Развој криптовалуте базиране на програмском језику Раст

ДИПЛОМСКИ РАД

Бојан Мијановић - SV 8/2020

Историја криптовалута

1982

Давид Чаум

Концепт дистрибуиране базе података са криптографијом

2008

Сатоши Накамото

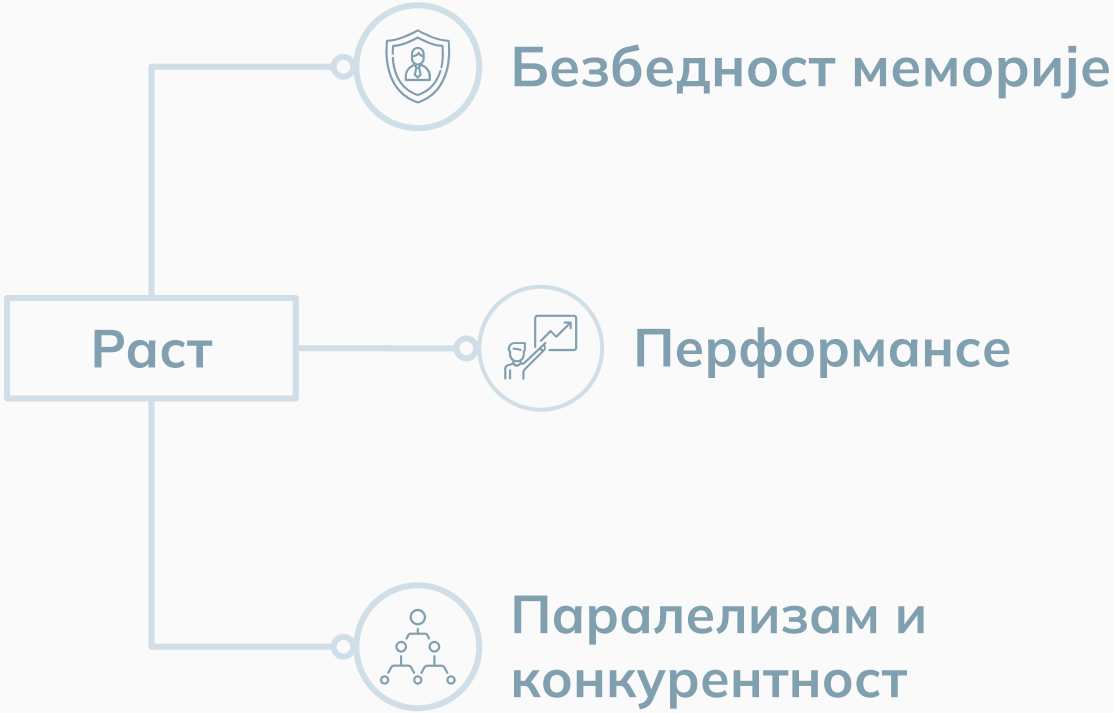
Bitcoin: Peer-to-peer електронски готовински систем

2015

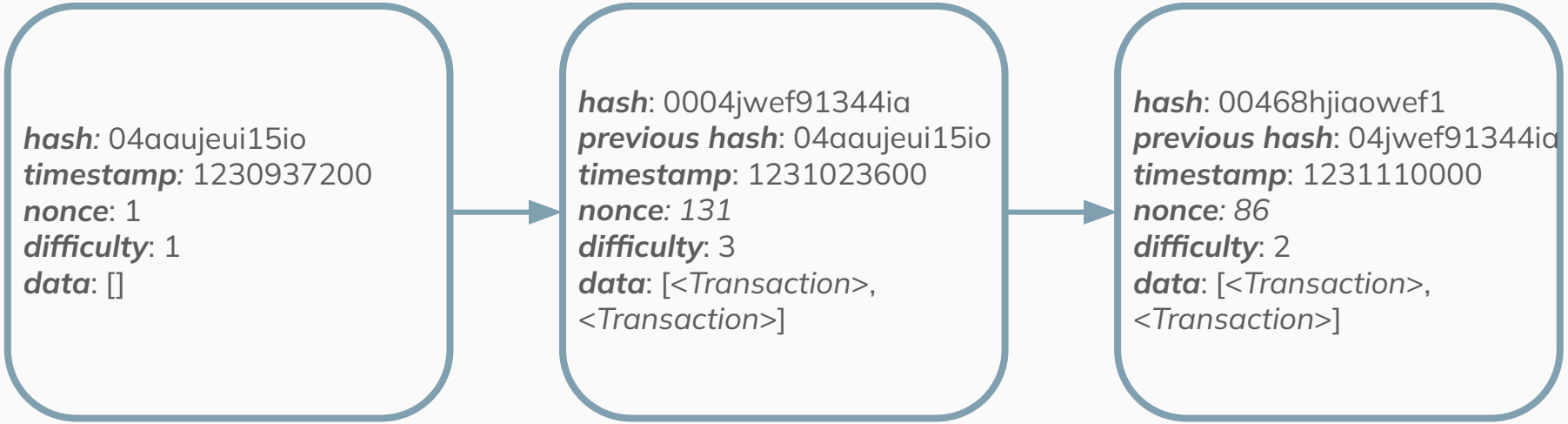
Виталик Бутерин

Увођење паметних уговора

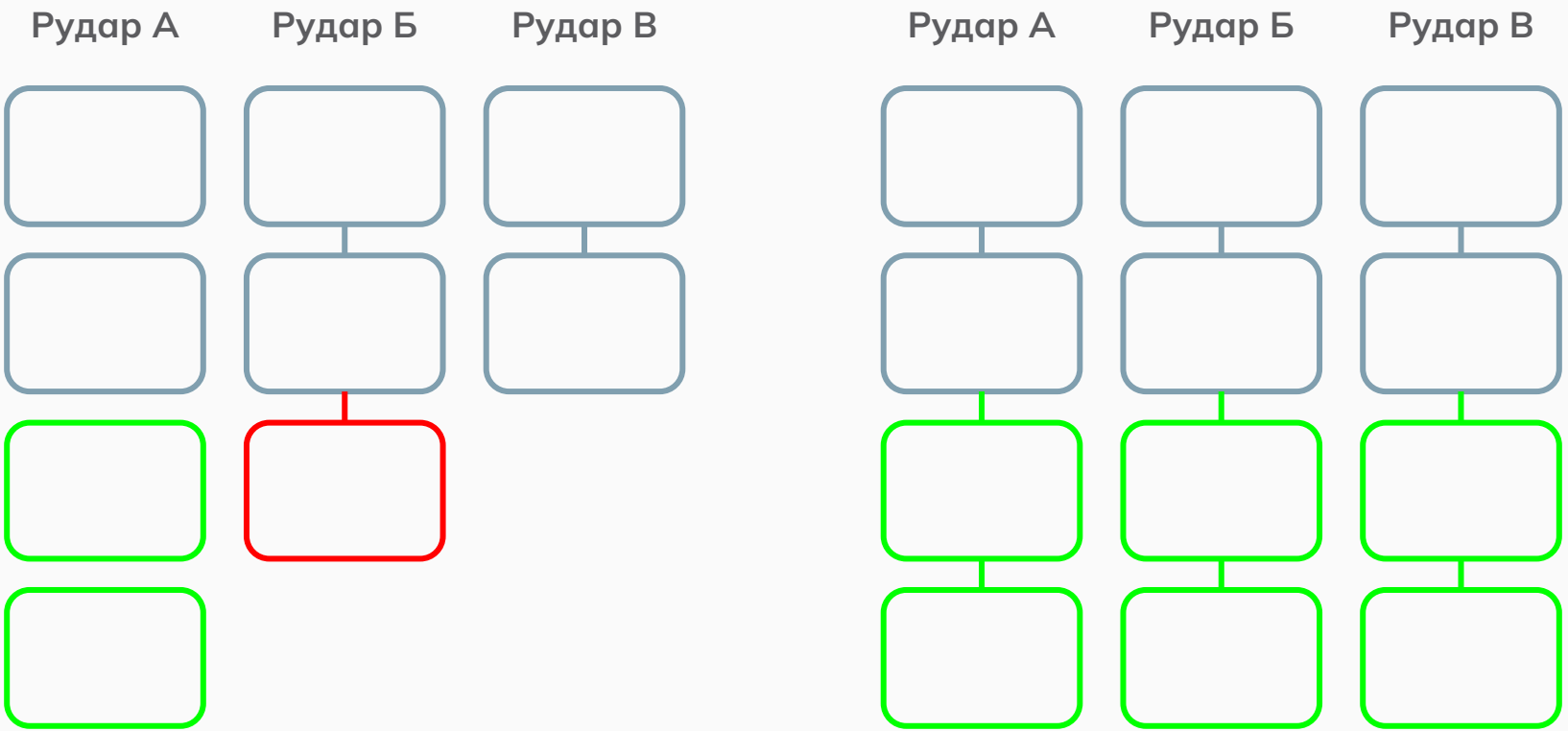
Зашто Раст?


