Blockchain

Documentation

Paolo Bettelini, Gianni Grasso, ~~Giacinto Di Santis~~
Scuola d'Arti e Mestieri di Trevano (SAMT)

Contents

1 Introduction

1.1 Abstract

This project is not meant to be an effectively secure or scalable blockchain.
The goal is to produce a *proof-of-concept* software for educational purposes.

1.2 Information

This is a project of the Scuola Arti e Mestieri di Trevano (SAMT) under the following circumstances

- **Section**: Computer Science
- **Year:** Third
- **Class:** Module 306
- **Supervisor:** Luca Muggiasca
- **Title:** Blockchain
- **Start date**: 2021-27-01
- **Deadline**: 2022-05-05

and the following requirements

- **Documentation**: a full documentation of the work done
- **Diary**: constant changelog for each work session
- **Source code**: working source code of the project

All the source code and documents can be found at https://github.com/LuMug/Blockchain [1].

1.3 Structure

This document is structured as such:

1. **Introduction:** General informations, requirements and scope of the project
2. **Blockchain:** How a blockchain works
3. **Blockchain implementation:** Our blockchain implementation
4. **Programming language:** How to build a programming language
5. **References:** References

1.4 Requirements

Req-01	
Name	BlockChain
Priority	1
Version	1.0
Notes	none
Description	It is required to create a Blockchain based on PoS interacting with each node of the chain.
Subrequirements	
Req-01_0	There must be implemented the Proof of Stake (PoS).
Req-01_1	There must be implemented a peer discovery algorithm.
Req-01_2	There must be implemented a consensus algorithm.
Req-01_3	There must be implemented a P2P algorithm.
Req-01_4	There must be implemented a Gossip algorithm.

Req-02	
Name	Node
Priority	1
Version	1.0
Notes	none
Description	It is required that a computing machine can become a node of the blockchain..
Subrequirements	
Req-01_0	Each node must have the blockchain saved locally as a SQLite database.
Req-01_1	There must be implemented an algorithm that allow al nodes to perform the proof of stake.
Req-01_2	Every node must be capable of executing a transaction.
Req-01_3	Any node must be able to make a smart contract.

Req-03	
Name	Transaction
Priority	1
Version	1.0
Notes	none
Description	On the blockchain it must be able to make transactions, both for cryptocurrency and for smart contacts.
Subrequirements	
Req-01_0	There must be implemented an algorithm that validates the transaction and adds it to the block.
Req-01_0	There must be a deflation system, which functions using gas fees.

Req-04	
Name	Smart Contract
Priority	2
Version	1.0
Notes	none
Description	There must be a system that generates a smart contract that is self-executing, containing the terms of the agreement between buyer and seller written directly in lines of code.
Subrequirements	
Req-01__0	There must be an algorithm dedicated to defalcation system for the transaction of the smart contract with gas fees.
Req-01__1	The code and the agreements in it must exist on the decentralized blockchain.
Req-01__2	The code controls execution and transactions are traceable and irreversible.

Req-05	
Name	WebApp
Priority	2
Version	1.0
Notes	none
Description	It is required that from a web application any user can request and see the basic information of the blockchain (transaction, block, ...).
Subrequirements	
Req-01__0	There must be a section on the site dedicated to information about blocks, transactions, gas fees.
Req-01__1	There must be a section on the site that allows the user to generate a wallet.
Req-01__2	There must be a section on the site that allows the user to carry out and control their transactions.
Req-01__3	There must be a section in the site that allows the user to carry out the proof of stake, that is to block a determined quantity of coins in order to be chosen as validator.

Req-06	
Name	Info Website
Priority	3
Version	1.0
Notes	Required by the mandator, but optional.
Description	It is required a website that explain how the blockchain works and how we've done it.
Subrequirements	
Req-01__0	IDK.

2 Blockchain

2.1 Block

Each user owns a pair of private and public key.

