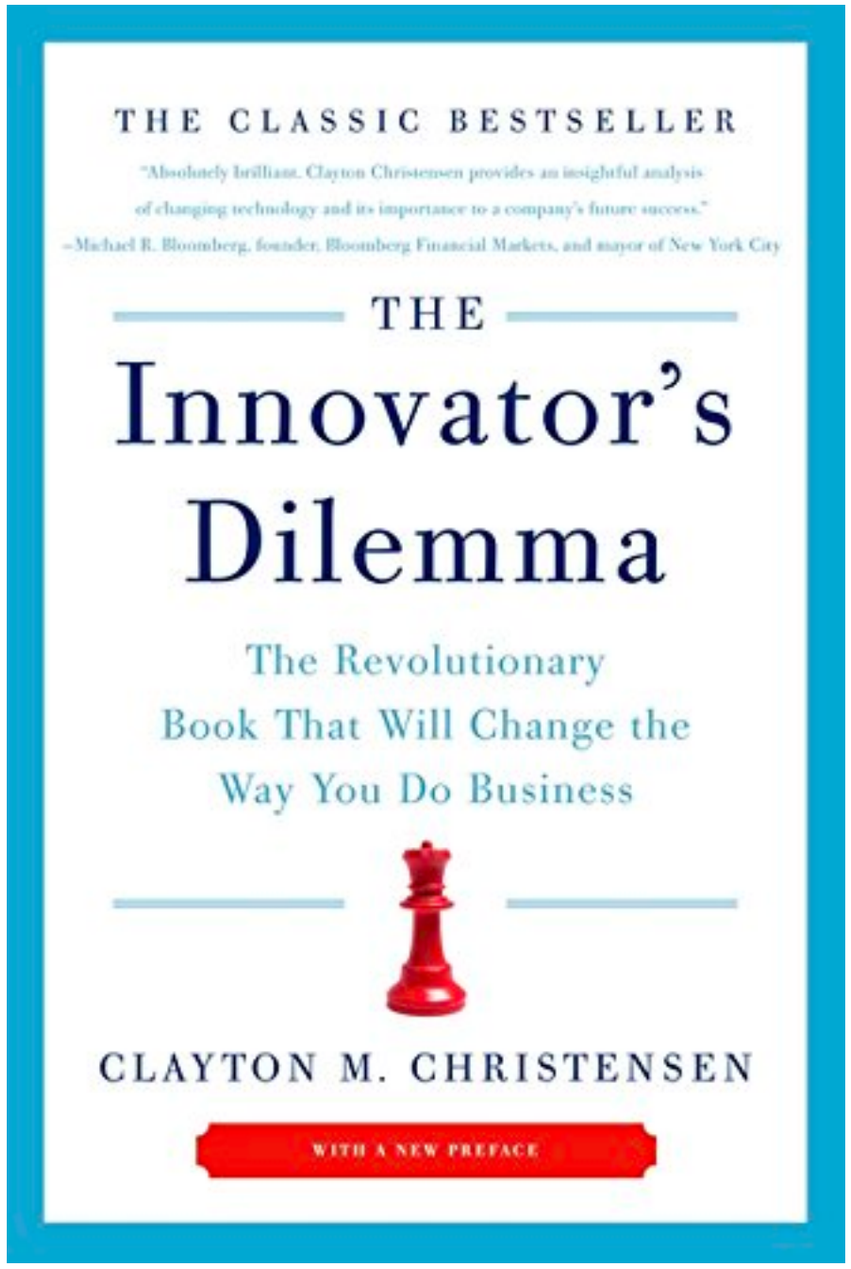
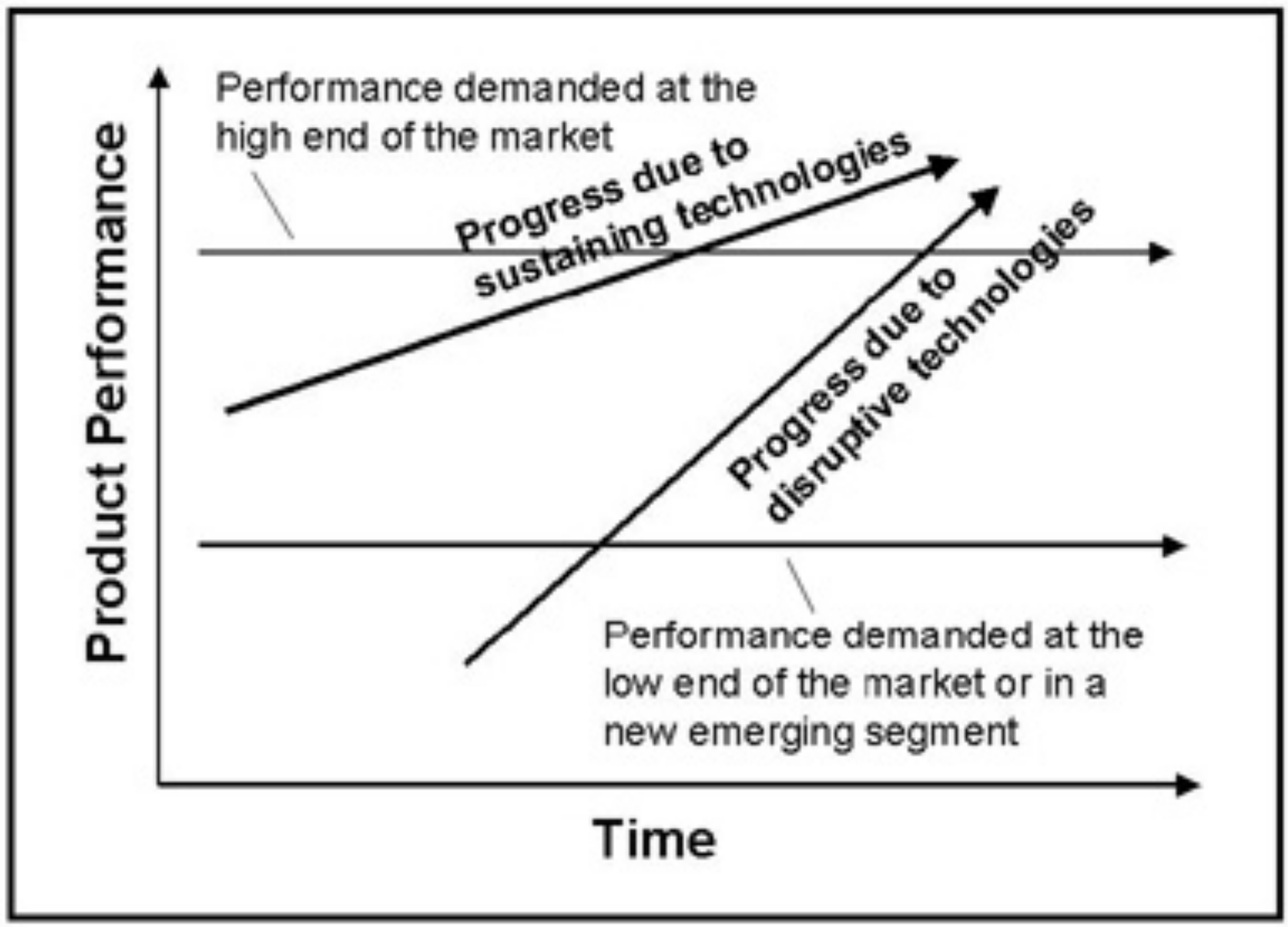
