RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: MASH-R04

Dissecting Bitcoin Security

Cassio Goldschmidt
Principal Info Sec Leader
NCR
@CassioGold

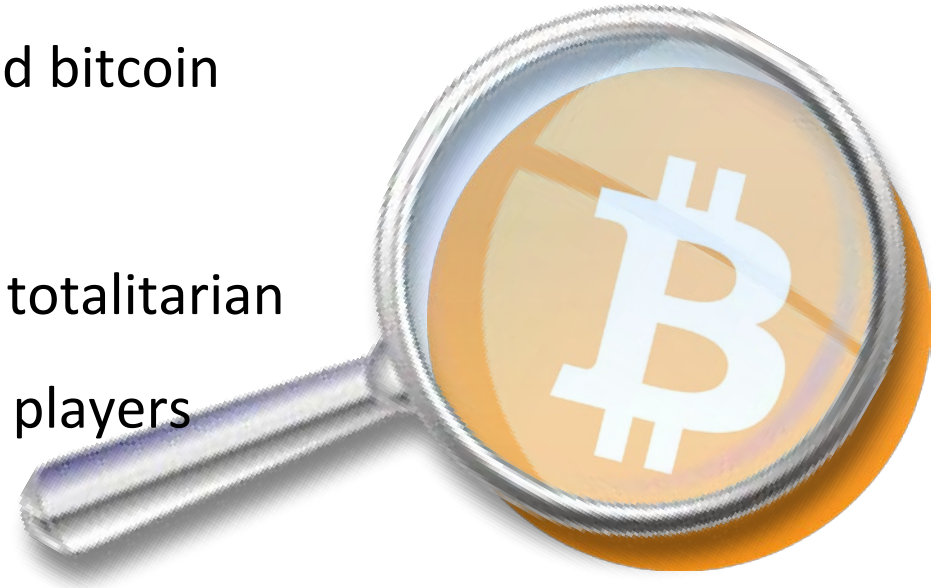
#RSAC

Bitcoin Technology is Game Changer

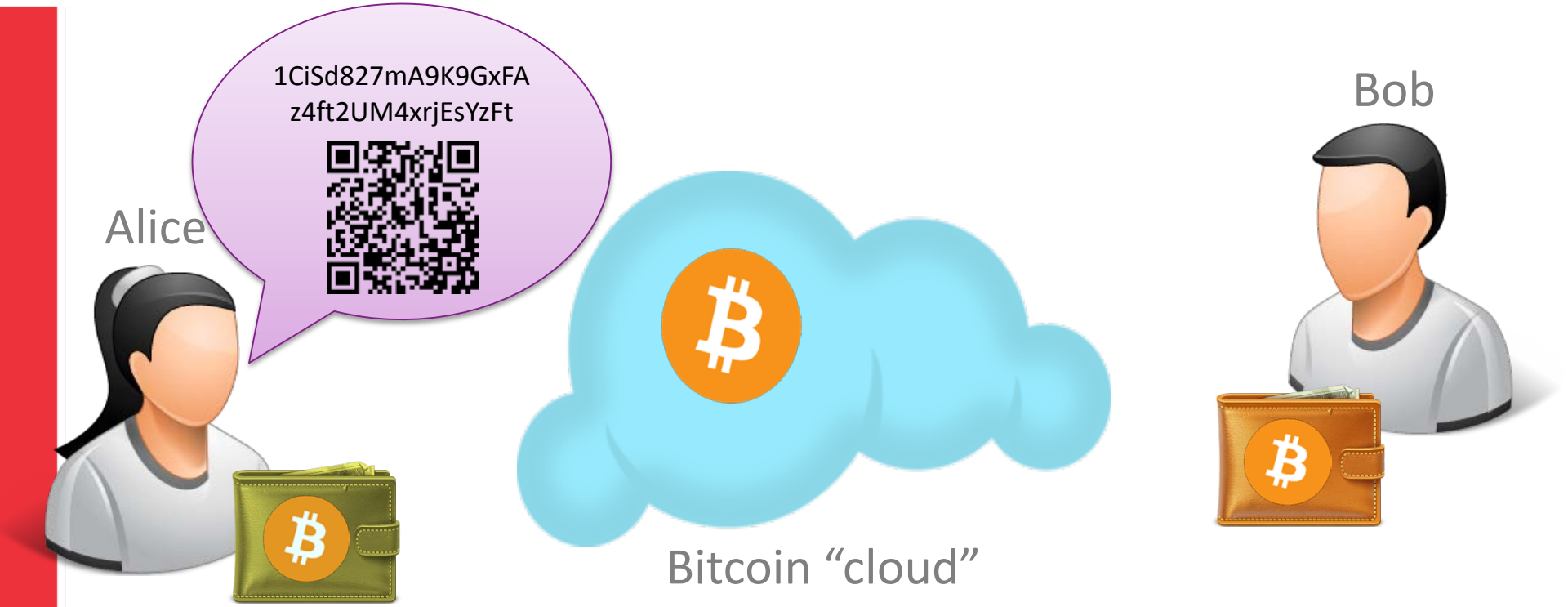
- Bitcoin != bitcoin
- Decentralized != distributed
  - Censorship Resistant
- Permission-less
- Public transactions
- Immutable record
- Standardize way to talk money
- Programmable money (for BTC)

