HS18

DISTRIBUTED SYSTEMS ADVANCED & BLOCKCHAIN

NEO

T. Bocek

thomas.bocek@hsr.ch

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

NEO

- **Hongfei Da, founder of NEO**
- **«Ethereum of China»**
  - Pushing engagement outside China
    - NEO Smart contract workshop in Santiago, Chile on Aug 2018
    - NEO Hackathon at TU Delft, 20.10.
  - Opinion: NEO: Is China Holding Its Best Blockchain Asset Back?
    - China's ban on ICOs and cryptocurrency trading
    - Other opinion
- **Formerly AntShares (2014) – rebranded**
  - Shanghai-based blockchain R&D company "OnChain" – 2 ICOs (in China!!)
    - 1st 550K USD (2100BTC), 2nd 4.5m USD

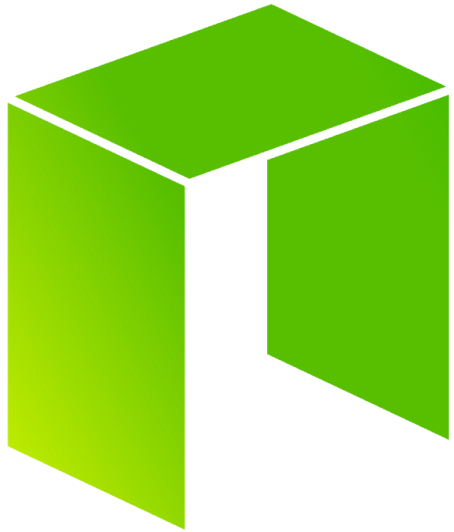
NEO Political

- "NEO Sponsor Giveback Plan" **Announcement**
  - Give back in the amount equal to the fiat value they contributed back then
  - «ICO, a highly-efficient yet controversial financing method has its two sides.»
  - China not ICO friendly, NEO gives back ICO investment
    - “undoing ICO”, but keeps price gains

NEO Hackathon

- **NEO Hackathon in Zurich**
  - 03.11 – 04.11.2018, 08:30 – 21:30
  - Swisscom AG Förrlibuckstrasse 181 8005 Zurich Switzerland
- **Schedule**
  - November 3rd (Saturday)
    - 8:30 Sign up
    - 9:00 Opening ceremony, announce hackathon theme and rules
    - 9:30 Free Team Up
    - **10:00 Start hacking!**
    - 12:30 Lunch
  - November 4th (Sunday)
    - **18:00 Project Submit Due**
    - 18:30 Presentations
    - 21:00 Awards Announcement
- **Judging Factors / Price**
  - Functionality, Ease to Use, Stability, Performance, Originality
  - First Prize - 500 NEO (1 team)
  - Second Prize - 450 GAS (1 team)
  - Third Prize - 300 GAS (3 teams)
  - Mystery Prize (It depends on the submitted work)

- **NEO is**
  - Digital Assets + Digital Identity + Smart Contract = Smart Economy
- **Active Blockchain**
  - Every block ~10-60 Tx
- **Attention: NEO Super (NEOX, hard fork), Blockchain Neo (Japan Brand Coin) - Scam?**
- **July 2018: NEO blockchain starts decentralization**
  - NEO == centralized consensus?
  - NEO voted for new consensus node CoZ
    - “City of Zion is a global, independent group of open source developers, designers and translators which support the NEO core and ecosystem.”



