Chapter 26

Eventual Consistency & Bitcoin

How would you implement an ATM? Does the following implementation work satisfactorily?

Algorithm 26.1 Naïve ATM

```
1: ATM makes withdrawal request to bank
2: ATM waits for response from bank
3: if balance of customer sufficient then
4:     ATM dispenses cash
5: else
6:     ATM displays error
7: end if
```

Remarks:

- A connection problem between the bank and the ATM may block Algorithm 26.1 in Line 2.
- A *network partition* is a failure where a network splits into at least two parts that cannot communicate with each other. Intuitively any non-trivial distributed system cannot proceed during a partition *and* maintain consistency. In the following we introduce the tradeoff between consistency, availability, and partition tolerance.
- There are numerous causes for partitions to occur, e.g., physical disconnections, software errors, or incompatible protocol versions. From the point of view of a node in the system, a partition is similar to a period of sustained message loss.

26.1 Consistency, Availability, and Partitions

Definition 26.2 (Consistency)**.** *All nodes in the system agree on the current state of the system.*

Definition 26.3 (Availability)**.** *The system is operational and instantly processing incoming requests.*

Definition 26.4 (Partition Tolerance)**.** *Partition tolerance is the ability of a distributed system to continue operating correctly even in the presence of a network partition.*

Theorem 26.5 (CAP Theorem)**.** *It is impossible for a distributed system to simultaneously provide Consistency, Availability, and Partition Tolerance. A distributed system can satisfy any two of these but not all three.*

Proof. Assume two nodes, sharing some state. The nodes are in different partitions, i.e., they cannot communicate. Assume a request wants to update the state and contacts a node. The node may either: 1) update its local state, resulting in inconsistent states, or 2) not update its local state, i.e., the system is no longer available for updates. □

Algorithm 26.6 Partition tolerant and available ATM

```
1: if bank reachable then
2:    Synchronize local view of balances between ATM and bank
3:    if balance of customer insufficient then
4:       ATM displays error and aborts user interaction
5:    end if
6: end if
7: ATM dispenses cash
8: ATM logs withdrawal for synchronization
```

Remarks:

- Algorithm 26.6 is partition tolerant and available since it continues to process requests even when the bank is not reachable.
- The ATM's local view of the balances may diverge from the balances as seen by the bank, therefore consistency is no longer guaranteed.
- The algorithm will synchronize any changes it made to the local balances back to the bank once connectivity is re-established. This is known as eventual consistency.

Definition 26.7 (Eventual Consistency)**.** *If no new updates to the shared state are issued, then eventually the system is in a quiescent state, i.e., no more messages need to be exchanged between nodes, and the shared state is consistent.*

Remarks:

- Eventual consistency is a form of *weak consistency*.
- Eventual consistency guarantees that the state is eventually agreed upon, but the nodes may disagree temporarily.
- During a partition, different updates may semantically conflict with each other. A *conflict resolution* mechanism is required to resolve the conflicts and allow the nodes to eventually agree on a common state.

26.2 Weak Consistency

Eventual consistency is only one form of weak consistency. A number of different tradeoffs between partition tolerance and consistency exist in literature.

Definition 26.8 (Monotonic Read Consistency)**.** *If a node u has seen a particular value of an object, any subsequent accesses of u will never return any older values.*

Remarks:

- Users are annoyed if they receive a notification about a comment on an online social network, but are unable to reply because the web interface does not show the same notification yet. In this case the notification acts as the first read operation, while looking up the comment on the web interface is the second read operation.

Definition 26.9 (Monotonic Write Consistency)**.** *A write operation by a node on a data item is completed before any successive write operation by the same node (i.e., system guarantees to serialize writes by the same node).*

Remarks:

- The ATM must replay all operations in order, otherwise it might happen that an earlier operation overwrites the result of a later operation, resulting in an inconsistent final state.

Definition 26.10 (Read-Your-Write Consistency)**.** *After a node u has updated a data item, any later reads from node u will never see an older value.*

Definition 26.11 (Causal Relation)**.** *The following pairs of operations are said to be causally related:*

- *Two writes by the same node to different variables.*
- *A read followed by a write of the same node.*
- *A read that returns the value of a write from any node.*
- *Two operations that are transitively related according to the above conditions.*

Remarks:

- The first rule ensures that writes by a single node are seen in the same order. For example if a node writes a value in one variable and then signals that it has written the value by writing in another variable. Another node could then read the signaling variable but still read the old value from the first variable, if the two writes were not causally related.

