## Developing an Ethereum blockchain application

#### Created by: Nikolaos-Petros Triantafyllidis

Who the frack am I?

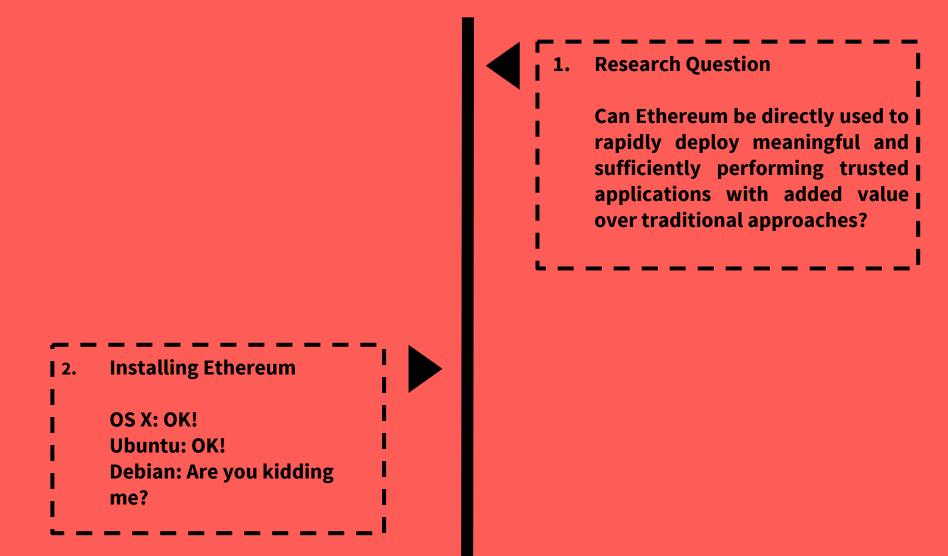
Who the frack am I?

> What the frack is Ethereum?

Who the frack am I?

> What the frack is Ethereum?

> > I cannot explain everything...



#### 0. Motivation

- I → Hype: 'The Internet how it was supposed to be'.
- → More hype: \$18.5M funding
- → Contracts: The 'safeguards' of liberty.

2. Installing Ethereum

OS X: OK!

Ubuntu: OK!

Debian: Are you kidding

me?

#### 1. Research Question

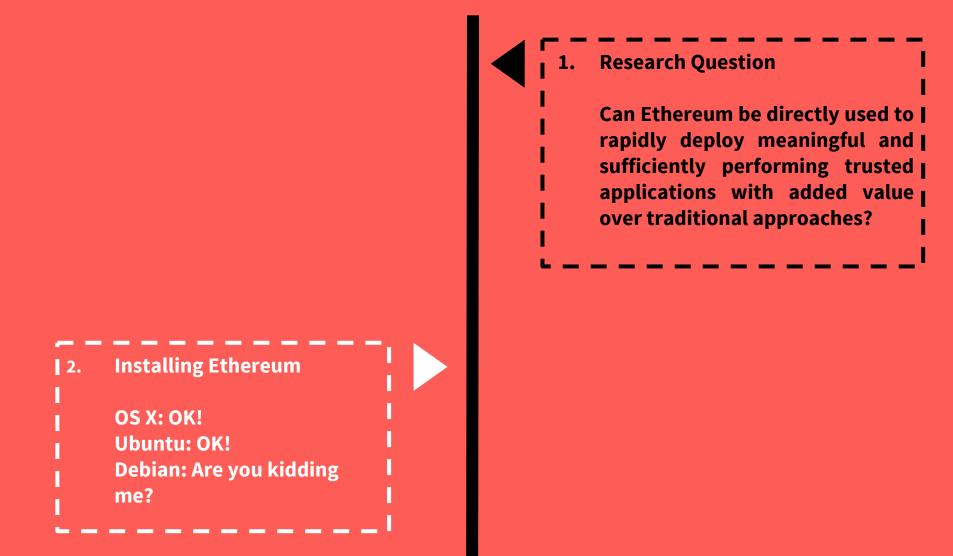
Can Ethereum be directly used to I rapidly deploy meaningful and I sufficiently performing trusted I applications with added value I over traditional approaches?

