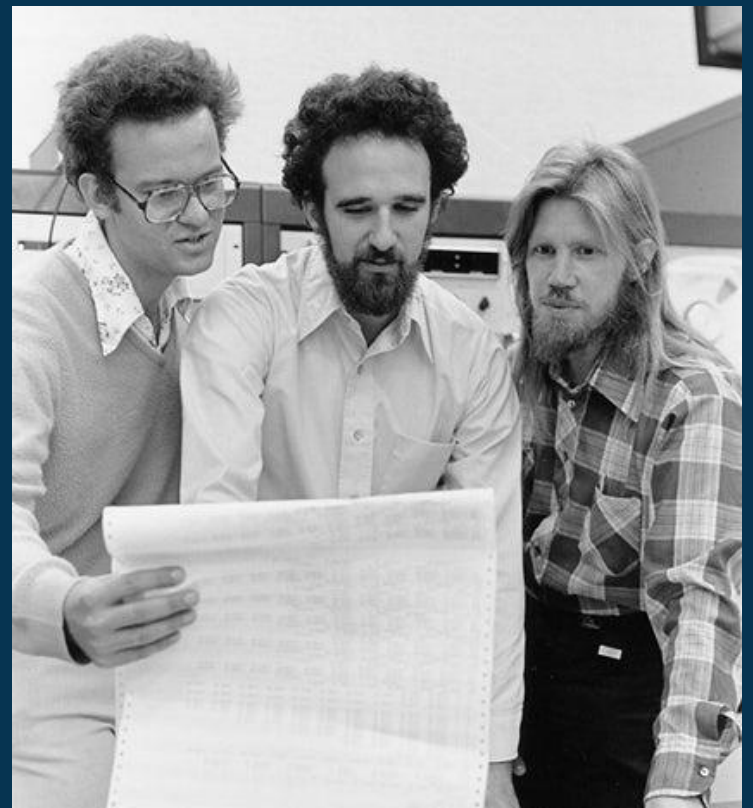
Oregon Blockchain

Week 2: Cryptography & Cypherpunks



OBG Onboarding Fall 22

Homework!

- Did anyone have any trouble getting set up

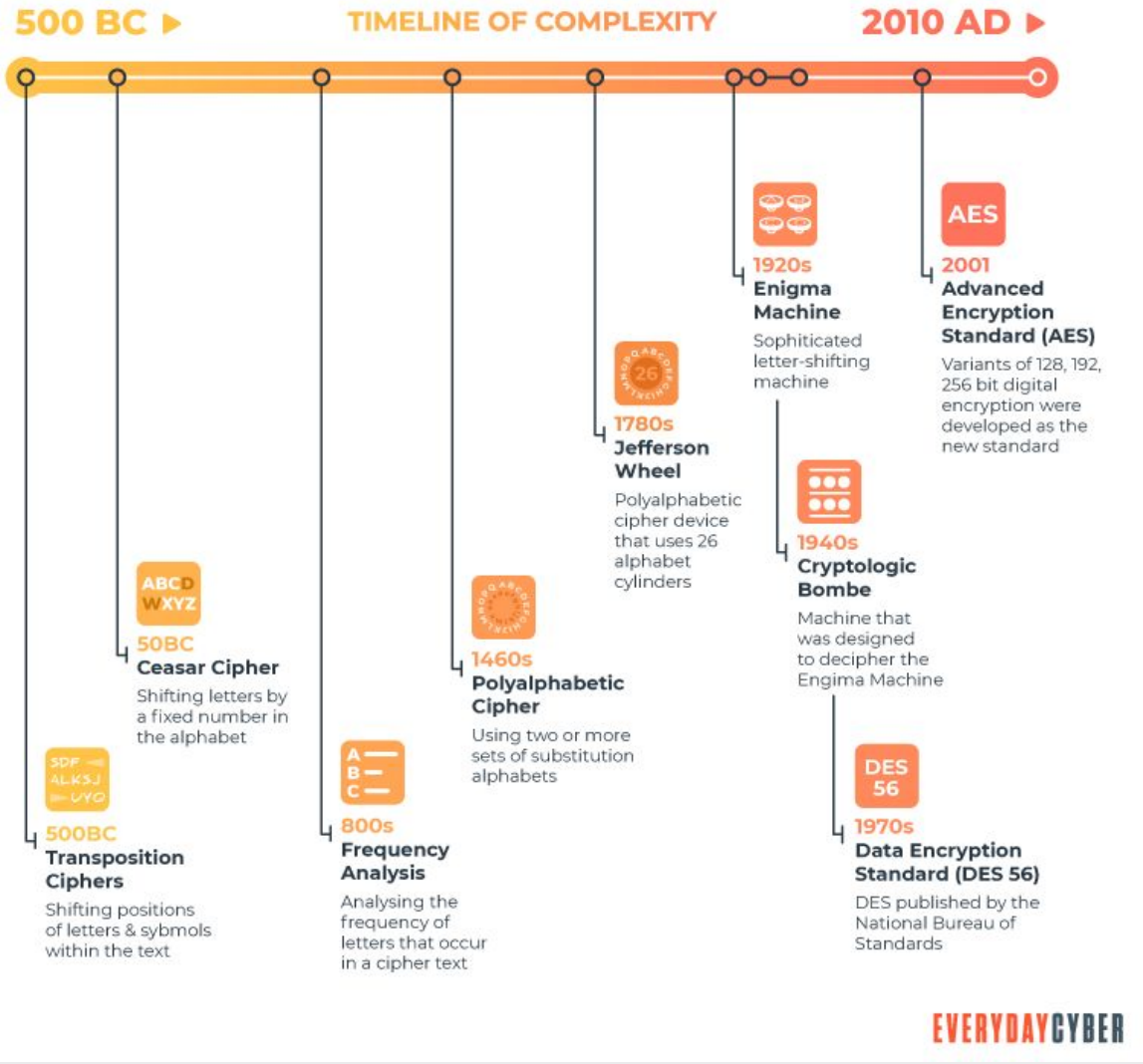
- Share one cool thing you found on twitter

