IT486 v3.0: Blockchains and Cryptocurrencies

Bitcoin blockchain

Proof of Work

- Puzzle: find a nonce such that

$$hash(nonce \parallel transaction\ data) < Target$$

Proof of Work

- Puzzle: find a nonce such that

$$hash(nonce \parallel transaction\ data) < Target$$

- The hash function is "puzzle hard":
    - given d and (small enough) T, it is hard to find n such that $hash(n \parallel d) < T$.

Mining hardness

- The total hashpower being contributed to the system varies with time
- If the cost to the solver decreases, the system becomes easier to attack

Mining hardness

- The total hashpower being contributed to the system varies with time
- If the cost to the solver decreases, the system becomes easier to attack
- Bitcoin's approach
  - Set the puzzle difficulty so that the expected time to find a solution is 10 mins (a constant)
  - Periodically change the difficulty so as to try to maintain this expected time

The coinbase transaction

- the first transaction in the block
- does not consume (spend) previous unpsent outputs contained in the blockchain
- Creates bitcoins from nothing
  - a single dummy input not linked to any output
  - the sum of the outputs is equal to the block reward + the transaction fees
  - output addresses: one or more of the miner's own bitcoin address

Block reward

- Increases the total supply of bitcoin in circulation while slowly distributing them over time
- When BTC first started, the block reward was 50 BTC

Block reward

- Increases the total supply of bitcoin in circulation while slowly distributing them over time
- When BTC first started, the block reward was 50 BTC
- Every 210,000 blocks (or approx. 4 years), the block reward halves
  - 2012 → 25 BTC
  - 2016 → 12.5 BTC
  - 2020 → 6.25 BTC
- By 2056, the reward will be about 0.0125 BTC

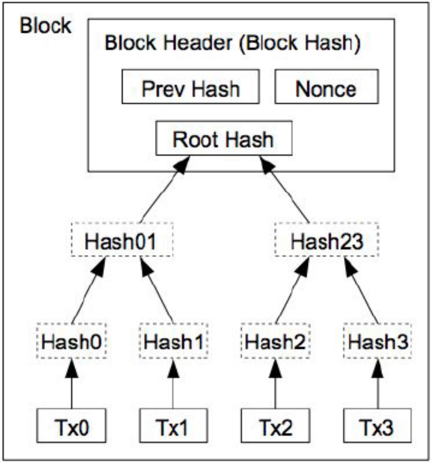
Block reward

- Increases the total supply of bitcoin in circulation while slowly distributing them over time
- When BTC first started, the block reward was 50 BTC
- Every 210,000 blocks (or approx. 4 years), the block reward halves
  - 2012 → 25 BTC
  - 2016 → 12.5 BTC
  - 2020 → 6.25 BTC
- By 2056, the reward will be about 0.0125 BTC
- At that point, miners will mainly profit from collecting transaction fees

Structure of a block

- a header (80 bytes) consisting of three sets of metadata
  - a hash of the block header of the previous (last added) block of the blockchain
  - information related to PoW
  - root of the Merkle tree summarizing all the transactions in the block
- a list of transactions that make up the bulk of its size
  - almost 1000 times larger than the block header

Structure of a block



Transactions Hashed in a Merkle Tree

Identifying blocks

- How to identify a block uniquely within the blockchain?
- By the block hash
  - computed by each node as the block is received from the network
  - not actually stored inside the block
  - not computed when the block is transmitted on the network

The genesis block

- Blocks have to reference their predecessor
- How does a blockchain start?

