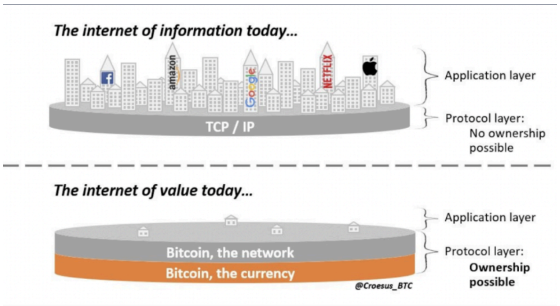
Bitcoin Research Club

What is B(b)itcoin?

History:
On October 31, 2008, Satoshi Nakamoto published the Bitcoin Whitepaper (a 9 page pdf), creating *"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"* and is the result of 40 years of research. **2 key attributes** were implicitly stated & shouldn't be overlooked: (1) There will only ever be 21,000,000 bitcoin (2) bitcoin requires a scarce input/resource (energy) through its consensus method called Proof of Work (PoW) (how it validates the information being stored).

Context: At this time, the world was reeling from the biggest financial crisis since the 1920s. Public trust in the financial system was at an all time-low, showing the need for a new financial system that didn't depend on a few key players who can, and did, fail.



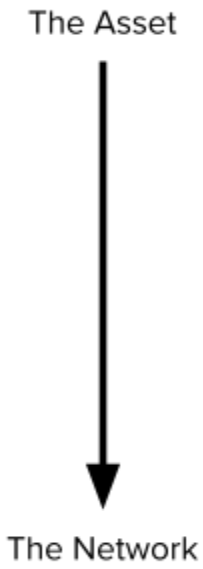
What is bitcoin? What is Bitcoin?
Lowercase "b" bitcoin is the asset. Uppercase "B" Bitcoin refers to the network. ***Analogy:*** *Think of dollars or euros as "fiatcoin" and the societal structures around us as being influenced by the "Fiat Network" (h/t Saifedean Ammous).* Bitcoin, is not a subset of "blockchain" or "cryptocurrency."

Elevator pitch: Why should I care about B(b)itcoin?

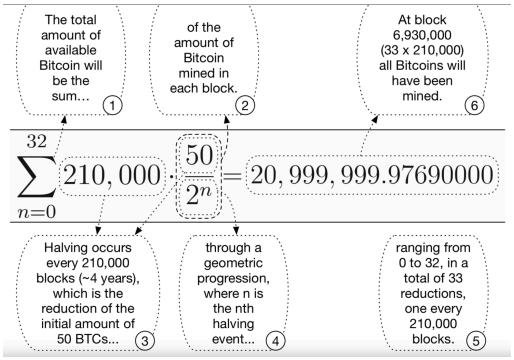
A tool to earn your wealth once (through your job), instead of twice (through job + investment portfolio) (h/t Saifedean Ammous). bitcoin is protection against monetary debasement and uncertainty. Given there will only ever be **21 million**, you can avoid monetary debasement as you'll always own the same fraction of the supply (no one can print more). The longer you denominate in fiat currency (i.e. dollars), the more expensive life gets (purchasing power declines). The longer you denominate in bitcoin, the less expensive life gets (purchasing power increases). (h/t Jeff Booth).
The U.S. dollar has lost 98% of its purchasing power since 1971.

Many come to bitcoin for "Number Go Up" i.e. monetary gains, and they stay in Bitcoin for "Freedom Go Up." Bitcoin is privacy-enabling freedom technology; it's the first way for humanity to store energy for generations; it's property every person can own; it's money the whole world can use. It protects human rights, property rights, liberty, and individual sovereignty, expands equitable access to energy, allows one the ability to save and think about the future with optimism, etc.

The 21,000,000 are tools for the 21st century. Economics and by extension money is the base layer of society. bitcoin is the best form of money, objectively fulfilling the characteristics of "sound" "hard" money. Through this reality, Bitcoin touches upon most all areas of life from energy to human rights. Whatever your interest, there is alignment.



Attributes of Bitcoin:
Decentralized, Truly scarce, Censorship resistant, Incorruptible, Permissionless, Auditable Transparent, Immutable, Borderless, Hard to counterfeit, Pseudonymous, Frictionless, Trustless Peer-to-peer, etc.



It will take **131 years** for all bitcoin to be "mined." Today, about **1.3%** of the world's population owns bitcoin and **93.4%** of the **21,000,000** bitcoin have been mined. Today, at "block height" 828,836 (how many blocks have been mined since Jan. 3, 2009) the price of bitcoin is $42,887. What does **98.7%** of the world seeking the final **6.6%** to be produced over the next **116** years look like?

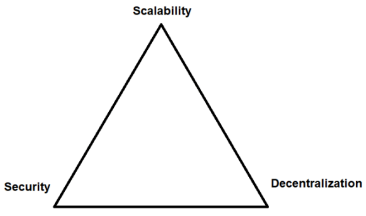
What is the difference between "money" and "currency?"

- (Properties of) **Money: Salability: (1)** across time/ **Store of Value** (scarcity, durability) **(2)** across space/ **Medium of exchange** (acceptability, portability), **(3)** across scales/ **Unit of Account** (divisibility, fungibility) (h/t Eric Yakes).
- **Money:** used to communicate value and to facilitate the exchange of preferences worldwide. Perfect money is one that holds its value and cannot be corrupted by an individual or state. **Fiat Money:** government-issued currency that is not backed by a physical commodity, such as gold or silver, but rather by the government that issued it. (i.e. trust in the government/ issuer). Ex: the dollar, euro, yen, etc. Our world today/current monetary system.
- **Currency:** tangible form of money.

What is Blockchain?
A way of storing (most commonly financial) information. It is digital, decentralized, immutable, ordered, append-only, verifiable ledger (more correctly, an ordered data structure because the data is not organized in a table like a ledger is) of information. Bitcoin was the first "blockchain," but "Bitcoiners" often refer to the bitcoin blockchain instead as the bitcoin "timechain."

Analogy: The longest running "blockchain" is the **New York Times (1851).** In its printed form, it was decentralized (every person could own every issue), immutable (can't be edited), ordered (by publication date), append-only (can only have successive issues printed), verified (can compare issues against each other).

All blockchains must solve "The Blockchain Trilemma" on creation.
They must choose to ⅔ to "optimize" for. The winning combo is security & decentralization. bitcoin is the only "blockchain" that successfully optimizes for security and decentralization on Layer 1, addressing "scalability" on Layer 2 (think of a building with levels). Basically, bitcoin is super secure and super decentralized. But, it's super slow at processing transactions.



Security and decentralization must be optimized on the ground level to build a building with a foundation that lasts (like steel for a building vs. sand) (h/t Preston Pysh & Michael Saylor).

Security + Decentralization = building made of steel
Security + Scalability OR Decentralization + Scalability = building made of sand