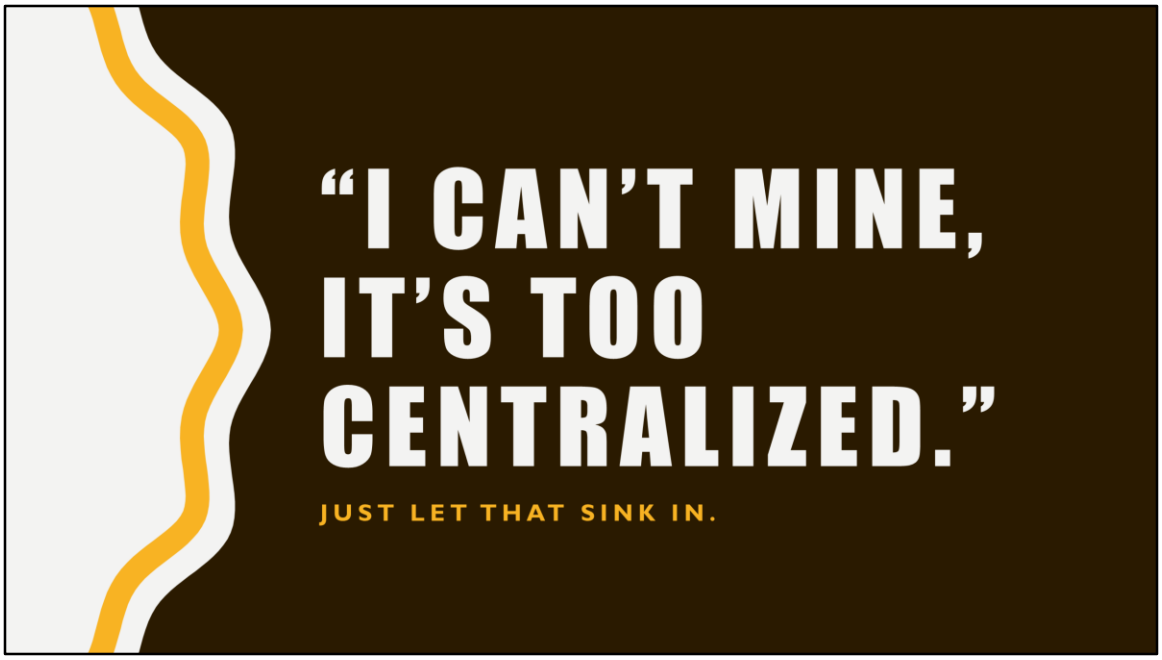
Political is the idea that those who disagree are compelled by the rest. **Consensus** is the idea that those who **agree** cooperate, **not** that everyone must agree.

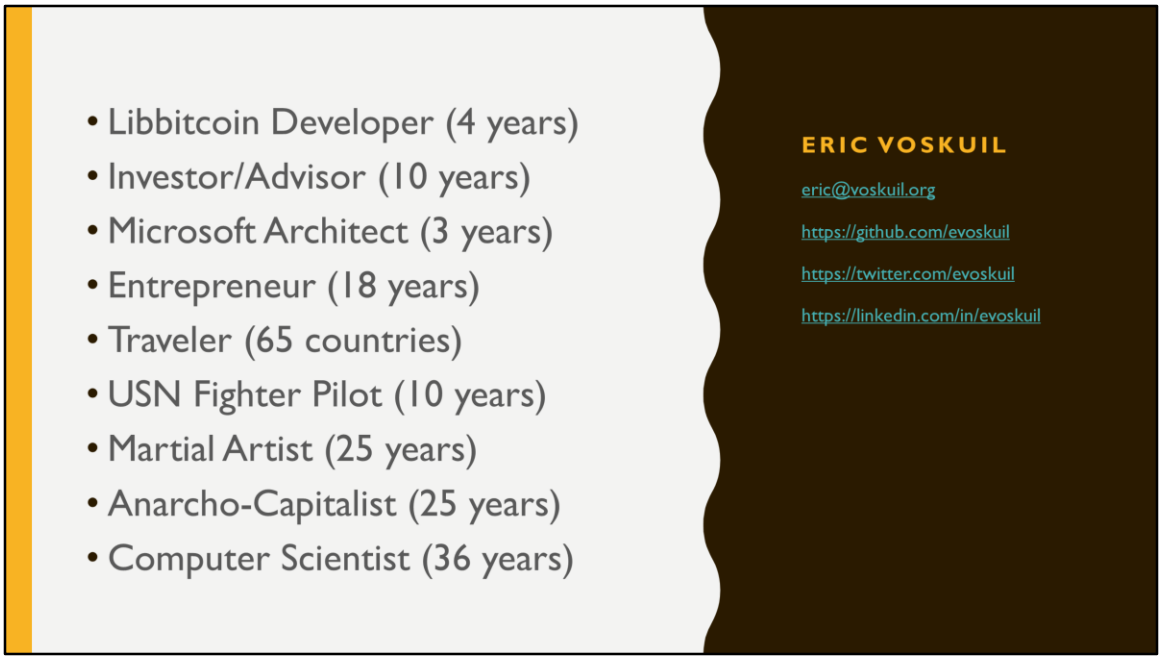
Bitcoin is **not a tool to compel** others to behave in a certain way. It is a **way for people to contribute** in mutual support of a common goal…