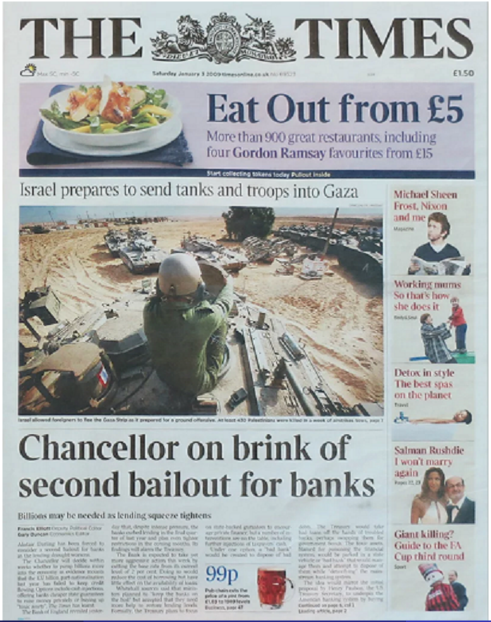
The genesis block

- Blocks have to reference their predecessor
- How does a blockchain start?
- Bitcoin's genesis block
  - mined at 2009-01-03 18:15:05
  - references a previous block with hash 0
  - created the first 50 BTC of mining reward

The genesis block

- Blocks have to reference their predecessor
- How does a blockchain start?
- Bitcoin's genesis block
  - mined at 2009-01-03 18:15:05
  - references a previous block with hash 0
  - created the first 50 BTC of mining reward
- Satoshi included a message in the coinbase txn of the genesis block

Data contained in the genesis block



THE TIMES

Max 5C, min -5C Saturday January 3 2009 timesonline.co.uk No 69523 £1.50

Eat Out from £5

More than 900 great restaurants, including four **Gordon Ramsay** favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes [illegible], page 7

Michael Sheen Frost, Nixon and me

Magazine

Working mums So that's how she does it

Body&Soul

Detox in style The best spas on the planet

Travel

Salman Rushdie I won't marry again

Pages 22, 23

Giant killing? Guide to the FA Cup third round

Sport

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", *The Times* has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the hook" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1999 levels
Business, page 47

How to mine

- miners construct a candidate block filling it with transactions
- transactions are inserted in the block as they are received from the network
- solve PoW:
  - calculate the hash of this block header, including the root of the Merkle tree, the hash of the previous block and the nonce and check if it is smaller than the current target
  - Since the nonce is a 32-bit integer, a miner has to try approx. 4 billion values; trying all values may not work

How to mine

- We can change something else in the block header:
  - the merkle tree

How to mine

- We can change something else in the block header:
  - the merkle tree
- Two mains ways to change the merkle tree
  - the coinbase txn has arbitrary data that can act as a second nonce
  - the miner can also reorder the transactions to create a different merkle tree

How to mine

- We can change something else in the block header:
  - the merkle tree
- Two mains ways to change the merkle tree
  - the coinbase txn has arbitrary data that can act as a second nonce
  - the miner can also reorder the transactions to create a different merkle tree
  - since there can be several thousand transactions in a block, this creates an inconceivable number of nonces that can be tried

How to mine

- with a Merkle tree, rehashing is more efficient when a new transaction is received

How to mine

- with a Merkle tree, rehashing is more efficient when a new transaction is received
- instead of rehashing all the transactions, compute the new root of the merkle tree, and execute the PoW by considering this new root
- only a few operations to recompute all the hashes along the branches on the path from the new txn to the root

Tamper resistance

- imagine an attacker tries to change the content of a block, for example a txn
    - it will also change the root of the merkle tree
    - the nonce of that block is no more valid
    - a new PoW has to executed to re-compute the correct nonce

Tamper resistance

- imagine an attacker tries to change the content of a block, for example a txn
    - it will also change the root of the merkle tree
    - the nonce of that block is no more valid
    - a new PoW has to executed to re-compute the correct nonce
- the hash pointer in the successor block has to be changed, because now the header of the block is changed
- and then the pointer of the successor of the successor must be changed and so on

Tamper resistance

- imagine an attacker tries to change the content of a block, for example a txn
  - it will also change the root of the merkle tree
  - the nonce of that block is no more valid
  - a new PoW has to executed to re-compute the correct nonce
- the hash pointer in the successor block has to be changed, because now the header of the block is changed
- and then the pointer of the successor of the successor must be changed and so on
- an attacker would have to recompute the PoW for the entire chain