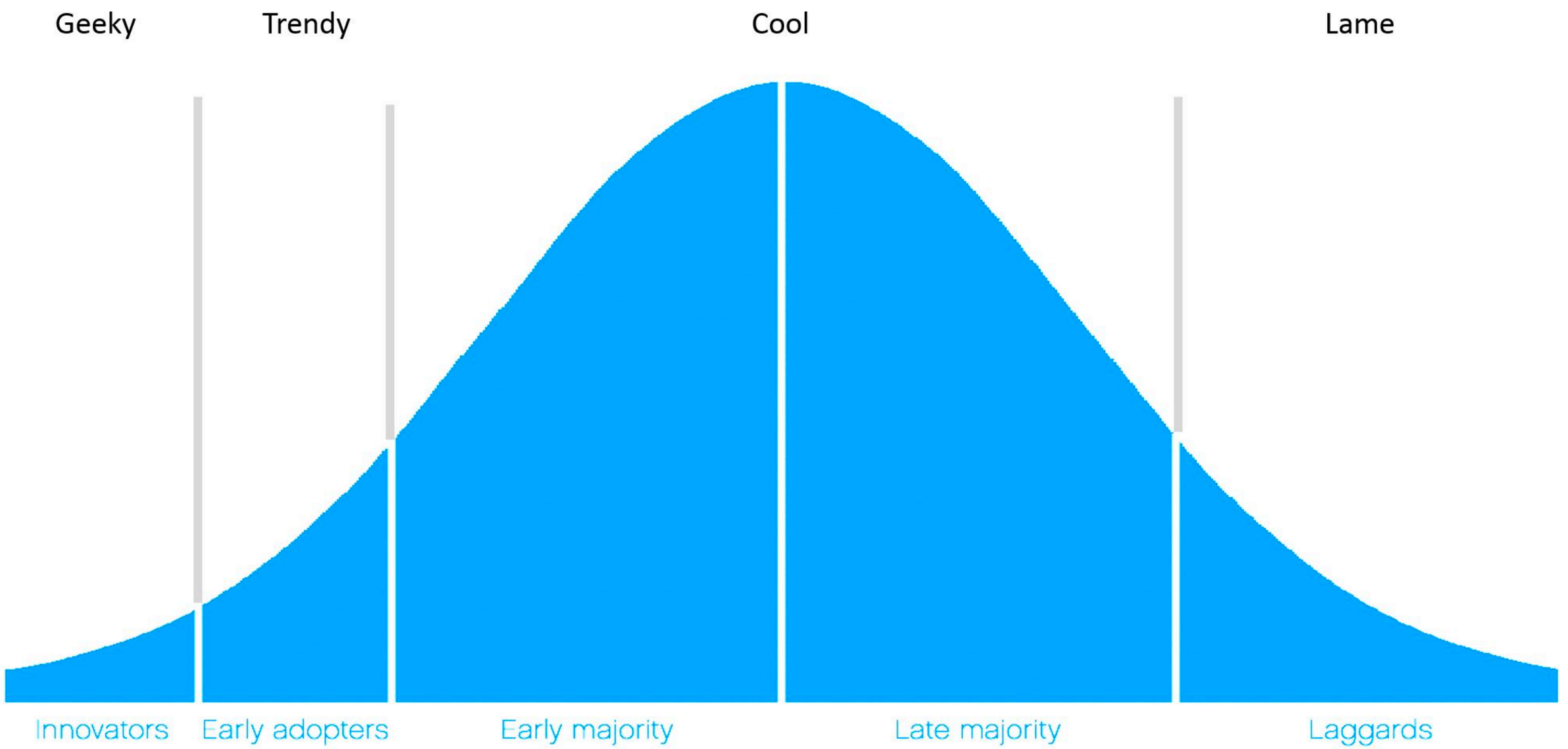
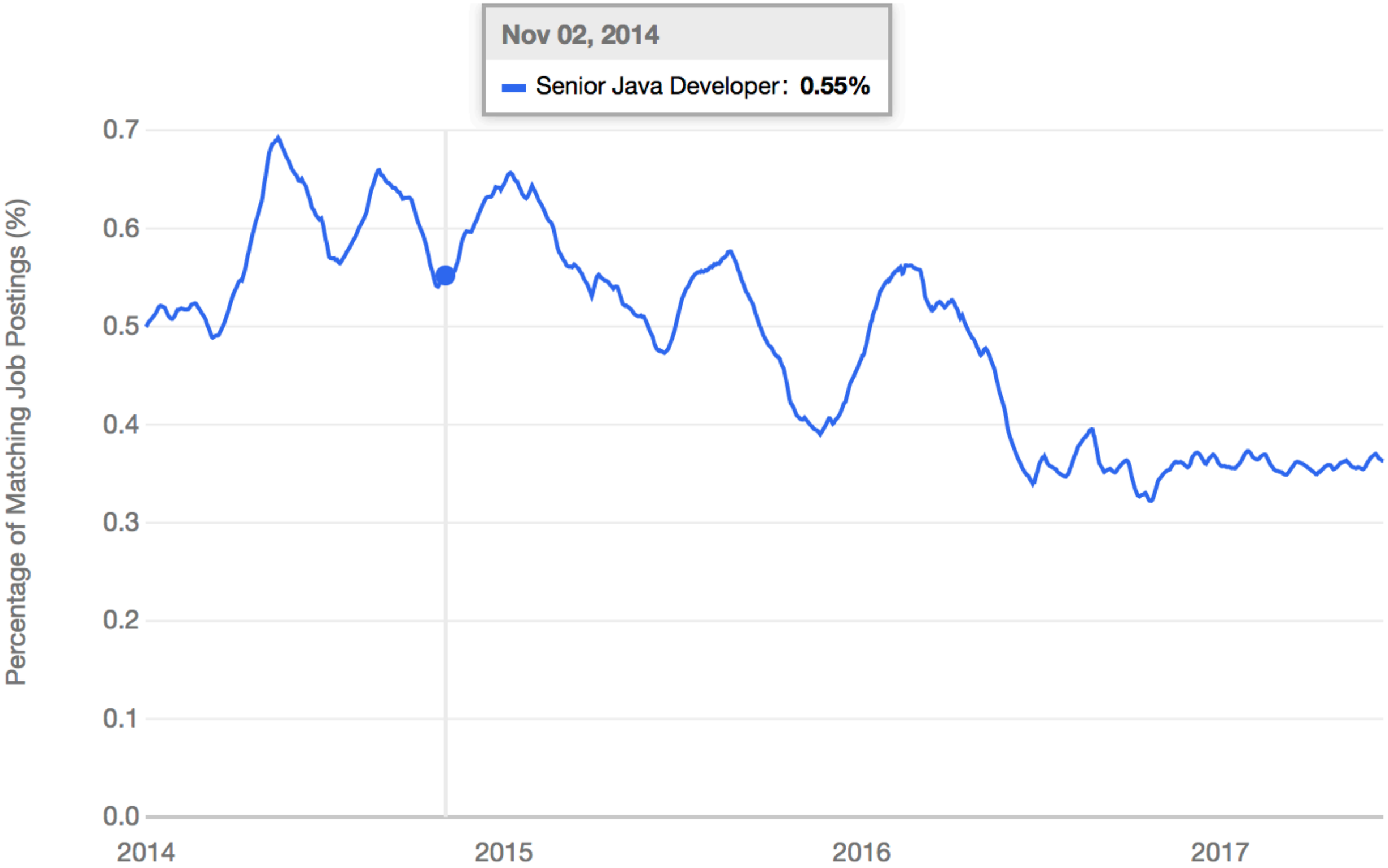
