

Фер игра на срећу имплементирана коришћењем blockchain технологије

Студент:
Ђорђе Гачић 626/2018

Професор:
Др. Владимир Миловановић

Крагујевац, август 2021.

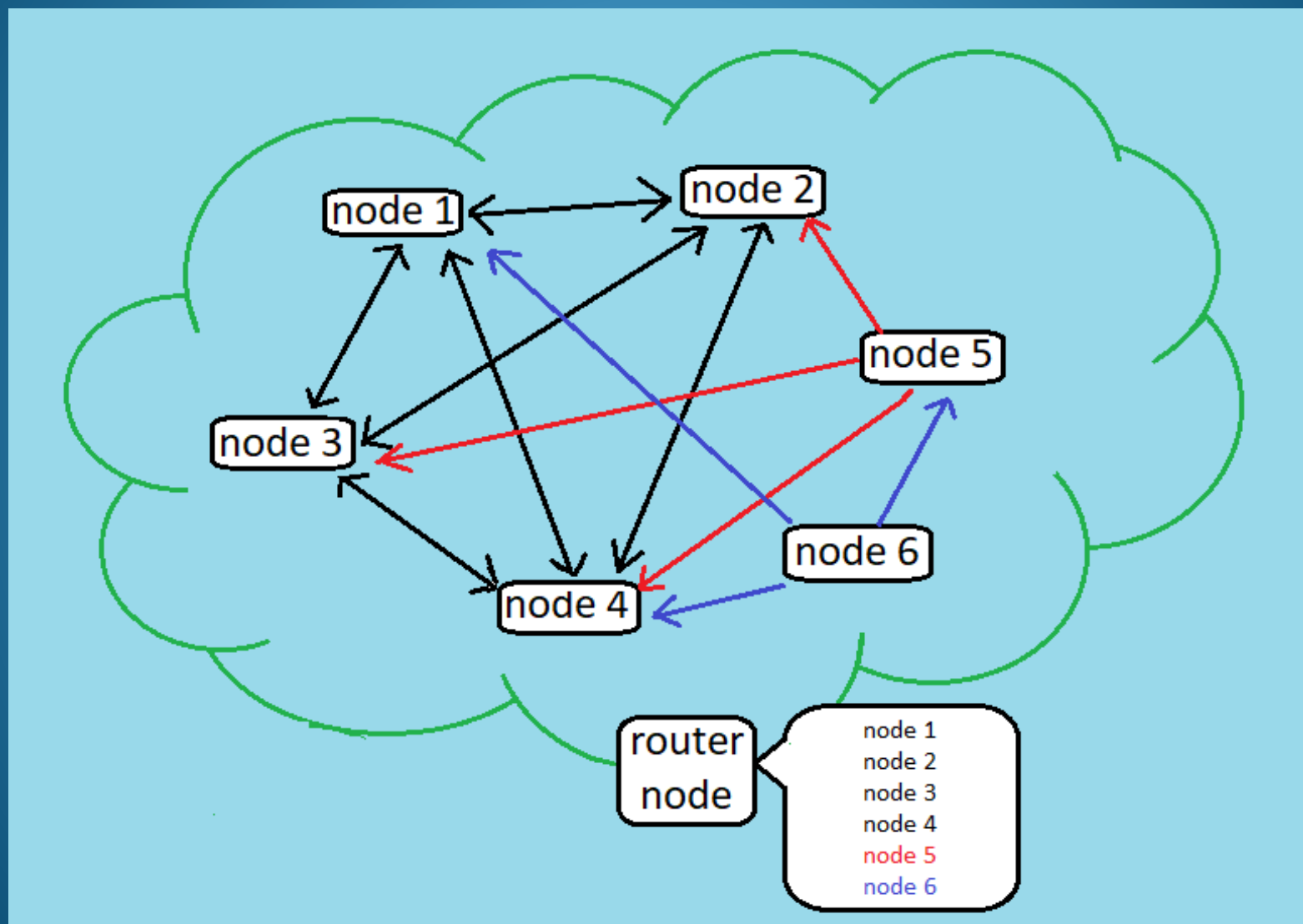
Основни елементи

- Peer to Peer мрежа
- Хеш функција
- “public key” криптографија и дигитални потпис
- Blockchain технологија