All the transactions broadcasted to the network are grouped into blocks, which contain

- Markle tree root hash
- Timestamp
- nBits (PoW)
- Nonce (PoW)
- Previous block hash
- Number of transactions

With each block being confirmed, the blockchain is created.

2.2 Proof of Work

Proof-of-Work (PoW) is a cryptographic proof that a party has spent a certian amount of computational effort.

When a miner solves the puzzle the current block is archived, a new block is generated and all the transactions in the previous block are confirmed. The miner is then rewarded by the system.

2.3 Proof of Stake

2.4 Smart Contracts

Smart contracs are programs associated with an address and run on the blockchain. The nodes run code from the contract program at a relevant event, such as a received transation.

Users can interact with the contract via transactions. Contracts can often interact with other contracts and some of them are Turing-complete.

2.4.1 Deployment

A smart contract is deployed by sending a transaction to the blockchain which includes the compiled program as well as a special receiver address.

The program is added to the current block. When the block is added to the blockchain, the contract will execute one time to set its initial state, at which point the smart contract will now be valid and running.

3 Blockchain Implementation

3.1 Peer Discovery

3.1.1 Seeder

The first step of our peer discovery solution is the *Seeder*. The Seeder is a server which stores information about node's service addresses.
A node might register himself to a seeder by opening a TCP connection and sending a `RegisterNode` packet. Likewise, a node might ask a seeder the service addresses of **N** nodes by sending a `RequestNodes` packet.

When the seeder receives a `RegisterNode` it will store its address in the services pool. The services pool has a fixed capacity of `POOL_CAPACITY`. Nodes are stored along with their registration timestamp, this means that when the pool reaches max capacity the oldest node will be uncached. If an already registered node send a registration packet, the timestamp is updated. Connection is then closed.

When the seeder receives a `RequestNodes` it will try to randomly draw as many nodes as requested (max `MAX_REQUEST`) excluding the requester itself. The `ServeRequestNodes` response packet will be sent back. Connection is then closed.

It is important to only rely on a seeder when 0 peers are known or when all the known peers are unreachable.

3.1.2 Cache

The nodes will also locally cache some of the peers. To do so we define the *node* table.

```
CREATE TABLE IF NOT EXISTS node (
    address VARCHAR(20),
    port INT,
    last_seen_alive DATETIME,
    PRIMARY KEY (address, port)
);
```

When a connection to a peer is established, the node is added to this table. If the node is already in the database, its *last_seen_alive* field is updated.
If the number of nodes in the cache exceeds `MAX_CACHED_NODES`, the node with the oldest *last_seen_alive* field is deleted.

3.1.3 Algorithm

A node will actively try to always have `MIN_CONNECTIONS` established connections. If the number of connections exceeds `MAX_CONNECTIONS`, a random peer is disconnected.

The node will periodically register himself to a random seeder every `REGISTER_INTERVAL` ms. By doing this dead nodes will stop registering and exit the seeder pool.

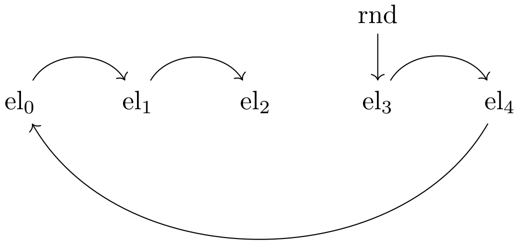
The node will periodically execute the following update every `UPDATE_INTERVAL` ms:

1. If peers are less than `MIN_CONNECTIONS`, update from a random peer up to `MAX_TRIES_NEIGHBOUR` times

2. If peers are less than `MIN_CONNECTIONS`, update from local cache

3. If peers are 0, update from a random seeder up to `MAX_TRIES_SEEDER` times

Picking a random seeder
Seeder addresses are hard-coded in the `SEEDERS` array. Start with a random index, if that seeder is unreachable traverse the array in a circular manner until one is reachable.