Definition 26.12 (Causal Consistency)**.** *A system provides causal consistency if operations that potentially are causally related are seen by every node of the system in the same order. Concurrent writes are not causally related, and may be seen in different orders by different nodes.*

26.3 Bitcoin

Definition 26.13 (Bitcoin Network)**.** *The Bitcoin network is a randomly connected overlay network of a few tens of thousands of individually controlled* ***nodes****.*

Remarks:

- The lack of structure is intentional: it ensures that an attacker cannot strategically position itself in the network and manipulate the information exchange. Information is exchanged via a simple gossip protocol (nodes tell their neighbors about new messages).
- Old nodes re-entering the system try to connect to peers that they were earlier connected to. If those peers are not available, they default to the new node behavior.
- New nodes entering the system face the bootstrap problem, and can find active peers any which way they want. If they cannot find an active peer, their node will look for active peers from a set of authoritative sources. These authoritative sources are hard-coded in the Bitcoin source code.

Definition 26.14 (Cryptographic Keys)**.** *Users can generate any number of private keys. From each private key, a corresponding public key can be derived using arithmetic operations over a finite field. A public key may be used to identify the recipient of funds in Bitcoin, and the corresponding private key can spend these funds.*

Remarks:

- Bitcoin supports the ECDSA and Schnorr digital signature algorithms to verify ownership of bitcoins.
- It is hard to link public keys to the user that controls them, hence Bitcoin is often referred to as *pseudonymous*.

Definition 26.15 (Bitcoin Currency)**.** *Bitcoin, the currency, is an integer value that is transferred in Bitcoin transactions. This integer value is measured in Satoshi; 100 million Satoshi is 1 bitcoin.*

Definition 26.16 (Transaction)**.** *A transaction is a data structure that describes the transfer of bitcoins from spenders to recipients. It consists of inputs and outputs. Outputs are tuples consisting of an amount of bitcoins and a spending condition. Inputs are references to outputs of previous transactions and code that meets the spending condition of the referenced output.*

Remarks:

- New transactions refer to old transactions, which refer to even older transactions. Every transaction can be publicly traced back to coinbase transactions of blocks (see Definition 26.23).

- A recipient with a public/private key pair can be paid by a transaction whose output's spending condition locks the payment with the public key. It can be unlocked and spent in the future if the recipient signs a future transaction with the private key.

- Inputs reference the output that is being spent by a (h, i)-tuple, where h is the hash of the transaction that created the output, and i specifies the index of the output in that transaction.

- Spending conditions are scripts that offer a variety of options. Apart from a single signature, they may include conditions that require multiple signatures, the result of a simple computation, or the solution to a cryptographic puzzle. However, Bitcoin spending scripts are not Turing complete.

- Transactions can be gossiped by any node in the network and are processed by every node that receives them through the gossip protocol.

- Outputs exist in two states: unspent and spent. An output is originally unspent, and can be spent at most once.

- The set of unspent transaction outputs (UTXO) is part of the shared state of Bitcoin. Every node in the Bitcoin network holds a complete replica of that state. Local replicas may temporarily diverge but consistency is eventually re-established.

Algorithm 26.17 Node Receives Transaction (Naïve)

```
1: Receive transaction $t$
2: for each input $(h, i)$ in $t$ do
3:   if output $(h, i)$ is not in local UTXO set or signature invalid then
4:     Drop $t$ and stop
5:   end if
6: end for
7: if sum of values of inputs $<$ sum of values of new outputs then
8:   Drop $t$ and stop
9: end if
10: for each input $(h, i)$ in $t$ do
11:   Remove $(h, i)$ from local UTXO set
12: end for
13: for each output $o$ in $t$ do
14:   add $o$ to local UTXO set
15: end for
16: Forward $t$ to neighbors in the Bitcoin network
```

Remarks:

- Note that the effect of a transaction on the state is deterministic. In other words if all nodes receive the same set of transactions in the same order (Definition 15.8), then the state across nodes is consistent.

- The outputs of a transaction may assign less than the sum of inputs, in which case the difference is called the transaction *fee*. The fee is used to incentivize other participants in the system (see Definition 26.23).
- Notice that so far we only described a local acceptance policy. Nothing prevents two nodes to locally accept different transactions that spend the same output.
- Transactions are in one of two states: unconfirmed or confirmed. Incoming transactions from the broadcast are unconfirmed and added to a pool of transactions called the *memory pool*.

