

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

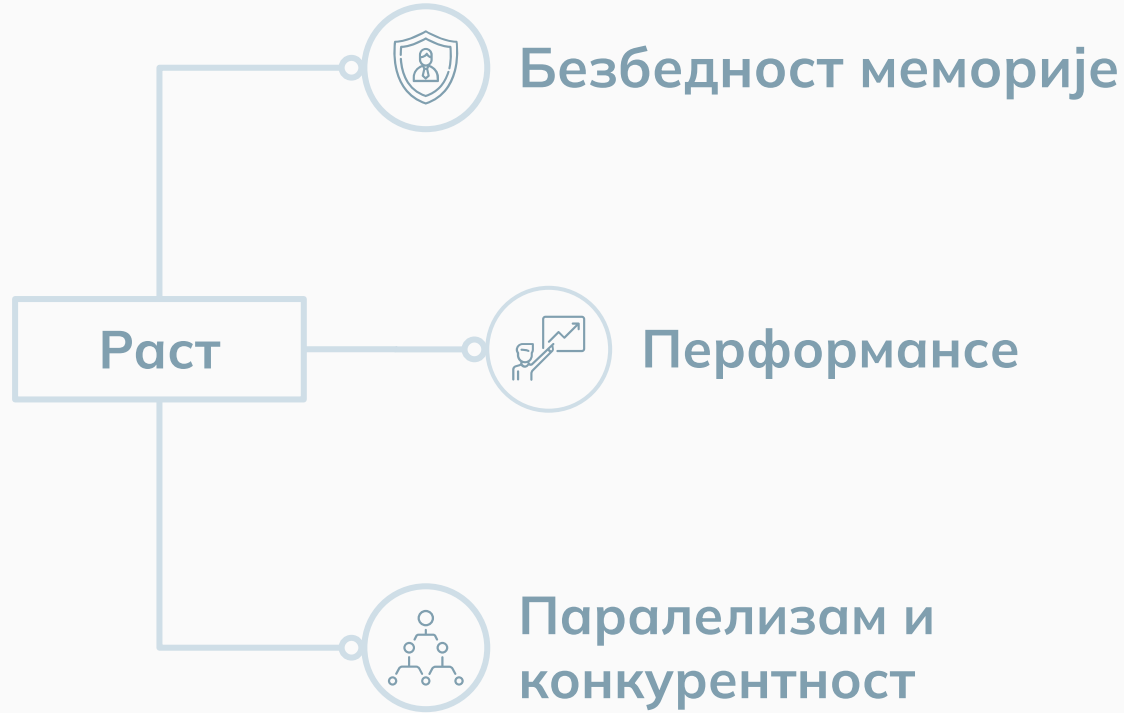
Bitcoin: Peer-to-peer
електронски готовински
систем

2015

Виталик Бутерин

Увођење паметних
уговора

Зашто Раст?



Архитектура

hash: 04aaujeui15io
timestamp: 1230937200
nonce: 1
difficulty: 1
data: []



hash: 0004jwef91344ia
previous hash: 04aaujeui15io
timestamp: 1231023600
nonce: 131
difficulty: 3
data: [<Transaction>,
<Transaction>]