…If you find yourself demanding that **someone else** do something, or shaming them for doing what **they** prefer, you aren't doing it right.

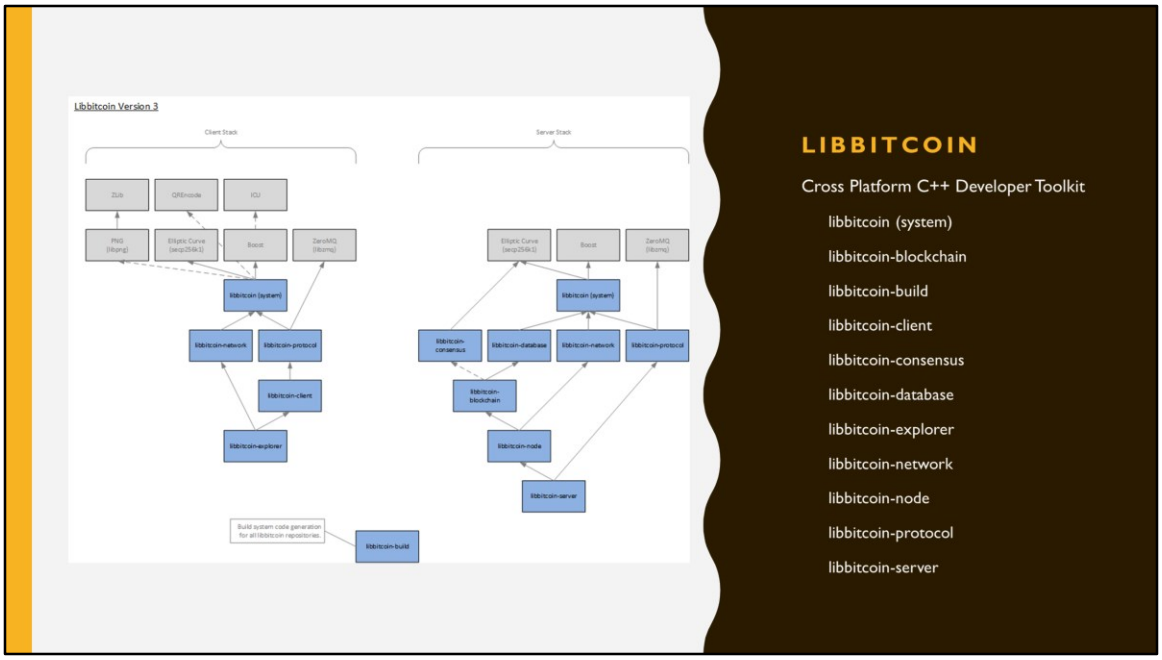
If you are unhappy with **developers**, then write code. If you are unhappy with the **rules**, then change them. If you are unhappy with **miners**, then mine. **That** is how you get your say, and **that** is the basis of security.