Peer to Peer мрежа

- Одсуство централног ауторитета
- Постиже се децентрализација
- Како наћи чвор за повезивање у мрежу?
 - Постојање рутер чвора (ипак мало централизовано?)
- Тестирање на локалном серверу – адресирање преко портова
- Сваки чвор се повезује на 3 чвора у мрежи
- Најмање 4 чвора за функционисање

Peer to Peer мрежа



Хеш функција

- SHA-256
- Користи се у Биткоину
- Излаз сматрамо као насумичан
- Неинвертибилна функција
- 256-битни излаз
- Још непронађена колизија (теоретски постоји јер је домен много већи скуп од кодомена код ових функција)

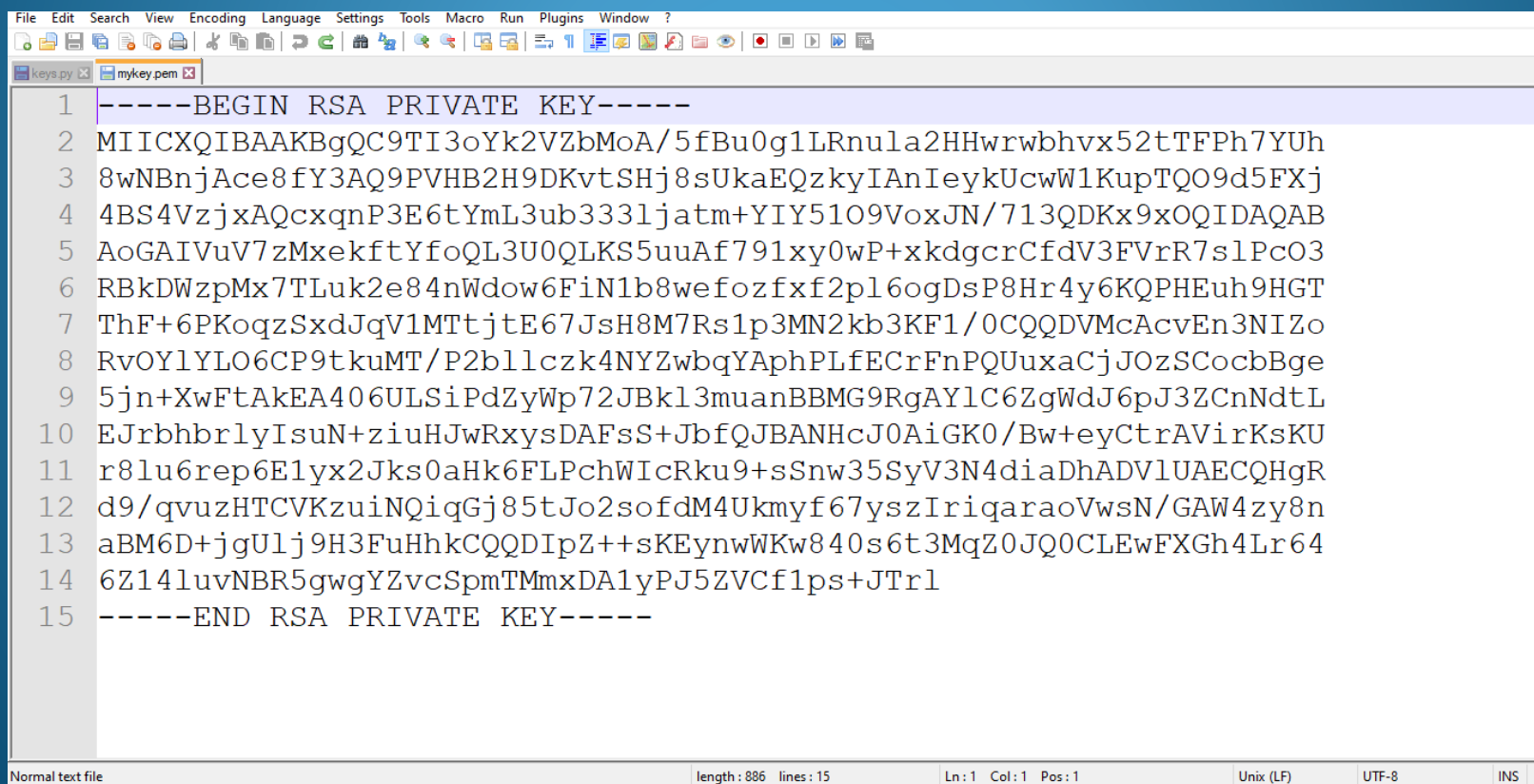
“public key” криптографија и ДИГИТАЛНИ ПОТПИС