At the End of This Talk You Will Understand

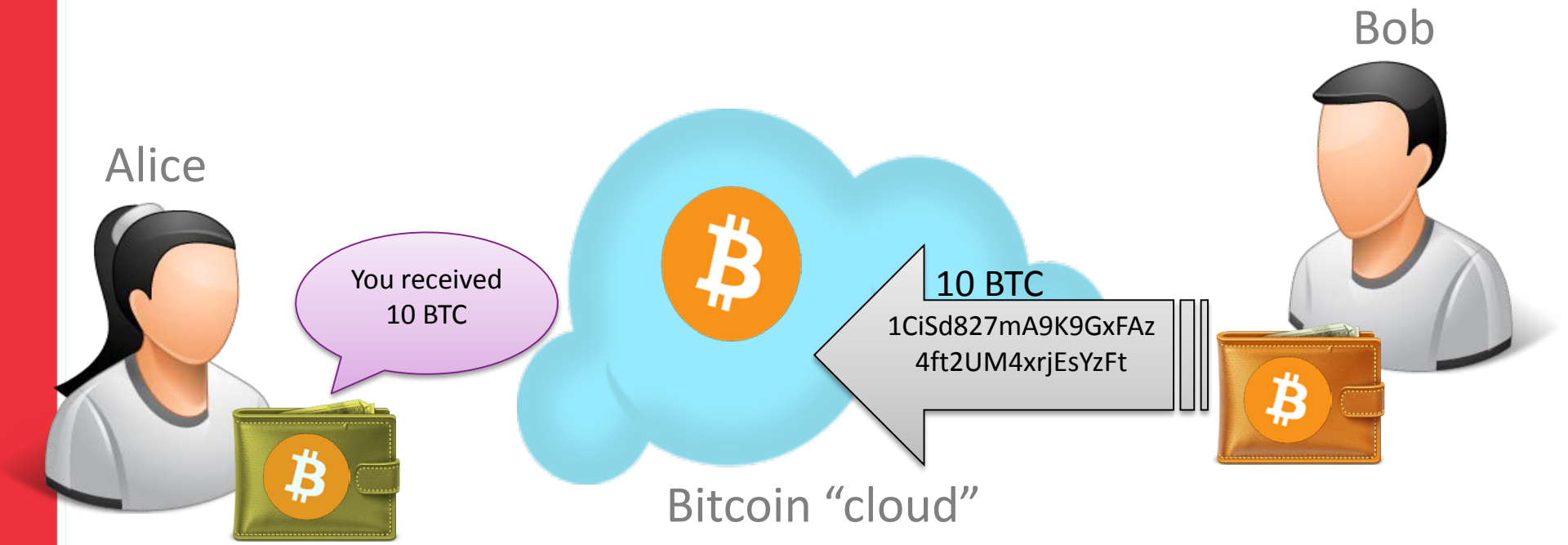
- The main components behind bitcoin
- How security is built in
- How libertarian can become totalitarian
- Why it's game over for small players
- Concerns around security
- How the technology can be repurposed