What is encryption

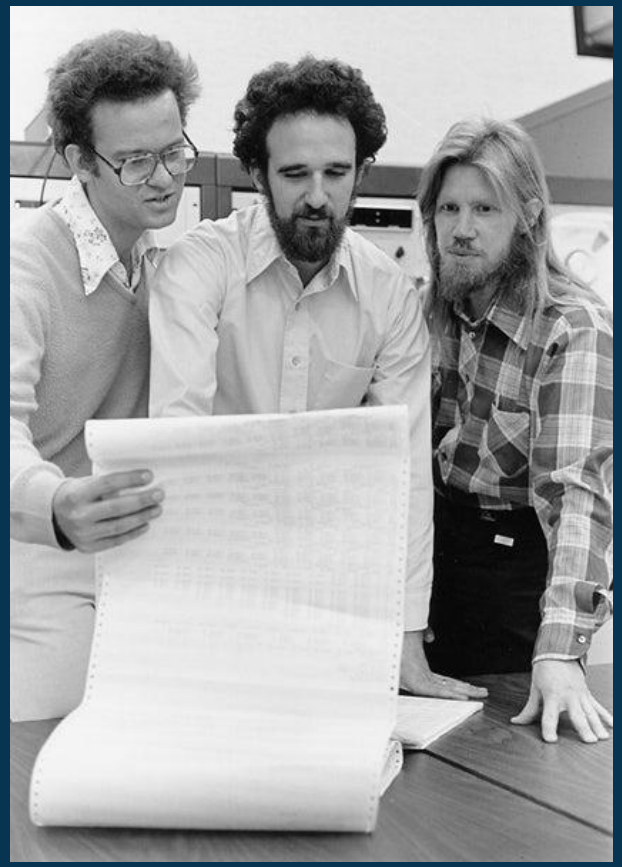
Lets you send sensitive messages out in the public!