- Генерисање пара тајни и јавни кључ
- RSA алгоритам за асиметричну криптографију
- 1024 – битни кључ (недовољно?)
- Потписивање поруке:

signature = (private key, message)
verify(public key, message, signature)

Пар тајни/јавни кључ - приказ

- Смјештен у фајл са екстензијом .pem
- Садржај фајла:



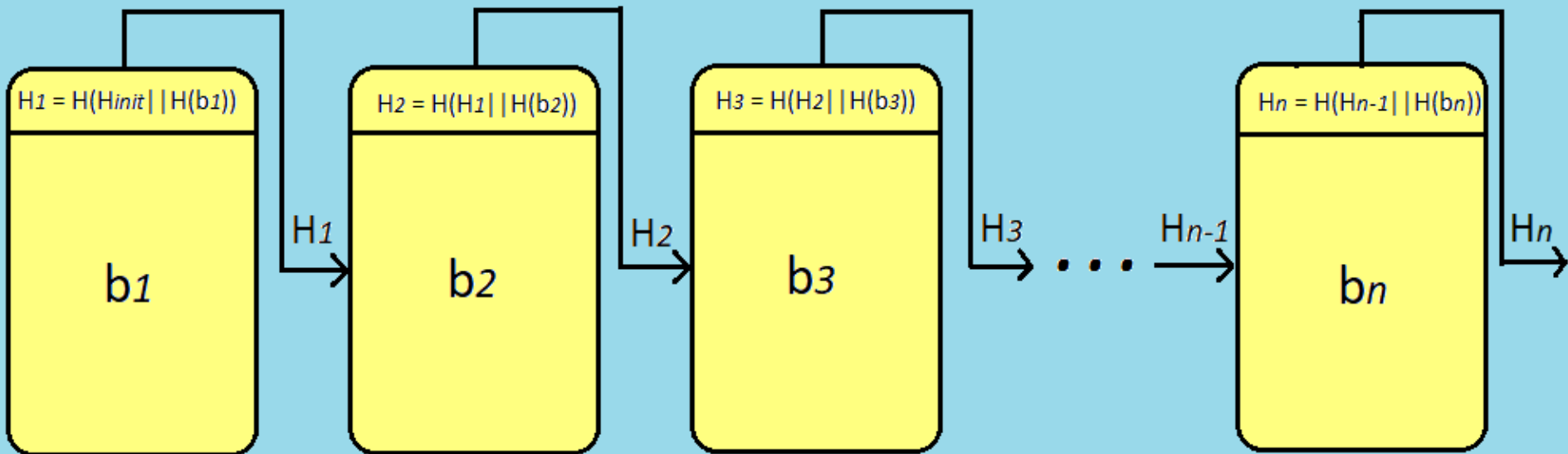
```
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
keys.py mykey.pem
1 -----BEGIN RSA PRIVATE KEY-----
2 MIICXQIBAAKBgQC9TI3oYk2VZbMoA/5fBu0g1LRnula2HHwrwbhvx52tTFPh7YUUh
3 8wNBnjAce8fY3AQ9PVHB2H9DKvtSHj8sUkaEQzkyIAAnIeykUcwW1KupTQO9d5FXj
4 4BS4VzjxAQcxqnP3E6tYmL3ub333ljatm+YIY51O9VoxJN/713QDKx9xOQIDAQAB
5 AoGAIVuV7zMxekftYfoQL3U0QLKS5uuAf791xy0wP+xkdgcrCfdV3FVrR7slPcO3
6 RBkDWzpMx7TLuk2e84nWdow6FiN1b8wefozfx2pl6ogDsP8Hr4y6KQPHEuh9HGT
7 ThF+6PKoqzSxdJqV1MTtjtE67JsH8M7Rs1p3MN2kb3KF1/0CQQDVMcAcvEn3NIZo
8 RvOY1YLO6CP9tkuMT/P2b1lczk4NYZwbqYAphPLfECrFnPQUuxaCjJOzSCocbBge
9 5jn+XwFtAkeA406ULSiPdZyWp72JBkl3muanBBMG9RgAYlC6ZgWdJ6pJ3ZCnNdtL
10 EJrbhbrlyIsuN+ziuHJwRxysDAFsS+JbfQJBANHCJOAiGK0/Bw+eyCtrAVirKsKU
11 r8lu6rep6E1yx2Jks0aHk6FLPchWicRku9+sSnw35SyV3N4diaDhADVLUAECQHgR
12 d9/qvuzHTCVKzuiNQiGj85tJo2sofdM4Ukmyf67yszIriqaraoVwsN/GAW4zy8n
13 aBM6D+jgUlj9H3FuHhkCQQDIpZ++sKEynwWKw840s6t3MqZ0JQ0CLEwFXGh4Lr64
14 6Z14luvNBR5gwgYZvcSpmTMmxDA1yPJ5ZVCf1ps+JTrl
15 -----END RSA PRIVATE KEY-----
Normal text file length: 886 lines: 15 Ln: 1 Col: 1 Pos: 1 Unix (LF) UTF-8 INS
```