Bitcoin Overview
Bob Sends 10 BTC to Alice



Bitcoin Overview
Bob Sends 10 BTC to Alice



Bitcoin Misconceptions

Users

Coins

Wallets

Pay to Public Key - P2PKH
Bitcoin Addresses Are Derived From Public Keys

1. Randomly generate a 256 bit number
2. Generate public key using bitcoin's ECDSA curve.
3. Public Key ➔ SHA256 ➔ RIPMD160 ➔ Base58 encode it (plus prefix + checksum).
4. 1CiSd827mA9K9GxFAz4ft2UM4xrjEsYzFt

Pay-to-Script-Hash (P2SH)

- Pay to a script matching the hash, a script that will be presented later when this output is spent

One of Two Signatures

Joint account

Backup

Two of Three Signatures

Business Partners

Extra Security

P2SH Example: Bob Pays Alice 10BTC
Alice Creates a P2SH address

Step 1 – Alice Creates Redeem Script

= <OP_1> <A pubkey> <B pubkey> <OP_2> <OP_CHECKMULTISIG>

Redeem Script

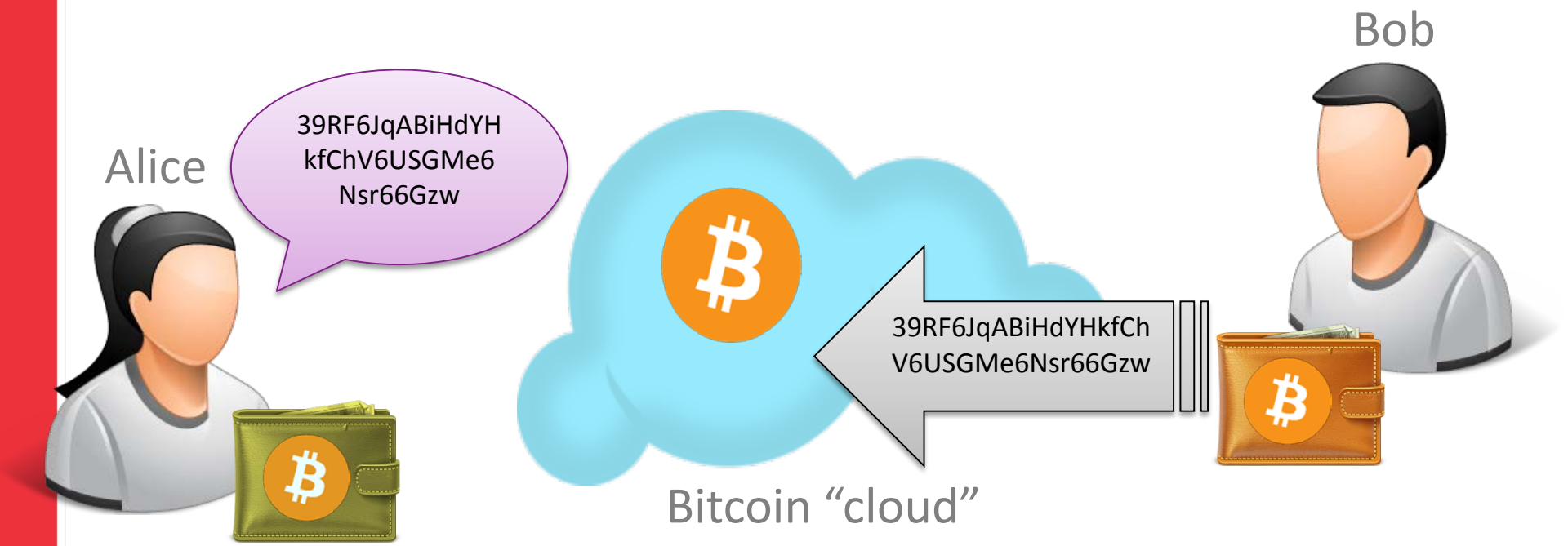
Step 2 – Alice Creates Address by Hashing the Script

Hash → To Address

Script Address

3 9RF6JqABiHdYHkfChV6USGMe6Nsr66Gzw

P2SH Example: Bob Pays Alice 10BTC
Bob Pays Alice, Exactly Like He Did Before



P2SH Example: Bob Pays Alice 10BTC
To Spend the funds, Alice needs to provide…

Alice

The Original Script

Signature for “A” Pubkey or “B” pubkey

Bitcoin Wallets
Types and Functions

Client Side Wallets

Application that **runs in your PC**. Can contain the entire blockchain. You manage and secure keys.