Раст
Безбедност меморије
Перформансе
Паралелизам и конкурентност

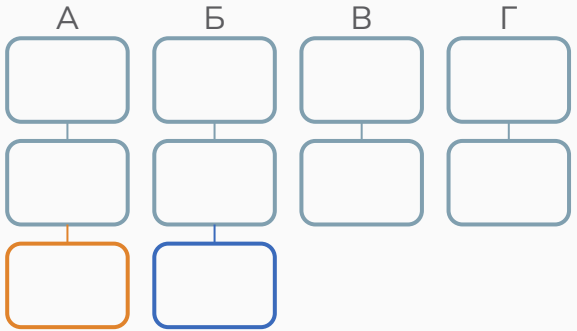
Архитектура

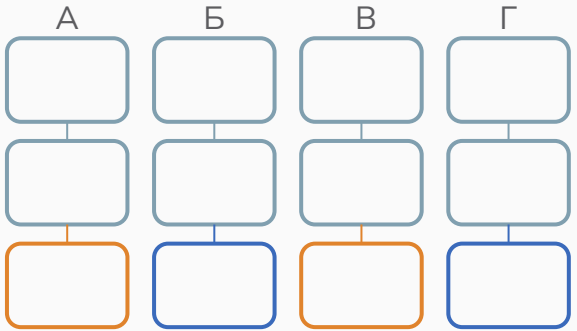


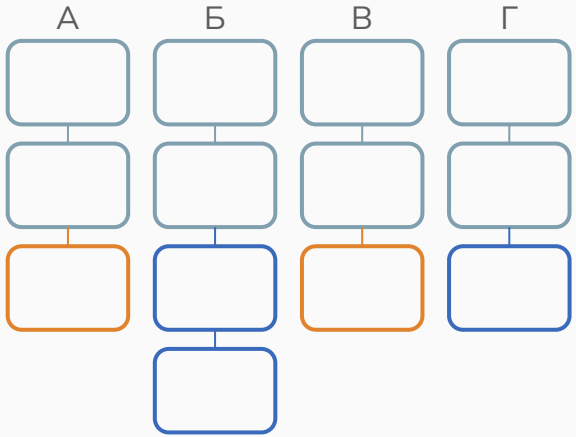
Валидација ланца

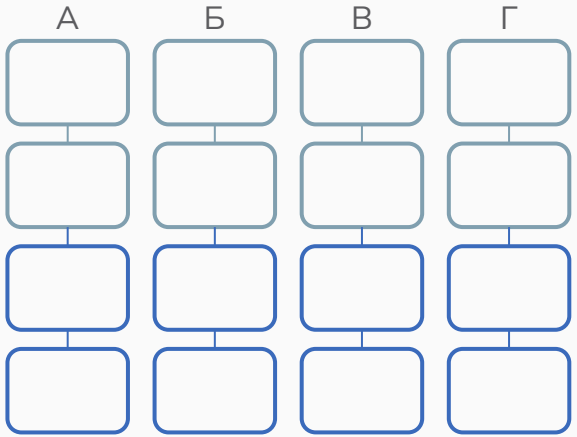


Проблем рачвања у ланцу





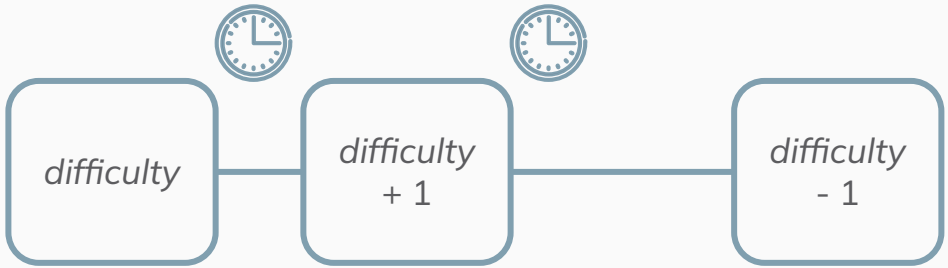




Рударење

hash: 000000haxi2910jasdflk
previous hash: 04aaujeui15io
timestamp: 1231023600
nonce: *16731*
difficulty: 6
data: [<*Transaction*>, <*Transaction*>]

difficulty = 6
hash = 000000haxi2910jasdflk

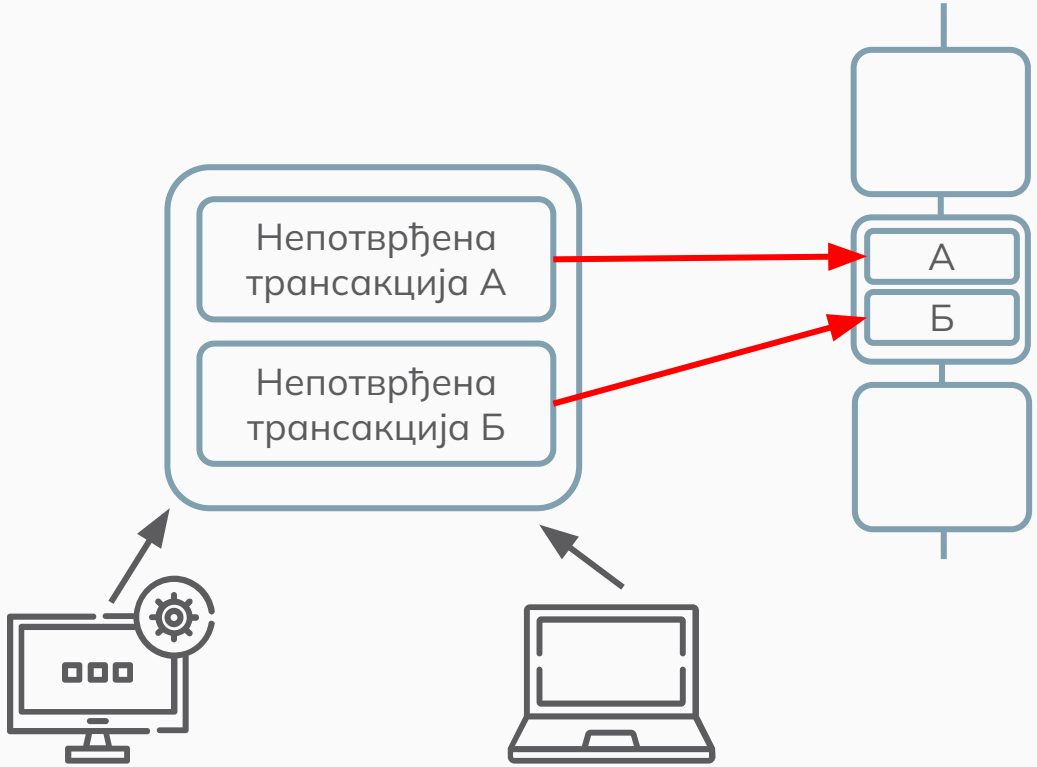


Трансакције и базен трансакција

***Input**: timestamp,*
Balance: 500, *signature,*
sender's public key: 0xfoo1

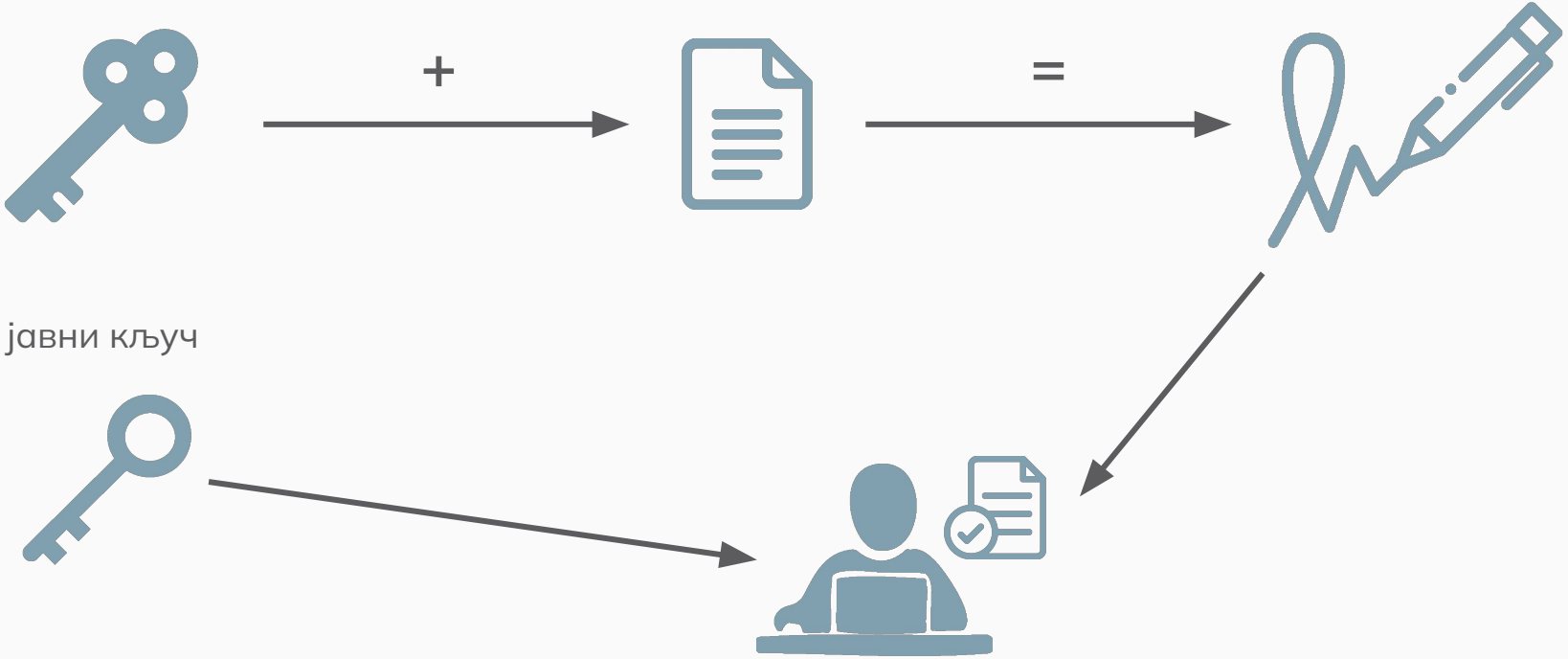
***Output**:*
Amount: 50
Address: 0xbar2