Компоненте тајног и јавног кључа

Увезено из mykey.pem фајла преко Пајтон-а

```
>>>
>>> from Crypto.PublicKey import RSA
>>> f = open('mykey.pem', 'r')
>>> key = RSA.importKey(f.read())
>>> key
RsaKey(n=13293030674062643761873708310176919128199899926123927159152442169873966183895561
15245263913062169051485642154428318499168908751790118908917016660931125204454285457549169
74945180693423312255879667210356969735882462949262202048585041094417480919735798563925780
716721501709774190832850454273332693802565263913273, e=65537, d=2342461327144680976317789
78053856134369590604195833962157654098462444065133075761568865551001369071415304481910280
34953197331198004387978325825355033541666962213406539286749496528624207766954219326967371
61840789620495579358772281151812196748048425694307692087188632052148648423165829529219503
3479426500581373, p=111658934803364953467539383876686958293622905331374299319072993833536
94669885938510824136735515258469589906822849512279483081199880262010016186003361825133, q
=1190503088487464687178932705038936172765770419784388680577430261721013691418981652712369
3402123567092111305119884970161904020494414378064887020941201267581, u=700660326008874911
41720878183055580793753036616546182950993716843053658435206694554612663034312625227870035
2079513541758252316870544343884092442875019629)
>>> key.publickey()
RsaKey(n=13293030674062643761873708310176919128199899926123927159152442169873966183895561
15245263913062169051485642154428318499168908751790118908917016660931125204454285457549169
74945180693423312255879667210356969735882462949262202048585041094417480919735798563925780
716721501709774190832850454273332693802565263913273, e=65537)
>>> _
```