- Ancient Egyptian monks to gatekeep knowledge
- Julius Caesar to communicate w/ Generals (would tattoo heads)
- Used really simple ciphers

Governments



Diffie, Hellman, and Merkle,

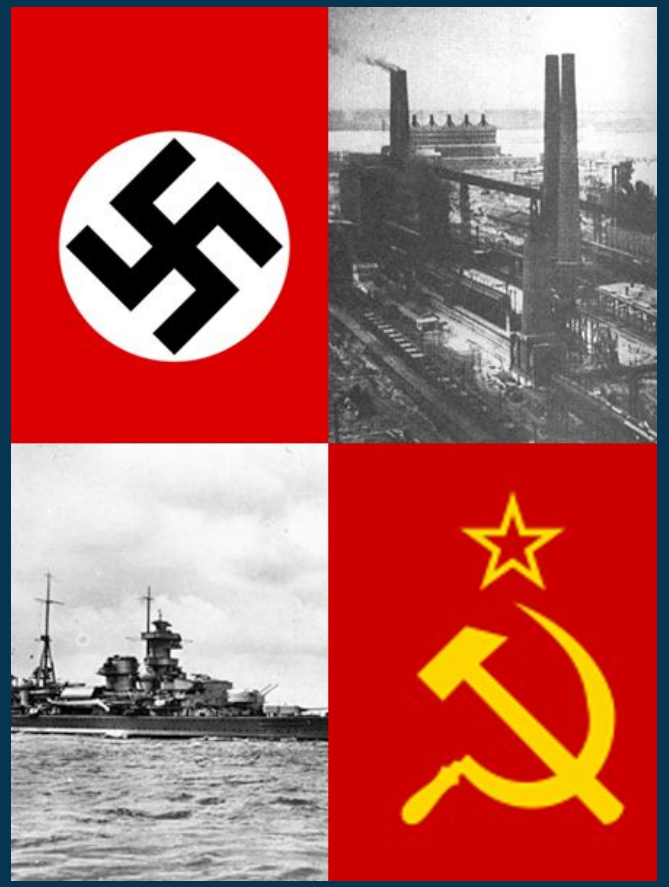


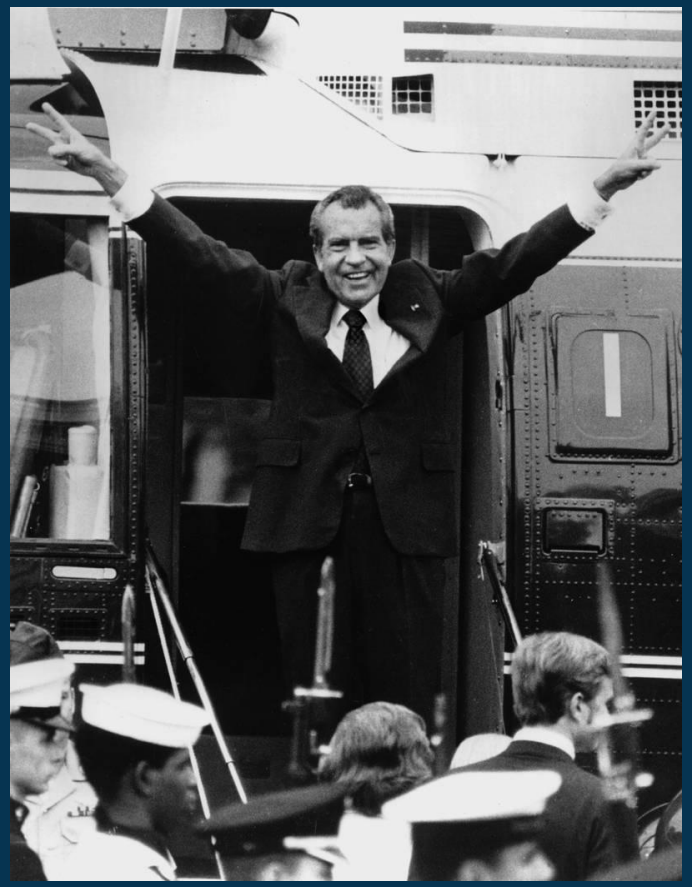
We want to learn this cool shit too!