NEO
smart economy

NEO Token

- **NEO and NeoGas**
  - Pre-mined, max 100 million tokens, 15 sec block time
- **50/50**
  - 50m distributed during ICO, 50m is kept by NEO
  - ~350m USD investment power
  - 15% dedicated to other blockchain projects
- **GAS is generated with each new block**
  - Total limit of 100 million GAS will be achieved in about 22 years
  - GAS will be distributed proportionally in accordance with the NEO holding ratio – PoS
  - 8 GAS every block, reduced by 1 ever 2m blocks

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
12	IOTA	$1,377,729,855	$0.495670	$18,078,573	2,779,530,283 MIOTA *	-3.15%	
13	Dash	$1,292,529,942	$154.06	$166,767,055	8,389,597 DASH	-3.36%	
14	Binance Coin	$1,269,918,405	$9.71	$25,522,164	130,799,315 BNB *	-2.12%	
15	NEO	$1,060,068,089	$16.31	$339,487,764	65,000,000 NEO *	-5.20%	
16	Ethereum Classic	$1,006,284,229	$9.55	$136,069,596	105,385,599 ETC	-1.98%	
17	NEM	$847,576,709	$0.094175	$5,161,489	8,999,999,999 XEM *	-1.67%	
18	Tezos	$793,965,923	$1.31	$2,501,514	607,489,041 XTZ *	-4.41%	

NEO Token / Technical

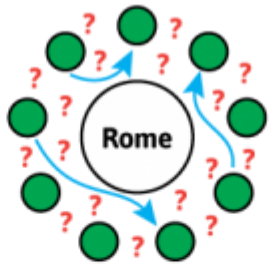
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
105	Mixin	$54,218,864	$122.19	$8,557	443,743 XIN *	-1.01%	
106	ZCoin	$54,150,119	$9.40	$555,789	5,757,841 XZC	-4.66%	
107	QuarkChain	$54,007,916	$0.067371	$5,095,024	801,649,919 QKC *	0.05%	
108	Gas	$52,051,444	$5.14	$581,217	10,128,375 GAS *	-4.42%	
109	Bitcoin Private	$50,922,778	$2.48	$95,935	20,524,490 BTCP	-2.32%	
110	Syscoin	$50,658,818	$0.093483	$221,244	541,902,755 SYS	-2.23%	
111	SALT	$48,036,029	$0.578418	$1,212,934	83,047,261 SALT *	-3.17%	

- **Consensus mechanism: dBFT**
  - Delegated Byzantine Fault Tolerant
  - Delegates create block, 2/3 need to approve through voting:
  - Works if more than 50% honest
- **Byzantine Generals' Problem**

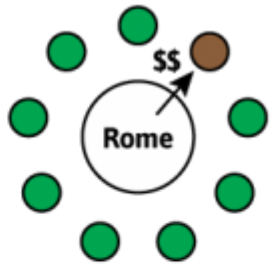
Imagine Rome being besieged by **nine armies**, each commanded by a (Byzantine) general.

In order to launch a succesful **attack** or retreat, all armies have to **do the same**, otherwise they will be decimated by Rome's armies.

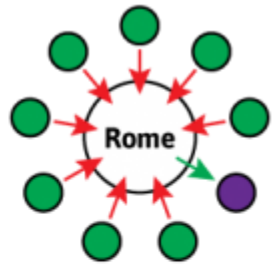
The decision to either **attack** or retreat is put up to a **vote**. Whichever option receives **more than 50%** of the votes, that's what the Generals will do (**retreat** in the example above).



Problem 1
The generals communicate by using **couriers**, who have to cross unknown areas controlled by the Romans, risking capture or their message becoming corrupt.



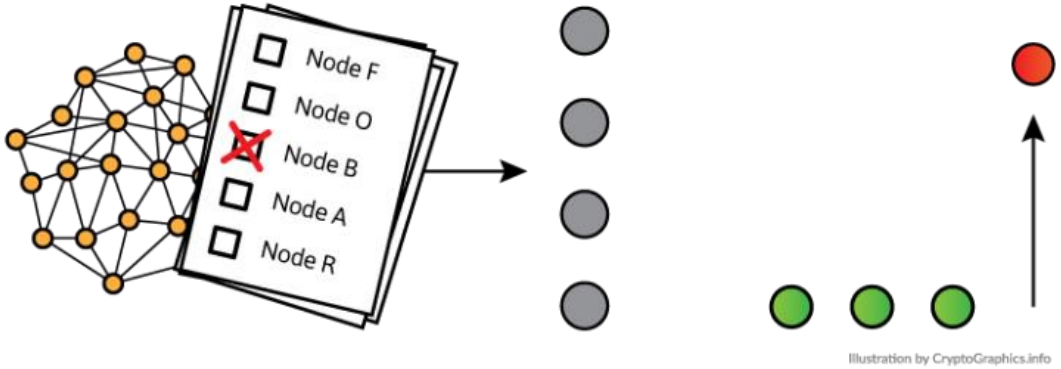
Problem 2
Each of the generals could be bribed by the Romans: **Traitorous Generals**.



