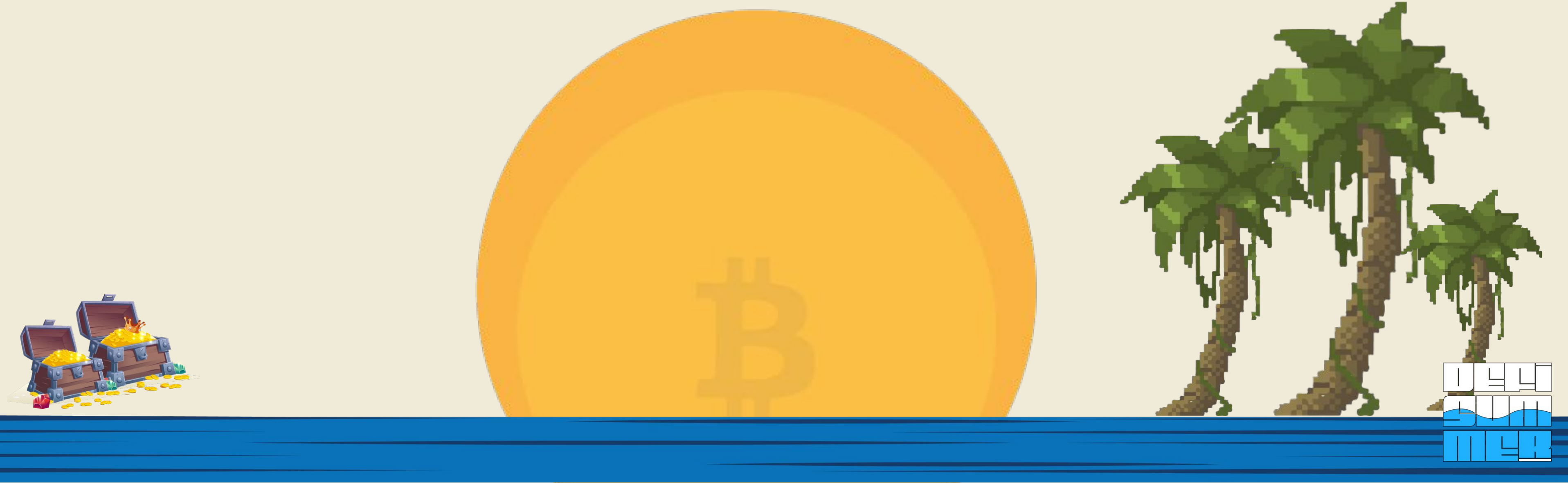
Available from TokenSets Set

Total Value Locked (USD) in DeFi

Drag and drop to build complex transactions with DeFi Saver. Try it now

DeFi Drawbacks

- Centralization of oracles
- Smart contract security issues
- Bad actors



Questions

- Ask away