Blockchain and smart contracts

what they are and why you should really care about as a developer
Who is Stefano?

- A young enthusiast open source developer
- Red Hat Principal software engineer and associate manager

My matching pairs game: Java & JBoss, Open Source & Red Hat, Blockchain & Ethereum

- [https://www.linkedin.com/in/maeste/](https://www.linkedin.com/in/maeste/)
- [https://twitter.com/maeste](https://twitter.com/maeste)
- [https://github.com/maeste/](https://github.com/maeste/)
- [http://www.onchain.it/](http://www.onchain.it/)
Who is Stefano?

- A young enthusiast open source developer
- Red Hat Principal software engineer

My matching pairs game: Java & JBoss, Open Source & Red Hat, Blockchain & Ethereum

- [https://www.linkedin.com/in/maeste/](https://www.linkedin.com/in/maeste/)
- [https://twitter.com/maeste](https://twitter.com/maeste)
- [https://github.com/maeste/](https://github.com/maeste/)
- [http://www.onchain.it/](http://www.onchain.it/)
Today’s Agenda

- Brief introduction to blockchain concepts
- Cryptocurrencies and why they have monetary value
- Smart contracts and why you should care about
- Developing smart contracts on ethereum blockchain
What is the block chain?
What is the block chain?
The Guardian: Blockchain is a digital ledger that provides a secure way of making and recording transactions, agreements and contracts – anything that needs to be recorded and verified as having taken place.

Wikipedia: A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. A blockchain can serve as "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way."
What is a blockchain...a nice bullet list

- It’s a ledger of transactions and datas
- It’s persistent, secure and unmodifiable
- It’s based on computational trust
- It’s distributed and unstoppable
- Transaction parties are anonymous, but tx are public and verifiable
- It’s transactions could be about values (cryptocurrency)
- It’s trustless about nodes and users
Blockchain by images

A visual explanation of SHA/KECCAK one way function #blockchain_by_images #blockchain #sha
Blockchain by images

A visual explanation of public key encrypting and private keys decrypting messages
#blockchain_by_images #cryptography #blockchain_onchain.it/2017/11/blockc ...
Blockchain by images

A visual explanation of private key signing messages and public key verifying the sender.
#blockchain_by_images #cryptography #blockchain_onchain.it/2017/11/blockc ...
Blockchain by images
Byzantine Generals Problem (BGP)

A.C. 330

- N Generals
- Some are traitors
- Message passing

• Goals
  - Consensus (same plan) btw. loyal generals
  - A small number of traitors cannot cause the loyals to adopt a bad plan
  - Do not have to identify the traitors
Byzantine Problem solution

- Easy voting system
- In a permissionless system we can’t trust nodes/generals
- Sybil attack
- Need proof of ownership defense against Sybil attack
PoW

- Proof of ownership is HW used to compute the puzzle
- Puzzle hard to perform, easy to verify
- Only solving puzzle a miner could mine a block
- 51% attack
- HW/Power is an economic resource external to the system
We have mining farm like this
PoS

- Proof of ownership using digital assets instead of computational power
- Easier to prove (just digital signing)
- Intrinsic secure (crypto based)
- Reduce power usage == cost of consensus
- Is based on internal resources
- IS MORE DEMOCRATIC 1 ETH == 1 ETH no cost scaling
What is a blockchain...a nice bullet list

- It’s a ledger of transactions and data
- It’s persistent, secure and unmodifiable
- It’s based on computational trust
- It’s distributed and unstoppable
- Transaction parties are anonymous, but transactions are public and verifiable
- It’s transactions could be about value (cryptocurrency)
- It’s trustless about nodes and users

Live Demo
It’s distributed and unstoppable
It’s distributed and unstoppable
It’s distributed and unstoppable
Has those cryptocurrencies a real economic value? And why?