Definition 26.18 (Double-spend)**.** *A double-spend is a situation in which multiple transactions attempt to spend the same output. Only one transaction can be valid since outputs can only be spent once. When nodes accept different transactions in a double-spend, the shared state across nodes becomes inconsistent.*

Remarks:

- Double-spends may occur naturally, e.g., if outputs are co-owned by multiple users who all know the corresponding private key. However, double-spends can be malicious as well – we call these double-spend attacks: An attacker creates two transactions both using the same input. One transaction would transfer the money to a victim, the other transaction would transfer the money back to the attacker.
- Double-spends can result in an inconsistent state since the validity of transactions depends on the order in which they arrive. If two conflicting transactions are seen by a node, the node considers the first to be valid, see Algorithm 26.17. The second transaction is invalid since it tries to spend an output that is already spent. The order in which transactions are seen, may not be the same for all nodes, hence the inconsistent state.
- If double-spends are not resolved, the shared state diverges. Therefore a conflict resolution mechanism is needed to decide which of the conflicting transactions is to be confirmed (accepted by everybody), to achieve eventual consistency.

Definition 26.19 (Proof-of-Work)**.** *Proof-of-Work (PoW) is a mechanism that allows a party to prove to another party that a certain amount of computational resources has been utilized for a period of time. A function $\mathcal{F}_d(c, x) \rightarrow \{true, false\}$, where difficulty d is a positive number, while challenge c and nonce x are usually bit-strings, is called a Proof-of-Work function if it has following properties:*

1. *$\mathcal{F}_d(c, x)$ is fast to compute if d, c, and x are given.*
2. *For fixed parameters d and c, finding x such that $\mathcal{F}_d(c, x) = true$ is computationally difficult but feasible. The difficulty d is used to adjust the time to find such an x.*

Definition 26.20 (Bitcoin PoW function)**.** *The Bitcoin PoW function is given by*

$$\mathcal{F}_d(c, x) \rightarrow \text{SHA256}(\text{SHA256}(c|x)) < \frac{2^{224}}{d}.$$

Remarks:

- This function concatenates the challenge c and nonce x, and hashes them twice using SHA256. The output of SHA256 is a cryptographic hash with a numeric value in $\{0, \ldots, 2^{256} - 1\}$ which is compared to a target value $\frac{2^{224}}{d}$, which gets smaller with increasing difficulty.

- SHA256 is a cryptographic hash function with pseudorandom output. No better algorithm is known to find a nonce x such that the function $\mathcal{F}_d(c, x)$ returns true than simply iterating over possible inputs. This is by design to make it difficult to find such an input, but simple to verify the validity once it has been found.

Definition 26.21 (Block)**.** *A block is a data structure used to communicate incremental changes to the local state of a node. A block consists of a list of transactions, a timestamp, a reference to a previous block, and a nonce. A block lists some transactions the block creator ("miner") has accepted to its memory pool since the previous block. A node finds and broadcasts a block when it finds a valid nonce for its PoW function.*

Algorithm 26.22 Node Creates (Mines) Block

```
1: block $b_t = \{coinbase\_tx\}$
2: while size($b_t$) $\leq$ 1 MB do
3:     Choose transaction $t$ in the memory pool that is consistent with $b_t$ and
       local UTXO set
4:     Add $t$ to $b_t$
5: end while
6: Nonce $x = 0$, difficulty $d$, previous block $b_{t-1}$, timestamp $= t_s$
7: challenge $c = (merkle(b_t), hash(b_{t-1}), t_s, d)$
8: repeat
9:     $x = x + 1$
10: until $\mathcal{F}_d(c, x) = true$
11: Gossip block $b_t$
12: Update local UTXO set to reflect $b_t$
```

Remarks:

- The function $merkle(b_t)$ creates a cryptographic representation of the set of transactions in b_t. It is compact and has a fixed length no matter how large the set is.

- With their reference to a previous block, the blocks build a tree, rooted in the so called *genesis block*. The genesis block's hash is hard-coded in the Bitcoin source code.

- The primary goal for using the PoW mechanism is to adjust the rate at which blocks are found in the network, giving the network time to synchronize on the latest block. Bitcoin sets the difficulty so that globally a block is created every 10 minutes in expectation.

- Finding a block allows the finder to impose the transactions in its local memory pool to all other nodes. Upon receiving a block, all nodes roll back any local changes since the previous block and apply the new block's transactions.