Blockchain технологија



- Blockchain у json фајлу (Пајтон објекат типа dict)

Изглед једног блока са 2 опкладе:

```
"ab72b7628dc058b0247945f3bc8b11399ea2d10c75e99901cbb385fb3dedd91c":
{
  "validatorPK": "-----BEGIN PUBLIC KEY-----\nMIA...QAB\n-----END PUBLIC KEY-----",
  "blockTimestamp": 1628778304.960544,
  "prevBlockHash": "367af80012b1c93...64d9c880f0dd",
  "bets":
  [
    {"ecb8bba30b4183243acfc4709a5260187c238a236848ddcb554a1ad23c765f28":
      {
        "gamblerPK": "-----BEGIN PUBLIC KEY-----\nQAB\n-----END PUBLIC KEY-----",
        "numForProbability": "2",
        "sequenceChoice": "1",
        "betTimestamp": 1628778302.729225,
        "betSignature": "9471d5720dbd98ed...d7b"
      }
    },
    {"e6af2e8a8cdcbc7476430ab5b0ab539d142c9b20e1d657ee0aa75bb6f836d7cb":
      {
        "gamblerPK": "-----BEGIN PUBLIC KEY-----\nMIGf....--END PUBLIC KEY-----",
        "numForProbability": "4",
        "sequenceChoice": "10",
        "betTimestamp": 1628778302.753308,
        "betSignature": "1a154c161...7b7822f"
      }
    },
    ...
  ],
  "blockSignature": "424660eef715a9aff08b00...561f7"
}
```

Врсте чворова у мрежи

- Рутер чвор (класа RouterNode)
- Валидатор чвор (класа ValidatorNode)
- Коцкар чвор – учесник у клађењу (класа GamblerNode)

Рутер чвор

- Фиксна адреса: 127.0.0.1 : 9000
- Разлог постојања: проблем проналаска активних чворова у мрежи
- Први се покреће и стално је активан
- Улога: да обезбједи листу активних валидатор чворова на које се могу повезати други чворови
- Мало нарушава децентрализацију?
- Нема додира са опкладама и blockchain-ом
- Избацује валидатора из листе активних чворова ако је прошло више од 5 минута од његовог последњег јављања