“We can use cryptography for privacy!” - Diffie, Hellman, and Merkle ~1970s

- Why is it important?
- What happens if we don’t have privacy?
- 2nd order effects of no privacy

MFers were paranoid af





“No you are not allowed”

- Cryptography classified as munitions/military exports
- Need license to handle it
- All work classified by NSA
- You can have DES instead

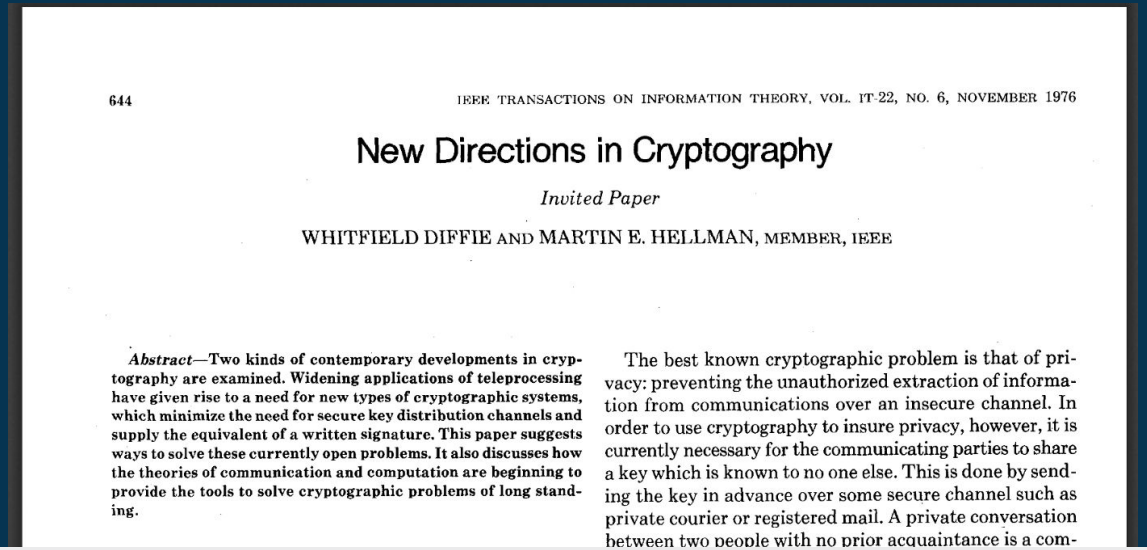
Public Cryptography!

Diffie-Hellman Key Exchange

Powerful public key encryption tech!

“You really shouldn’t publish this paper” - Diffie’s colleagues

“Fk it we ball” - Diffie & Hellman



644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

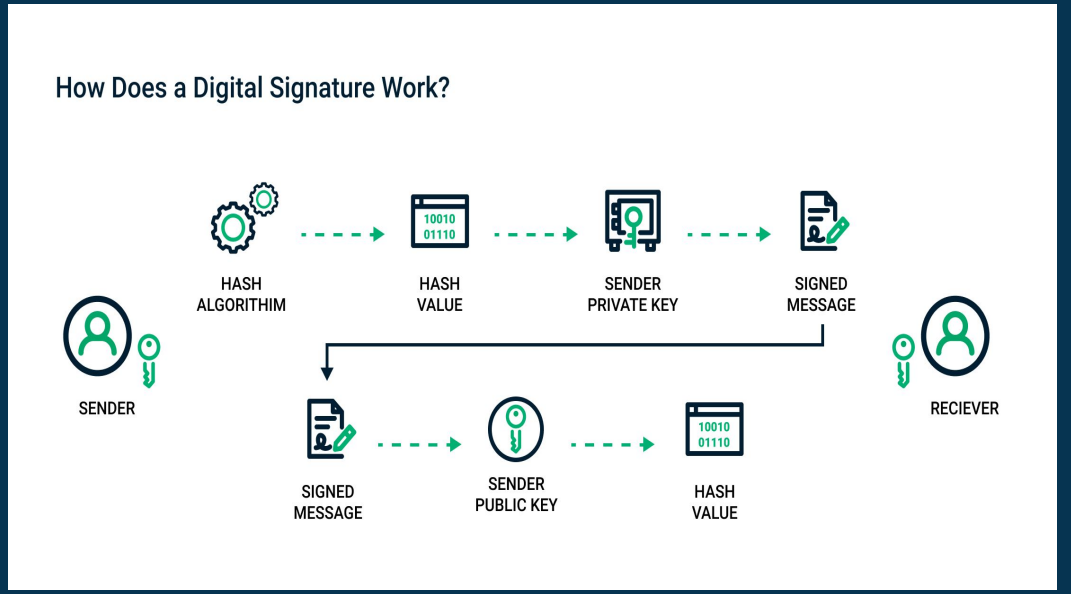
WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Abstract—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a com-

Digital signatures (Eli)