Updating from local cache

1. Read all cached peers from the database
2. Filter the ones without an estblished connection
3. While there is still room, try to establish a connection with them

Updating from seeder

1. Establish a TCP connection with the seeder
2. Send a `RequestNodes` packet requesting (`MIN_CONNECTIONS` − `CONNECTIONS`) peers
3. Filter the ones without an estblished connection
4. Try to connect to each of them

Update from a peer

1. Send a `RequestNodes` packet requesting (`MIN_CONNECTIONS` − `CONNECTIONS`) peers
2. Filter the ones without an estblished connection
3. Try to connect to each of them

3.2 Constants

Here is a list of hard-coded values.

Database
Constants related to the database node caching

Name	Value
MAX_CACHED_NODES	50

Blockchain
Constants related to the blockchain system:

Name	Value
BLOCK_REWARD	1000

Node
Constants related to the peer connections:

Name	Value
MAX_CONNECTIONS	150
MIN_CONNECTIONS	100
REGISTER_INTERVAL	180000
UPDATE_INTERVAL	180000
MAX_TRIES_SEEDER	5
MAX_TRIES_NEIGHBOUR	5
SEEDERS	127.0.0.1:4670 127.0.0.1:4671 127.0.0.1:4672

3.3 Packets

Packets are sent over a TCP socket stream. Each packet is preceded by the length of the packet, encoded as a Little-Endian 32-bit integer.

3.3.1 PoWSolvedPacket

3.3.2 RegisterNodePacket

3.3.3 RequestBlockchainLengthPacket

3.3.4 RequestIfHashExistsPacket

3.3.5 RequestNodesPacket

3.3.6 SendTransactionPacket

3.3.7 ServeBlockchainLengthPacket

3.3.8 ServeIfHashExistsPacket

3.3.9 ServeNodesPacket

4 Programming language

4.1 Introduction

We have developed a custom programming language to design smart contracts, *piccions*.
The following sections contain a generic approach to designing a bytecode and the final implementation itself.

4.2 Bytecode

The bytecode is a set of low-level 1-byte long instructions (opcodes) in which a program is compiled. This set of instruction is run on a Virtual Machine (VM).

The life of a program looks as follows:

Source code → compiler → bytecode → VM

When the program is run on the Virtual Machine it is given a finite amount of memory (RAM), this memory is divided into stack and heap.

Programs run in a virtual machine are generally slower, but the advantage is that the compiled program is not CPU-specific and the program can be safely virtualed within the VM itself.

4.3 Stack

The stack is a piece of memory in which values are stacked on top of eachother. The purpose of the stack is to keep in memory temporary values for evaluating nested expressions and variables of the local scope.

4.4 Heap

The heap is the space in memory where all the objects are stored. The objects are (usually) indexed by 32-bit pointers which point to the beginning of the object within the heap. These pointers are the actual values stored in the stack. This means that for a given variable *a*, its pointers will be stored on the stack, and the pointer will point to *a* in the heap memory. The Java programming language however directly stored primitive values (numbers and such) on the stack, without a pointer to the heap.

4.5 Instructions

The two fundamental stack operations are **PUSH** and **POP**:
PUSH → pushes a value on top of the stack
POP → removes the topmost value from the stack

A simple bytecode for working with 8-bit values:

Code	**Stack before**	**Stack after**	**Description**
PSH		value	pushes the next value in the bytecode onto the stack
ADD	v1, v2	result	pop the two topmost values, adds them and pushes the result onto the stack
SUB	v1, v2	result	pop the two topmost values, subtracts them and pushes the result onto the stack
DIV	v1, v2	result	pop the two topmost values, divides them and pushes the result onto the stack
MUL	v1, v2	result	pop the two topmost values, multiplies them and pushes the result onto the stack

All of these operator work on and change the state of the stack.

