Block Chain 101

CONFIDENTIAL

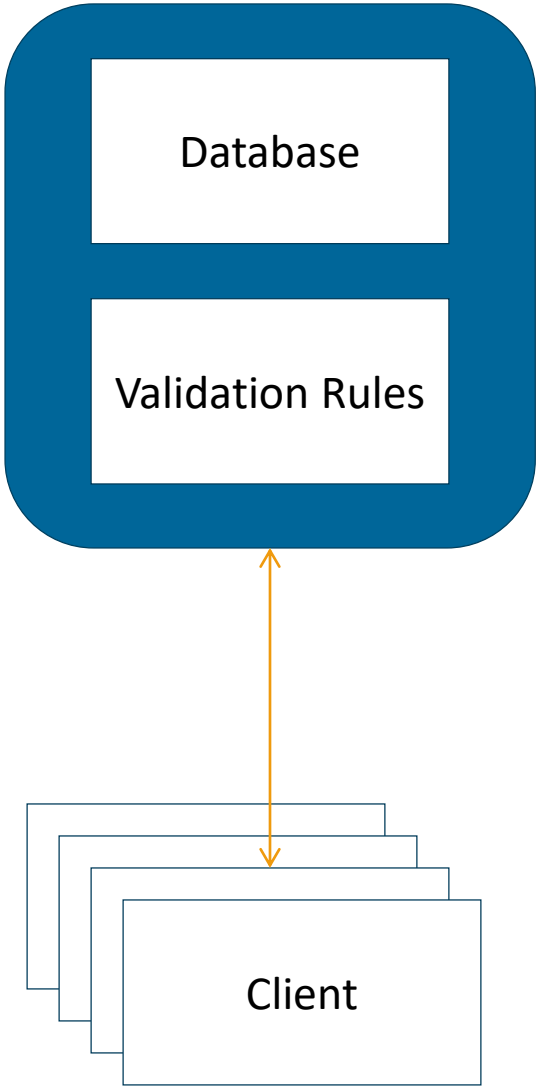
ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

May 2017

Goals

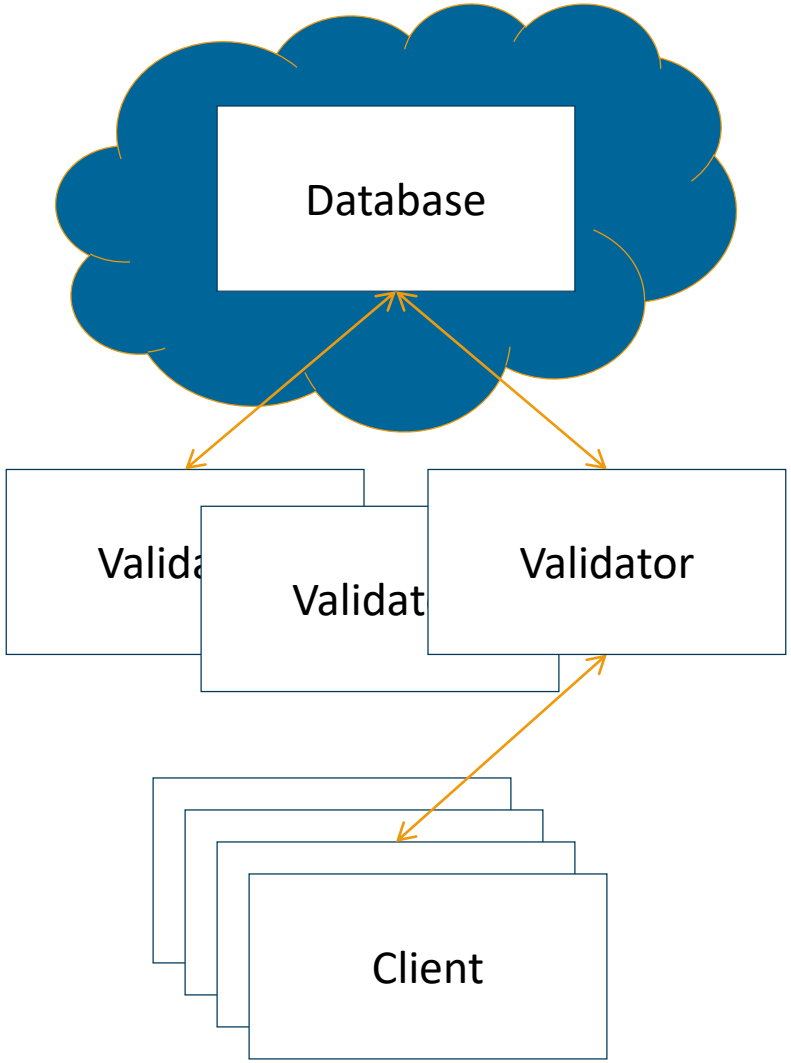
- Get a technical understanding of:
  - Blockchain technology
  - Bitcoin and other crypto currencies
  - Smart contracts
- Why they are important and how cryptography enables these mechanisms

What do block chains replace?