***Output**:*
Amount: 460
Address: 0xfoo1



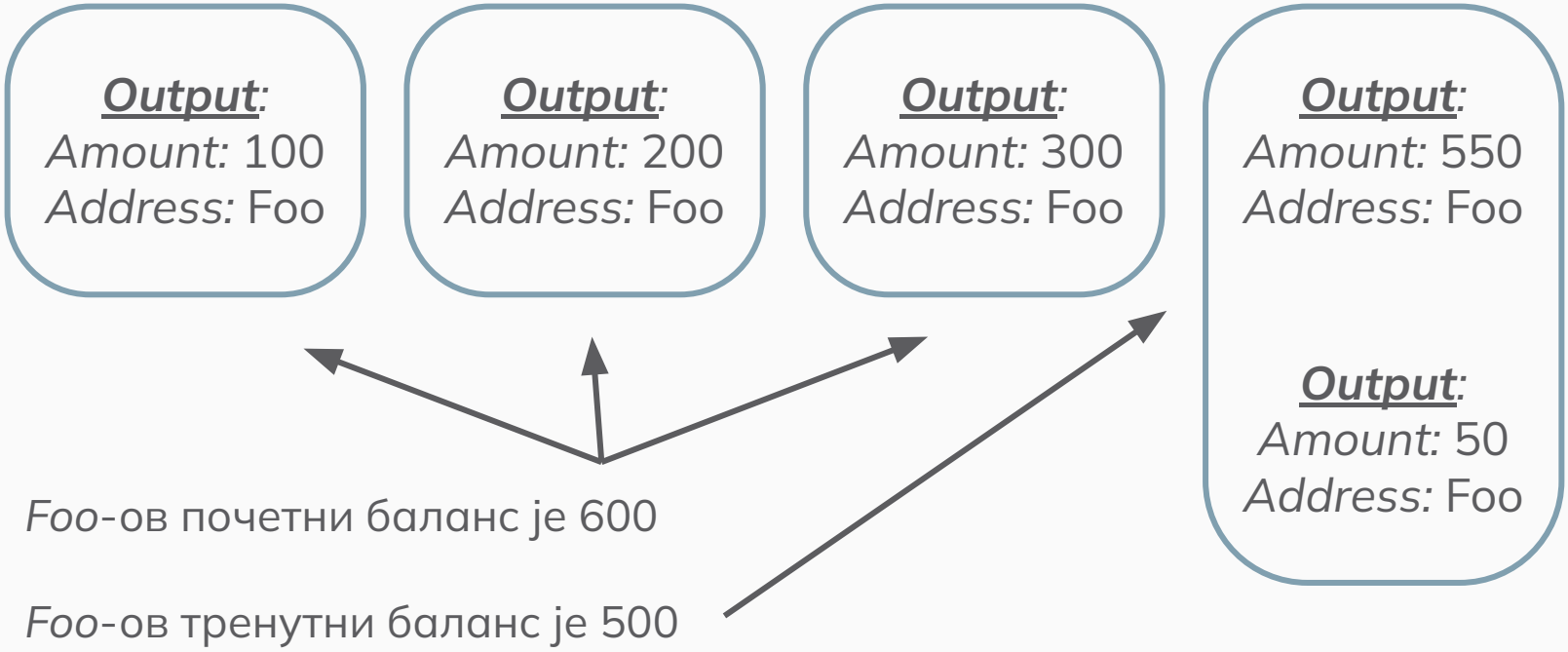
Новчаник

приватни кључ

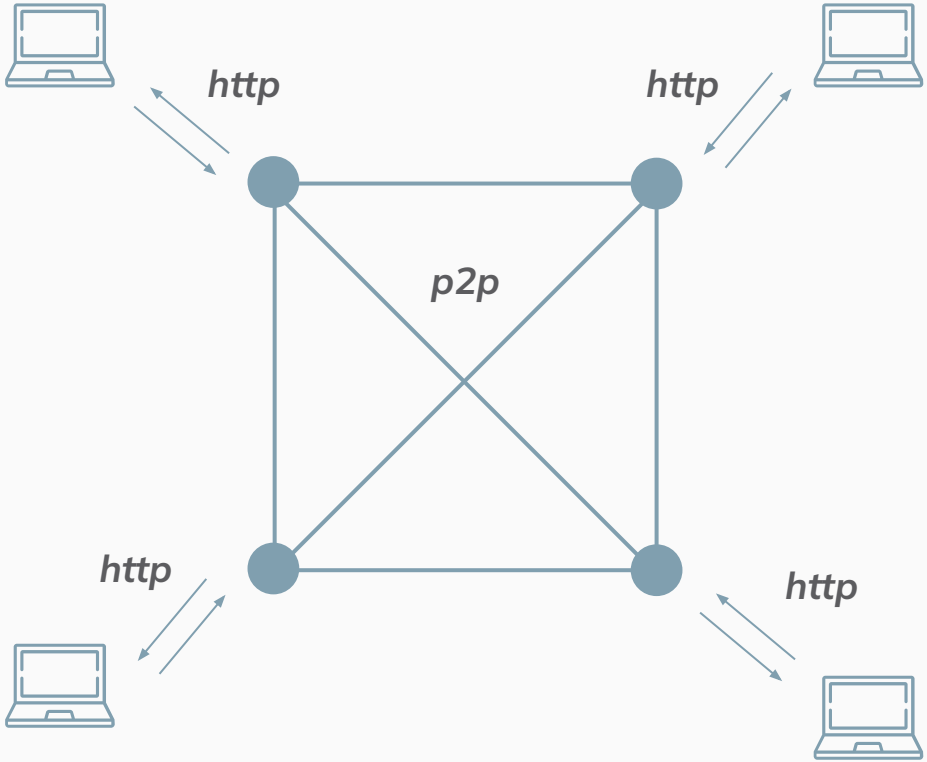


јавни кључ

Рачунање стања новчаника

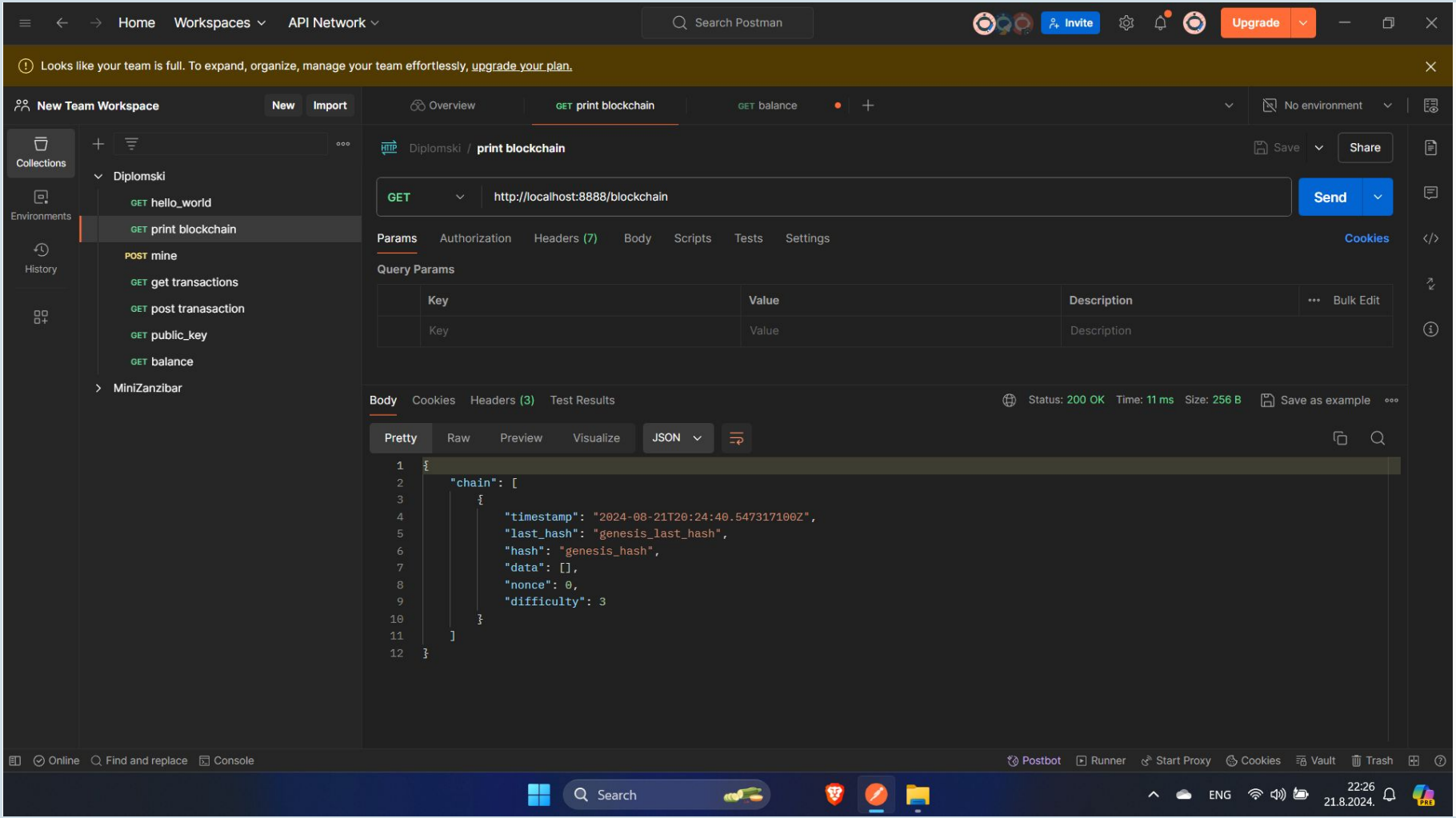


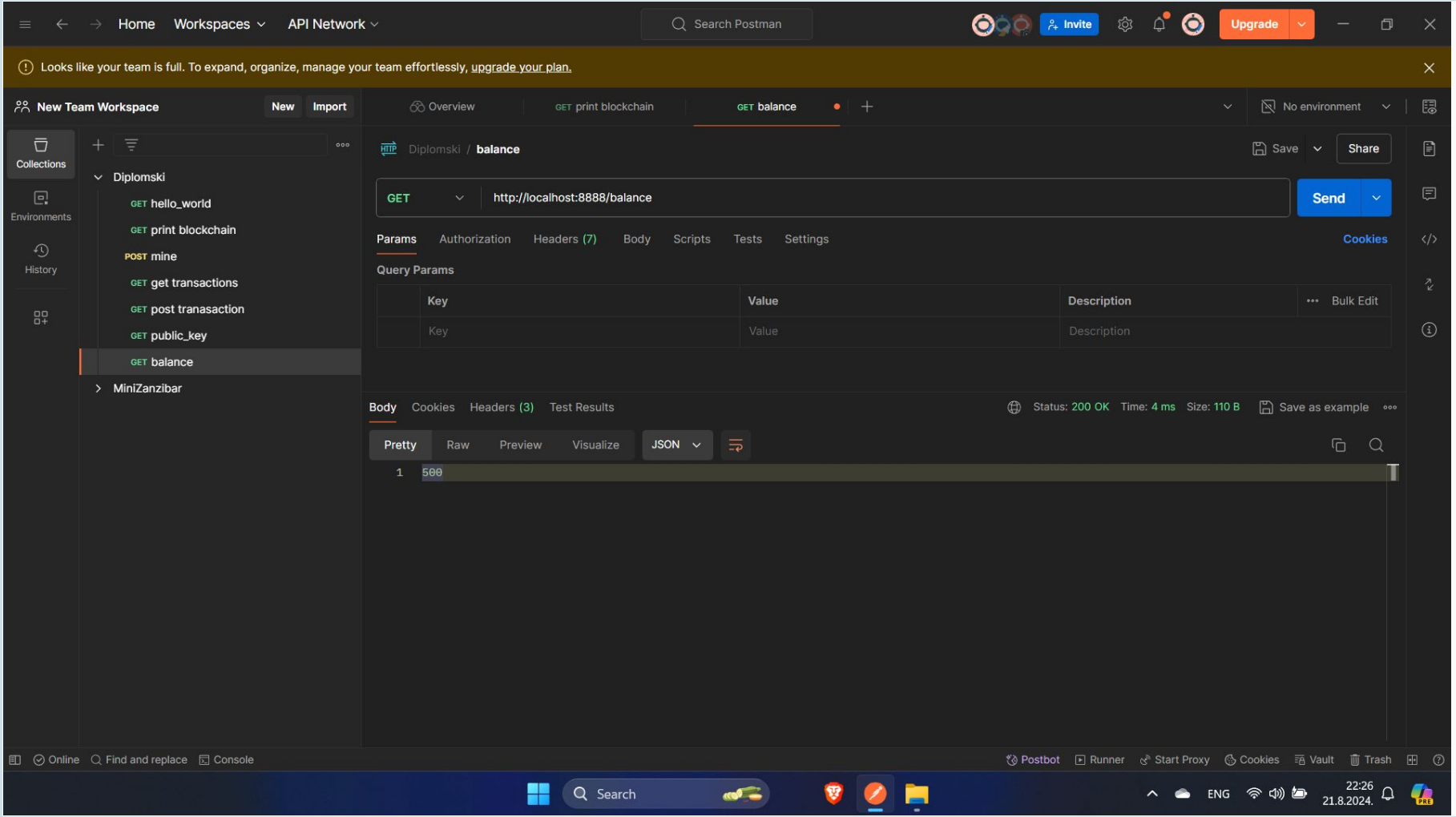
