ОНЛАЙН-ОБРАЗОВАНИЕ

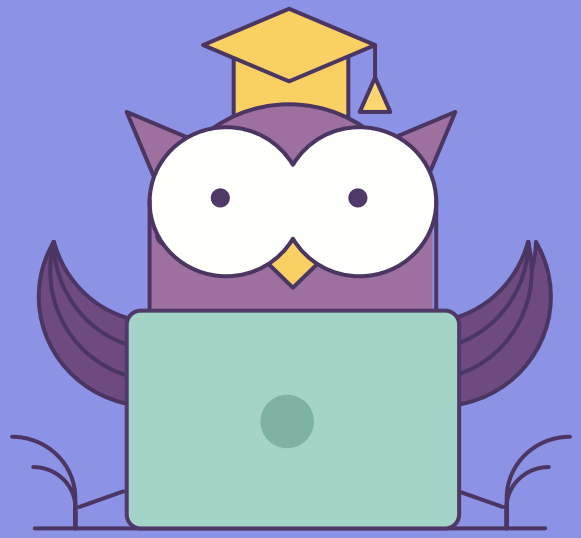
OTUS

Ethereum

Архитектуры и паттерны проектирования

Егор Зуев

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

- Свойства ethereum
- Основные структуры
- Адреса
- Форматы приватных ключей
- Переводы и nonce
- Merkle root
- Контракты
- Майнинг
- Где применять

01

Свойства ethereum

Свойства

- Использует POS консенсус
- Транзакции жестко зависят от предыдущих
- Быстрая сборка блока (около 10 секунд)
- Тоже использует merkle root для валидации целостности блока

02

Основные структуры

Блок

```
const receivedBlock = {
  number: 1,
  hash: '0x1761c0f04b5a1b03eb8a8d2cb14e9ebc28db69eb63444ff733e4810de0606aaf',
  transactionsRoot: '0x726a8c24cd754f80e934ccf98687c6dc33f053bbaeb5b2203066c66d9cadaa17',
  stateRoot: '0x3bdf5593dd3b069bcda371ee3939cdc0bac9960be5c93a518afeac49f1a87942',
  receiptsRoot: '0x056b23fbba480696b65fe5a59b8f2148a1299103c4f57df839233af2cf4ca2d2',
  miner: '0x0000000000000000000000000000000000000000',
  difficulty: '0’,
  totalDifficulty: '0',
  extraData: '0x',
  size: 1000,
  gasLimit: 6721975,
  gasUsed: 21000,
  timestamp: 1581361808,
  transactions: ['0x48b465577ead8163c482489d9b4c94dea52030965b8237162c2ebc97df85fd63']
}
```

Транзакция

```
const receivedTx = {
  hash: '0xed01b954f4238d540b6a4a3dacf16ef34bf91901a6175432adb3b0f22ef41e6b',
  nonce: 0,
  blockHash: '0x82573e410cc86d869279ef0ace7c6e0a4b574371cec7b2d2ece6531b4badb8b6',
  blockNumber: 1,
  transactionIndex: 0,
  from: '0x188d061521070af6A75A05Eed4af09b6C37d0000',
  to: '0x9ad14219984bBd6C26bdeaF5014884dBe0784DdE',
  value: '12’,
  gas: 90000,
  gasPrice: '2000000000',
  input: '0x',
  v: '0x26',
  r: '0xb4f89b6e7cc7da92e791fb28b5183c3fc94019f7bbfe68e2ebc1b93e95a1e077',
  s: '0x5f9126e3a279c85e29fbd58013ce0443026081e506cc95a3d84d5e6934a70b82'
}
```