- Access protected writes to an authoritative database
- Transactions, time stamping, contracts, etc.

What do block chains replace?



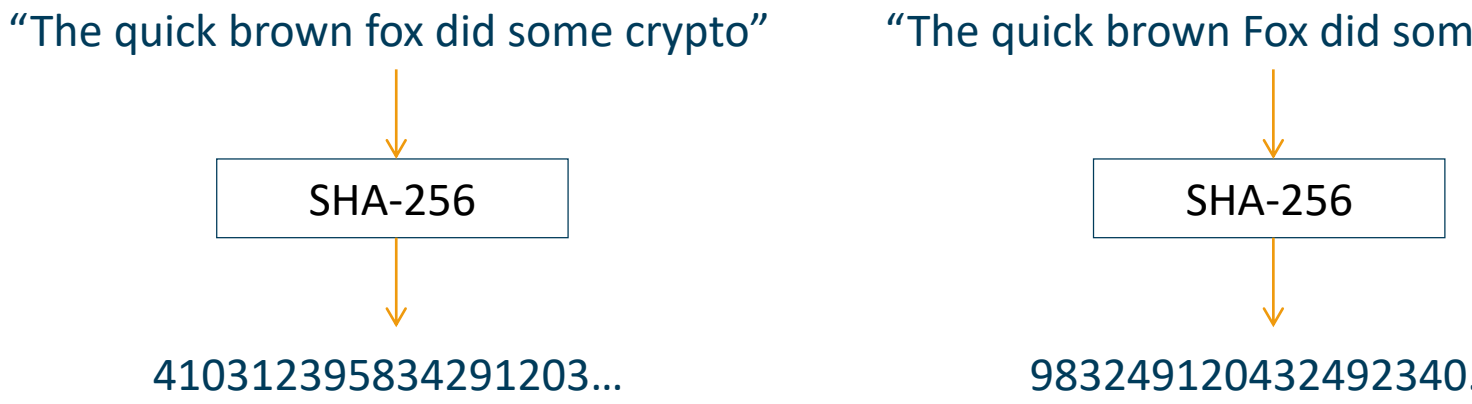
- Authoritative access control replaced with distributed consensus
- Database state dependent upon majority agreement of update validity

Trust

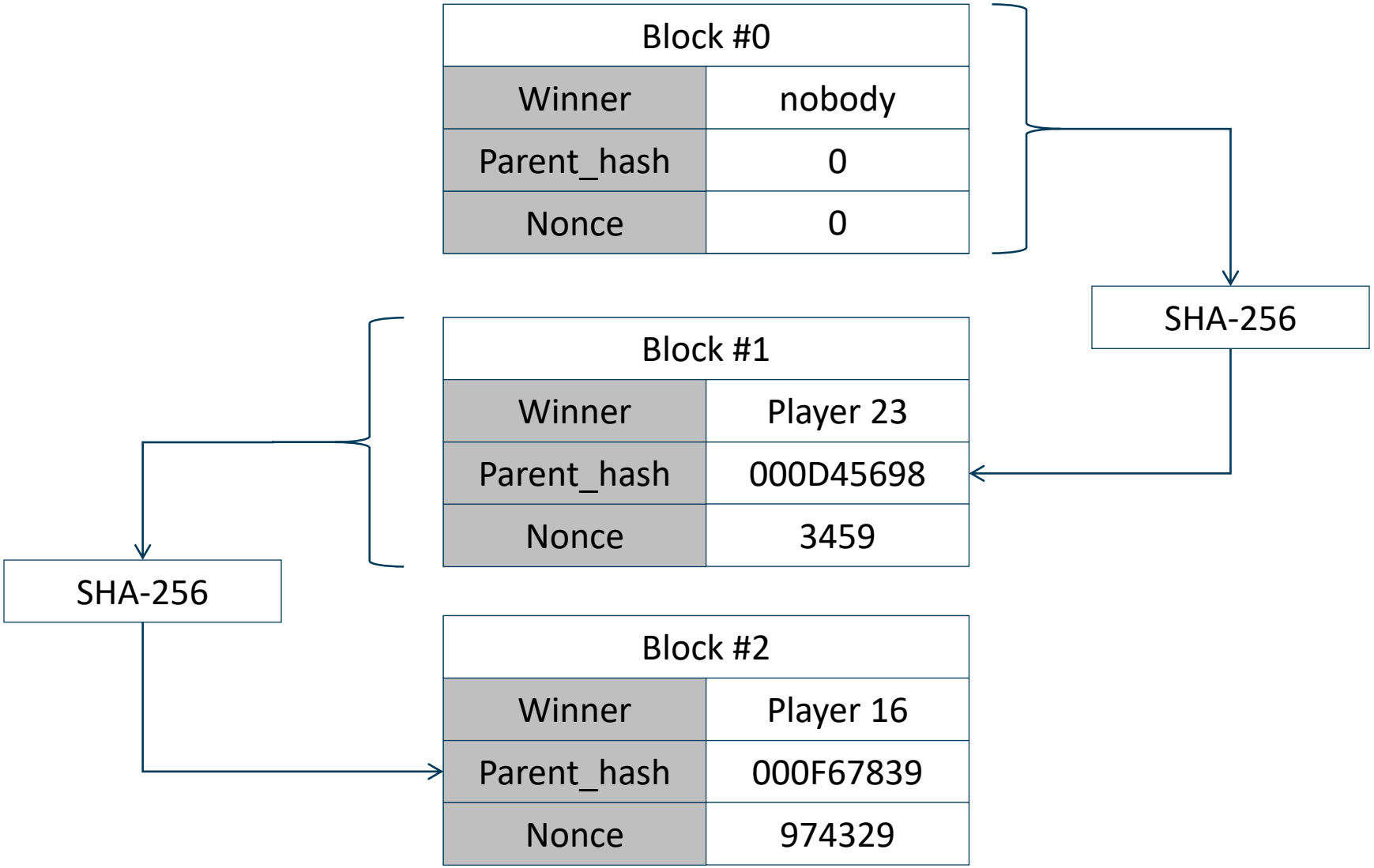
- Distributed consensus allows:
  - Parties to trust each other without knowing each other
  - Completely unambiguous rules about validity
  - Removing authentication and identity