Here is the code to compute $4 + 3$ and place the result on top of the stack

```
00    PSH    // push 4 onto the stack
01     4
02    PSH    // push 3 onto the stack
03     3
04    ADD
```

The stack now only contains the result of the addition, 8, which we could now print.
When the Virtual Machine will execute this code, it will do the following operations:

```
push(next())      // push next value
push(next())      // push next value
push(add(pop(), pop())) // pop two values, add them, push
```

Here's a simple pseudo-code for executing bytecode

```
while (!done) {
    var code = next()

    if (code == PSH)
        var value = next()
        push(value)

    if (code == ADD)
        var v1 = pop()
        var v2 = pop()
        var result = v1 + v2
        push(result)

    if (code == MUL)
        var v1 = pop()
        var v2 = pop()
        var result = v1 * v2
        push(result)

    if (code == SUB)
        var v1 = pop()
        var v2 = pop()
        var result = v2 - v1
        push(result)

    if (code == DIV)
        var v1 = pop()
        var v2 = pop()
        var result = v2 / v1
        push(result)
}
```

You might notice that in the DIV and SUB code, we compute v2 / v1 or v2 - v1 instead of using v1 and then v2. This is because pushing elements on top of the stack means that they will be popped in the reverse order, for MUL and ADD this is not a problem since they are commutative operations.

4.6 Nested expressions

You might think that we need some extra steps, however our stack already supports all kinds of complex nested computations.
Let's consider the following nested expression: **(2 + 2) * 4 / ((3 - 1) * 2)**.

- Start with 2+2
- Multiply it by 4

At this point we must "pause' the current value to compute to other side of the expression

- Compute 3-1
- Multiply by 2

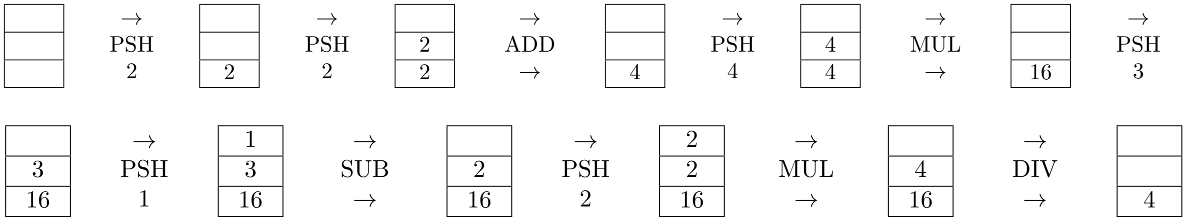
And now we will have both values on top of the stack

- Divide

The bytecode looks as follows

```
    PSH 2
    PSH 2
    ADD
    PSH 4
    MUL
    PSH 3
    PSH 1
    SUB
    PSH 2
    MUL
    DIV
```

Here's how the stack evolves whilst computing the expression



The beauty of the stack is that it will keep stacking elements on top of eachother, but eventually everything will simplify and the result will be on top of the stack.

With the stack, you can compute any nested expression no matter how complex. The only limitation is the size of the stack, if an element is pushes to the stack but there's no more space for it, the program crashes. This is called a stack overflow.

4.7 Data types

So far we've only worked with 8-bit (1 byte) values. This means that every value pushes or popped from the stack is very limited in size [-127;128] or [0;255] depending on how you do the math on the Virtual Machine. Eventually you might want to define other data types, such as 32-bit integers (4 bytes). When pushing an i32 onto the stack, you will need to decompose it into its 4 bytes components, and push each one separately. The action of popping the i32 from the stack, is actually 4 different pops. Each byte will then be recomposed by the VM into an i32 so that you can work on it.

Another data type could be 32-bit floating-point numbers (f32), boolean values, strings and so on.