- Transactions contained in a block are said to be *confirmed* by that block.

Definition 26.23 (Coinbase Transaction)**.** *The first transaction in a block is called the coinbase transaction. The block's miner is rewarded for confirming transactions by allowing it to mint new coins. The coinbase transaction has a dummy input, and the sum of outputs is determined by a fixed subsidy plus the sum of the fees of transactions confirmed in the block.*

Remarks:

- A coinbase transaction is the sole exception to the rule that the sum of inputs must be at least the sum of outputs. New bitcoins enter the system through coinbase transactions.

- The number of bitcoins that are minted by the coinbase transaction and assigned to the miner is determined by a subsidy schedule that is part of the protocol. Initially the subsidy was 50 bitcoins for every block, and it is being halved every 210,000 blocks, or 4 years in expectation. Due to the halving of the value of the coinbase transaction, the total amount of bitcoins in circulation never exceeds 21 million bitcoins.

- It is expected that the cost of performing the PoW to find a block, in terms of energy and infrastructure, is close to the value of the reward the miner receives from the coinbase transaction in the block.

Definition 26.24 (Blockchain)**.** *The longest path from the genesis block (root of the tree) to a (deepest) leaf is called the blockchain. The blockchain acts as a consistent transaction history on which all nodes eventually agree.*

Remarks:

- The path length from the genesis block to block b is the height h_b.

- Only the longest path from the genesis block to a leaf is a valid transaction history, since branches may contradict each other because of double-spends.

- Since only transactions in the longest path are agreed upon, miners have an incentive to append their blocks to the longest chain, thus agreeing on the current state.

- The mining incentives quickly increased the difficulty of the PoW mechanism: initially miners used CPUs to mine blocks, but CPUs were quickly replaced by GPUs, FPGAs and even application specific integrated circuits (ASICs) as bitcoins appreciated. This results in an equilibrium today in which only the most cost efficient miners, in terms of hardware supply and electricity, make a profit in expectation.
- If multiple blocks are mined more or less concurrently, the system is said to have *forked*. Forks happen naturally because mining is a distributed random process and two new blocks may be found at roughly the same time.

Algorithm 26.25 Node Receives Block

```
1: Receive block $b_t$
2: For this node, the current head is block $b_{max}$ at height $h_{max}$
3: For this node, $b_{max}$ defines the local UTXO set
4: From $b_t$, extract reference to $b_{t-1}$, and find $b_{t-1}$ in the node's local copy of
   the blockchain
5: $h_b = h_{b_{t-1}} + 1$
6: if $h_b > h_{max}$ and $is\_valid(b_t)$ then
7:     $h_{max} = h_b$
8:     $b_{max} = b$
9:     Update UTXO set to reflect transactions in $b_t$
10: end if
```

Remarks:

- Algorithm 26.25 describes how a node updates its local state upon receiving a block. Like Algorithm 26.17, this describes the local policy and may also result in node states diverging, i.e., by accepting different blocks at the same height as current head.
- Unlike extending the current path, switching paths may result in confirmed transactions no longer being confirmed, because the blocks in the new path do not include them. Switching paths is referred to as a *reorganization* ("*reorg*").

Theorem 26.26. *Forks are eventually resolved and all nodes eventually agree on which is the longest blockchain. The system therefore guarantees eventual consistency.*

Proof. In order for the fork to continue to exist, pairs of blocks need to be found in close succession, extending distinct branches, otherwise the nodes on the shorter branch would switch to the longer one. The probability of branches being extended almost simultaneously decreases exponentially with the length of the fork, hence there will eventually be a time when only one branch is being extended, becoming the longest branch. □

Definition 26.27 (Consensus Rules)**.** *The is_valid function in algorithm 26.25 represents the consensus rules of Bitcoin. All nodes will converge on the same shared state if and only if all nodes agree on this function.*

Remarks:

- If nodes have different implementations of the *is_valid* function, some nodes will reject blocks that other nodes will accept. This is called a *hard fork*, which is different than a regular fork. A regular fork happens because different nodes see different blocks that are mined at around the same time. Hard forks happen because the rules of Bitcoin itself have changed.
- Getting all nodes to change their implementation of *is_valid* together, at the same time, so that new features can be added to the Bitcoin system, is difficult, as there is no centralized authority to coordinate such an upgrade.
- In Bitcoin, hard forks are distinguished from soft forks:

Definition 26.28 (Hard/Soft Fork)**.** *If the set of valid transactions is expanded, we have a hard fork. If the set of valid transactions is reduced, we have a soft fork.*

Remarks:

- As all nodes cannot upgrade at the same time, miners can create blocks that have more restrictive *is_valid* rules and older nodes will still accept them as they accept broader rules. This way, rules can still be changed without having to upgrade all nodes at the same time. Miners, on the other hand, have to upgrade almost at the same time.