If this is unsatisfying because you alone cannot have a large impact, **that is sort of the point.**

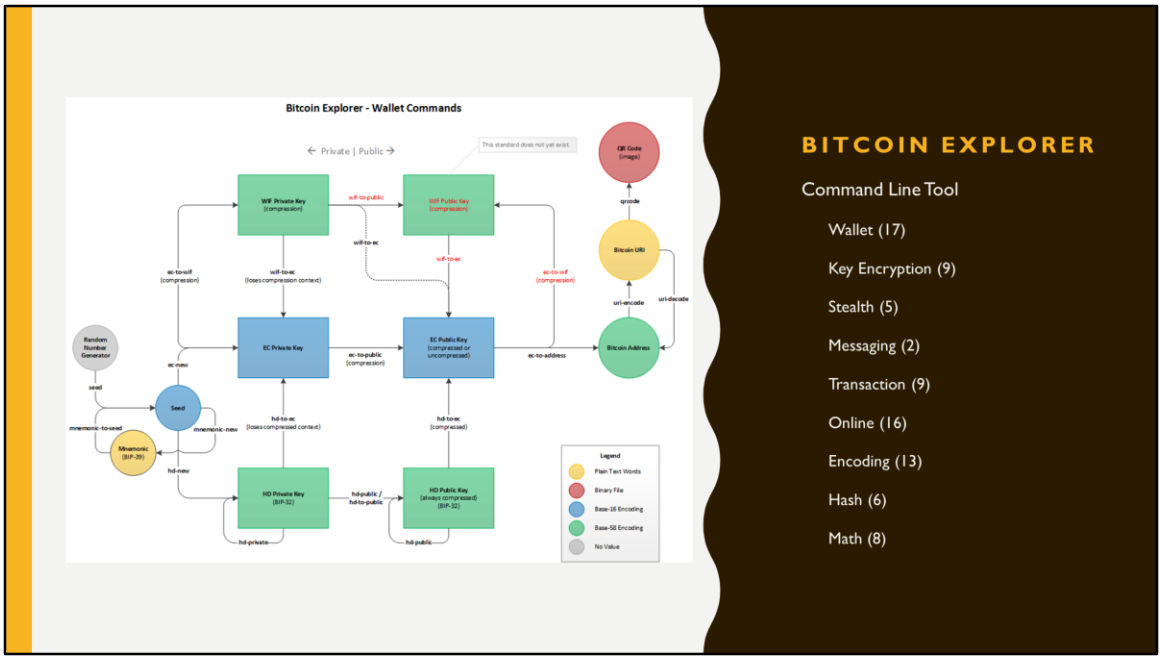

“I CAN’T MINE, IT’S TOO CENTRALIZED.”
JUST LET THAT SINK IN.



First, just a little about me…



Libbitcoin is a cross-platform Bitcoin developer toolkit, begun by Amir Taaki in 2011.



It includes command line applications built on the libraries, such as Bitcoin Explorer…

… and Bitcoin Server, a full node and query server.

It was the **first** implementation of Bitcoin not based on Satoshi's prototype.

While we talk about **breaking bitcoin**, we should understand that it's **already broken**.

Bitcoin exists as a **consensual** solution to the problem of **political** money.

In distributed systems terminology, Satoshi's solution to this problem is an anonymous leader election.

Leadership is determined by the greatest sufficient proof of work. The leader produces order, which triggers another election…

…A **public** leader would be subject to political control. Yet **anonymity** implies the leader may actually be the state. The solution to the state as monetary leader is for individuals to **literally** overpower it.

This is fundamentally a subversive act. Eventually it will require personal risk. Sharing this risk with other people is the **purpose** of decentralization.

People secure the money, software is just a tool they use to do so.

We call the avoidance of **political** control "censorship resistance". The **assumption** of Bitcoin is that resistance is **not** futile. If you don't accept this principle, you are not working on Bitcoin.