In economy “intrinsic value” concept doesn’t exist at all. We give value to money by convention, and more general anything gain value almost for 3 reasons (not strictly needed, but true in almost cases at least)

- It’s rare
- It’s hard to reproduce
- It could be exchanged
- Someone want to buy it (law of supply and demand)
Has those cryptocurrencies a real economic value? And why?

In economy, the “intrinsic value” concept doesn’t exist at all by convention, and more general anything gain value almost for 3 reasons (not strictly needed, but true in almost cases at least):

- It’s rare
- It’s hard to reproduce
- It could be exchanged
- Someone want to buy it (law of supply and demand)

1 Euro

1 Euro

~ 7K Euro

Fontana’s paint ~ 8M Euro

Manzoni’s artist’s shit: ~275K Euro
Traditional payments

Current payment systems require third-party intermediaries that often charge high processing fees...
Traditional payments

And isn’t ok to simply trust in a Bank?

What could happen?

Lehman Brothers…..

Current payment systems require third-party intermediaries that often charge high processing fees...
Traditional payments
So...what is the solution?

Grandmum solution?
So...what is the solution?

Could be at least unpractical...
The solution is the blockchain

- It's a ledger of transactions and datas
- It's persistent and secure
- It's based on computational trust
- It's distributed and unstoppable
- Transaction parties are anonymous, but transactions are public
- **It's transactions could be about values (cryptocurrency)**
- **It's trustless about nodes and users**
The solution is the blockchain

- It’s a ledger of transactions and data
- It’s persistent and secure
- It’s based on computational trust
- It’s distributed and unstoppable
- Transaction parties are anonymous, but transactions are public
- It’s transaction values can be public
- It’s trustless about nodes and users

Am I going to transfer my money without trusting anyone?
What does trustless mean?

You are not trusting in peers of transaction or even in nodes of the network, you are trusting in the protocol itself. In other words you are trusting blockchain and cryptocurrency itself and not people owning them....moreover they are anonymous...

Does it recall anything you well known and use everyday?
What does trustless mean?

You are not trusting in peers of transaction or even in nodes of the network, you are trusting in the protocol itself. In other words you are trusting blockchain and cryptocurrency itself and not people owning them. Moreover they are anonymous...

Does it recall anything you well known and use everyday?
What does trustless mean?

You are not trusting in peers of transaction or even in nodes of the network, you are trusting in the protocol itself, trusting blockchain and cryptocurrency itself and not people owning them. Moreover they are anonymous...

Does it recall anything you well known and use everyday?
Smart Contracts
What is a smart contract?

A **contract** is a voluntary arrangement between two or more parties that is enforceable by law as a binding legal agreement.

A **smart contract** is a computer protocol intended to facilitate, verify, or enforce the negotiation or performance of a contract.
Real world smart contracts

With the present implementations¹ "smart contract" is general purpose computation that takes place on a blockchain
Smart contracts: unstoppable Dapp

- Distributed
- Can transfer money/assets
- Unmodifiable state history
Ethereum: a blockchain for smart contracts

- Every node run a built in Virtual Machine (EVM)
- It provide a compiler from high level languages to EVM
- 2 different kind of accounts:
  - Externally owned account (EOAs), controlled by private keys
  - Contract accounts, controlled by code
Ethereum Virtual Machine

Internals

- TURING COMPLETE VM
- Stack based byte code (push, jump)
- Memory
- Storage
- Environment variables
- Logs
- Sub-calling

High level languages

- Solidity (c-like)
- Viper (python like)
- LLL (lisp inspired)
- Bamboo (experimental morphing language influenced by Erlang)

Everyone compiling to EVM code
EVM code execution

- Transaction sent to a **contract address**
- *Every full node of ethereum run the code at this address and store the state*
- Smart contract code can:
  - Could run any program (turing complete machine)
  - Read/write state
  - Call another contract
  - Send ETH to other address (both EOA and contract)
Ethereum GAS

Halting problem: determine if the program will finish running or continue to run forever. Classic NP-hard problem

Ethereum solution: GAS, a fee per computational step

GAS is not a currency is just a unit of measurement of computational step

In Tx you have “maximum GAS” you would give to the miner and “GAS price” to determine how much you will actually pay.