04

Адреса

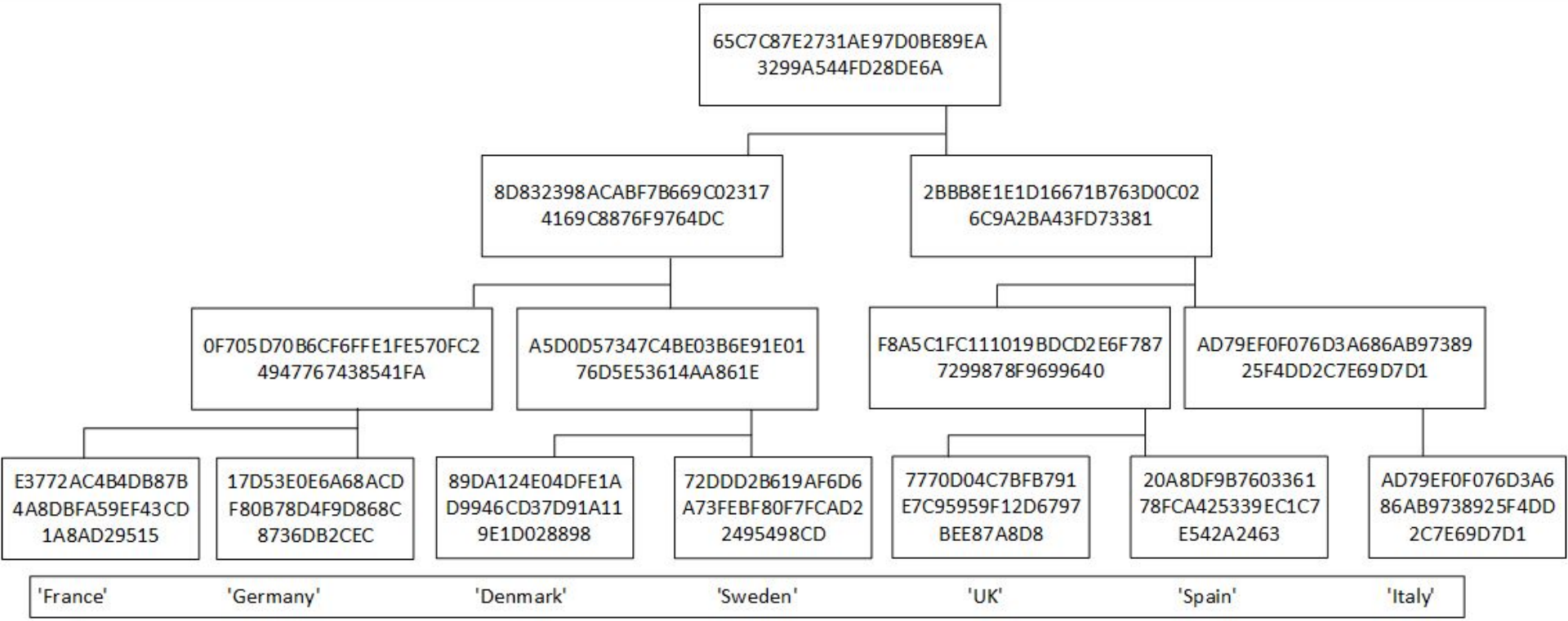
Виды адресов

- Всего один вид в hex формате

05

Merkle root

Merkle root


65C7C87E2731AE97D0BE89EA
3299A544FD28DE6A
8D832398ACABF7B669C02317
4169C8876F9764DC
2BBB8E1E1D16671B763D0C02
6C9A2BA43FD73381
0F705D70B6CF6FFE1FE570FC2
4947767438541FA
A5D0D57347C4BE03B6E91E01
76D5E53614AA861E
F8A5C1FC111019BDCD2E6F787
7299878F9699640
AD79EF0F076D3A686AB97389
25F4DD2C7E69D7D1
E3772AC4B4DB87B
4A8DBFA59EF43CD
1A8AD29515
17D53E0E6A68ACD
F80B78D4F9D868C
8736DB2CEC
89DA124E04DFE1A
D9946CD37D91A11
9E1D028898
72DDD2B619AF6D6
A73FEBF80F7FCAD2
2495498CD
7770D04C7BFB791
E7C95959F12D6797
BEE87A8D8
20A8DF9B7603361
78FCA425339EC1C7
E542A2463
AD79EF0F076D3A6
86AB9738925F4DD
2C7E69D7D1
'France'
'Germany'
'Denmark'
'Sweden'
'UK'
'Spain'
'Italy'

06

Типы приватных ключей

Виды приватных ключей

- Mnemonic (bip39)*
- Hex private key

07

Майнинг

Как происходит валидация

- Раз в определенный промежуток времени (около 10 секунд)
- Валидатор собирает блок и подписывает его
- При выпуске блока, валидатор поручается своими средствами (эфирами), что блок корректный. Если это не так – то эти средства списываются с его счета
- Разблокировка происходит, когда еще несколько блоков будет провалидировано после текущего

08

EVM

EVM

- EVM – Ethereum virtual machine
- Все действия на Ethereum требуют изменения состояния
- Каждое изменение сопровождается тратой ресурсов
- Для этих целей, в Ethereum придуман GAS. Gas – это как топливо
- То есть, чтобы выполнить какую либо операцию по мутации состояния, нужно предоставить достаточное кол-во газа
- У gas есть своя цена (за одну единицу) – GasPrice
- Таким образом, fee = gas * gasPrice