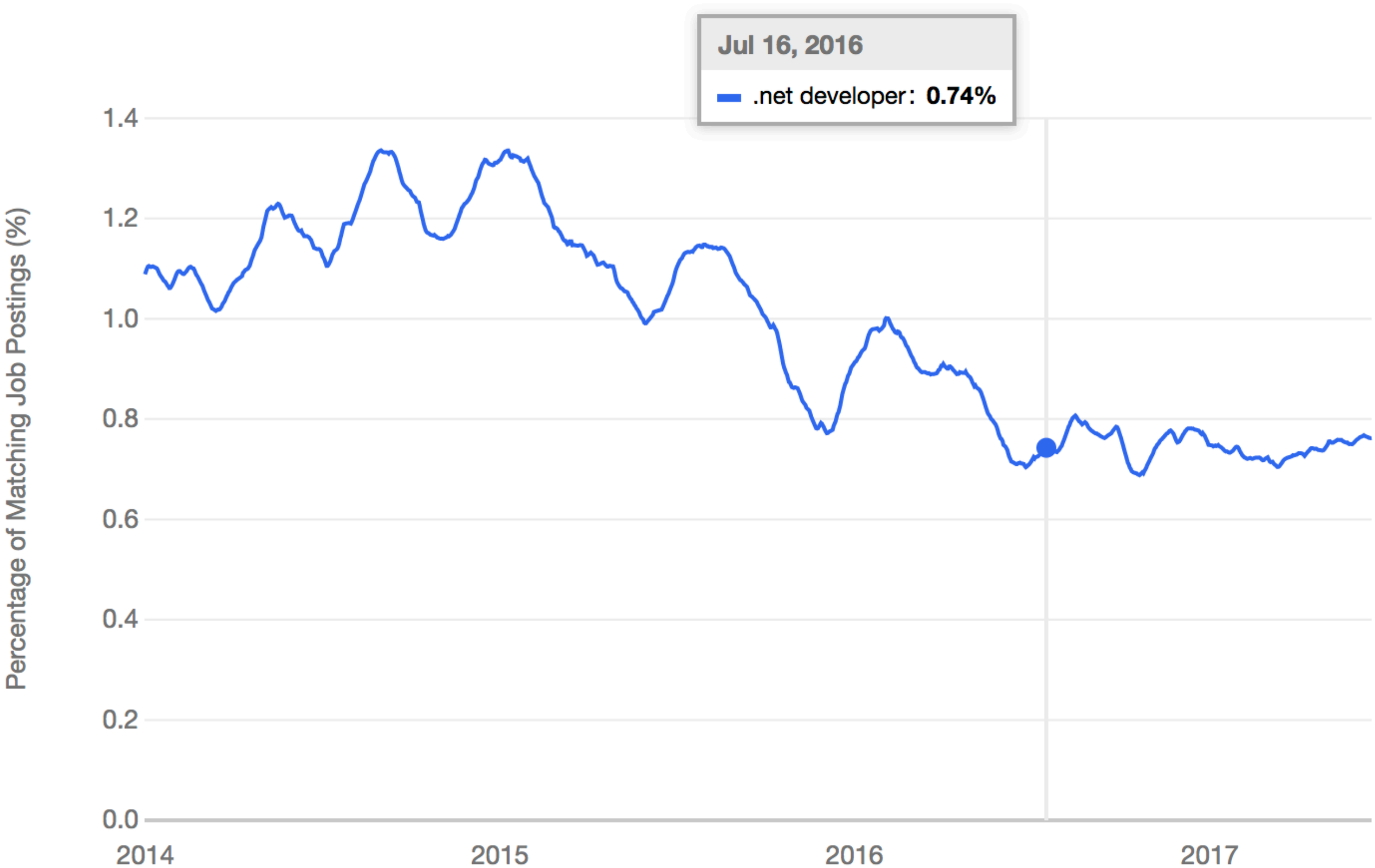
FROM BLOCKCHAIN TO ETHEREUM