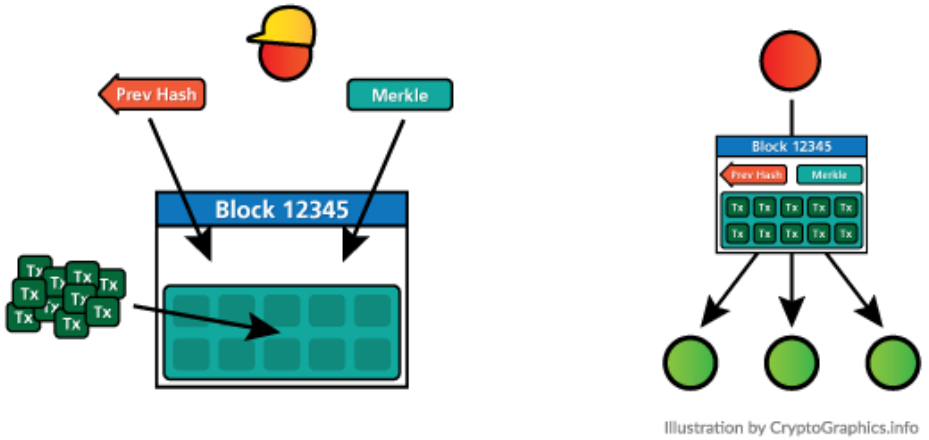
Problem 3
Any of the Generals can make the wrong decision, regardless of the vote: **Improperly Functioning Generals**.

Delegated Byzantine Fault Tolerant

- **Nodes in the network elect a group of consensus nodes (e.g. CoZ)**
- **Leader/speaker randomly chosen from consensus nodes, rest are delegates**



- **Leader/speaker creates new block, needs to be positively checked by 2/3 of delegates**
- **If 2/3 agrees, block added to the chain**