Hashes

- A hash function (like SHA-256) takes a block of data in, and produces an effectively random fixed size number.
- Any change to the input randomizes it



The Chain


Block #0
Winner
nobody
Parent_hash
0
Nonce
0
SHA-256
Block #1
Winner
Player 23
Parent_hash
000D45698
Nonce
3459
SHA-256
Block #2
Winner
Player 16
Parent_hash
000F67839
Nonce
974329

What about cheaters?

- Make a fake hash
- What happens then?
  - The algorithm will fail
  - Other participants will not use your block, making it not part of the chain

Solving the Bitcoin puzzle

- Miners “create” bitcoins (or other tokens)
- Transactions send value (bitcoins) from key to key
- The blockchain prevents overspending without the need for a central authority
- Crypto currency code can only change by miner consensus
- Consensus replaces authority
  - Number of tokens in Bitcoin is limited to 21 million
  - Reward per block
  - Mining difficulty grows

Where are the rules?

- The laws of Bitcoin (or any blockchain) are coded in the miner nodes
- Decisions are made collectively by the miners
  - If 51% of the miners agree, the decision is valid
  - This includes each individual transaction
- The source of the node is law
- How do you change rules?
  - We want to add more coins
  - We want to change the block format

Take over

- What happens if you obtain the majority of mining power?
  - Ability to approve your own transaction

  But

  - The value of Bitcoin will most likely become zero

Operational Realities

- Assumes cheap storage and networking
  - Nodes store every transaction ever
  - Transactions and blocks are broadcast
  - Might limit scale...
- Transactions are slow
  - To verify a transaction, have to wait for a public block
- Control of private keys is crucial
  - Lose your private key: unspendable coins
  - Steal your private key: stolen coins
  - Blacklisting keys breaks the block chain

Beyond Bitcoin

- Transactions don’t have to just be transactions
- Transactions can contain:
  - Executable code
    - In fact, BTC transactions are scripts
    - Scripts specify when outputs can be spent
  - Contracts
    - Set conditions for allowing outputs to move
  - Random data to be time stamped
    - “Colored coins” – add data to a transaction
    - Transaction is recorded, so can be a hash of a document or other external data

Private Chains

- Require signed blocks
- Limit miners to some authorized set
- Useful for adding other rules or preventing block “takeovers”
- Approach being used to trade securities on a blockchain
- Same crypto physics apply….

For More Information

- Blockchain.info – a view onto the BTC chain
- Ethereum.org – blockchain programming
- Hyperledger.org – standards for blockchains
- R3CEV.com – bank consortium for chains
- Bank of England Distributed Ledgers
  - http://www.bankofengland.co.uk/banknotes/Pages/digitalcurrencies/default.aspx