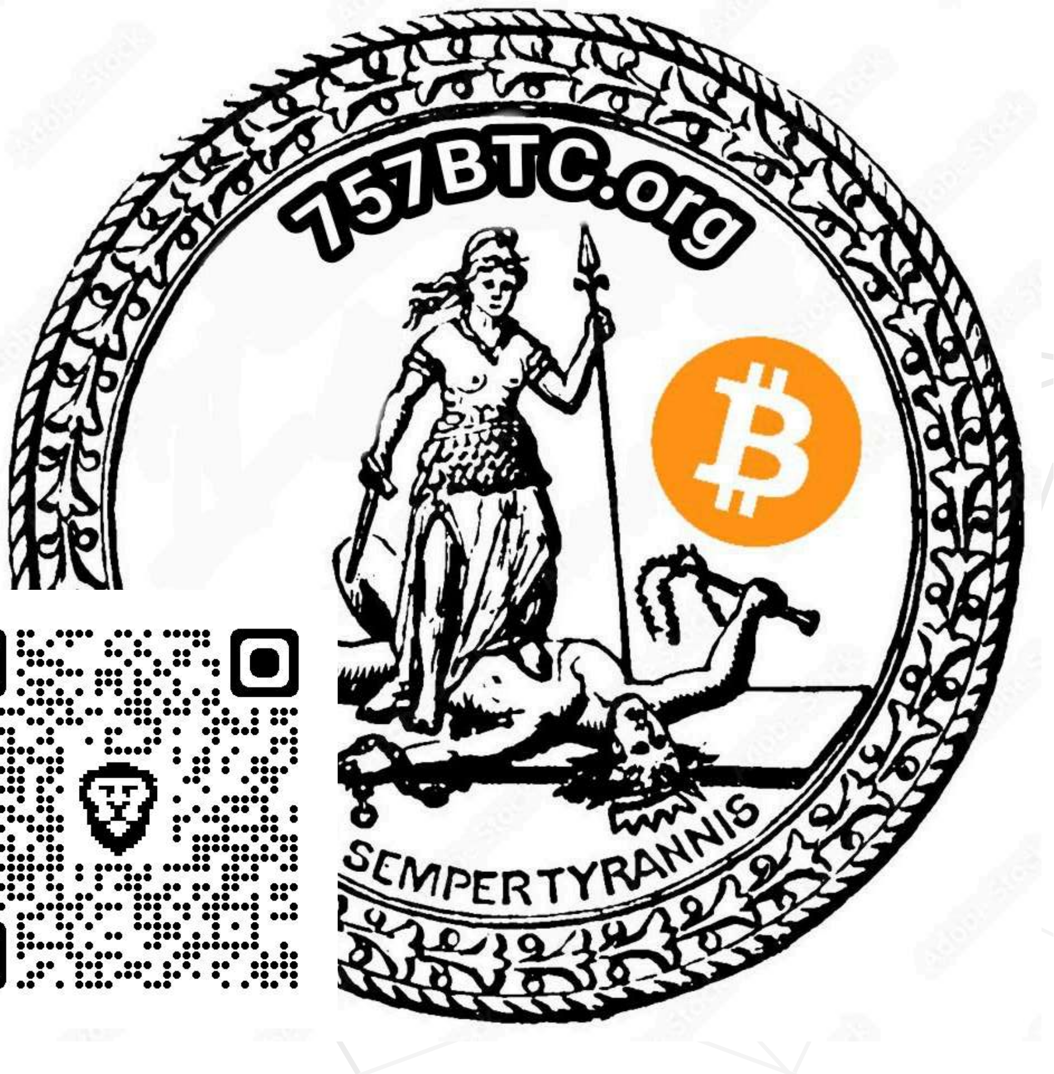
Bitcoin, Freedom, Security

757BTC

https://www.757btc.org/



Presentation Conversation Over Bitchat

- This conversation will be deep in philosophy and are fundamental to understanding the foundations of Bitcoin
- Critically challenge every idea
- Participate through local mesh communication
    - anon or use a name if you like
    - https://bitchats.app/
    - Moderators can interrupt presentation to address relevant points

Topics

- Cryptography History
- Information vs. Physical
- Relationship between Speech and thought
- What Money Actually is
- Trust vs. Verification
- Proof of Work
- Asymmetric Defense