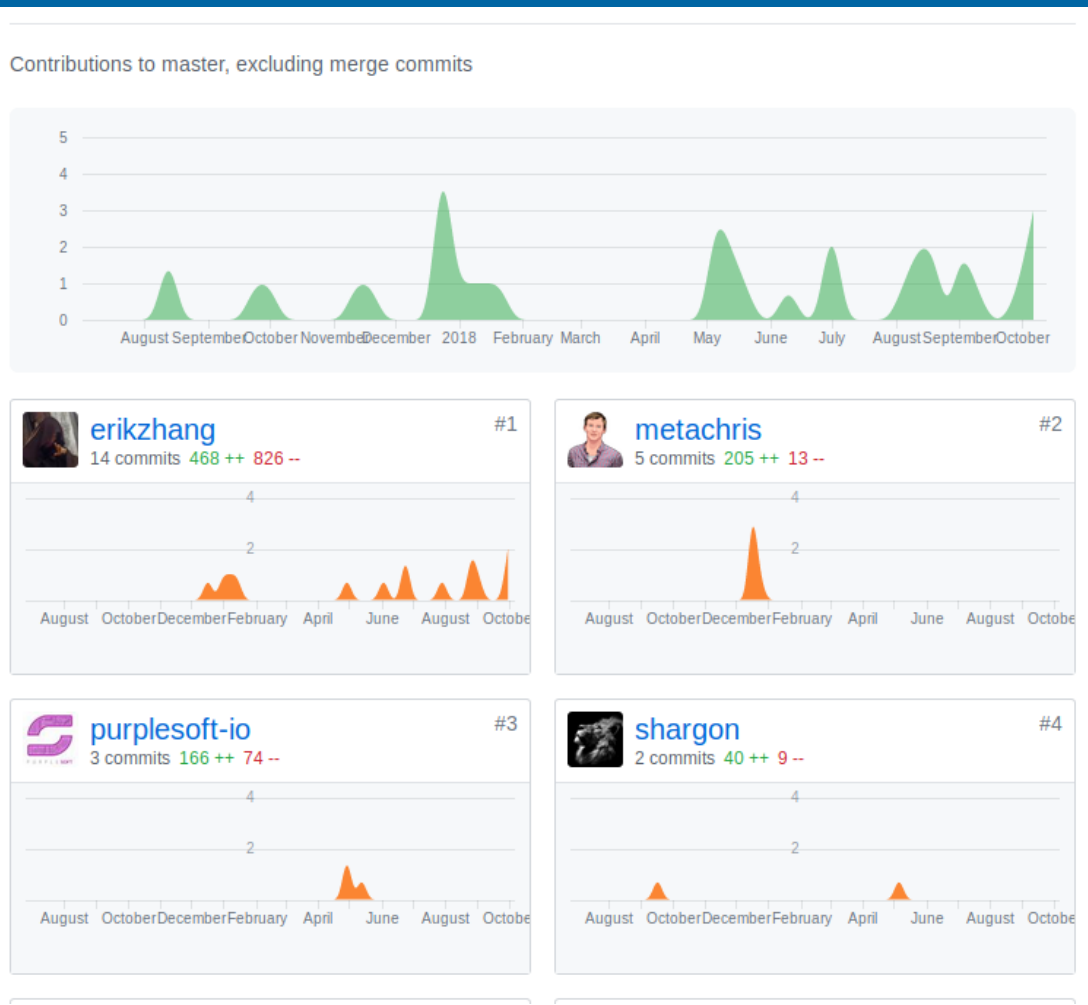


- **Countermeasures for dishonest leader/speakers or delegates**

(source)

NEO Technical

- **C# driven**
  - Github repos – shows activity, e.g., neo-cli
- **Smart Contracts:**
  - C#, Python, Golang
  - Visual Studio, Eclipse, etc.
  - NeoVM – Stack-based VM
- **15-20s block time**
  - 1000 TPS, claiming to reach 10000 TPS
- **NeoVM: «like introducing a JIT»**
  - Not there yet. Compile to avm, execute in NeoVM
- **NeoX (Cross-chain interoperability agreement) / NeoFS (Distributed Storage Protocol) / NeoQS (Anti-quantum cryptography mechanism)**
  - Ideas in the whitepaper



NEO Outlook

- **“Ethereum requires developers to learn to program with Solidity. Neo, on the other hand, will support almost all programming languages via a compiler, including those on Microsoft.net, Java, Kotlin, Go and Python”**
  - Based on the docs/web: looks solid - Good Documention
  - Based on neoscan: looks solid
  - Github activity: good
  - Beginner friendly: room for improvement

Smart Contract Example - Lock (Lock Contract)

```
public class Lock : SmartContract
{
    public static bool Main(uint timestamp, byte[] pubkey, byte[] signature)
    {
        Header header = Blockchain.GetHeader(Blockchain.GetHeight());
        if (header.Timestamp < timestamp)
            return false;
        return VerifySignature(signature, pubkey);
    }
}
```

URL: b.socrative.com/student/

Room: HSR

Token Interface Comparison: Ethereum / NEO

ERC-20

- Functions
  - `function totalSupply() public constant returns (uint);`
  - `function balanceOf(address tokenOwner) public constant returns (uint balance);`
  - `function allowance(address tokenOwner, address spender) public constant returns (uint remaining);`
  - `function transfer(address to, uint tokens) public returns (bool success);`
  - **`function approve(address spender, uint tokens) public returns (bool success);`**
  - **`function transferFrom(address from, address to, uint tokens) public returns (bool success);`**
- Events
  - `event Transfer(address indexed from, address indexed to, uint tokens);`
  - **`event Approval(address indexed tokenOwner, address indexed spender, uint tokens);`**