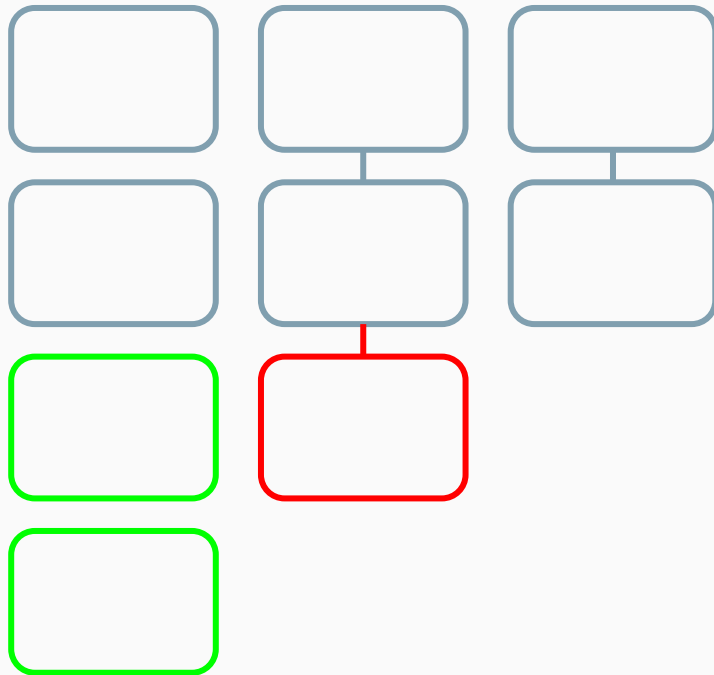
hash: 00468hjiaowef1
previous hash: 04jwef91344ia
timestamp: 1231110000
nonce: 86
difficulty: 2
data: [<Transaction>,
<Transaction>]