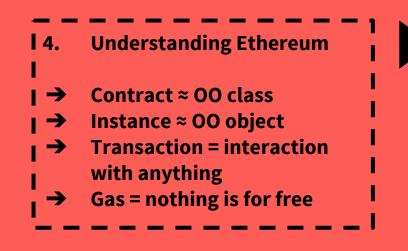
#### I 2. Installing Ethereum

- OS X: OK!
- Ubuntu: OK!
- Debian: Are you kidding
  - me?

#### . **Research Question**

Can Ethereum be directly used to I rapidly deploy meaningful and I sufficiently performing trusted I applications with added value over traditional approaches?

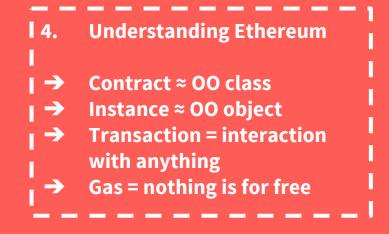




3.	Understanding Ethereum
→	WHERE IS THE
	DOCUMENTATION????
<b>→</b>	Ether = the internal currency
	Blockchain = our motivating
	factor
	Smart contracts, smart
	'democracy'

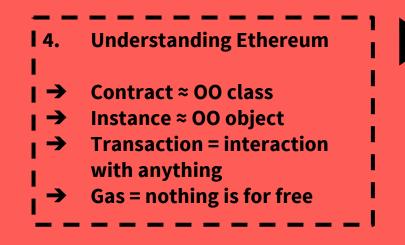
#### 5. Understanding Ethereum

- → Ethereum ≠ Bitcoin
- → Ethash (Dagger-Hashimoto)
- → 12 sec. block time
- → Genesis block???



3.	Understanding Ethereum
→	WHERE IS THE
	DOCUMENTATION????
<b>→</b>	Ether = the internal currency
<b>→</b>	Blockchain = our motivating
	factor
<b>→</b>	Smart contracts, smart
	'democracy'

# 5. Understanding Ethereum → Ethereum ≠ Bitcoin → Ethash (Dagger-Hashimoto) → 12 sec. block time → Genesis block???



3.	Understanding Ethereum
→	WHERE IS THE
	DOCUMENTATION????
→	Ether = the internal currency
<b>→</b>	Blockchain = our motivating
l	factor
→	Smart contracts, smart
	'democracy'

# 5. Understanding Ethereum → Ethereum ≠ Bitcoin → Ethash (Dagger-Hashimoto) → 12 sec. block time → Genesis block???

#### 7. Setting up a test network

- → 'Useless peer'...!!!
- ► Peers largely out of sync
- → Nodes mining frantically
- I → Raise the initial mining
   I difficulty

#### Setting up a test network

- No 'real' ether to spend
- Using 'counterfeit' ether
- → Nodes can't peer :(
- → 'Use a large network ID'
- → ...not too large

#### 8.

6.

- Setting up a test network
- → Turn off peer discovery
- → Add peers statically
- → Network stabilizes
- I → Send sample transactions
- I → SUCCESS!!!

#### 7. Setting up a test network

- · → · Useless peer'...!!!
- I → Peers largely out of sync
- I → Nodes mining frantically
- I → Raise the initial mining
   I difficulty

## Setting up a test network → No 'real' ether to spend → Using 'counterfeit' ether → Nodes can't peer :(

- → 'Use a large network ID'
- → …not too large

#### 8.

- Setting up a test network
- → Turn off peer discovery
- → Add peers statically
- → Network stabilizes
- I → Send sample transactions
- I → SUCCESS!!!