NEP-5 / NEP5(.1)

- Functions
  - `BigInteger totalSupply()`
  - `string name()`
  - `string symbol()`
  - `byte decimals()`
  - `BigInteger balanceOf(byte[] account)`
  - `bool transfer(byte[] from, byte[] to, BigInteger amount)`
- Events
  - `event transfer(byte[] from, byte[] to, BigInteger amount)`

NEO HSR Smart Contract in Golang

- **Run private NEO blockchain**
  - Simple NEP-5 contract costs 500 gas (2700$)
  - https://github.com/slipo/neo-scan-docker
  - `docker-compose up`
  - UI: http://localhost:4000/
- **Neo-storm – compiles go to NeoVM (avm)**
  - https://github.com/tbocek/DSA-NEO-Testtoken (golang)
  - `neo-storm compile -i main.go -o main.avm`
  - Copy main.avm to NEO docker
  - `sudo docker exec -it 8ca09028062a /bin/bash`
  - `neopy - open wallet neo-privnet.wallet`
  - Commands: `wallet, tx 0x…, contract search HSR, testinvoke deploy / transfer`
- **Deploy:**
  - import contract main.avm 0710 05 True False False
- **Interact with NEO smart contract**
  - https://neo-python.readthedocs.io/en/latest/neo/SmartContract/smartcontracts.html
- **More infos:**
  - https://medium.com/coinmonks/neo-token-contract-nep-5-in-go-f6b0102c59ee

NEO Blockchain

- **The NEO network was faced with “malicious” spam attacks in August and was flooded with meaningless transactions.**
  - https://neo.org/blog/details/4095
    - Announcements about “Malicious” Transactions
    - MaxFreeTransactionsPerBlock: 20
- **Bounty: https://neo.org/dev/bounty**
  - https://neo.org/blog/details/4102
  - 1000 NEO payed
    - Aug 15, 2018 15:00 Bug identified and tested
    - Aug 15, 2018 18:57 Bug report emailed to NEO
    - Aug 15, 2018 19:04 NEO officially confirmed it
    - Aug 15, 2018 20:00 NEO founder, Erik Zhang, released a bug fix

```
private void SerializeStackItem(StackItem item, BinaryWriter writer)
{
    switch (item)
    {
        case ByteArray _:
            writer.Write((byte)StackItemType.ByteArray);
            writer.WriteVarBytes(item.GetByteArray());
            break;
        case VMBoolean _:
            writer.Write((byte)StackItemType.Boolean);
            writer.Write(item.GetBoolean());
            break;
        case Integer _:
            writer.Write((byte)StackItemType.Integer);
            writer.WriteVarBytes(item.GetByteArray());
            break;
        case InteropInterface _:
            throw new NotSupportedException();
        case VMArray array:
            if (array is Struct)
                writer.Write((byte)StackItemType.Struct);
            else
                writer.Write((byte)StackItemType.Array);
            writer.WriteVarInt(array.Count);
            foreach (StackItem subitem in array)
                SerializeStackItem(subitem, writer);
            break;
        case Map map:
            writer.Write((byte)StackItemType.Map);
            writer.WriteVarInt(map.Count);
            foreach (var pair in map)
            {
                SerializeStackItem(pair.Key, writer);
                SerializeStackItem(pair.Value, writer);
            }
            break;
    }
}
```

Source: http://blogs.360.cn/post/neo-runtime_serialize-dos.html

URL: b.socrative.com/student/

Room: HSR

Questions?

Prof. Dr. Thomas Bocek thomas.bocek@hsr.ch
Roman Blum roman.blum@hsr.ch