Валидатор чвор

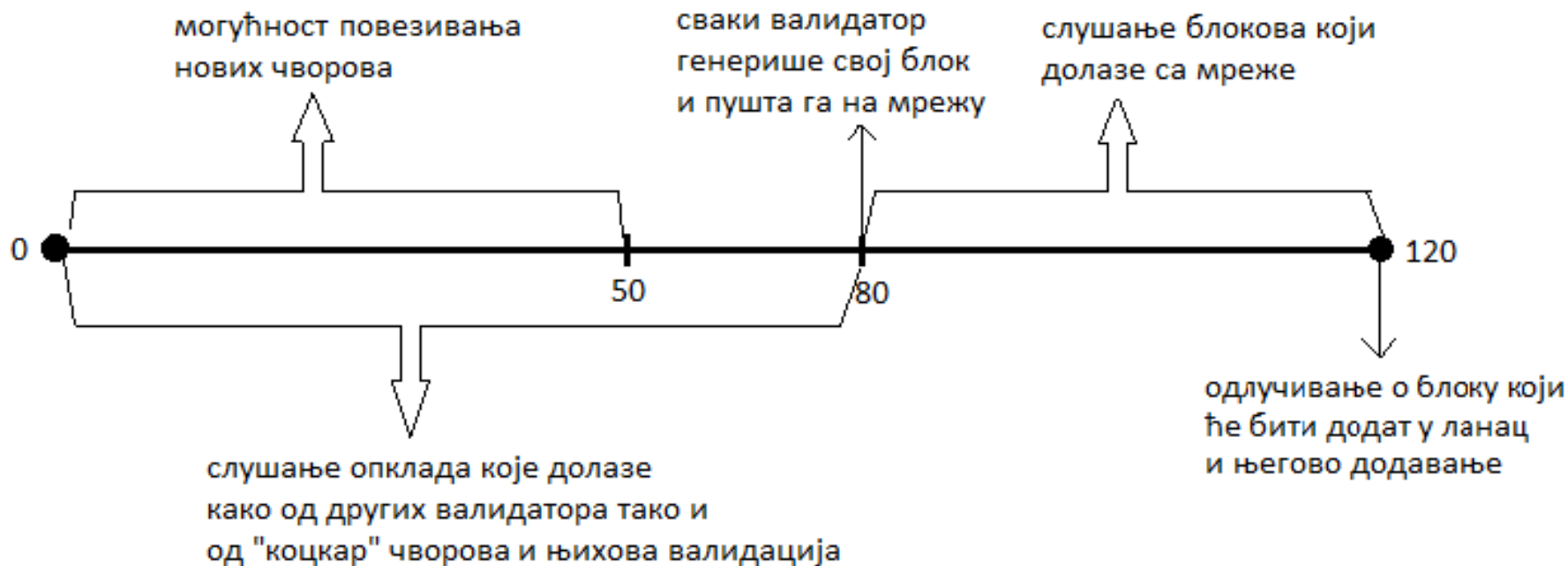
- Ради највећи дио посла у мрежи
- Договара се са другим валидаторима о уградњи блока у blockchain
- Повезује се преко рутер чвора на три насумично одабрана валидатор чвора
- Преузима blockchain и ажурира га после сваког круга како би учесницима (коцкар чворовима) и другим валидаторима који се повезују била доступна најновија верзија

Валидатор чвор

- Улога: слуша опкладе и провјерава њихову исправност, слуша блокове и провјерава њихову исправност, уграђује нови блок у blockchain, служи као сервер за повезивање коцкар чворовима
- Уградња новог блока у blockchain на свака 2 минута
- Нови резултат извлачења на свака 2 минута
- Јавља се рутер чвору на свака 2 минута (приликом провјере активности валидатора на које је повезан)

Процес генерисања блока

Генерисање једног блока (трајање 120 секунди)



Провјера исправности опкладе

- Структура опкладе

Опклада је неисправна ако је:

- Timestamp опкладе мањи од timestamp-а последњег блока у blockchain-у (тј. ако је опклада млађа од последњег блока у ланцу)
- тренутни timestamp мањи од timestamp-а опкладе (опклада генерисана “у будућности”)
- хеш вриједност прослијеђена уз опкладу различита од хеш вриједности над стварним подацима опкладе
- Ако се хеш вриједност опкладе поклапа са неком опкладом која већ постоји у blockchain-у
- Ако се потпис опкладе не поклапа са јавним кључем у опклади и подацима опкладе

У супротном, опклада је исправна

Провјера исправности блока

- Структура блока

Блок је неисправан ако је:

- timestamp блока мањи од timestamp-а последњег блока у blockchain-у (тј. ако је блок млађи од последњег блока у ланцу)
- тренутни timestamp мањи од timestamp-а блока (блок генерисан “у будућности”)
- хеш вриједност прослијеђена уз блок различита од хеш вриједности над стварним подацима блока
- Ако нека од опклада у блоку није исправна
- Ако се опкаде у блоку који се провјерава разликују од опклада за које је валидатор који провјерава блок чуо у протеклом интервалу слушања опклада
- Ако се потпис блока не поклапа са подацима блока и јавним кључем онога ко је генерисао блок

У супротном, блок је исправан

Договор о уградњи блока

- Провјерава се валидност блока
- Да ли блок стиже у вријеме кад се слушају блокови
- Блок са најмањом хеш вриједношћу од свих до тада примљених блокова у текућем кругу је кандидат за уградњу у blockchain
- Сви “поштени” валидатори уграђују исти блок у blockchain и на крају круга сви имају исту вриједност blockchain-а