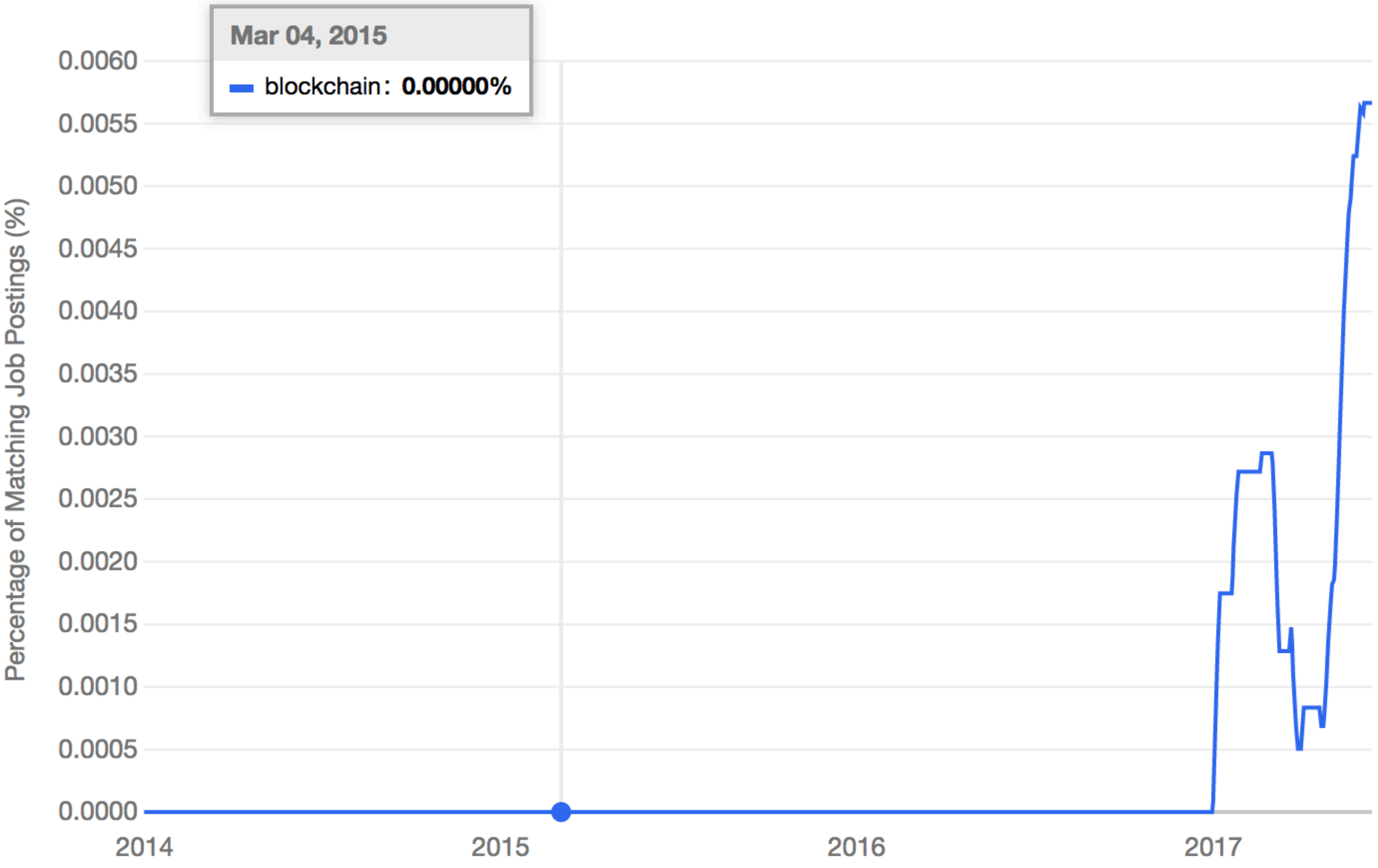

THE CLASSIC BESTSELLER
"Absolutely brilliant. Clayton Christensen provides an insightful analysis of changing technology and its importance to a company's future success."
–Michael R. Bloomberg, founder, Bloomberg Financial Markets, and mayor of New York City
THE
Innovator's Dilemma
The Revolutionary Book That Will Change the Way You Do Business
CLAYTON M. CHRISTENSEN
WITH A NEW PREFACE