Комуникација

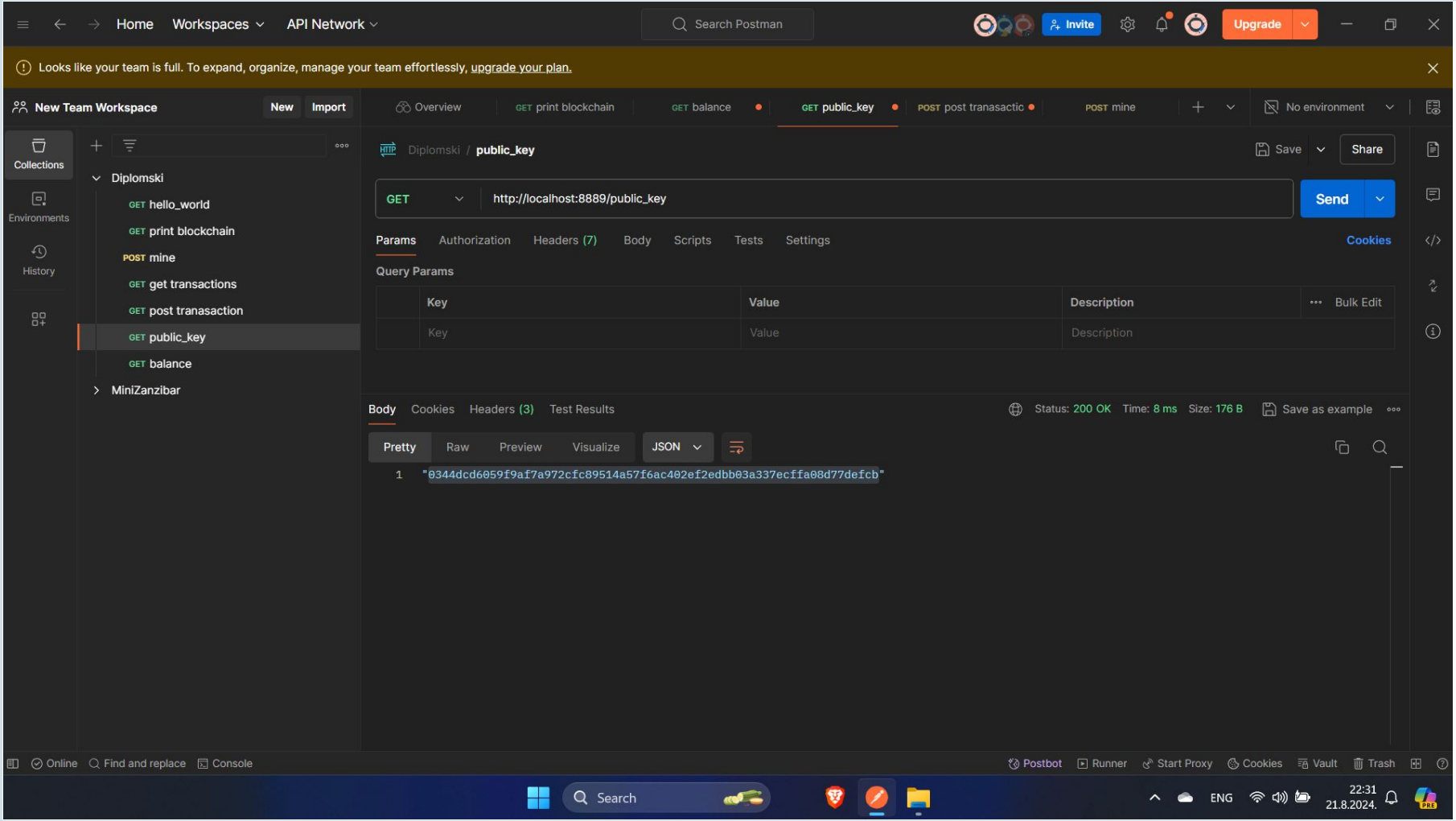


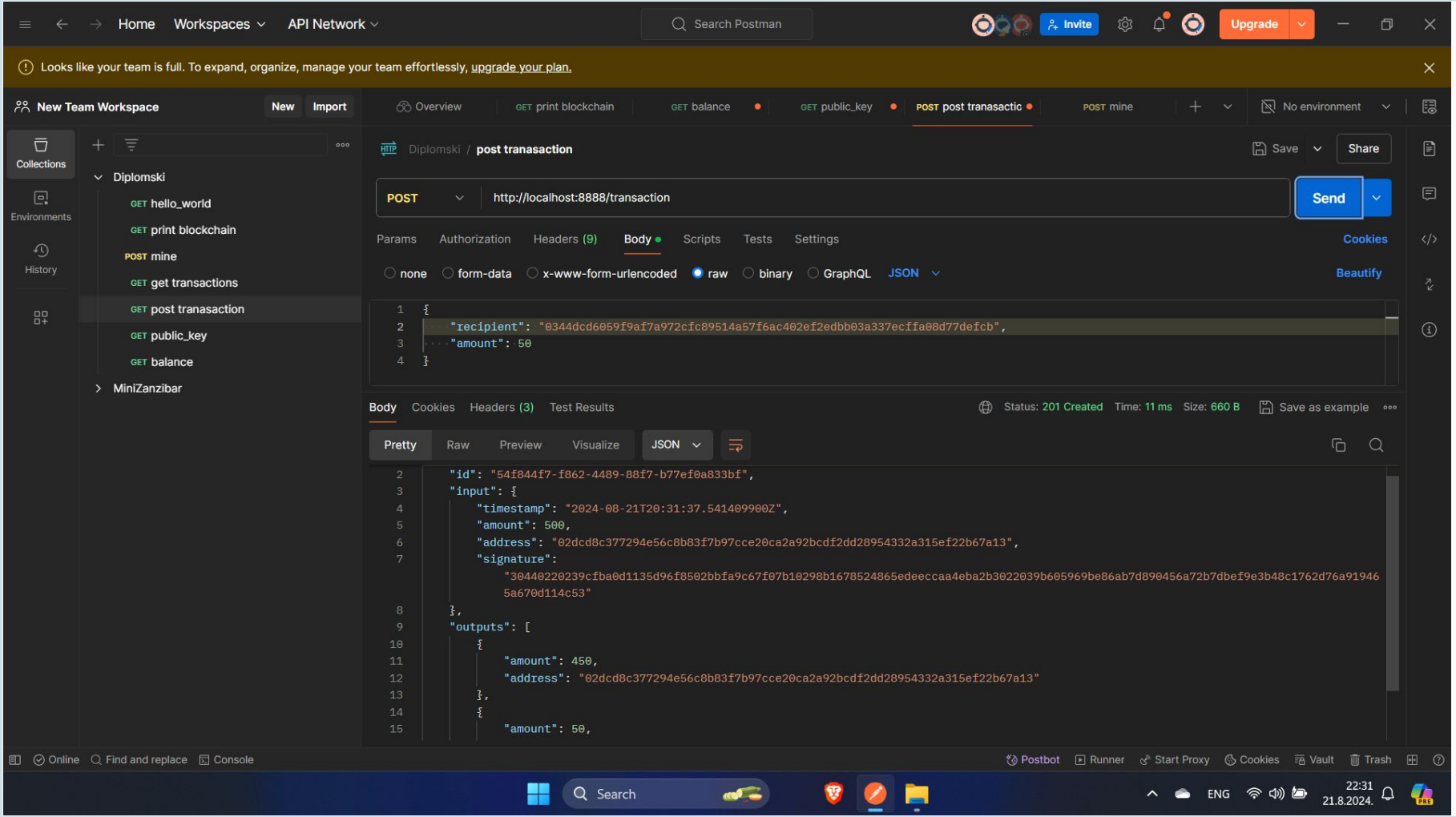
Поређење *blockchain* технологије са традиционалним базама

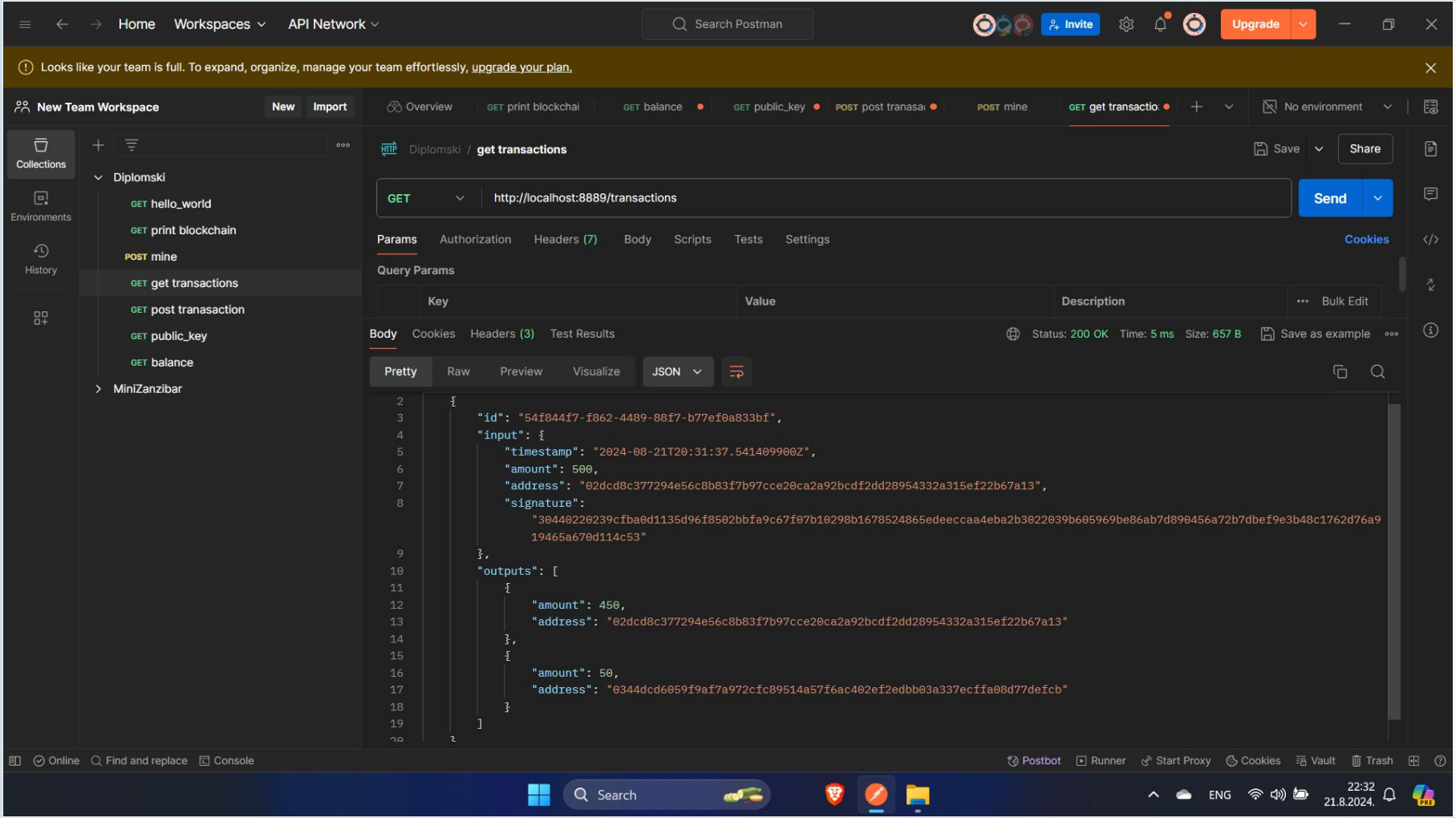
Карактеристика	Традиционалне базе података	*Blockchain*
Централизација	Централизоване	Децентрализован
Транспарентност	Ограничена	Висока
Поверљивост	Зависи од система	Потпуна
Сигурност	Осетљиве	Отпоран
Отпорност на цензуру	Ниска	Висока
Ефикасност обраде података	Брза	Спорија
Трошкови	Јефтинија	Скупља

