Bitcoin – 4 Pillars

1. Peer-to-Peer Digital Cash

1. Censorship resistant payment system
2. Un-seizable store of value

2. Decentralization

1. No centralized entity manages Bitcoin
    1. Different versions of the Bitcoin software
2. Consensus achieved through nodes

Diatribe about Blockchain

- Most fundamental issue of anything digital is the copy & paste issue. In the past there was no way to have digital money without a centralized clearinghouse. But centralized clearinghouses can be coerced by bad actors.
- The block chain was the solution. It is a database with a history of every transaction that has ever occurred. HOWEVER! The block chain is the *worst* part of Bitcoin. It is the toxic waste of the Bitcoin protocol. But it is eminently critical and cannot be removed.
- The block chain, in essence, is the world’s least efficient database
    - Bananas on the block chain. Digital cats on the blockchain
    - All better done with a centralized server tracking everything.

3. Cryptography

1. Public Key (Asymmetric) Cryptography
    1. 2^256 (or ~10^77) private keys. 10^80 atoms in the known universe
    2. Whit Diffie: https://onezero.medium.com/the-untold-story-of-the-man-that-made-mainstream-encryption-possible-231c749d5005
2. Hashing
    1. SHA-256
    2. Proof-of-Work is critically important here. No entity can afford to mine maliciously because the the immense asymmetry between successfully mounting an attack and successfully completing an attack.
        1. Use double spend as an example. Expense large amounts of electricity to mine a bad block only to have nodes almost instantaneously declare it invalid.
3. Difficulty adjustment
    1. Every 2016 blocks, which at exactly 10 minutes per block would be every two weeks. A person can expect the difficulty adjustment to occur slightly less than every two weeks as prices are rising and slightly more than every 2 weeks

4. Economics

1. Halving
    1. Currently set for May 9th. This will be my first halving event, but the third in Bitcoin's history. Block reward will decrease from 12.5 to 6.25 BTC per block.
2. Stock-to-Flow
    1. Ratio of how much has been mined & stored to how much is being mined annually. Gold has a S2F of about 66—meaning it'll take 66 years of mining at current rates to double the current already-mined supply of Gold
    2. Stock-to-Flow of the following
        1. Bitcoin (pre halvening) *actual numbers*
            1. ~30 (10 day average), 25 (365 day average)
        2. Bitcoin (post-halvening) *estimates only*
            1. ~90 (10 days after halving), ~85 (1 year after halving)
        3. Silver 22
        4. Gold 66
    3. The difference between Bitcoin and any other is that the issuance or mining rate of Bitcoins is predetermined and cannot be changed. As the price of Gold increases, the incentive to mine increases. The less-efficient mining companies are not financially feasible once again, they will begin mining again, which will increase the supply of Gold, which will decrease its S2F ratio.

        Bitcoin is designed so that one block of transactions is mined approximately every 10 minutes. This cannot change. As the price goes up, more miners are insentivized to mine, but the difficulty target adjusts every 2016 blocks to keep blocks approximately every 10 minutes apart.

        Supply does not increase or decrease based on price. This is the fist thing that has ever existed where that can be said. Given a free market, as prices of cars goes up, people supply more cars. As the prices of computers goes up, people supply more computers. As the price of Gold goes up, people supply more gold. But as the price of Bitcoin goes up, the supply stays the same.
    4. The Bitcoin Standard

5. How it works

1. Nodes, Miners, Users
2. Transaction created, broadcast, mempool, mined, verified
3. Security
    1. Offline keys
        1. Hardware wallets (coldcard, ledger, trezor)
    2. Run your own node
    3.

6. More resources

1. The Bitcoin Whitepaper, Satoshi Nakamoto
    1. Bitcoin.org – NOT BITCOIN.com
2. Introductions & Technical Information
    1. The Little Bitcoin Book (simple, informational)
    2. Grokking Bitcoin (illustrated)
    3. Bitcoin Money: The Tale of Bitville (children’s book)
3. Statistics and Network Information
    1. Digitalik.net
    2. https://bitcoin.clarkmoody.com/dashboard/
    3. https://www.lopp.net/
4. Economics
    1. The Bitcoin Standard, Saifdean Ammous
    2. S2F Modeling
        1. @100TrillionUSD (twitter)
        2. (March 22nd!) https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25
5. Podcasts
    1. The What Bitcoin Did Podcast
        1. Especially his Bitcoin for Beginners series
    2. The Steven Livera Podcast (focusing mostly on economics)