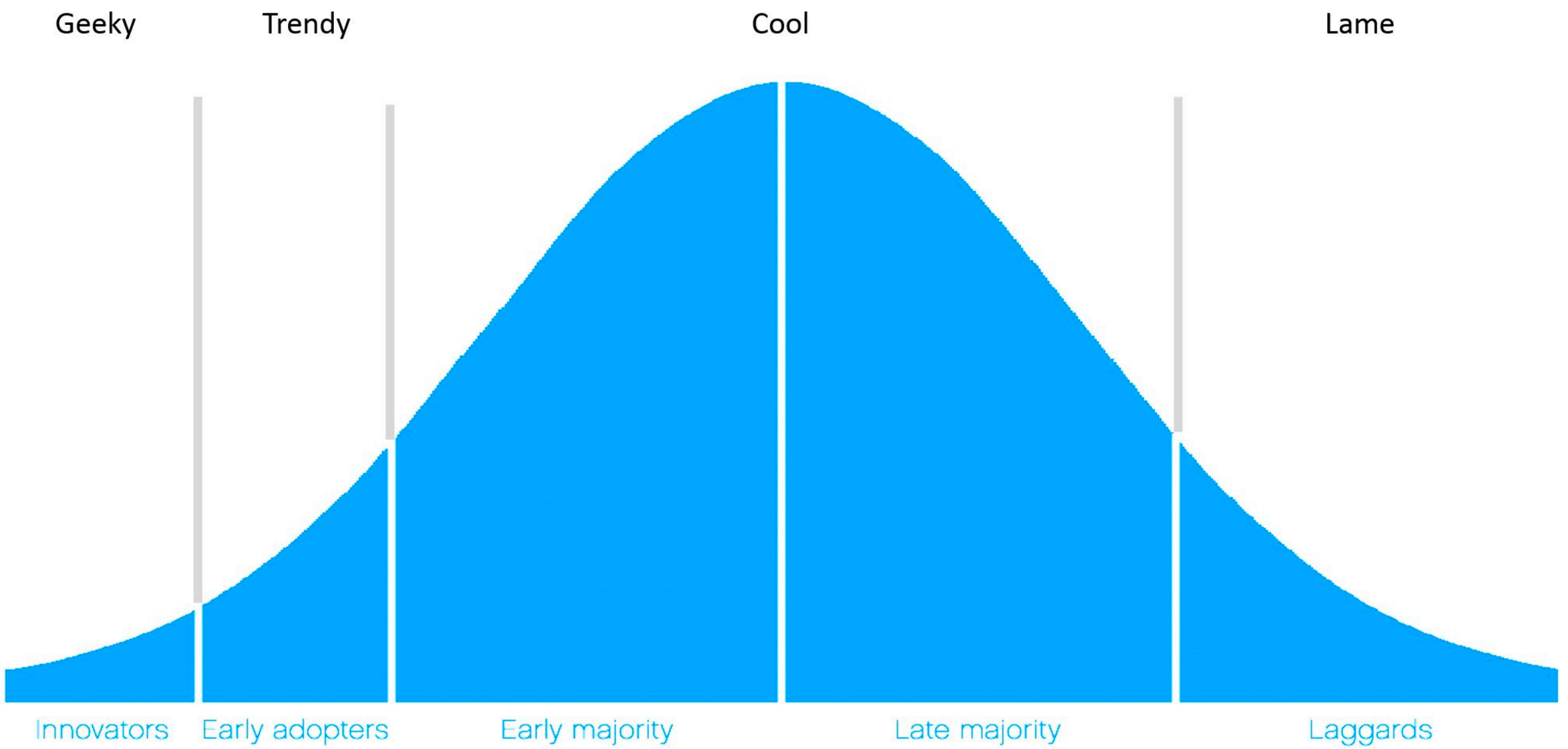

Performance demanded at the high end of the market
Progress due to sustaining technologies
Progress due to disruptive technologies
Performance demanded at the low end of the market or in a new emerging segment
Product Performance
Time


Geeky
Trendy
Cool
Lame
Innovators
Early adopters
Early majority
Late majority
Laggards


Nov 02, 2014
Senior Java Developer: 0.55%
Percentage of Matching Job Postings (%)
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
2014
2015
2016
2017


Jul 16, 2016
.net developer: 0.74%
Percentage of Matching Job Postings (%)
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0
2014
2015
2016
2017


Mar 04, 2015
blockchain: 0.00000%
Percentage of Matching Job Postings (%)
0.0060
0.0055
0.0050
0.0045
0.0040
0.0035
0.0030
0.0025
0.0020
0.0015
0.0010
0.0005
0.0000
2014
2015
2016
2017


Geeky
Trendy
Cool
Lame
Innovators
Early adopters
Early majority
Late majority
Laggards

BLOCKCHAIN

Problem: Trust

Bitcoin

Bitcoin is a cryptocurrency and a digital payment system invented by an unknown programmer, or a group of programmers, under the name Satoshi Nakamoto. It was released as open-source software in 2009.

- Cryptocurrency
- Fully distributed
- Blockchain
- One shared distributed ledger
- There is only one
- No double spending

Bitcoin Under the Hood

- All full nodes download the whole blockchain
- Transactions are emitted to the network
- Miners sign blocks for reward
- Everybody checks the rules
- You cheat, you get forked

Ledger

From	To	Amount
Alice	Bob	15
Jon	Ann	3
Bob	Ryan	30
Bob	Danny	10

Blockchain

From	To	Amount
1JCe8z4jJVNXSjohjM4i9Hh813dLCNx2Sy	3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v	15
3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v	2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r	3
2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r	1JCe8z4jJVNXSjohjM4i9Hh813dLCNx2Sy	30
2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r	3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx	10

ETHEREUM

Blockchain

From	To	Data
0x52bc44d5378309ee2abf1539bf71de1b7d7be3b5	0x5379718a93F46d9d2E8ac2e355f2087b6C43C010	Value: 15
0xe0Cd84c2FfE0e86C29556DF4efBA65f86E864627	0xfe02a56127affbba940bb116fa30a3af10d12f80	Value: 3

0x27dcf986BC1151B39CeadD53660e4AF56B0D5f84		Code:
		contract Escrow {
		function f() {
		…
		}
		}
		
		0x2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r

0x40cA1a9ddc9840D19bB679D85cC0DFe9De985fd5	0x2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r	call f();

ETHEREUM

Ethereum is blockchain-based distributed computing platform featuring smart contract functionality. It provides a decentralised virtual machine.