- Old backups can disclose current keys
- Incomplete wallets may disclose transaction information

Web Wallets

Your keys are **stored on the web** and protected by a 3rd party. Sometimes they look like banks

- Centralization ➔ big target ➔ breach

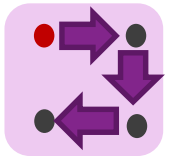
Bitcoin Wallets Implementation

Non Deterministic (random) wallets

Just a **bunch of keys**

Need to back up keys frequently

Deterministic (Seeded) wallets



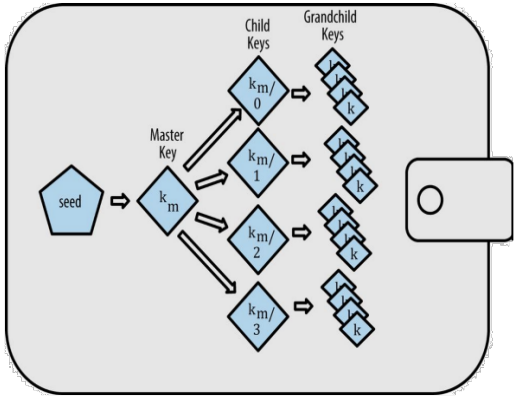
Seed + index or chain code is used to derive the private keys

All keys can be recovered with the seed

Bitcoin Wallets Implementation

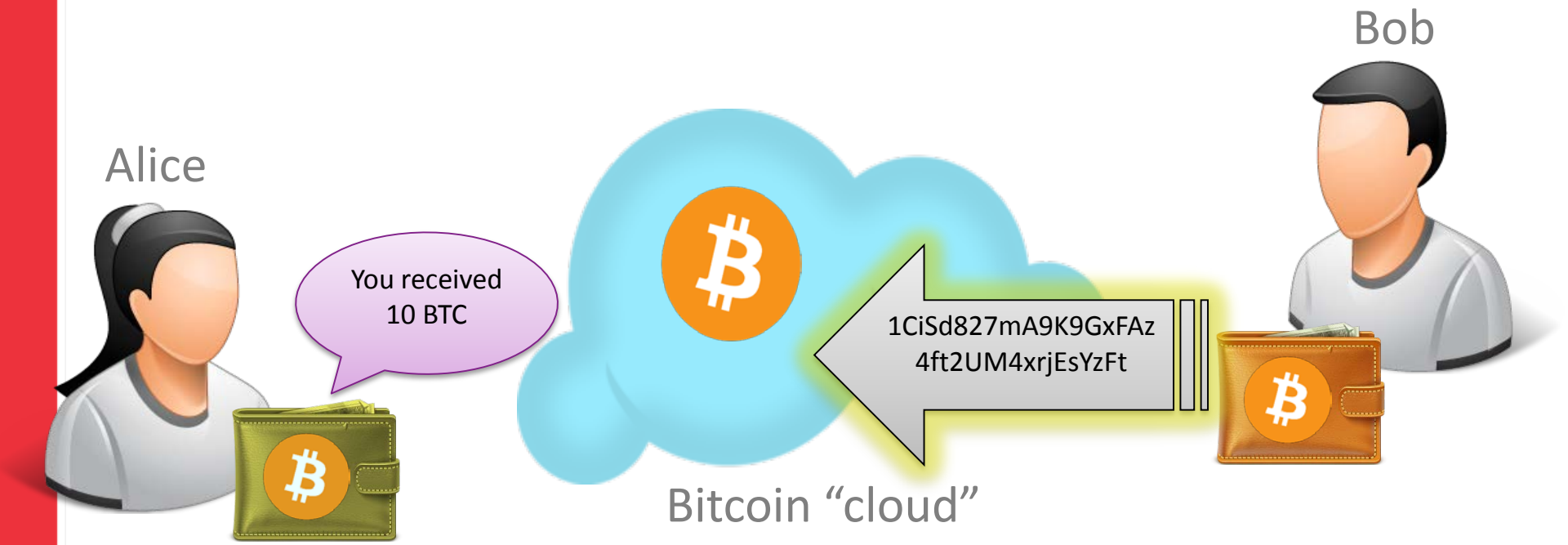
Hierarchical Deterministic (HD) Wallets (BIP-44)