Валидација ланца

Рудар А

Рудар Б

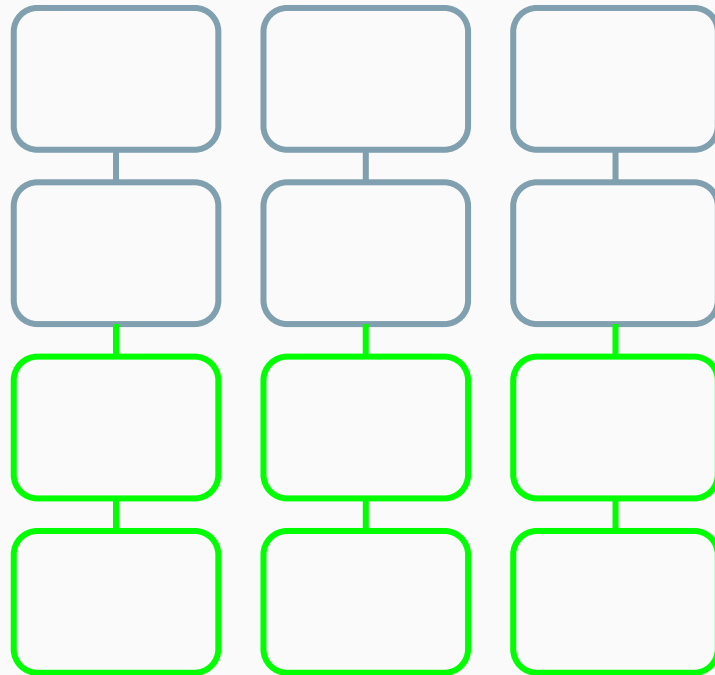
Рудар В



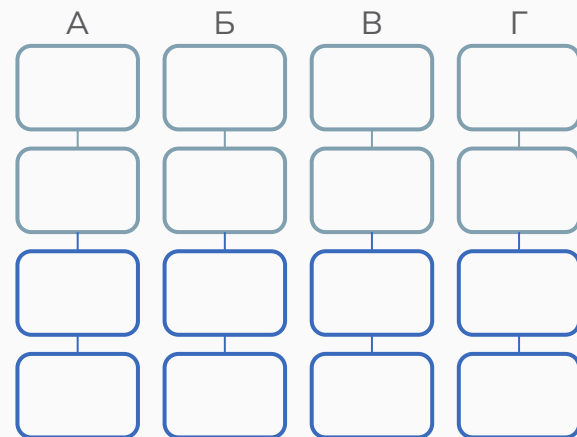
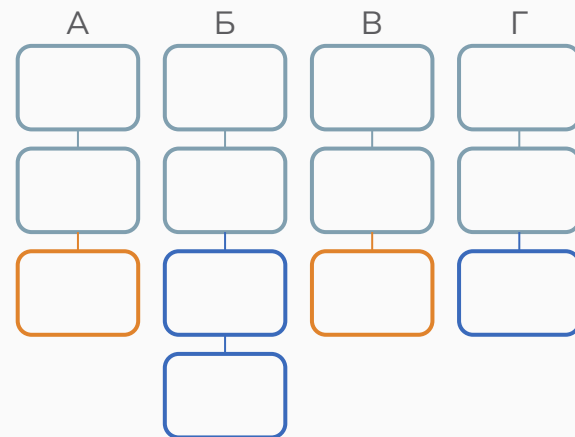
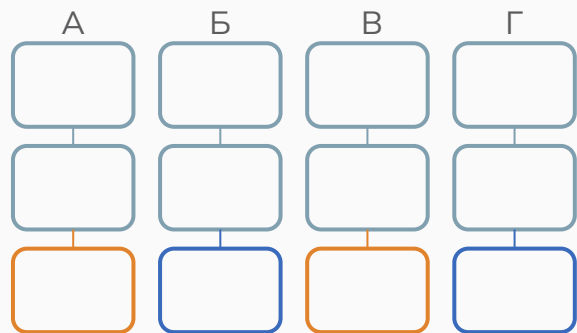
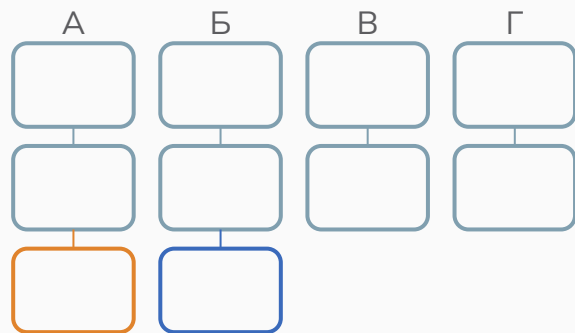
Рудар А

Рудар Б

Рудар В



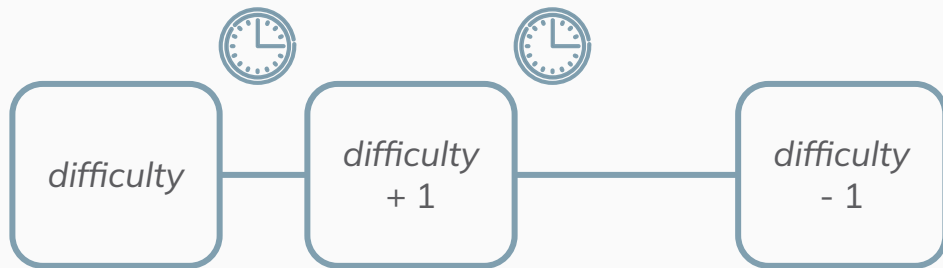
Проблем рачвања у ланцу



Рударење

hash: 000000haxi2910jasdfk
previous hash: 04aaujeui15io
timestamp: 1231023600
nonce: 16731
difficulty: 6
data: [<Transaction>,
<Transaction>]