26.4 Layer 2

Definition 26.29 (Smart Contract)**.** *A smart contract is an agreement between two or more parties, encoded in such a way that the correct execution is guaranteed by the blockchain.*

Remarks:

- Contracts allow business logic to be encoded in Bitcoin transactions which mutually guarantee that an agreed upon action is performed. The blockchain acts as conflict mediator, should a party fail to honor an agreement.
- The use of scripts as spending conditions for outputs enables smart contracts. Scripts, together with some additional features such as timelocks, allow encoding complex conditions, specifying who may spend the funds associated with an output and when.

Definition 26.30 (Timelock)**.** *Bitcoin provides a mechanism to make transactions invalid until some time in the future:* ***timelocks****. A transaction may specify a locktime: the earliest time, expressed in either a Unix timestamp or a blockchain height, at which it may be included in a block and therefore be confirmed.*

Remarks:

- Transactions with a timelock are not released into the network until the timelock expires. It is the responsibility of the node receiving the transaction to store it locally until the timelock expires and then release it into the network.
- Transactions with future timelocks and blocks with such transactions are invalid. Upon receiving invalid transactions or blocks, nodes discard them immediately and do not forward them to their neighbors.
- Timelocks can be used to replace or supersede transactions: a timelocked transaction t_1 can be replaced by another transaction t_0, spending some of the same outputs, if the replacing transaction t_0 has an earlier timelock and can be broadcast in the network before the replaced transaction t_1 becomes valid.

Definition 26.31 (Singlesig and Multisig Outputs)**.** *When an output can be claimed by providing a single signature it is called a **singlesig output**. In contrast the script of **multisig outputs** specifies a set of m public keys and requires k-of-m (with $k \leq m$) valid signatures from distinct matching public keys from that set in order to be valid.*

Remarks:

- Many Bitcoin smart contracts begin with the creation of a 2-of-2 multisig output, requiring a signature from both parties. Once the transaction creating the multisig output is confirmed in the blockchain, both parties are guaranteed that the funds of that output cannot be spent unilaterally.

Algorithm 26.32 Parties A and B create a 2-of-2 multisig output o

```
1: $B$ sends a list $I_B$ of inputs with $c_B$ coins to $A$
2: $A$ selects its own inputs $I_A$ with $c_A$ coins
3: $A$ creates transaction $t_s\{[I_A, I_B], [o = c_A + c_B \to (A, B)]\}$
4: $A$ creates timelocked transaction $t_r\{[o], [c_A \to A, c_B \to B]\}$ and signs it
5: $A$ sends $t_s$ and $t_r$ to $B$
6: $B$ signs both $t_s$ and $t_r$ and sends them to $A$
7: $A$ signs $t_s$ and broadcasts it to the Bitcoin network
```

Remarks:

- t_s is called a *setup transaction* and is used to lock in funds into a shared account. If t_s is signed and broadcast immediately, one of the parties could not collaborate to spend the multisig output, and the funds become unspendable. To avoid a situation where the funds cannot be spent, the protocol also creates a timelocked *refund transaction* t_r which guarantees that, should the funds not be spent before the timelock expires, the funds are returned to the respective party. At no point in time does one of the parties hold a fully signed setup transaction without the other party holding a fully signed refund transaction, guaranteeing that funds are eventually returned.

- Both transactions require the signature of both parties. The setup transaction has two inputs from A and B respectively which require individual signatures. The refund transaction requires both signatures because of the a 2-of-2 multisig input.

Algorithm 26.33 Simple Micropayment Channel from s to r with capacity c

```
1: $c_s = c$, $c_r = 0$
2: $s$ and $r$ use Algorithm 26.32 to set up output $o$ with value $c$ from $s$
3: Create settlement transaction $t_f\{[o], [c_s \rightarrow s, c_r \rightarrow r]\}$
4: while channel open and $c_r < c$ do
5:   In exchange for good with value $\delta$
6:   $c_r = c_r + \delta$
7:   $c_s = c_s - \delta$
8:   Update $t_f$ with outputs $[c_r \rightarrow r, c_s \rightarrow s]$
9:   $s$ signs and sends $t_f$ to $r$
10: end while
11: $r$ signs last $t_f$ and broadcasts it
```

Remarks:

- Algorithm 26.33 implements a Simple Micropayment Channel, a smart contract that is used for rapidly adjusting micropayments from a spender to a recipient. Only two transactions are ever broadcast and inserted into the blockchain: the setup transaction t_s and the last settlement transaction t_f. There may have been any number of updates to the settlement transaction, transferring ever more of the shared output to the recipient.