- Wallets
- Contracts

- Money transactions
- Method calls

ETHEREUM

Contracts

- Execute code
- Store information

- Turing complete
- Deterministic

- Ether (cryptocurrency)
- Pay for execution with Gas (bought with Ether)

WHY DO I CARE?

Imagine…

- I send some ether to
- You send some ether to
- Person at random gets all the ether

Imagine…

- I send some ether to
- You send some ether to
- Depends on the result of the match one of us gets all the “money”

Imagine…

- I bet against you if I will have a fire in two years in my apartment

How about?

- Company on a blockchain?
- International registry of…
- Transparent supply chain

Problem: Trust

Trust

The same way internet redefined how we communicate; The same way blockchain will redefine the notion of trust.

TOKENS

Tokens

- Smart contract
- Lightweight cryptocurrency
- Use Ethereum infrastructure
- You can use Ethereum wallet

ICO

- Initial Coin Offering
- New crowdfunding platform
- Done on entirely Ethereum

- Companies raised over 1,5 billion USD via ICO in 2017!
- vs. 358 millions from VCs for blockchain related startups
- Becoming real competitor to VC money!

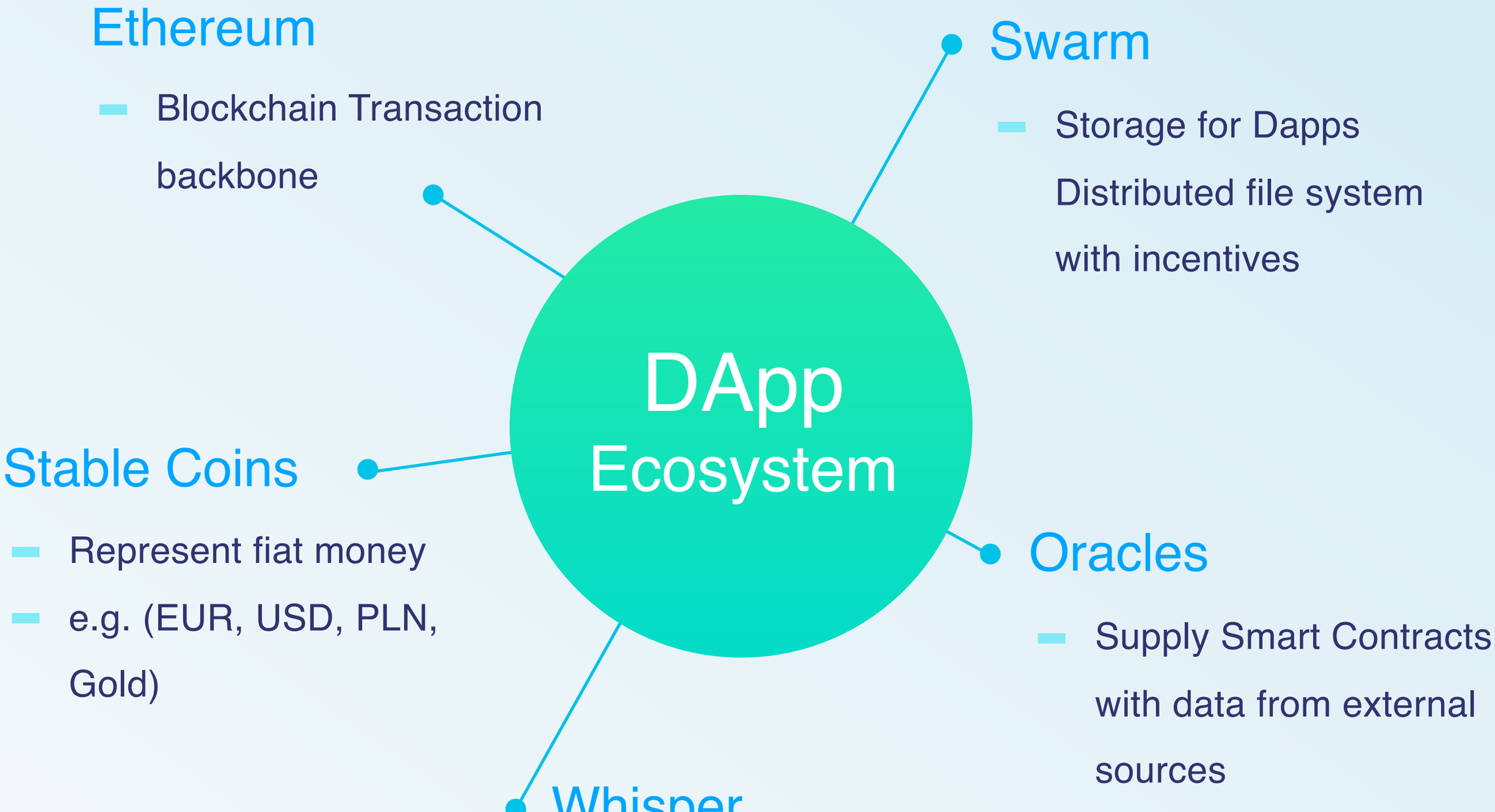
SMART CONTRACTS

```
contract mortal {

    address owner;

    function mortal() { owner = msg.sender; }

    function kill() { if (msg.sender == owner) selfdestruct(owner); }
}

contract greeter is mortal {
    string greeting;

    function greeter(string _greeting) public {
        greeting = _greeting;
    }

    function greet() constant returns (string) {
        return greeting;
    }
}
```

```
contract Purchase {
    uint public value;
    address public seller;
    address public buyer;
    enum State { Created, Locked, Inactive }
    State public state;

    function Purchase() payable {
        seller = msg.sender;
        value = msg.value / 2;
        require((2 * value) == msg.value);
    }

    function confirmPurchase()
        inState(State.Created)
        condition(msg.value == (2 * value))
        payable
{
    buyer = msg.sender;
    state = State.Locked;
}

function confirmReceived()
    onlyBuyer
    inState(State.Locked)
{
    state = State.Inactive;
    buyer.transfer(value);
    seller.transfer(this.balance);
}
```

```
    modifier condition(bool _condition) {
        require(_condition);
        _;
    }

    modifier onlyBuyer() {
        require(msg.sender == buyer);
        _;
    }

    modifier onlySeller() {
        require(msg.sender == seller);
        _;
    }

    modifier inState(State _state) {
        require(state == _state);
        _;
    }

    function abort()
        onlySeller
        inState(State.Created)
    {
        state = State.Inactive;
        seller.transfer(this.balance);
    }

}
```