If Tx complete successfully you pay just for effective GAS used.

If the Tx would consume all GAS the TX will be revert, but you still pay for GAS

Ethereum hasn’t block size limit, but Gas Limit (6.7M currently, but voted by miners)
Ethereum GAS
Ethereum GAS price
Ethereum Out of GAS
To get the unstoppable world computer

Last year I was saying....

- Transaction sent to a **contract address**
- **Every full node of ethereum run the code at this address and store the state**

(and it’s bold because it’s important)
Wrold computer performing like this
And it’s busy
Scalability trilemma

The Blockchain Trilemma

Scalability

Security

Decentralization
Scalability solutions?

Off chain solution/child chain (raiden, lightning coin, plasma)

On chain solution (sharding, PoS, aka Ethereum 2.0)
Solidity

- C/Java-like syntax
- Statically typed
- Support inheritance (multiple)
- Complex user defined types (struct)
- Polymorphism
- Overriding
- ..... 

http://solidity.readthedocs.io/en/develop/index.html#
Our development environment

- testRPC (local in memory ethereum blockchain)
- Truffle (maven-like tool to compile and deploy contract)
- A bit of javascript (npm) for some raw Dapp interface
- Metamask to inject ethereum protocol in our html/javascript Dapp
- Intellij to edit solidity and javascript

More info: http://truffleframework.com/
SmartNotary

- The easiest contract notarizing a document
- Receiving document hash and owner name. It will write them in the blockchain state
- Giving the hash it will return the owner name
- It’s a pet project just to play with code

Talk is cheap....show me the f****ing code (Linus Torvalds)

https://github.com/onchainit/SmartNotary/tree/baseExample
We are using current EOA (from metamask) as owner.

It will give us the opportunity to play a bit with metamask

https://github.com/onchainit/SmartNotary/tree/baseExample
SmartNotary 2.0: paying for notarization

We are adding money transfer.

Basically the user will pay in ether the service of notarization.

The ethers are stored in contract balance, and only contract creator could withdraw them in his EOA

https://github.com/onchainit/SmartNotary/tree/pay4Notarization
Contract security - reentrancy attack

// INSECURE
mapping (address => uint) private userBalances;

function withdrawBalance() public {
    uint amountToWithdraw = userBalances[msg.sender];
    require(msg.sender.call.value.value(amountToWithdraw)());
    // At this point, the caller's code is executed, and can call withdrawBalance again
    userBalances[msg.sender] = 0;
}

Contract security - reentrancy attack

// VERY SIMPLIFIED MALICIOUS CODE (WOULD NEED CONSIDERATION ON BLOCK MAXIMUM GAS)
function() payable {
    vulnerable.withDraw();
}
Contract security - reentrancy attack solution

```solidity
mapping (address => uint) private userBalances;

function withdrawBalance() public {
    uint amountToWithdraw = userBalances[msg.sender];
    userBalances[msg.sender] = 0;
    require(msg.sender.call.value(amountToWithdraw)());
    // The user's balance is already 0, so future invocations won't withdraw anything
}
```

Or just using primitive send() instead of .call.value which limit gas to 2300 (pure transfer)

SmartNotary 3.0: paying for notarization and notarized document market

A bit more complex example

More money transfer

Blind auction

https://github.com/onchainit/SmartNotary/tree/marketplace
Who is behind ethereum?

A very young... extremely focused guy
Who is behind ethereum?

A Very young....extremely focused guy

Don’t you recall another very young extremely focused guy?
Who is behind Ethereum?
Thanks for coming

0x41a6021A6Dc82cbB0cd7ee0E3855654D225F48C6
I’ll use ethers only for beers :)

- https://www.linkedin.com/in/maeste/
- https://twitter.com/maeste
- https://github.com/maeste/
- http://www.onchain.it/