- Parent key can derive a **sequence of children keys**
- Branches can be used to **only receive or to only spend funds**
- User can **create public keys without having access to private keys**



Graphic: Antonopoulos, Andreas M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies

Bitcoin Overview
How Payments (transactions) Work?

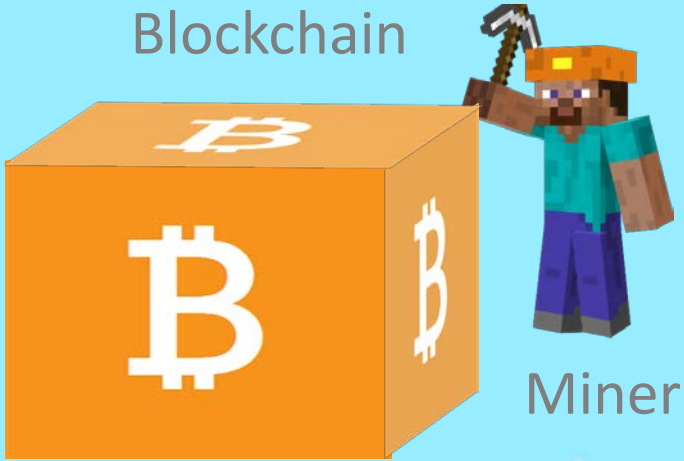


How Payments Work?
Essential Transactions Structure Overview

One or more inputs:	Unspent transactions Public Key, Signature
One or more outputs:	Addresses to pay, BTC
Timestamp:	<time, date>

- Clear text transmissions allows for **Packet Sniffing** and **Sibil attack** (i.e. connect to fake nodes)
- Transactions can contain arbitrary data ➔ could be used for exploit

Bitcoin Overview
A Peek Inside the “Cloud”



Bitcoin Overview
A Peek Inside the “Cloud”

The Job of miners

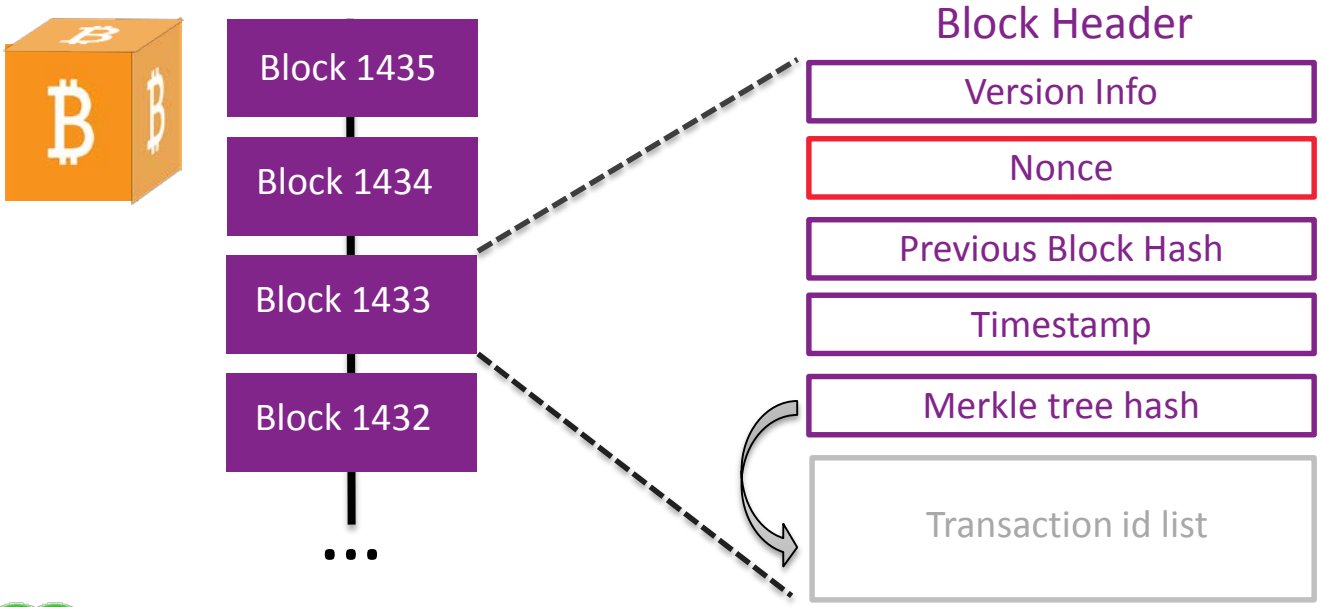
- **Validate** new **transactions** and **the work of other miners**
- **Record the work** in the blockchain
- Rewarded fees
  - Earn BTCs for successfully mined blocks (coinbase transactions)
- **Proof of work**