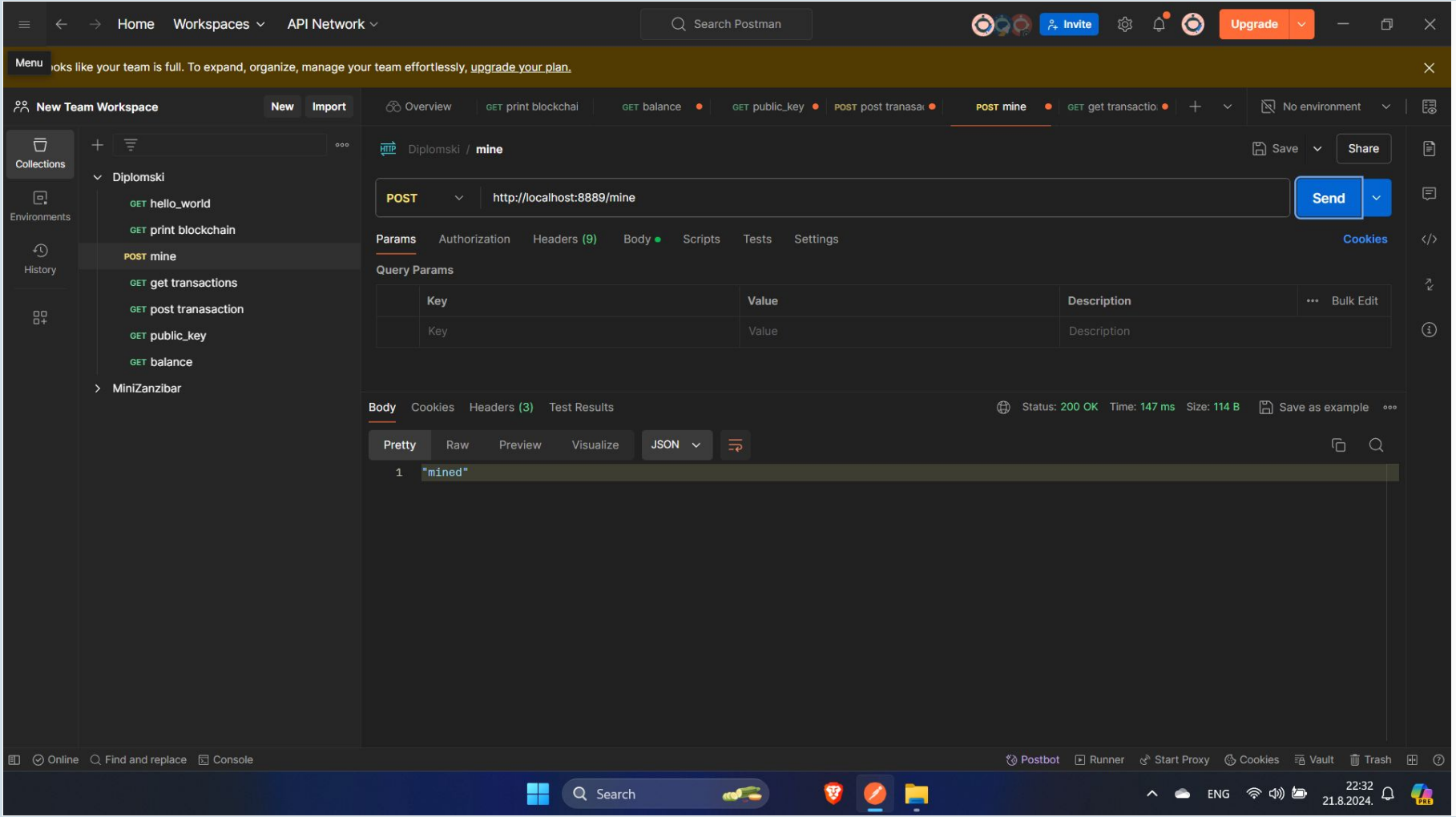

Home
Workspaces
API Network
Search Postman
Invite
Upgrade
Looks like your team is full. To expand, organize, manage your team effortlessly, upgrade your plan.
New Team Workspace
New
Import
Overview
GET print blockchain
GET balance
No environment
Collections
Environments
History
Diplomski
GET hello_world
GET print blockchain
POST mine
GET get transactions
GET post tranasaction
GET public_key
GET balance
MiniZanzibar
Diplomski / print blockchain
Save
Share
GET
http://localhost:8888/blockchain
Send
Params
Authorization
Headers (7)
Body
Scripts
Tests
Settings
Cookies
Query Params
Key
Value
Description
Bulk Edit
Body
Cookies
Headers (3)
Test Results
Status: 200 OK
Time: 11 ms
Size: 256 B
Save as example
Pretty
Raw
Preview
Visualize
JSON
{
"chain": [
{
"timestamp": "2024-08-21T20:24:40.547317100Z",
"last_hash": "genesis_last_hash",
"hash": "genesis_hash",
"data": [],
"nonce": 0,
"difficulty": 3
}
]
}
Online
Find and replace
Console
Postbot
Runner
Start Proxy
Cookies
Vault
Trash
Search
ENG
22:26
21.8.2024.

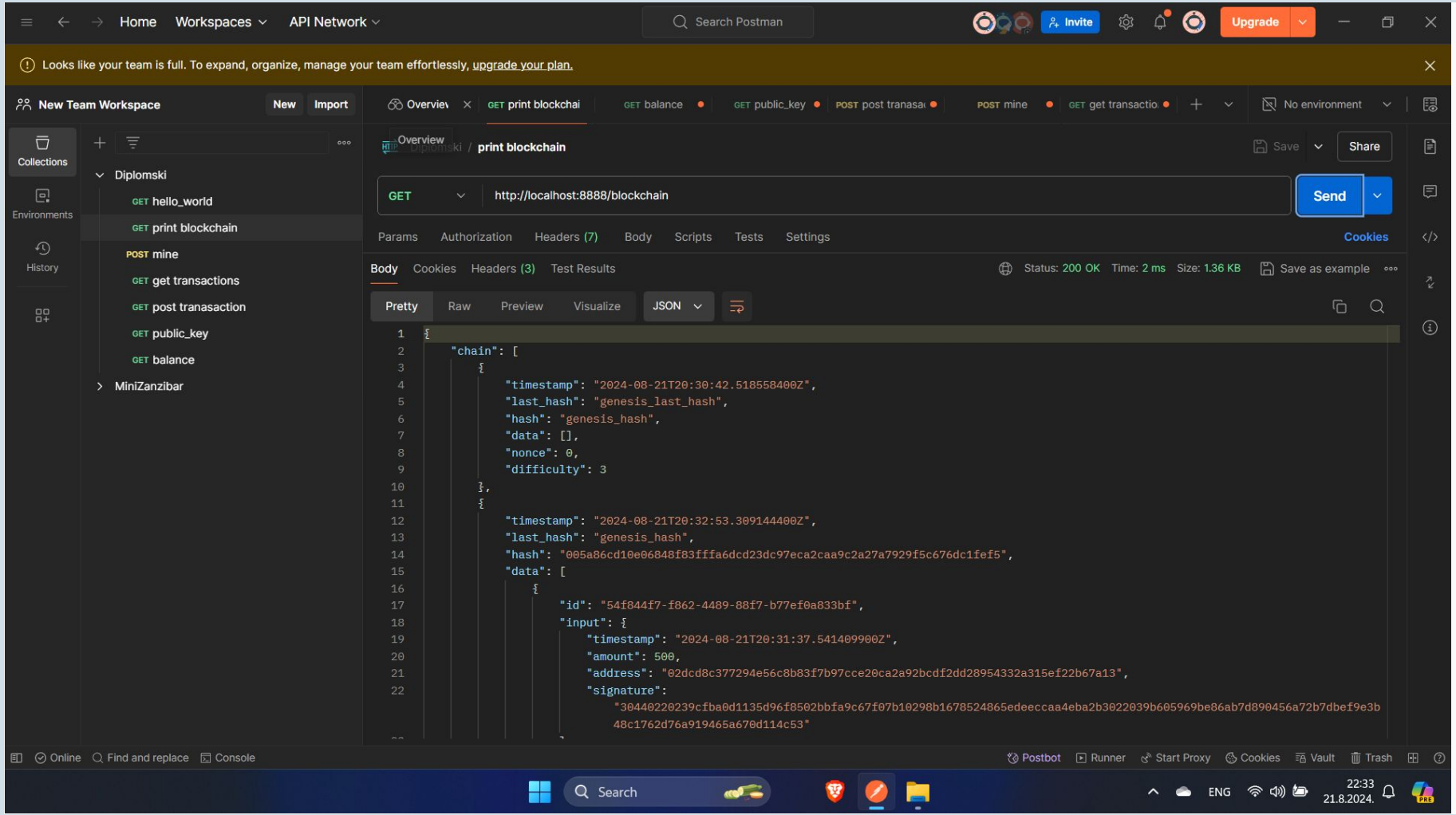

Home
Workspaces
API Network
Search Postman
Invite
Upgrade
Looks like your team is full. To expand, organize, manage your team effortlessly, upgrade your plan.
New Team Workspace
New
Import
Overview
GET print blockchain
GET balance
No environment
Collections
Environments
History
Diplomski
GET hello_world
GET print blockchain
POST mine
GET get transactions
GET post tranasaction
GET public_key
GET balance
MiniZanzibar
Diplomski / balance
Save
Share
GET
http://localhost:8888/balance
Send
Params
Authorization
Headers (7)
Body
Scripts
Tests
Settings
Cookies
Query Params
Key
Value
Description
Bulk Edit
Body
Cookies
Headers (3)
Test Results
Status: 200 OK
Time: 4 ms
Size: 110 B
Save as example
Pretty
Raw
Preview
Visualize
JSON
1 500
Online
Find and replace
Console
Postbot
Runner
Start Proxy
Cookies
Vault
Trash
Search
ENG
22:26
21.8.2024.