- Verifiable “facts” for the digital world
- Authentication or “proof of interaction”
- Impossible (really hard) to forge or “crack”



Cypherpunks, Crypto Wars, & Censorship

Nerds on a mailing list

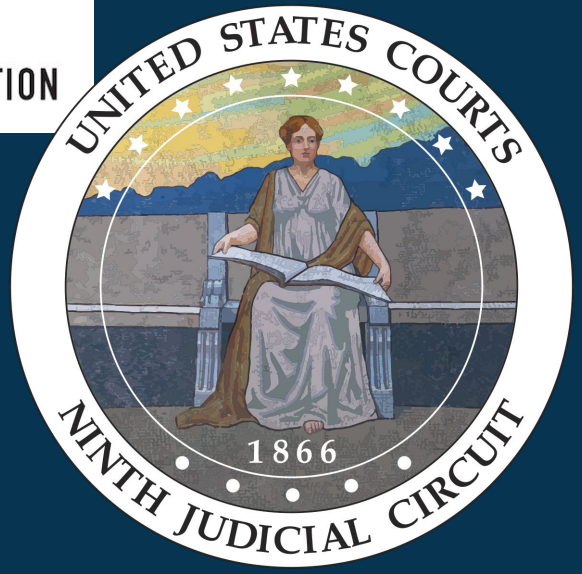
Traffic analysis problem (Metadata)

Decentralized Systems to compliment privacy

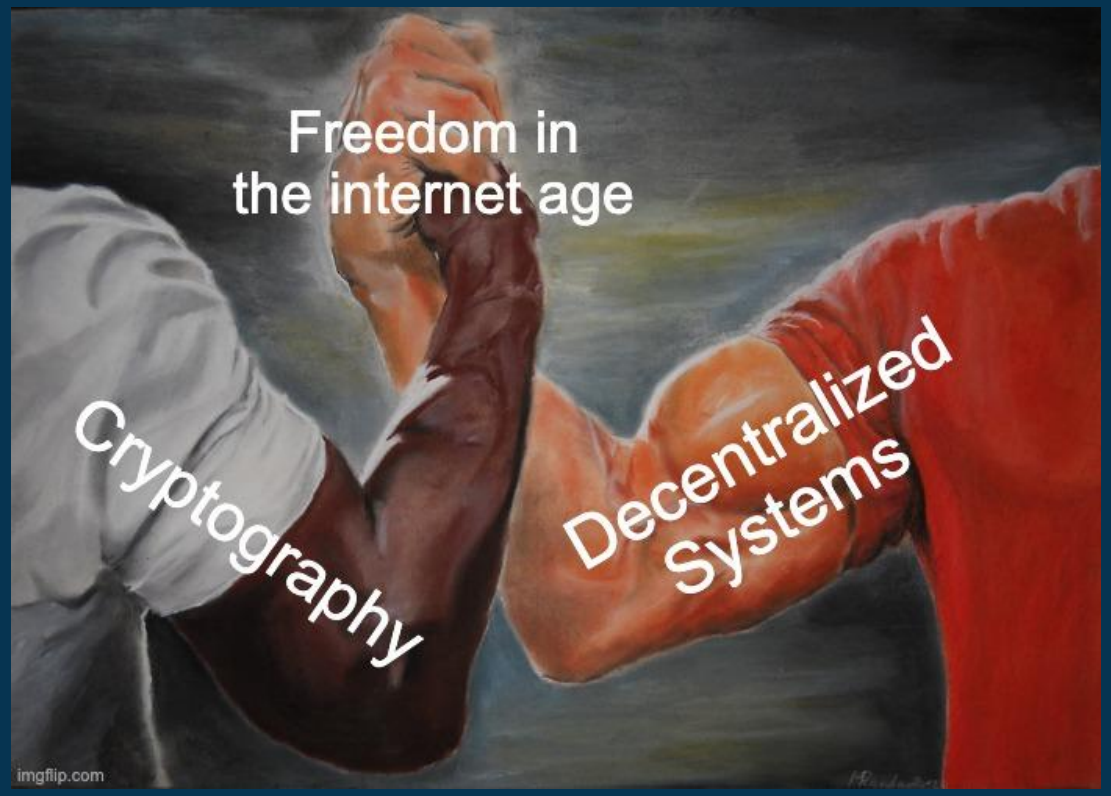
Government no likey!