Коцкар чвор

- Повезује се насумично на три валидатора преко рутер чвора
- Период за повезивање (првих 50 секунди круга)
- Формира опкладу на основу унесених података од стране учесника
- Шаље опкладу ка валидаторима на које је повезан
- По потреби преузима blockchain и провјерава статус опкладе (да ли је секвенца добитна)
- Опција да се само преузме blockchain од валидатора без учешћа у клађењу

Структура пројекта

Коришћен Пајтон програмски језик

- Датотека “routerNode.py” – имплементација класе “RouterNode”
- Датотека “routerApp.py” – покреће рутер чвор
- Датотека “validatorNode.py” – имплементација класе “ValidatorNode”
- Датотека “validatorApp.py” – покреће валидатор чвор
- Датотека “gamblerNode.py” – имплементација класе “GamblerNode”
- Датотека “gamblerApp.py” – покреће коцкар чвор

Покретање чворова

- 1) Покретање рутер чвора
- 2) Покретање најмање 4 валидатор чвора
- 3) Могућност повезивања коцкар чворова тј. учесника у клађењу као и још валидатор чворова
 - Чворови се повезују само у термину предвиђеном за повезивање у мрежу тј. у првих 50 секунди сваког круга извлачења

Опис игре на срећу



- На шта се учесници кладе?
- Резултат извлачења: бинарна репрезентација хеш вриједности блока који ће бити генерисан
- Гледају се последњи битови – битови најмање тежине

```
>>>
>>> from Crypto.Hash import SHA256
>>> hash = SHA256.new("hello, world!".encode())
>>> hexHash = hash.hexdigest()
>>> hexHash
'68e656b251e67e8358bef8483ab0d51c6619f3e7a1a9f0e75838d41ff368f728'
>>> intHash = int(hexHash, 16)
>>> intHash
47447509435240178963798524362534432113195114210189468302358324674552893339432
>>> binHash = bin(intHash)
>>> binHash
'0b110100011100110010101101011001001010001111001100111111010000011010110001011111011111
000010010000011101010110000110101010001110001100110000110011111001111100111101000011010
10011111000011100111010110000011100011010100000111111110011011010001111011100101000'
>>> binHash[2:].zfill(256)
'01101000111001100101011010110010010100011110011001111110100000110101100010111110111110
000100100000111010101100001101010100011100011001100001100111110011111001111010000110101
001111110000111001110101100000111000110101000001111111110011011010001111011100101000'
```

Опције за клађење

Могућност уноса за вјероватноћу од стране учесника	вјероватноћа	Број последњих битова који се предвиђају
2	$1/2$	1
4	$1/4$	2
8	$1/8$	3
16	$1/16$	4
32	$1/32$	5
64	$1/64$	6
128	$1/128$	7
256	$1/256$	8

Опције учешћа у игри

1. Са клађењем

Уноси се кључ, ознака за вјероватноћу, секвенца која се предвиђа (дужине у складу са вјероватноћом). Шаље се потписана опклада на мрежу. Даље постоје 2 могућности:

- а) Чекамо да се круг заврши да бисмо преузели blockchain и провјерили да ли смо остварили добитак или не
- б) Излазимо из програма без провјере резултата опкладе

2. Без клађења

Уноси се кључ и чека се преузимање најновије верзије blockchain-а како би провјерили да ли посједујемо неку опкладу (тј. да ли постоји опклада повезана са унијетим јавним кључем)

Закључак

- Повјерење учесника
- Сваки учесник буквално учествује у генерисању резултата извлачења
- Валидан власник blockchain-а може постати свако ко преузме последњу верзију и ажурира је сваких 2 минута (тј. након сваког генерисања новог блока)
- Овде није имплементирана криптовалута!
- Недостаци пројекта
- Демонстрација

Хвала на пажњи!