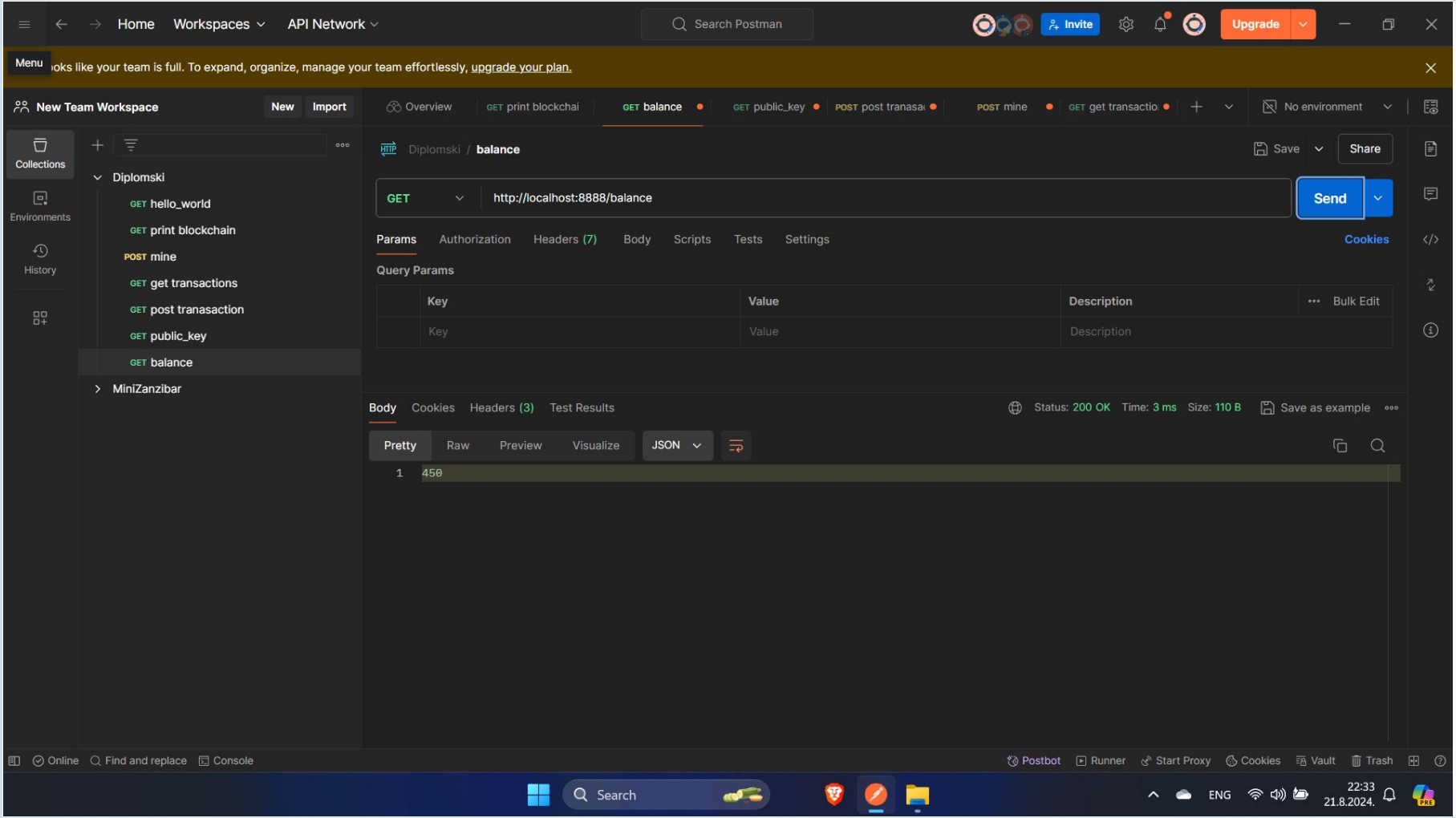

Home
Workspaces
API Network
Search Postman
Invite
Upgrade
Looks like your team is full. To expand, organize, manage your team effortlessly, upgrade your plan.
New Team Workspace
New
Import
Collections
Environments
History
Diplomski
GET hello_world
GET print blockchain
POST mine
GET get transactions
GET post tranasaction
GET public_key
GET balance
MiniZanzibar
Overview
GET print blockchain
GET balance
GET public_key
POST post tranasactic
POST mine
No environment
Diplomski / public_key
Save
Share
GET
http://localhost:8889/public_key
Send
Params
Authorization
Headers (7)
Body
Scripts
Tests
Settings
Cookies
Query Params
Key
Value
Description
Bulk Edit
Body
Cookies
Headers (3)
Test Results
Status: 200 OK
Time: 8 ms
Size: 176 B
Save as example
Pretty
Raw
Preview
Visualize
JSON
1 "0344dcd6059f9af7a972cfc89514a57f6ac402ef2edbb03a337ecffa08d77defcb"
Online
Find and replace
Console
Postbot
Runner
Start Proxy
Cookies
Vault
Trash
Search
ENG
22:31
21.8.2024.