Bernstein vs. DoJ

ELECTRONIC FRONTIER FOUNDATION



Decentralized Systems to compliment privacy



TorProject.org

WikiLeaks

BitTorrent™

Blockchains are for censorship resistance

satoshi
Founder
Sr. Member

Activity: 364
Merit: 4940

Re: They want to delete the Wikipedia article
July 20, 2010, 06:38:28 PM
Merited by EFS (100), nullius (10), ChiBitCTy (1)

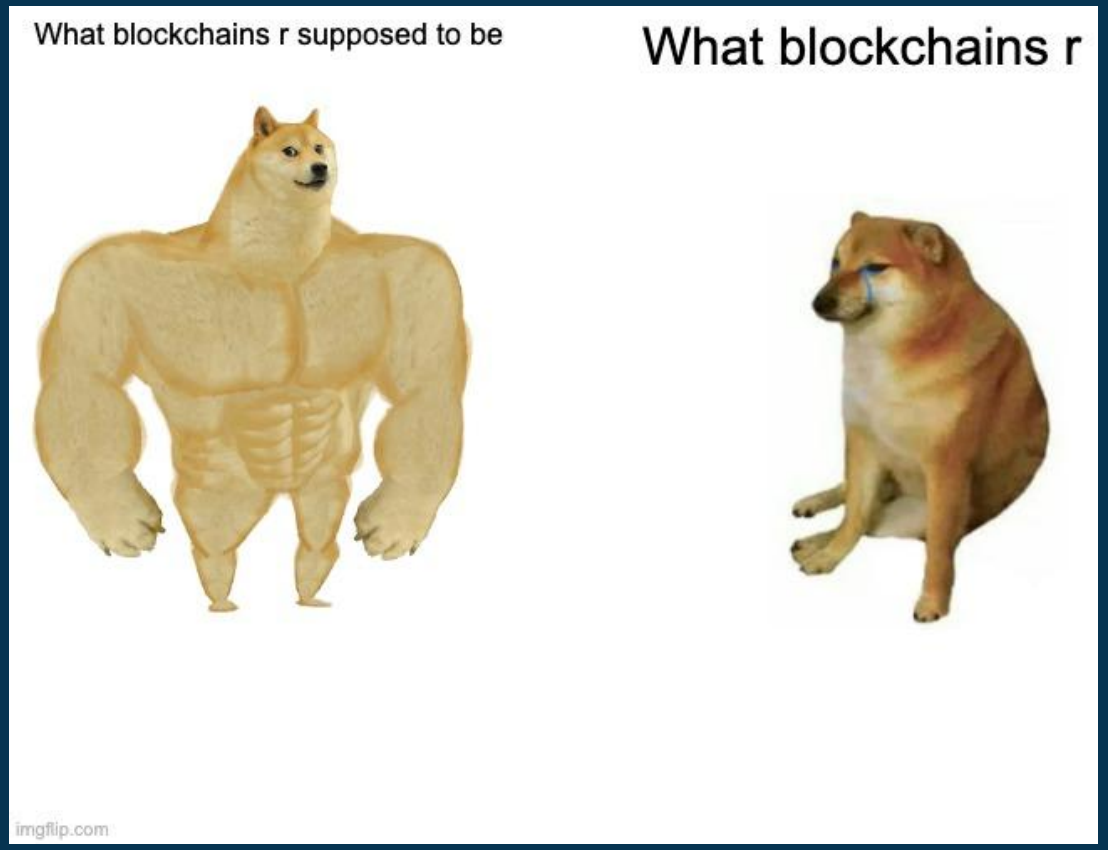
#14

Bitcoin is an implementation of Wei Dai's b-money proposal http://weidai.com/bmoney.txt on Cypherpunks http://en.wikipedia.org/wiki/Cypherpunks in 1998 and Nick Szabo's Bitgold proposal http://unenumerated.blogspot.com/2005/12/bit-gold.html

- Permissionless (anyone can participate at anytime)

- FOSS (don’t trust, verify!)