### 7. Setting up a test network

- → 'Useless peer'...!!!
- ► Peers largely out of sync
- → Nodes mining frantically
- I → Raise the initial mining
   I difficulty

## Setting up a test network → No 'real' ether to spend

- → Using 'counterfeit' ether
- → Nodes can't peer :(
- → 'Use a large network ID'
- → …not too large

#### 8. Setting up a test network

- → Turn off peer discovery
- Add peers statically
- → Network stabilizes
- I → Send sample transactions
- SUCCESS!!!

#### **10.** A simple contract

- → Broadcast some messages
- → Only the recipient can read their own messages
- → (Not really...)

#### I 9. Setting up a registrar

- → At least 3 different guides
- → This makes no sense
- → 'With a little help from my friends'
- → Works, no idea why...

#### **11.** An advanced contract

- → A court of law for civil cases
- I → Are you kidding?
- I → Plaintiff, defendant, bench,
   jury, treasurer.
  - → 'Justice' token
  - → Adversary system (debate, vote)

#### **10.** A simple contract

 → Broadcast some messages
 → Only the recipient can read their own messages

I → (Not really...)

9. Setting up a registrar

- → At least 3 different guides
- → This makes no sense
- → 'With a little help from my friends'
- → Works, no idea why...

#### **11.** An advanced contract

- → A court of law for civil cases
- I → Are you kidding?
- I → Plaintiff, defendant, bench,
   jury, treasurer.
  - → 'Justice' token
  - → Adversary system (debate, vote)

#### **10.** A simple contract

→ Broadcast some messages

- Only the recipient can read their own messages
- → (Not really...)

(Not really...)

9. Setting up a registrar

- → At least 3 different guides
- → This makes no sense
- → 'With a little help from my friends'
- → Works, no idea why...

**11.** An advanced contract

- → A court of law for civil cases
- I → Are you kidding?
- $I \rightarrow$  Plaintiff, defendant, bench,
  - jury, treasurer.
  - → 'Justice' token
  - → Adversary system (debate, vote)

#### **13.** Writing setup scripts

- → Instantiate a registrar
- → Register entities
- → Distribute ether
- → Compile and instantiate case contract
- → Watchbots.js to consume events

#### 12. Developing the contract

- → 'Solidity'
  - Variables, mappings
- → Constant Functions
- → Transactional Functions
- Events
- → Modifiers

#### 14. Executing the contract

- → Assume roles for each participating node
- → Run the setup scripts
- → Interact with the contract and see events flowing in
- → Mostly works as designed

#### 13. Writing setup scripts

- I → Instantiate a registrar
- I → Register entities
- **→** Distribute ether
- → Compile and instantiate case contract
- → Watchbots.js to consume events

### 12. Developing the contract

- → 'Solidity'
- → Variables, mappings
- Constant Functions
- Transactional Functions
- Events
- → Modifiers

#### **14.** Executing the contract

- → Assume roles for each participating node
- → Run the setup scripts
- → Interact with the contract and see events flowing in
- → Mostly works as designed

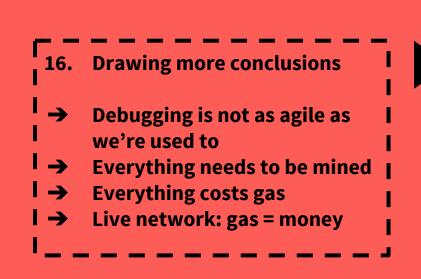
#### **13.** Writing setup scripts

- → Instantiate a registrar
- → Register entities
- → Distribute ether
- Compile and instantiate case contract
- → Watchbots.js to consume events

# 12. Developing the contract → 'Solidity' → Variables, mappings → Constant Functions → Transactional Functions → Events → Modifiers

#### **14.** Executing the contract

- → Assume roles for each participating node
- I → Run the setup scripts
  - → Interact with the contract
    - and see events flowing in
  - → Mostly works as designed