DAPPS



Ethereum

- Blockchain Transaction backbone

Swarm

- Storage for Dapps
- Distributed file system with incentives

Stable Coins

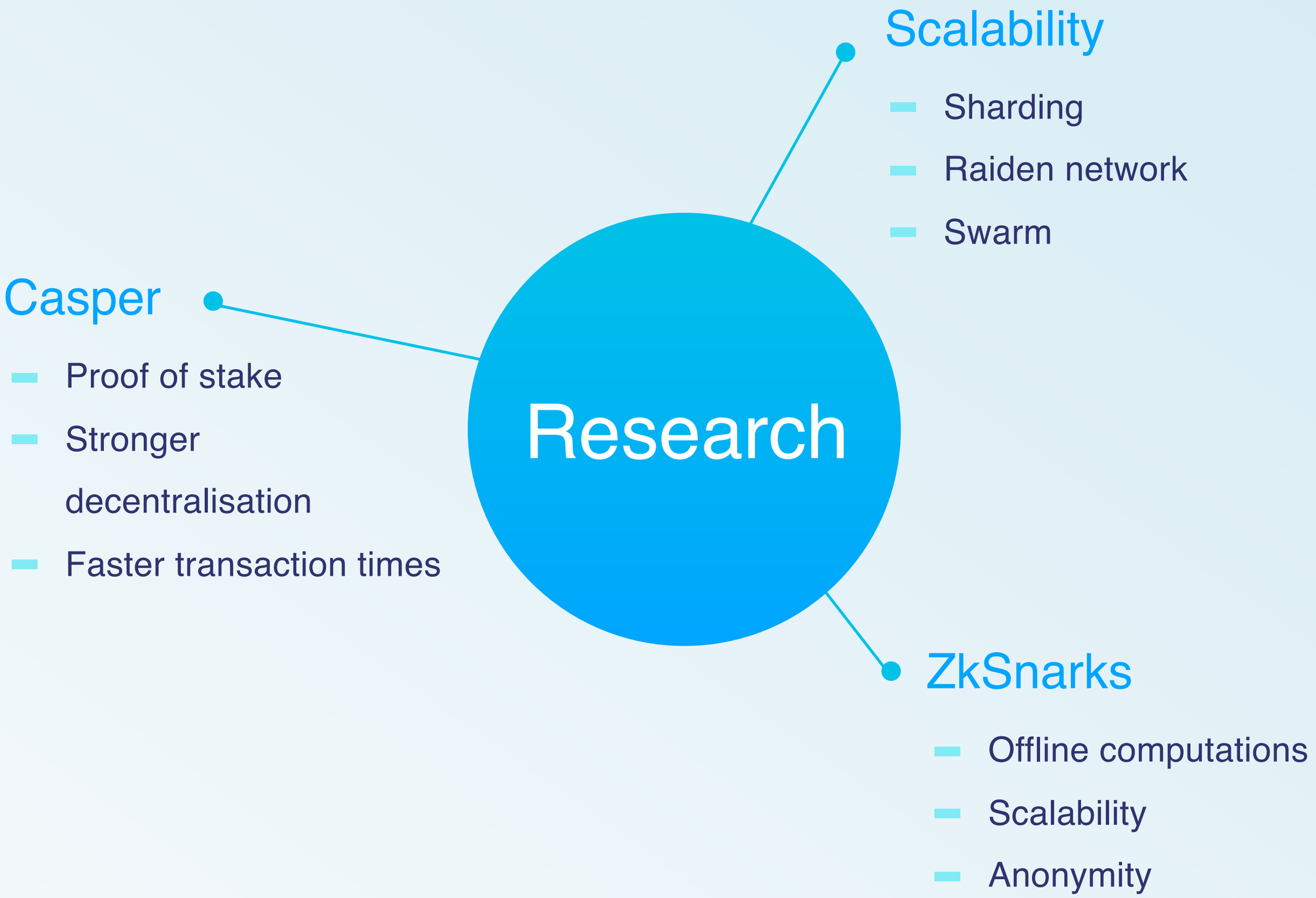
- Represent fiat money
- e.g. (EUR, USD, PLN, Gold)

Oracles

- Supply Smart Contracts with data from external sources

Whisper

- Anonymous distributed messaging system


Scalability
Sharding
Raiden network
Swarm
Casper
Proof of stake
Stronger decentralisation
Faster transaction times
Research
ZkSnarks
Offline computations
Scalability
Anonymity

Early internet

Server

Client

Web 2.0

Cloud (Servers)