4.8 Storing variables

The stack is also used to store local variables (variables usable on the current scope of the code). This is done by using a stack frame, which is a frame od data that gets pushes onto the stack.
Whenever a function is called (we'll cover functions later, for now we only have 1 big function which is the whole program) a stackframe is allocated. When the functions ends the stackframe is deallocated.

let's execute the collowing code

```
variable = 54
54 + 46
```

When compiling the code the compiler will decide how big the stack frame for each function will be, depending on the number of variables used. In this case we only need 1 variables (1 byte)

```
ALLOC   // Allocate stack frame of 1 byte
1
PSH     // Push 54
54
STORE   // Store 'variable' into the stack frame
−1
PSH     // Push 46
46
LOAD    // Load 'variable' from the stack frame
−2
ADD     // Add
```

STORE -1 This instruction can be decomposed as:

- pop a value from the stack
- store it at an offset (-1)

After the value is popped, the space for our variable within the stack frame is 1 byte before the current point, hence we use -1 as an offset.

When we call **LOAD -2**, the variable is 2 bytes from us since we previously pushes 46 onto the stack. The compiler automatically fills these values in

4.9 If statement

The first step to implement conditions is to define the bool (boolean) type. We only need 1-bit of information to store a boolean value, however we can only allocate a multiple of 8-bits.

We define the bool type with a byte:

$$\begin{aligned} 00000000 &\rightarrow \text{FALSE} \\ \text{else} &\rightarrow \text{TRUE} \end{aligned}$$

We still lack of a fundamental operation in the bytecode: **GOTO**
The **GOTO** operation tells the code to jump to another instruction.

To define the if structure, we could say that if the condition is FALSE, then we need to skip the body of the statement. For simplify sake, I'll define the **GOTO_IF_NOT** instruction, which pops a boolean value and goes to the instruction given by the next value in the bytecode if the bool value is false.
The condition boolean will be pushed on top of the stack before the if execution. It doesn't matter if it is hardcoded on the bytecode, read from the stack frame or is the return type of a function.

```
if (true) {
    PSH
    2
}
PSH
4
```

There are many ways to implement if statements, here's one:

```
PSH          // Push condition
TRUE
GOTO_IT_NOT // Go to <checkpoint> if value is false
<checkpoint>
PSH          // If body
2
PSH          // Outer code (<checkpoint> instruction)
4
```

4.10 If-Else Statements

For the if-else statement we can just expand the if logic.
If the condition is not satisfied we will jump to the else body instructions.
If the condition is satisfied, we will execute the if body instructions. At the end of the if body we will jump after the else body.

```
– Condition on top of stack
– GOTO_IF_NOT <checkpoint1>
– ... (if body)
– GOTO <checkpoint2>
– ... (else body) <checkpoint1>
– ... (outer program) <checkpoint2>
```

Consider the following program:

```
 if (true) {
     PSH
     2
} else {
     PSH
     4
}
PSH 6
ADD
```

The bytecode looks as follows:

```
PSH
TRUE
GOTO_IT_NOT
<checkpoint1>
PSH
2
GOTO
<checkpoint2>
PSH                 (<checkpoin1 >)
4
PSH                 (<checkpoin2 >)
6
```

4.11 While loop

LOGIC:
Push condition
If the condition is not satisfied, jump to the end of the body
If the condition is satisfied, execute the body. At the end of the body jump to the beginning.

For this example a new instruction is needed: **EQUALS**

Code	**Stack before**	**Stack after**	**Description**
EQUALS	v1, v2	bool	Pops the two topmost values from the stack, compares them and pushes the (boolean) result onto the stack.

```
00  PSH  2
02  PSH  3
04  EQUALS
```

will result in FALSE in top of the stack

I am also going to use the **PRINT** (v1 -> _), which pops a values and "prints" it to some standard output.