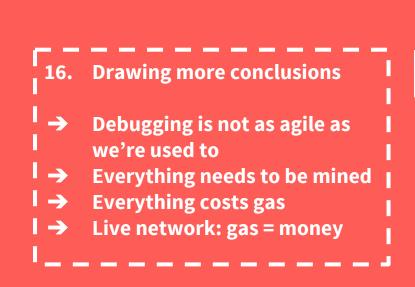


#### 15. Drawing a conclusion

- Dev < Ops
- → Setting up: 2.5 Weeks
- ➔ Developing: 2.5 Days
- → Very intuitive language



- 17. Drawing further conclusions
  - Great leverage for 'trustless' applications
- → Very powerful concepts
- → Huge lack of documentation
- → Low project maturity
- → Great potential

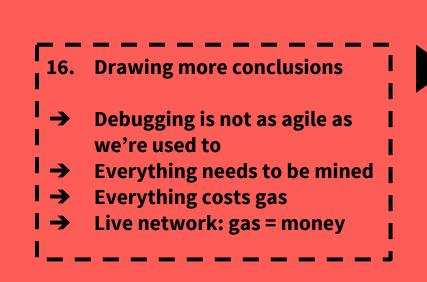


#### 15. Drawing a conclusion

- → Dev < Ops</p>
- → Setting up: 2.5 Weeks
- → Developing: 2.5 Days
- → Very intuitive language



- 17. Drawing further conclusions
  - → Great leverage for 'trustless' applications
- → Very powerful concepts
- → Huge lack of documentation
- → Low project maturity
- → Great potential

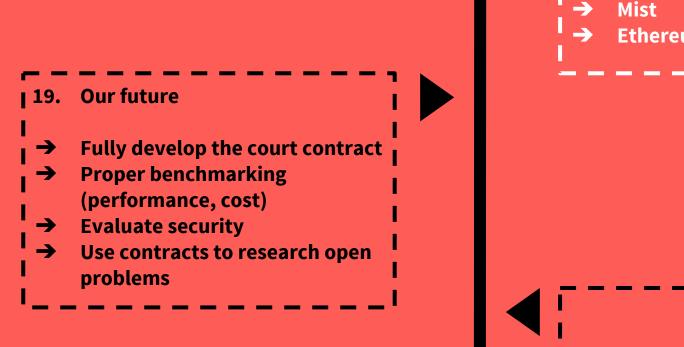


#### 15. Drawing a conclusion

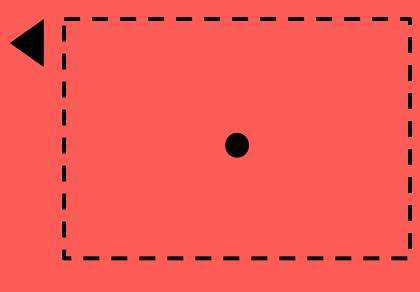
- → Dev < Ops</p>
- → Setting up: 2.5 Weeks
- → Developing: 2.5 Days
- → Very intuitive language

#### 17. Drawing further conclusions

- Great leverage for 'trustless' applications
- I → Very powerful concepts
- I → Huge lack of documentation
- I → Low project maturity
- → Great potential



## 18. Ethereum future → Whisper → Swarm → Mist → Ethereum itself



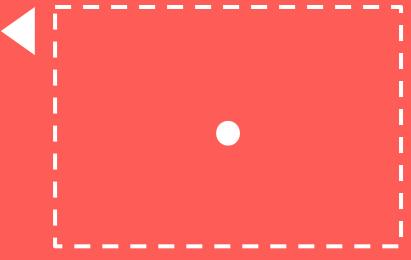


#### 18. Ethereum future

- → Whisper
- → Swarm
- → Mist
  - Ethereum itself



## 18. Ethereum future → Whisper → Swarm → Mist → Ethereum itself



Kthx

Ask me stuff!