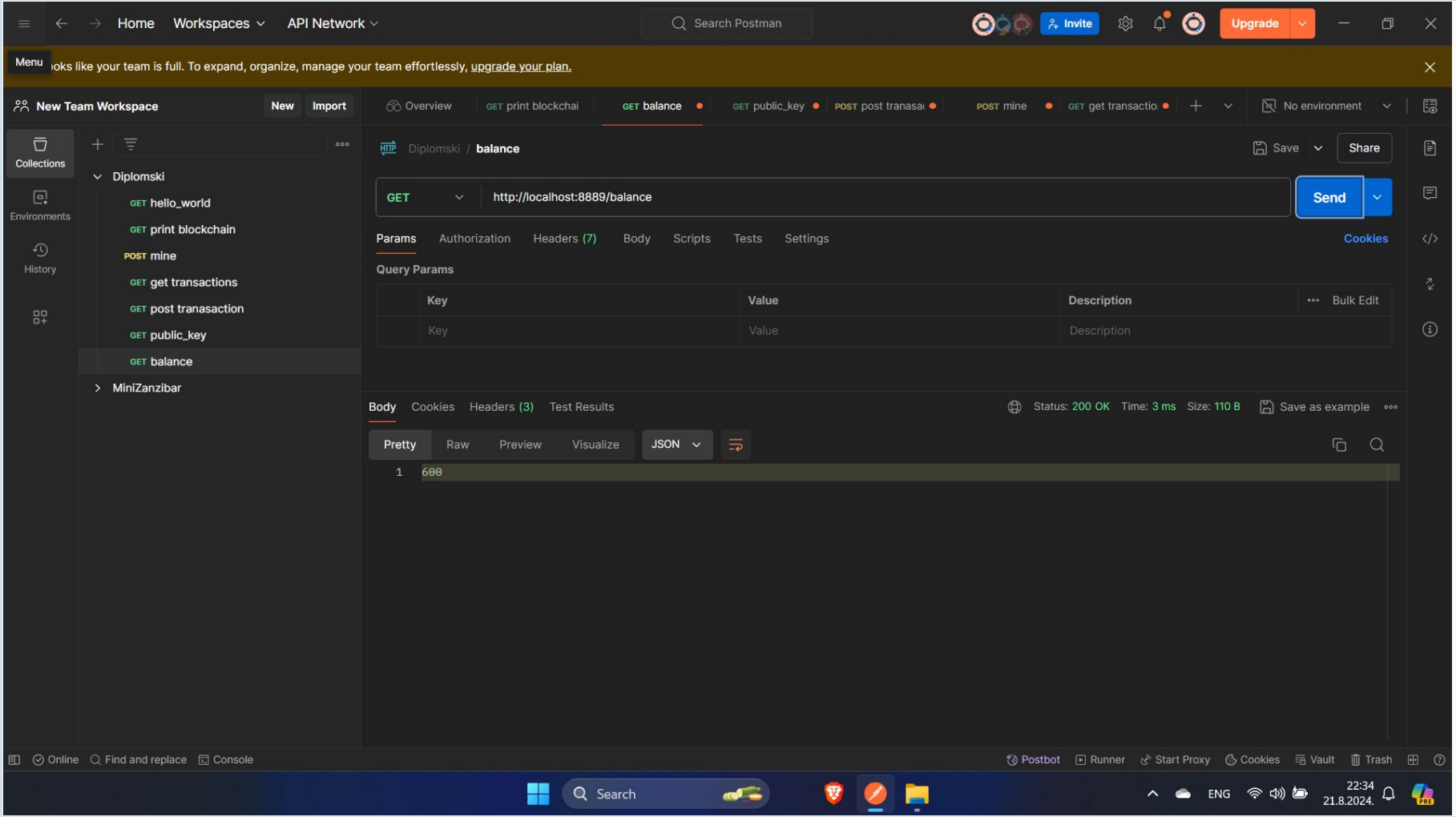

Home
Workspaces
API Network
Search Postman
Invite
Upgrade
Looks like your team is full. To expand, organize, manage your team effortlessly, upgrade your plan.
New Team Workspace
New
Import
Overview
GET print blockchain
GET balance
GET public_key
POST post tranasactio
POST mine
No environment
Collections
Environments
History
Diplomski
GET hello_world
GET print blockchain
POST mine
GET get transactions
GET post tranasaction
GET public_key
GET balance
MiniZanzibar
Diplomski / post tranasaction
Save
Share
POST
http://localhost:8888/transaction
Send
Params
Authorization
Headers (9)
Body
Scripts
Tests
Settings
Cookies
none
form-data
x-www-form-urlencoded
raw
binary
GraphQL
JSON
Beautify
{
"recipient": "0344dcd6059f9af7a972cfc89514a57f6ac402ef2edbb03a337ecffa08d77defcb",
"amount": 50
}
Body
Cookies
Headers (3)
Test Results
Status: 201 Created
Time: 11 ms
Size: 660 B
Save as example
Pretty
Raw
Preview
Visualize
JSON
"id": "54f844f7-f862-4489-88f7-b77ef0a833bf",
"input": {
"timestamp": "2024-08-21T20:31:37.541409900Z",
"amount": 500,
"address": "02dcd8c377294e56c8b83f7b97cce20ca2a92bcdf2dd28954332a315ef22b67a13",
"signature":
"30440220239cfba0d1135d96f8502bbfa9c67f07b10298b1678524865edeeccaa4eba2b3022039b605969be86ab7d890456a72b7dbef9e3b48c1762d76a919465a670d114c53"
},
"outputs": [
{
"amount": 450,
"address": "02dcd8c377294e56c8b83f7b97cce20ca2a92bcdf2dd28954332a315ef22b67a13"
},
{
"amount": 50,
Online
Find and replace
Console
Postbot
Runner
Start Proxy
Cookies
Vault
Trash
Search
ENG
22:31
21.8.2024.


Home
Workspaces
API Network
Search Postman
Invite
Upgrade
Looks like your team is full. To expand, organize, manage your team effortlessly, upgrade your plan.
New Team Workspace
New
Import
Overview
GET print blockchai
GET balance
GET public_key
POST post tranasa
POST mine
GET get transactio
No environment
Collections
Environments
History
Diplomski
GET hello_world
GET print blockchain
POST mine
GET get transactions
GET post tranasaction
GET public_key
GET balance
MiniZanzibar
Diplomski / get transactions
Save
Share
GET
http://localhost:8889/transactions
Send
Params
Authorization
Headers (7)
Body
Scripts
Tests
Settings
Cookies
Query Params
Key
Value
Description
Bulk Edit
Body
Cookies
Headers (3)
Test Results
Status: 200 OK
Time: 5 ms
Size: 657 B
Save as example
Pretty
Raw
Preview
Visualize
JSON
{
"id": "54f844f7-f862-4489-88f7-b77ef0a833bf",
"input": {
"timestamp": "2024-08-21T20:31:37.541409900Z",
"amount": 500,
"address": "02dcd8c377294e56c8b83f7b97cce20ca2a92bcdf2dd28954332a315ef22b67a13",
"signature":
"30440220239cfba0d1135d96f8502bbfa9c67f07b10298b1678524865edeeccaa4eba2b3022039b605969be86ab7d890456a72b7dbef9e3b48c1762d76a919465a670d114c53"
},
"outputs": [
{
"amount": 450,
"address": "02dcd8c377294e56c8b83f7b97cce20ca2a92bcdf2dd28954332a315ef22b67a13"
},
{
"amount": 50,
"address": "0344dcd6059f9af7a972cfc89514a57f6ac402ef2edbb03a337ecffa08d77defcb"
}
]
}
Online
Find and replace
Console
Postbot
Runner
Start Proxy
Cookies
Vault
Trash
Search
ENG
22:32
21.8.2024.


Home
Workspaces
API Network
Search Postman
Invite
Upgrade
Menu
ooks like your team is full. To expand, organize, manage your team effortlessly, upgrade your plan.
New Team Workspace
New
Import
Overview
GET print blockchai
GET balance
GET public_key
POST post tranasa
POST mine
GET get transactio
No environment
Collections
Environments
History
Diplomski
GET hello_world
GET print blockchain
POST mine
GET get transactions
GET post tranasaction
GET public_key
GET balance
MiniZanzibar
Diplomski / mine
Save
Share
POST
http://localhost:8889/mine
Send
Params
Authorization
Headers (9)
Body
Scripts
Tests
Settings
Cookies
Query Params
Key
Value
Description
Bulk Edit
Body
Cookies
Headers (3)
Test Results
Status: 200 OK
Time: 147 ms
Size: 114 B
Save as example
Pretty
Raw
Preview
Visualize
JSON
1 "mined"
Online
Find and replace
Console
Postbot
Runner
Start Proxy
Cookies
Vault
Trash
Search
ENG
22:32
21.8.2024.


Home
Workspaces
API Network
Search Postman
Invite
Upgrade
Looks like your team is full. To expand, organize, manage your team effortlessly, upgrade your plan.
New Team Workspace
New
Import
Collections
Environments
History
Diplomski
GET hello_world
GET print blockchain
POST mine
GET get transactions
GET post tranasaction
GET public_key
GET balance
MiniZanzibar
Overview
GET print blockchai
GET balance
GET public_key
POST post tranasa
POST mine
GET get transactio
No environment
Diplomski / print blockchain
Save
Share
GET
http://localhost:8888/blockchain
Send
Params
Authorization
Headers (7)
Body
Scripts
Tests
Settings
Cookies
Body
Cookies
Headers (3)
Test Results
Status: 200 OK
Time: 2 ms
Size: 1.36 KB
Save as example
Pretty
Raw
Preview
Visualize
JSON
{
"chain": [
{
"timestamp": "2024-08-21T20:30:42.518558400Z",
"last_hash": "genesis_last_hash",
"hash": "genesis_hash",
"data": [],
"nonce": 0,
"difficulty": 3
},
{
"timestamp": "2024-08-21T20:32:53.309144400Z",
"last_hash": "genesis_hash",
"hash": "005a86cd10e06848f83fffa6dcd23dc97eca2caa9c2a27a7929f5c676dc1fef5",
"data": [
{
"id": "54f844f7-f862-4489-88f7-b77ef0a833bf",
"input": {
"timestamp": "2024-08-21T20:31:37.541409900Z",
"amount": 500,
"address": "02dcd8c377294e56c8b83f7b97cce20ca2a92bcdf2dd28954332a315ef22b67a13",
"signature":
"30440220239cfba0d1135d96f8502bbfa9c67f07b10298b1678524865edeeccaa4eba2b3022039b605969be86ab7d890456a72b7dbef9e3b
48c1762d76a919465a670d114c53"
Online
Find and replace
Console
Postbot
Runner
Start Proxy
Cookies
Vault
Trash
Search
ENG
22:33
21.8.2024.


Home
Workspaces
API Network
Search Postman
Invite
Upgrade
Menu
oks like your team is full. To expand, organize, manage your team effortlessly, upgrade your plan.
New Team Workspace
New
Import
Overview
GET print blockchai
GET balance
GET public_key
POST post tranasa
POST mine
GET get transactio
No environment
Collections
Environments
History
Diplomski
GET hello_world
GET print blockchain
POST mine
GET get transactions
GET post tranasaction
GET public_key
GET balance
MiniZanzibar
Diplomski / balance
Save
Share
GET
http://localhost:8888/balance
Send
Params
Authorization
Headers (7)
Body
Scripts
Tests
Settings
Cookies
Query Params
Key
Value
Description
Bulk Edit
Body
Cookies
Headers (3)
Test Results
Status: 200 OK
Time: 3 ms
Size: 110 B
Save as example
Pretty
Raw
Preview
Visualize
JSON
1 450
Online
Find and replace
Console
Postbot
Runner
Start Proxy
Cookies
Vault
Trash
Search
ENG
22:33
21.8.2024.


Home
Workspaces
API Network
Search Postman
Invite
Upgrade
Menu
oks like your team is full. To expand, organize, manage your team effortlessly, upgrade your plan.
New Team Workspace
New
Import
Overview
GET print blockchai
GET balance
GET public_key
POST post tranasa
POST mine
GET get transactio
No environment
Collections
Environments
History
Diplomski
GET hello_world
GET print blockchain
POST mine
GET get transactions
GET post tranasaction
GET public_key
GET balance
MiniZanzibar
Diplomski / balance
Save
Share
GET
http://localhost:8889/balance
Send
Params
Authorization
Headers (7)
Body
Scripts
Tests
Settings
Cookies
Query Params
Key
Value
Description
Bulk Edit
Body
Cookies
Headers (3)
Test Results
Status: 200 OK
Time: 3 ms
Size: 110 B
Save as example
Pretty
Raw
Preview
Visualize
JSON
1 600
Online
Find and replace
Console
Postbot
Runner
Start Proxy
Cookies
Vault
Trash
Search
ENG
22:34
21.8.2024.

Хвала на пажњи