- The number of bitcoins c used to fund the channel is also the maximum total that may be transferred over the simple micropayment channel.

- At any time the recipient R is guaranteed to eventually receive the bitcoins, since she holds a fully signed settlement transaction, while the spender only has partially signed ones.

- The simple micropayment channel is intrinsically unidirectional. Since the recipient may choose any of the settlement transactions in the protocol, she will use the one with maximum payout for her. If we were to transfer bitcoins back, we would be reducing the amount paid out to the recipient, hence she would choose not to broadcast that transaction.

26.5 Selfish Mining

Satoshi Nakamoto suggested that it is rational to be altruistic, e.g., by always attaching newly found block to the longest chain. But is it true?

Definition 26.34 (Selfish Mining)**.** *A selfish miner hopes to earn the reward of a larger share of blocks than its hardware would allow. The selfish miner achieves this by temporarily keeping newly found blocks secret.*

Algorithm 26.35 Selfish Mining

```
1: Idea: Mine secretly, without immediately publishing newly found blocks
2: Let $d_p$ be the depth of the public blockchain
3: Let $d_s$ be the depth of the secretly mined blockchain
4: if a new block $b_p$ is published, i.e., $d_p$ has increased by 1 then
5:    if $d_p > d_s$ then
6:       Start mining on that newly published block $b_p$
7:    else if $d_p = d_s$ then
8:       Publish secretly mined block $b_s$
9:       Mine on $b_s$ and publish newly found block immediately
10:   else if $d_p = d_s - 1$ then
11:      Publish all secretly mined blocks
12:   end if
13: end if
```

Theorem 26.36 (Selfish Mining)**.** *It may be rational to mine selfishly, depending on two parameters α and γ, where α is the ratio of the mining power of the selfish miner, and γ is the share of the altruistic mining power the selfish miner can reach in the network if the selfish miner publishes a block right after seeing a newly published block. Precisely, the selfish miner share is*

$$\frac{\alpha(1-\alpha)^2(4\alpha+\gamma(1-2\alpha))-\alpha^3}{1-\alpha(1+(2-\alpha)\alpha)}.$$

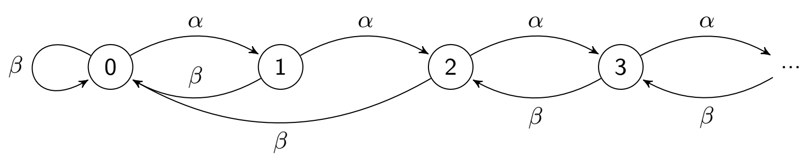
$$\begin{tikzcd}
0 \arrow[loop left, "\beta"] \arrow[r, bend left, "\alpha"] & 1 \arrow[l, bend left, "\beta"] \arrow[r, bend left, "\alpha"] & 2 \arrow[ll, bend left=40, "\beta"] \arrow[r, bend left, "\alpha"] & 3 \arrow[l, bend left, "\beta"] \arrow[r, bend left, "\alpha"] & \cdots \arrow[l, bend left, "\beta"]
\end{tikzcd}$$

Figure 26.37: Each state of the Markov chain represents how many blocks the selfish miner is ahead, i.e., $d_s - d_p$. In each state, the selfish miner finds a block with probability α, and the honest miners find a block with probability $\beta = 1 - \alpha$. The interesting cases are the "irregular" β arrow from state 2 to state 0, and the β arrow from state 1 to state 0 as it will include three subcases.

Proof. We model the current state of the system with a Markov chain, see Figure 26.37.

