CS 581: Blockchain Science and Technology

January 5, 2024

Course Objectives

> Bitcoin is the first decentralized cryptocurrency. Nodes in the peer-to-peer bitcoin network verify transactions through cryptography and record them in a public distributed ledger, called a blockchain, without central oversight
>
> *Wikipedia*

Course Objectives

> Bitcoin is the first decentralized cryptocurrency. Nodes in the peer-to-peer bitcoin network verify transactions through cryptography and record them in a public distributed ledger, called a blockchain, without central oversight
>
> *Wikipedia*

Understand each of those “features”, the tradeoffs involved and generalize when possible.

Lecture Plan

- Currency/Money

Lecture Plan

- Currency/Money
- Permissionless Digital Identity

Lecture Plan

- Currency/Money
- Permissionless Digital Identity
- Hashing

Currency

- Everyone deposits their assets at a central godown.

Currency

- Everyone deposits their assets at a central godown.
- The godown issues certificates.

Currency

- Everyone deposits their assets at a central godown.
- The godown issues certificates.
- People trade the certificates.

Currency

- Everyone deposits their assets at a central godown.
- The godown issues certificates.
- People trade the certificates.
- Anyone can redeem the certificates for the underlying anytime.

Currency

- Everyone deposits their assets at a central godown.
- The godown issues certificates.
- People trade the certificates.
- Anyone can redeem the certificates for the underlying anytime.
- Standardize the certificates.

Currency

- Everyone deposits their assets at a central godown.
- The godown issues certificates.
- People trade the certificates.
- Anyone can redeem the certificates for the underlying anytime.
- Standardize the certificates.
- Build electronic exchanges for trade.

Simplified Currency

- Just one type of asset!
- The certificate contains just a number.

Ledger for currency(First Attempt)

Universal Cash Positions

Name	Value	Remark
Aadarshraj	35	
Amjad	87	
Gunjan	-43	
Harsh	-34	

Digital Identity via PKC

We can find e, d and n such that

$$(m)^{ed} \equiv (m) \mod n$$

Digital Identity via PKC

We can find e, d and n such that

$$(m)^{ed} \equiv (m) \mod n$$

Knowing e, and n such that doesn't help in computing d.

RSA Cryptosystem

- Choose large primes p and q. Let $n = pq$
- Choose large d s.t $gcd(d, \phi(n)) = 1$.
- Fix e as inverse of d $(\mod \phi(n))$

$$(m)^{ed} = (m)^{k*\phi(n)+1} = (m^{\phi(n)})^{k} \times m = m \mod n$$

Immutability via Hashing

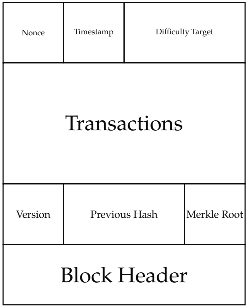
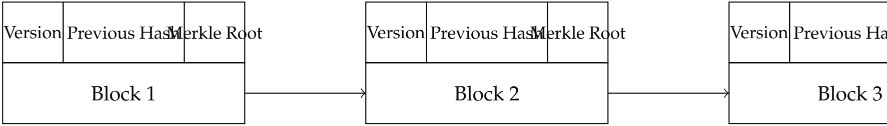


Figure: Bitcoin Block Structure


Version

Previous Hash

Merkle Root

Block 1

Version

Previous Hash

Merkle Root

Block 2

Version

Previous Ha

Block 3

Figure: Bitcoin Blocks with Zigzag Pointers