$difficulty = 6$
 $hash = \underline{000000}haxi2910jasdfk$

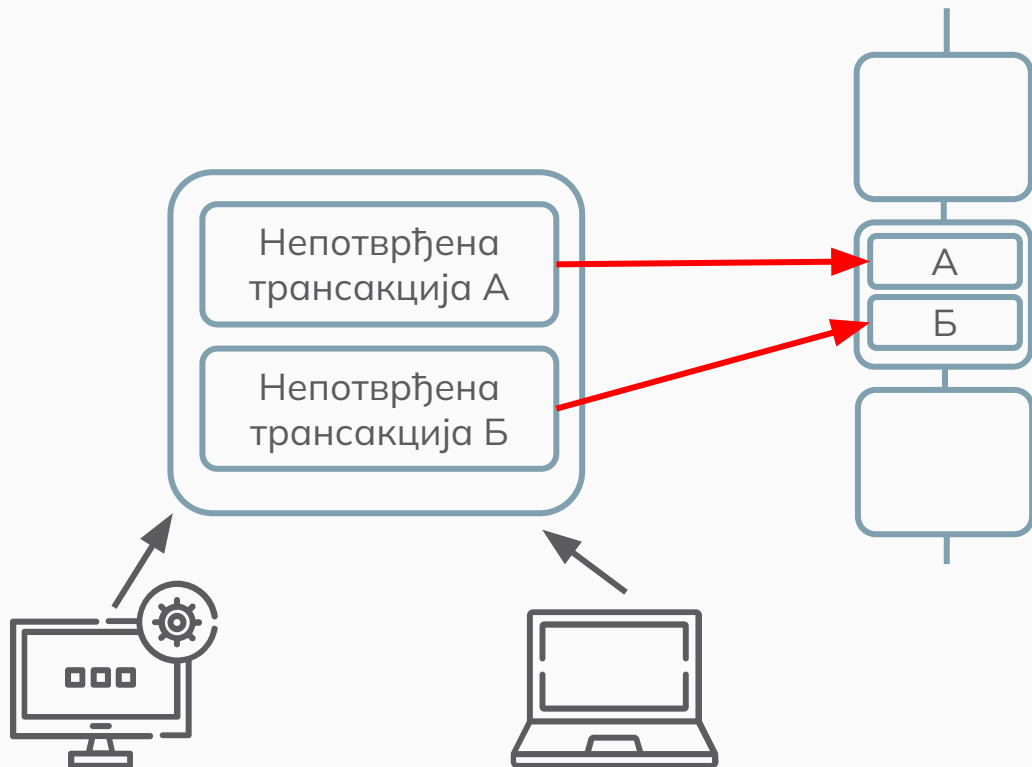


Трансакције и базен трансакција

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

Output:
Amount: 50
Address: 0xbar2

Output:
Amount: 460