Pushing a condition (from the bytecode) will result in either an infinite loop or no iterations at all. We will read and write to a variable in the stackframe, this is the pseudo-code:

```
variable = 10
while (variable / 10 == 2) {
    print(variable)
    variable = variable + 1
}
```

Here's the bytecode

```
ALLOC 1        // Store variable=10
PSH 10
STORE −1

LOAD −2        // Push condition <checkpoint1>
PSH 10
DIV
PSH 1
EQUALS

GOTO_IF_NOT <checkpoint2>

LOAD −1        // While body
PRINT
LOAD −1
PUSH 1
ADD
STORE −1

GOTO <checkpoint1>
 ... (outer program) <checkpoint2>
```

This will produce the following output (since integer division is rounded the loop will stop at *var = 20*):

10 11 12 13 14 15 16 17 18 19

4.12 Functions

The simpliest form of 'function' is a macro: the compiler places the same instructions multiple times throughout the program. This is not good memory-wise. We need a jump-system.

The first problem is that the function must be defined within the program but not executed (unless it has been called) A simple solution could be

```
 ... code

GOTO <checkpoint1>
 ... (function body)

 ... code <checkpoint1>
```

When we want to call the function we can just jump to the beginning of its instruction. However, when the function has ended we must continue doing what we were previously executing. To solve this problem, before jumping to a function, we push the current position. When the function has finished, it pops the index and jumps to it.

```
 ... code

GOTO <checkpoint1>
 ... (function body)      <function>
GOTO <checkpoint2>
```

```
... code <checkpoint1>
GOTO <function>
... code <checkpoint2>
```

4.13 Function with parameters

Before jumping to the function, push the parameters values onto the stack. The function will pop them and use them.

4.14 Function with return value

Before the function finishes, it pushes the return value onto the stack. However, remember that the function must then jump back to the call checkpoint, but the topmost value is the return value rather than the index to jump to. To solve this we could create an instruction **SWAP**, which swaps the last two values on top of the stack. Using the **SWAP** operation, we can then pop the index to jump to. The following instructions will be able to pop the result value from the stack.

4.15 Storing objects and pointers

The solution is pointers and heap memory. The heap memory is another frame of memory (bigger than the stack) used to allocated every objects. Pointers are values (usually 32-bit integers) that point to an object within the heap memory. Instead of storing the *actual* values in the stackframe, we will only store pointers. Those pointers will point to the *actual* values we care about in the heap memory.

As stated at the beginning, Java doesn't use pointers for primitive values. Integers and such are directly stored in the stack frame (since they are as small as a pointer).

To explain how the heap memory works we can use the C language. The C programming language provides the malloc(size) function, which returns a pointer to a chunk of <size> in the heap that you can use. It also provides the free(pointer) method, to free memory from the heap.

```
void* chunk = malloc(100);
free(chunk);
```

Other languages don't require you to manually free memory:
Java implements a ”Garbage Collector”, which frees all the unused memory from the heap.
Rust automatically frees unused memory, however this features comes with some extra retrictions.

Helpful resources: https://gameprogrammingpatterns.com/bytecode.html [2].

5 Structure

5.1 common

5.2 mandate

5.3 node

5.4 piccions

5.5 scripts

5.6 seeder

5.7 website-backend

5.8 website-frontend

5.9 forger

5.9.1 Usage

Generate wallet

```
java -jar forger.jar -gen -out ./key.priv
```

Create transaction

```
java -jar forger.jar -priv ./key.priv --amount 10000
     -out transaction.tx -to <address>
```

Create transaction (no HTTP request for lastHash)

```
java -jar forger.jar -priv ./key.priv -last ./last.tx --amount 10000
     -out transaction.tx -to <address>

java -jar forger.jar -priv ./key.priv -first --amount 10000
     -out transaction.tx -to <address>
```

Dump transaction file content

```
java -jar forger.jar --dump ./transaction.tx
```

6 Conclusion

Paolo Bettelini

Gianni Grasso

7 References

Sitography

[1] Paolo Bettelini and Gianni Grasso. *blockchain*. 2021. URL: https://github.com/LuMug/blockchain.

[2] Bob Nystrom. *Game Programming Patterns*. 2014. URL: https://gameprogrammingpatterns.com/bytecode.html.