We can solve the following Markov chain equations to figure out the probability of each state in the stationary distribution (using $\alpha + \beta = 1$):

$$\begin{aligned} p_0 &= \beta(p_1 + p_2) \\ p_1 &= \alpha p_0 \\ \alpha p_i &= \beta p_{i+1}, \text{ for all } i > 1 \\ \text{and } 1 &= \sum_i p_i. \end{aligned}$$

Using $\rho = \alpha/\beta$, we express all terms of above sum with p_1:

$$1 = \frac{p_1}{\alpha} + p_1 \sum_{i \geq 0} \rho^i = \frac{p_1}{\alpha} + \frac{p_1}{1-\rho}, \text{ hence } p_1 = \frac{2\alpha^2 - \alpha}{\alpha^2 + \alpha - 1}.$$

Each state has an outgoing arrow with probability β. If this arrow is taken, one or two blocks (depending on the state) are attached that will eventually end up in the main chain of the blockchain. In state 0 (if arrow β is taken), the honest miners attach a block. In all states i with $i > 2$, the selfish miner eventually attaches a block. In state 2, the selfish miner directly attaches 2 blocks because of Line 11 in Algorithm 26.35.

State 1 in Line 8 is interesting. The selfish miner secretly was 1 block ahead, but now (after taking the β arrow) the honest miners are attaching a competing block. We have a race who attaches the next block, and where. There are three possibilities:

- Either the selfish miner manages to attach another block to its own block, giving 2 blocks to the selfish miner. This happens with probability α.
- Or the honest miners attach a block (with probability β) to their previous honest block (with probability $1-\gamma$). This gives 2 blocks to the honest miners, with total probability $\beta(1-\gamma)$.
- Or the honest miners attach a block to the selfish block, giving 1 block to each side, with probability $\beta\gamma$.

The blockchain process is just a biased random walk through these states. Since blocks are attached whenever we have an outgoing β arrow, the total number of blocks being attached per state is simply $1 + p_1 + p_2$ (all states attach a single block, except states 1 and 2 which attach 2 blocks each).

As argued above, of these blocks, $1 - p_0 + p_2 + \alpha p_1 - \beta(1-\gamma)p_1$ are blocks by the selfish miner, i.e., the ratio of selfish blocks in the blockchain is

$$\frac{1 - p_0 + p_2 + \alpha p_1 - \beta(1-\gamma)p_1}{1 + p_1 + p_2}.$$

□

Remarks:

- If the miner is honest (altruistic), then a miner with computational share α should expect to find an α fraction of the blocks. For some values of α and γ the ratio of Theorem 26.36 is higher than α.
- In particular, if $\gamma = 0$ (the selfish miner only wins a race in Line 8 if it manages to mine 2 blocks in a row), the break even of selfish mining happens at $\alpha = 1/3$.
- If $\gamma = 1/2$ (the selfish miner learns about honest blocks very quickly and manages to convince half of the honest miners to mine on the selfish block instead of the slightly earlier published honest block), already $\alpha = 1/4$ is enough to have a higher share in expectation.
- And if $\gamma = 1$ (the selfish miner controls the network, and can hide any honest block until the selfish block is published) any $\alpha > 0$ justifies selfish mining.

Chapter Notes

The CAP theorem was first introduced by Fox and Brewer [FB99], although it is commonly attributed to a talk by Eric Brewer [Bre00]. It was later proven by Gilbert and Lynch [GL02] for the asynchronous model. Gilbert and Lynch also showed how to relax the consistency requirement in a partially synchronous system to achieve availability and partition tolerance.

Bitcoin was introduced in 2008 by Satoshi Nakamoto [Nak08]. Nakamoto is thought to be a pseudonym used by either a single person or a group of people; it is still unknown who invented Bitcoin, giving rise to speculation and conspiracy theories. Among the plausible theories are noted cryptographers Nick Szabo [Big13] and Hal Finney [Gre14]. The first Bitcoin client was published shortly after the paper and the first block was mined on January 3, 2009. The genesis block contained the headline of the release date's The Times issue "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*", which serves as proof that the genesis block has been indeed mined on that date, and that no one had mined before that date. The quote in the genesis block is also thought to be an ideological hint: Bitcoin was created in a climate of financial crisis, induced by rampant manipulation by the banking sector, and Bitcoin quickly grew in popularity in anarchic and libertarian circles. The original client is nowadays maintained by a group of independent core developers and remains the most used client in the Bitcoin network.

Central to Bitcoin is the resolution of conflicts due to double-spends, which is solved by waiting for transactions to be included in the blockchain. This however introduces large delays for the confirmation of payments which are undesirable in some scenarios in which an immediate confirmation is required. Karame et al. [KAC12] show that accepting unconfirmed transactions leads to a non-negligible probability of being defrauded as a result of a double-spending attack. This is facilitated by *information eclipsing* [DW13], i.e., that nodes do not forward conflicting transactions, hence the victim does not see both transactions of the double-spend. Bamert et al. [BDE$^+$13] showed that the odds of detecting a double-spending attack in real-time can be improved by connecting to a large sample of nodes and tracing the propagation of transactions in the network.