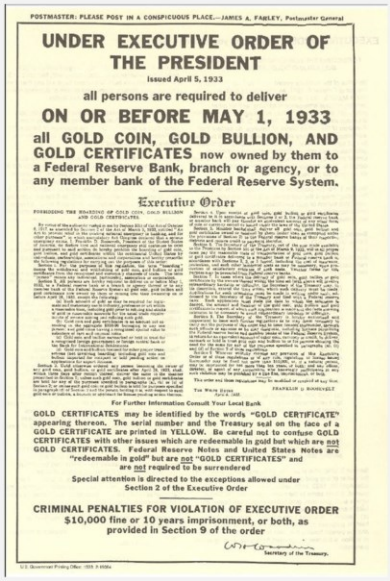
Without resistance a **political**, as opposed to anonymous, leader election is not only sufficient, but inevitable.

Political money however, as we are all familiar, does not have the beneficial characteristics of Bitcoin.

Attempting to explain Bitcoin without incorporating the axiom of resistance leads to **irrational statements**.

A favorite of these is that, “states cannot ban popular things,” replacing resistance with popularity in the security model.

I refer to this as the Hearn error. Apologies to anyone with that name, it was chosen at random.



POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE.—JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

Issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, or to any member bank of the Federal Reserve System.

Executive Order

FORBIDDING THE HOARDING OF GOLD COIN, GOLD BULLION AND GOLD CERTIFICATES.

For Further Information Consult Your Local Bank

GOLD CERTIFICATES may be identified by the words "GOLD CERTIFICATE" appearing thereon. The serial number and the Treasury seal on the face of a GOLD CERTIFICATE are printed in YELLOW. Be careful not to confuse GOLD CERTIFICATES with other issues which are redeemable in gold but which are not GOLD CERTIFICATES. Federal Reserve Notes and United States Notes are "redeemable in gold" but are not "GOLD CERTIFICATES" and are not required to be surrendered

Special attention is directed to the exceptions allowed under Section 2 of the Executive Order

CRIMINAL PENALTIES FOR VIOLATION OF EXECUTIVE ORDER
$10,000 fine or 10 years imprisonment, or both, as provided in Section 9 of the order

Secretary of the Treasury.

EXECUTIVE ORDER 6102

"Executive Order 6102 required all persons to deliver on or before May 1, 1933, all but a small amount of gold coin, gold bullion, and gold certificates owned by them to the Federal Reserve, in exchange for $20.67 per troy ounce… thereafter raised to $35.00… The resulting profit [seigniorage]… funded the Exchange Stabilization Fund…This price remained in effect until August 15, 1971 [when it went to infinity]… parties could again include so-called gold clauses in contracts formed after 1977."

- Wikipedia

It is quite evident that states actually **prefer** to ban popular things, as they are the most profitable.

Consider that gold was, until 1933, not only extremely popular, but the basis of the world's financial system.

In that year it was banned for all financial uses, and seized, by the United States government.

The recent “fork wars” have led to a curious misperception of the Bitcoin threat model.

THREAT MODEL

Perception

Reality

On the left is the **perception**, and on the right is the **reality**.

Miners and users (or "merchants" as the term "user" is ambiguous) are **not** locked in a power struggle. They are trading partners, in a **mutually-beneficial** market that they together create.

The security of Bitcoin is **not in any way** based on a conflict between them, it is based on their mutual **defense** of this market from attack by **anti-market** forces.