Browsers

Web 3.0

Blockchain,

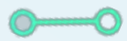
Distributed storage,

Browser/Whisper

Blockchain,

Distributed storage,

Browser/Whisper



Blockchain,

Distributed storage,

Browser/Whisper

Web 1.0

Service provider

Server

Customers

Web 2.0

Platform provider

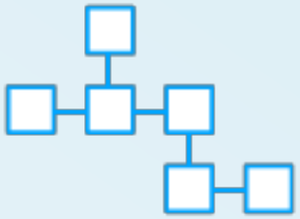
Cloud

Service providers

Customers

Web 3.0

Developers



Blockchain (DApps)

Service providers

Customers

ARAGON

Company on the blockchain

- Ownership
- Voting and
- Liquid democracy
- Salaries
- Transparency
- Raised over 25mln USD in ICO

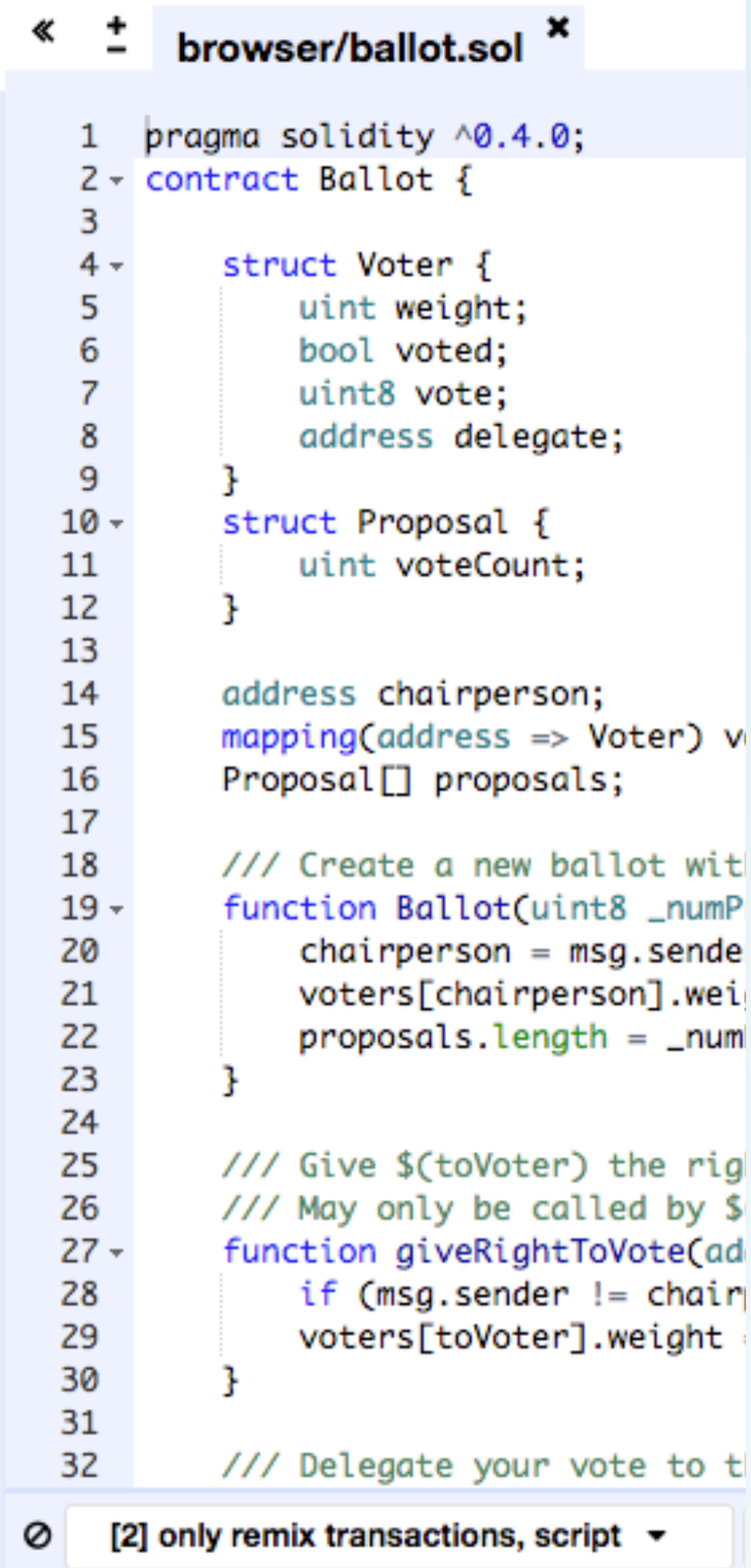
Ambrosus

- Transparent Food Supply Chain
- Tracking items as they travel through supply chain
- IOT hardware
- Automatic contract settlement
- Raised over 30mln USD in ICO

Introduction to Solidity

CHEAT SHEET

goo.gl/qXKZvi



Remix IDE

- Online programming environment
- Works in a browser
- remix.ethereum.org
- Start point: https://goo.gl/imb1qT

Task 1

Note:
Function addPoints is not verifying _student parameter.

Problem:
In the map points can contain people that are not members of the course.

Task:
Add validation.

Gas

- Used to pay a fee for code execution
- Goes to a miner who signs a block
- Two parts:
  - Constant: 21000
  - Variable - sum of cost of all the instructions
- Decided by transaction creator accepted (or not) by the miner

https://ethgasstation.info/

Task 2

Note:

One needs to call addPoints for each student separately.

Problem:

One pays base cost each time.

Task:

Add function addPoints which will take two arrays of the same length of student addresses and marks.

Homework

Implement a contract that will provide functions of a map(bytes32 => bytes32) with a feature to iterate over keys.

We will check the homework on the next course.

Marek Kirejczyk

Follow us on twitter
@ethworks

marek@ethworks.io

ETHWORKS