08

Контракты

Контракты

- Контракт – это программа, которая исполняется на EVM
- Контракт имеет методы и интерфейсы, как и многие другие ЯП
- Представляет из себя набор инструкций (bytecode), на подобии ассемблера
- Контракт позволяет создать программу, которая решает проблемы с нулевым доверием, а также, позволяет покрыть кейсы, связанные с децентрализованным хранением информации

09

DApps

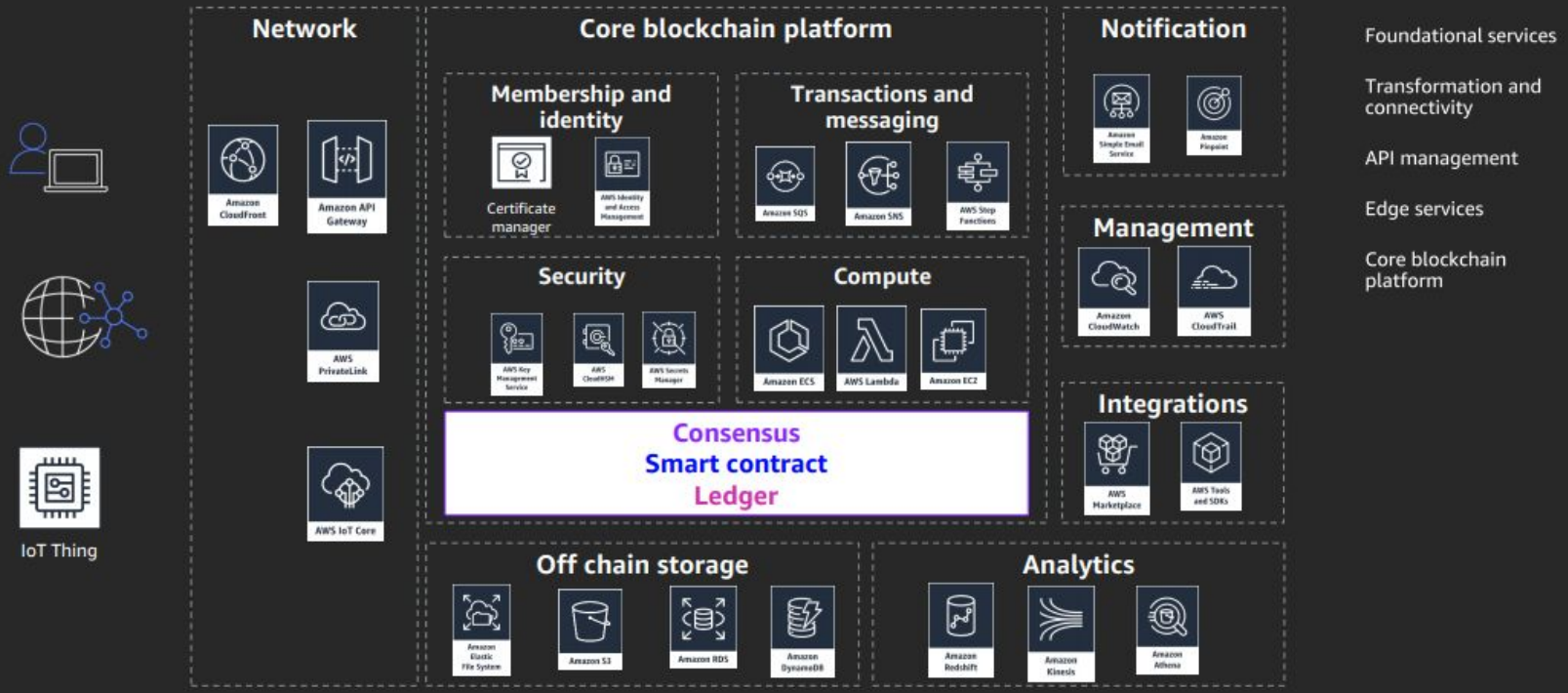
DApps

- DApps – decentralized applications
- Все действия атомарны
- Результат действия влияет на глобальный state
- Результат всех действий хранится в blockchain
- Также, можно всегда узнать кто какое действие совершал
- Нет единой точки истины

Events

- События в контракте можно отслеживать
- Эти события можно перечитывать, как на подобии kafka
- События являются асинхронными

Blockchain in cloud



Опрос

https://otus.ru/polls/6415/

Спасибо
за внимание!