Blockchains in original context

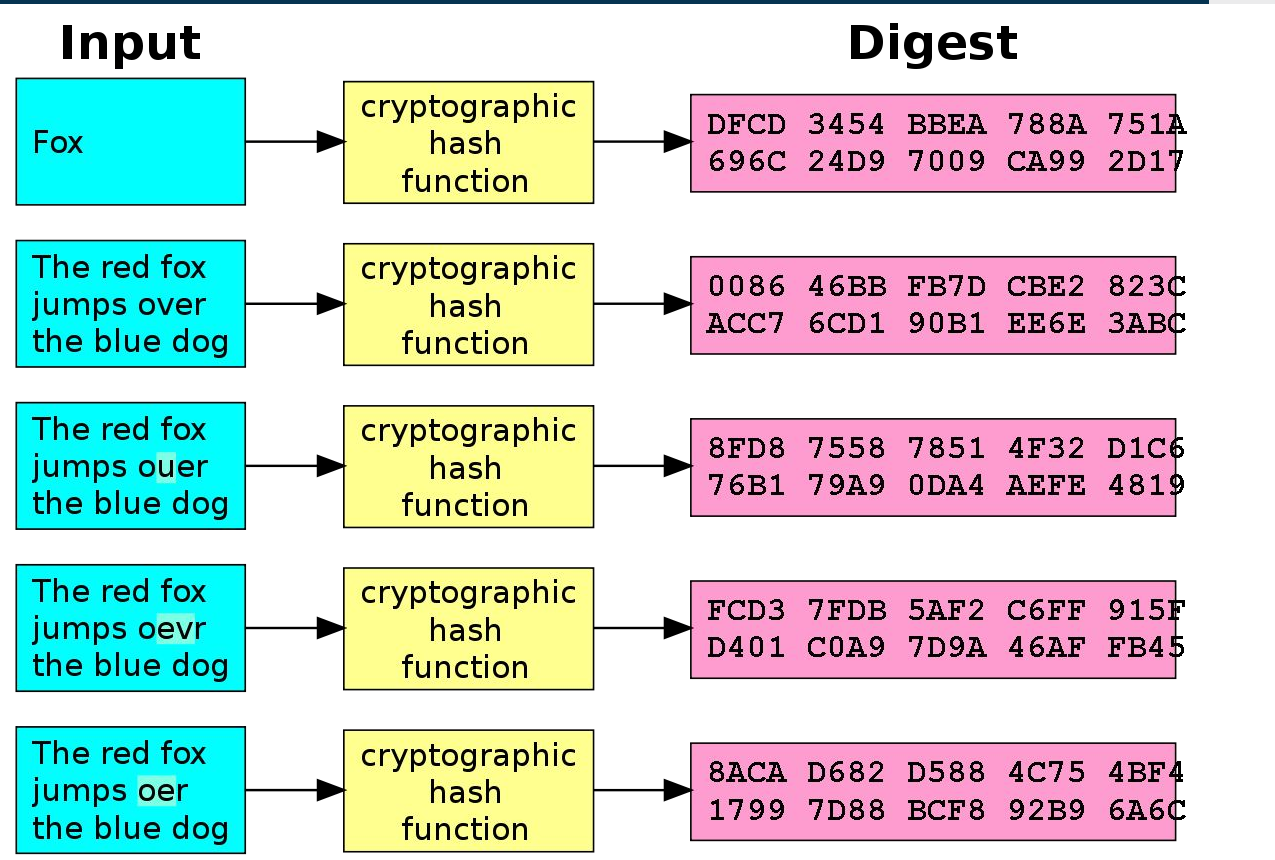


- Everything is transparent
- Lots of financial activity
- Address reuse
- Gud surveillance tool

Cryptographic Primitives (if time permits)

Hashing (Royce)

- Hashing is the process of putting a string through a function that returns a unique string
- Examp: You could fit the library of congress into a 256 bit hash would come out. But if you change one letter the hash would completely change



Deriving a hash

- Trapdoor function - easy to go from starting point to ending point (hash).
- But it’s hard to from ending point to the being point.

Future Primitives (Eli)

FHE

- Computation on encrypted data
- Users retain privacy*

MPC/DKG

- Using *distributed* systems to perform cryptographic ops
- Form of consensus “built-in”

Next week

Learn how blockchains
actually work!

- Come up with 5 apps on your phone/computer that use cryptography

https://www.youtube.com/watch?v=NmM9HA2MQGI&ab_channel=Computerphile

- Mess around with Sha256 online