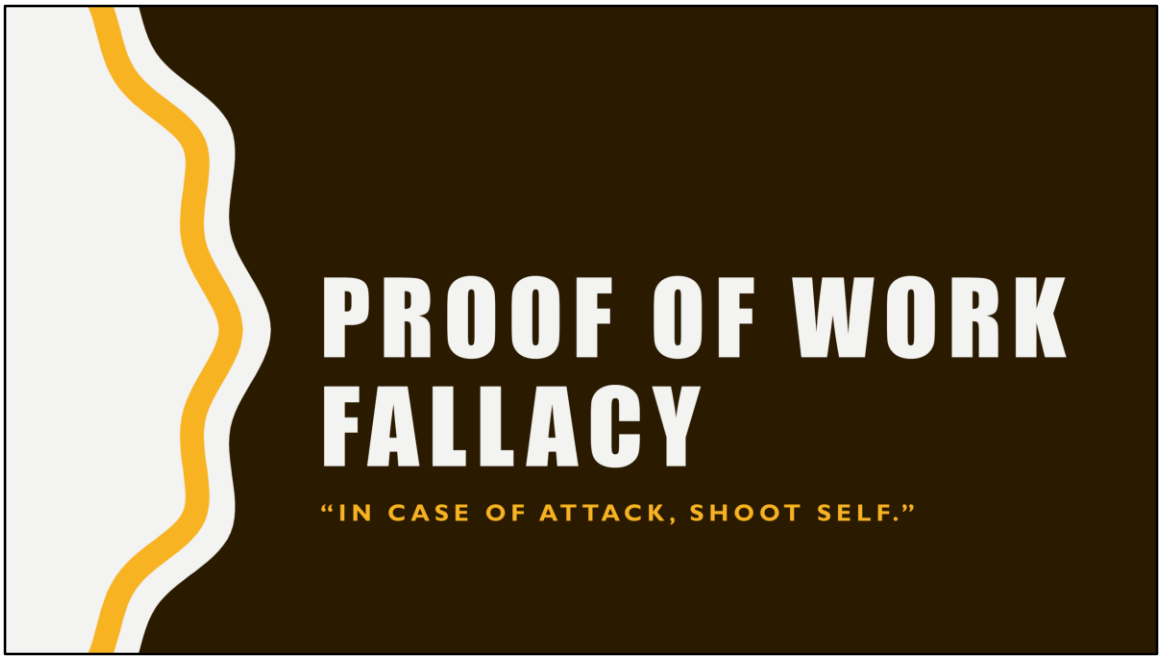
The idea that mining is somehow **powerless**, or that "**users rule**", is deeply flawed.

Mining has absolute power over **transaction selection**, while **merchants** have absolute power over property offered for sale, and therefore **transaction validity**.

These are **orthogonal** aspects of security, not in opposition to each other, but in mutual defense…

…It is true that miners have no **financial incentive** to attack merchants. They are, after all, **engaged in mutually-beneficial trade**.

But miners are **not the threat**. The threat is the state, which has a **strong** financial motivation to destroy the market, and can do so with **sufficient hash power**.



If some part of the **economy** is unsatisfied with the selections of miners it can offer its property for sale in a **split coin** with a different **work rule** that obsoletes specialized mining hardware.

This is typically described as a **proof-of-work hard fork.**

PROOF OF WORK FALLACY

- Buyers can always obsolete specialized equipment by abandoning its product (not unique).
- There is no reason that existing miners would exit, it is common for businesses to rebuild.
- New miners will likely make the same decisions, as they are in the same business.
- Larger miners are disproportionately more profitable and therefore better capitalized.
- Smaller miners operate closer to the margin and will fail as larger miners retool.
- Experienced miners have an inherent advantage, and therefore greater access to capital.
- If the state is attacking, its co-opted miners will continue at a declining energy cost.
- Future miners must insure against a similar event, increasing the cost of hash power.
- The economy ends up with higher fees, the same problem miners and greater centralization.
- It's not a "nuclear option" it's a suicide attack.

So I'll leave you with this. Centralized mining might as well be the **Federal Reserve**.

The fact that Bitcoin doesn't appear to be **under attack** does not mean that it is secure against the **envisioned threat**.

At some point we will need to actually resolve the **pooling pressures** of **proximity** premium and **variance** discount, but that is a talk for another day.

SUMMARY

PERCEPTION

- Miners and merchants are adversarial.
- Mining is controlled by the economy.
- Miners cannot afford to attack.
- Bitcoin is defenseless against the state.
- States cannot ban popular things.
- A PoW change mitigates pooling.
- Authoritarian tx ordering is sufficient.
- Crypto secures Bitcoin.

REALITY

- Miners and merchants are *trading partners*.
- Miner and economic powers are *orthogonal*.
- Miners are *not the threat*.
- Bitcoin *must* defend against the state.
- States *prefer* to ban popular things.
- A PoW change *exacerbates* pooling.
- Resistance to authority *is Bitcoin's innovation*.
- *People* secure Bitcoin.

QUESTIONS