⚠ 50% attack?

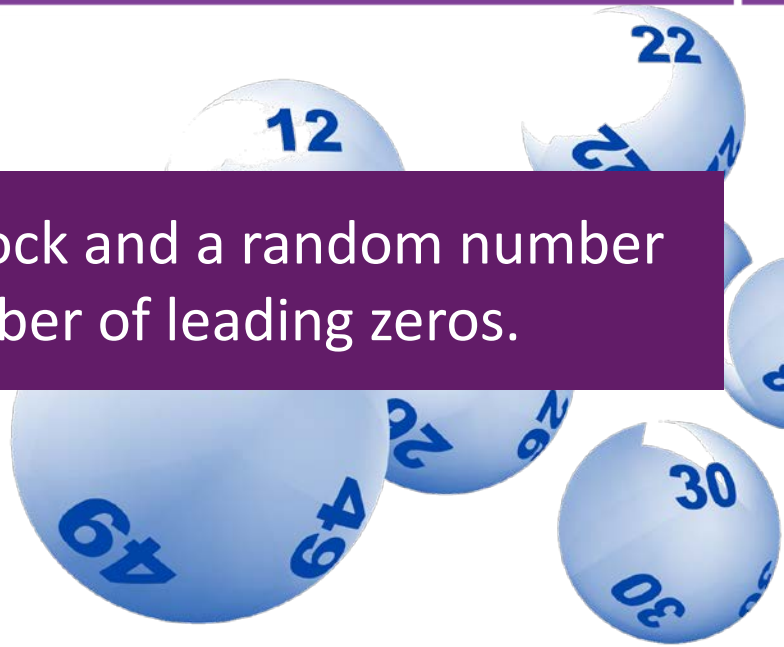
⚠ Resolved block does not need to be delivered immediately; Time sync issues

Bitcoin Overview
Blockchain

Simplified Block Structure



Proof of Work
Like a Lottery or a Game of Sodoku



Proof of Work

Repeatedly hash the header of the block and a random number until the hash has a certain number of leading zeros.

- A **hard to solve** problem
- But **easy to verify** the result!
- **Keeps the generation of new bitcoins constant!**

Apply - Alternative Uses for the Blockchain

Namecoin

A decentralized key-value registration and transfer platform using a blockchain. **Alternative DNS**.

Notary Services

Blockchain based solutions to store a **proof of existence**

Ethereum Frontier

Decentralized platform to create your own blockchain app.

Apply – Lessons learned from bitcoin

- **Bitcoin Addresses**
  - Asymmetric system, protected keys, base 58, decentralization
- **Wallets**
  - Key management, entitlement
- **Transactions**
  - Higher integrity
- **Proof of work**
  - DDoS protection

In Conclusion

- Bitcoin is an invention with multiple uses
- Different security models
- Technology can be used in a open or closed way

- It’s evolving fast… with a lot more to come!

Thank You!
Questions & Answers

@CassioGold

NCR