Bitcoin does not scale very well due to its reliance on confirmations in the blockchain. A copy of the entire transaction history is stored on every node in order to bootstrap joining nodes, which have to reconstruct the transaction history from the genesis block. Simple micropayment channels were introduced by Hearn and Spilman [HS12] and may be used to bundle multiple transfers between two parties but they are limited to transferring the funds locked into the channel once. Duplex Micropayment Channels [DW15] and the Lightning Network [PD15] were the first suggestions for bidirectional micropayment channels in which the funds can be transferred back and forth an arbitrary number of times, greatly increasing the flexibility of Bitcoin transfers and enabling a number of features, such as micropayments and routing payments between any two endpoints.

Selfish mining has already been discussed shortly after the introduction of Bitcoin [RHo10]. A few years later, Eyal and Sirer formally analyzed selfish mining [ES14]. If the selfish miner is two or more blocks ahead, this original research suggested to always answer a newly published block by releasing the oldest unpublished block, so have two blocks at the same level. The idea was that honest miners will then split their mining power between these two blocks. However, what matters is how long it takes the honest miners to find the next block to extend the public blockchain. This time does not change whether the honest miners split their efforts or not. Hence the case $d_p < d_s - 1$ is not needed in Algorithm 26.35.

Similarly, Courtois and Bahack [CB14] study subversive mining strategies. Nayak et al. [NKMS15] combine selfish mining and eclipse attacks. Algorithm 26.35 is not optimal for all parameters, e.g., sometimes it may be beneficial to risk even a two-block advantage. Sapirshtein et al. [SSZ15] describe and analyze the optimal algorithm.

This chapter was written in collaboration with Christian Decker.

Bibliography

[BDE+13] Tobias Bamert, Christian Decker, Lennart Elsen, Samuel Welten, and Roger Wattenhofer. Have a snack, pay with bitcoin. In *IEEE Internation Conference on Peer-to-Peer Computing (P2P), Trento, Italy*, 2013.

[Big13] John Biggs. Who is the real satoshi nakamoto? one researcher may have found the answer. http://on.tcrn.ch/l/R0vA, 2013.

[Bre00] Eric A. Brewer. Towards robust distributed systems. In *Symposium on Principles of Distributed Computing (PODC)*. ACM, 2000.

[CB14] Nicolas T. Courtois and Lear Bahack. On subversive miner strategies and block withholding attack in bitcoin digital currency. *CoRR*, abs/1402.1718, 2014.

[DW13] Christian Decker and Roger Wattenhofer. Information propagation in the bitcoin network. In *IEEE International Conference on Peer-to-Peer Computing (P2P), Trento, Italy*, September 2013.

[DW15] Christian Decker and Roger Wattenhofer. A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels. In *Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS)*, 2015.

[ES14] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography and Data Security*, pages 436–454. Springer, 2014.

[FB99] Armando Fox and Eric Brewer. Harvest, yield, and scalable tolerant systems. In *Hot Topics in Operating Systems*. IEEE, 1999.

[GL02] Seth Gilbert and Nancy Lynch. Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. *SIGACT News*, 2002.

[Gre14] Andy Greenberg. Nakamoto's neighbor: My hunt for bitcoin's creator led to a paralyzed crypto genius. http://onforb.es/1rvyecq, 2014.

[HS12] Mike Hearn and Jeremy Spilman. Contract: Rapidly adjusting micro-payments. https://en.bitcoin.it/wiki/Contract, 2012. Last accessed on November 11, 2015.

[KAC12] G.O. Karame, E. Androulaki, and S. Capkun. Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin. In *Conference on Computer and Communication Security (CCS)*, 2012.

[Nak08] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.

[NKMS15] Kartik Nayak, Srijan Kumar, Andrew Miller, and Elaine Shi. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. Technical report, IACR Cryptology ePrint Archive 2015, 2015.

[PD15] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network. 2015.

[RHo10] RHorning. Mining cartel attack, 2010.

[SSZ15] Ayelet Sapirshtein, Yonatan Sompolinsky, and Aviv Zohar. Optimal selfish mining strategies in bitcoin. *arXiv preprint arXiv:1507.06183*, 2015.