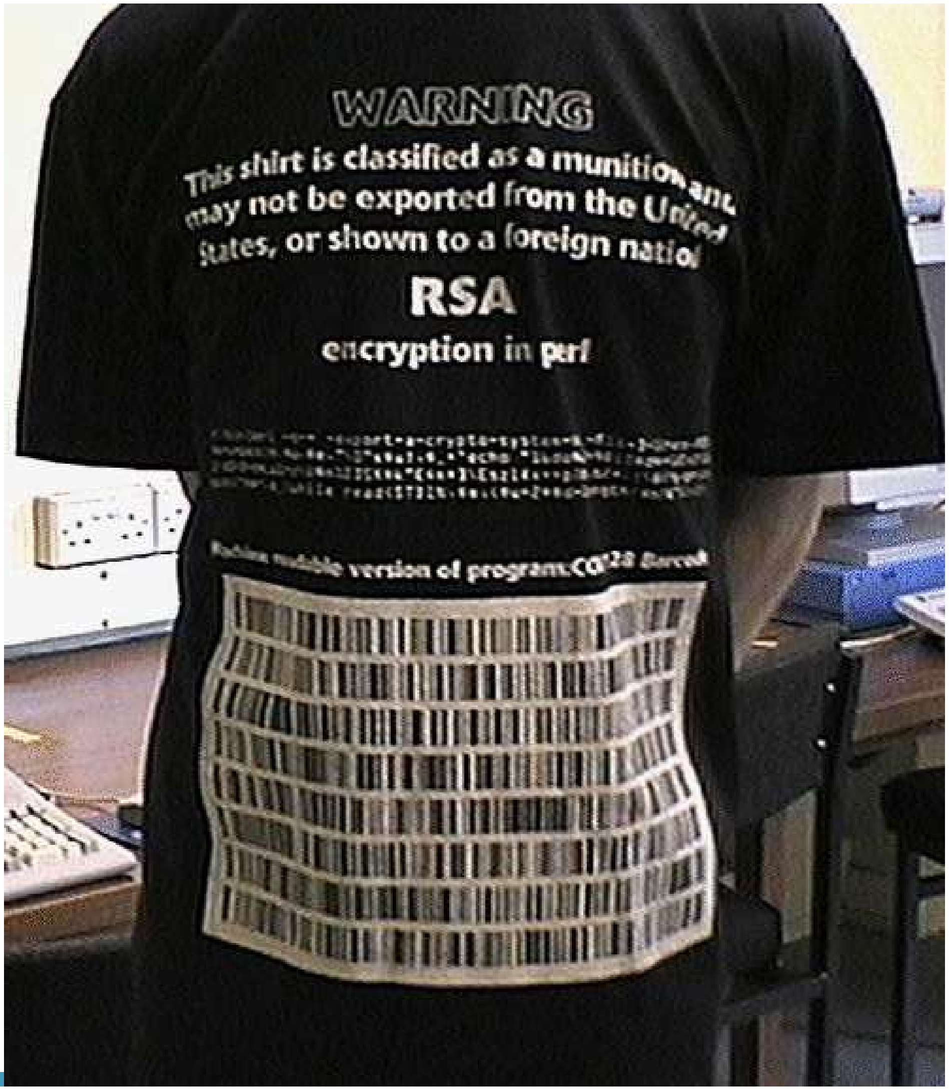
Common Discussed Threats of Bitcoin (FUD)

- Someone can just change the fixed supply
- Centralized control of developers
- Centralized control of mining
- Government will ban it
- Wasteful energy consumption

https://endthefud.org/

Cryptography History

- Legal battle with USA Gov’t
  - DoD wanted to establish that RSA encryption was a munition
- Math expressions and cryptographic code are constitutionally protected speech
- Proved that decentralized, voluntary adoption of cryptographic tools could defeat government control


WARNING
This shirt is classified as a munition and may not be exported from the United States, or shown to a foreign national
RSA
encryption in perl
Machine readable version of program:CQ28 Barcode

Arms Export Control Act Investigation

- In 1991 he wrote the popular PGP program and made it available to freely be downloaded.
  - first widely available program implementing public-key cryptography
- The US arms trafficking export controls considered it munitions
  - a method for encryption considered at the time by the US Government to be impermissible
  - started a Criminal Investigation
- The investigation lasted three years, but was finally dropped without filing charges after MIT Press published the source code of PGP

Information vs. Physical

- Information can be copied perfectly
- Physical objects cannot be in two places at once
- This creates the double-spending problem for digital money
- Bitcoin doesn’t solve this by making information uncopyable
  - it makes invalid information useless

Relationship Between Thought and Speech

- Free speech is necessary for free thought
- Censoring expression censors the underlying ideas
- Bitcoin transactions are essentially speech acts
- Banning Bitcoin would require banning mathematical expressions

Trust vs. Verification Paradigm

- Traditional systems require trusted third parties
- These parties become single points of failure and control
- Bitcoin eliminates this through mathematical and economic verification
- Individual sovereignty requires the ability to verify independently

- Cypherpunk Manifesto
  - https://www.activism.net/cypherpunk/manifesto.html
- Free Open Source Software (FOSS)

What Money Actually Is

- Money is fundamentally a ledger of who owes what to whom
- It enables cooperation beyond trust relationships
- Control of money issuance = control of society's purchasing power
- Money is both a coordination tool AND a measurement system
- A means of communication

Proof of Work

- Proof-of-work transforms energy into unforgeable information
- It creates a "costly signal" that proves work was done
- This makes the digital ledger behave like a physical object
- The cost creates an economic incentive structure that secures the network

Asymmetric Defense

- **Cryptographic**: Guessing a private key is computationally impossible
- **Economic**: Attacking the network costs more than protecting it
- Both favor defenders over attackers by enormous margins
- Rules can emerge from individual choices rather than authority
- Consensus doesn't require a central coordinator
- Voluntary participation creates more robust systems than coercion

Gigi Inalienable Property Rights

https://dergigi.com/2022/04/03/inalienable-property-rights/