Address: 0xfoo1



Новчаник

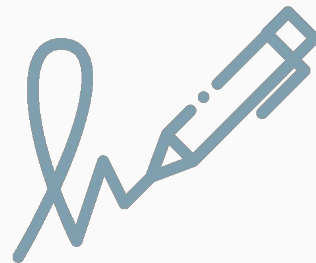
приватни кључ



+



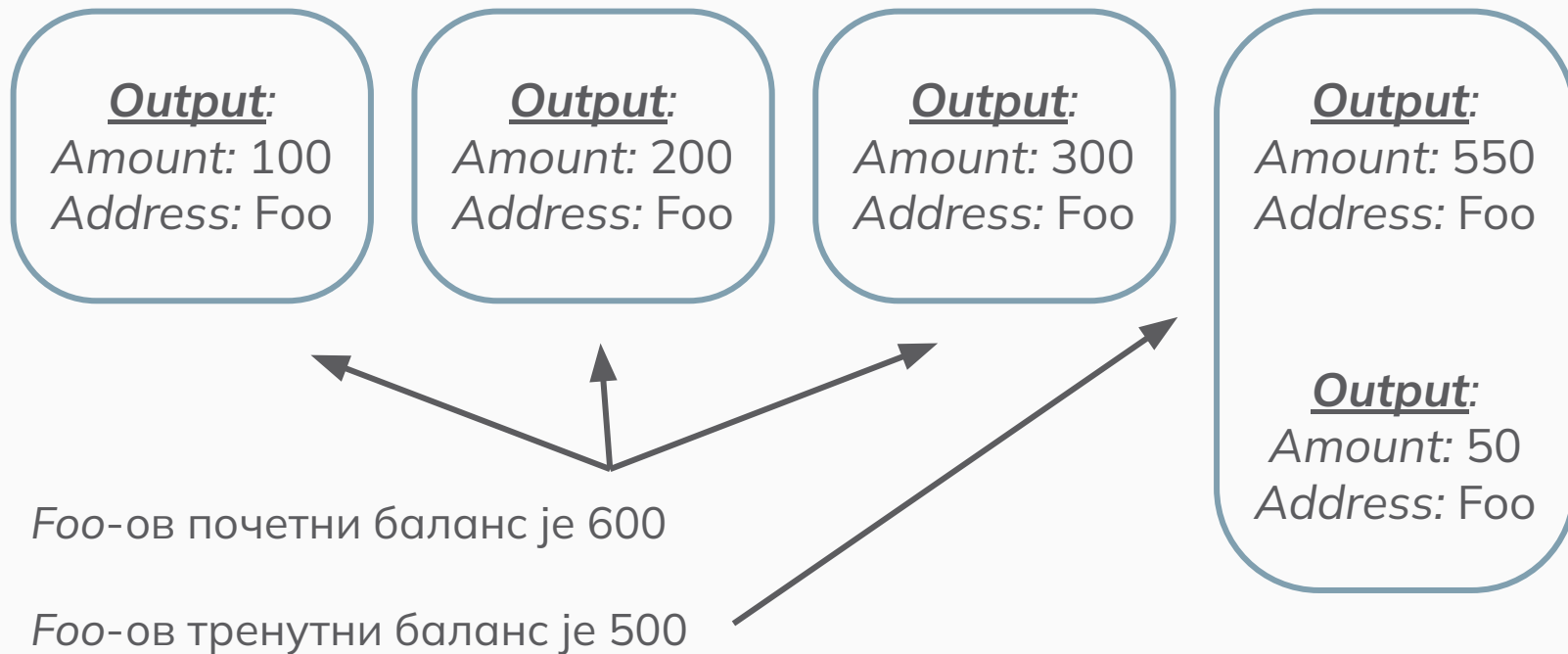
=



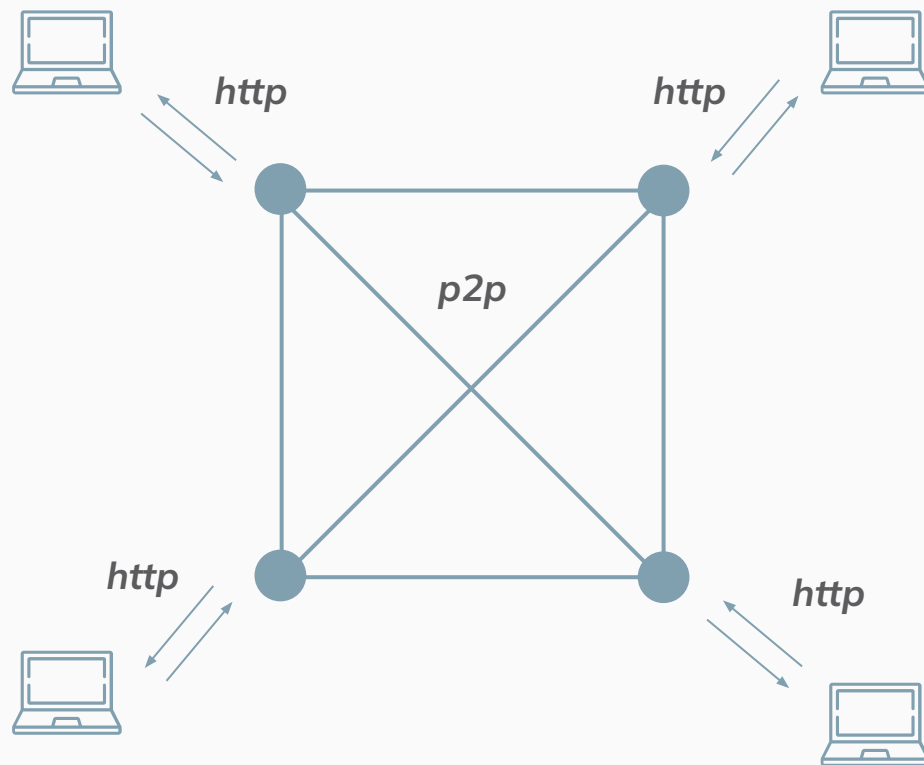
јавни кључ



Рачунање стања новчаника



Комуникација



Поређење *blockchain* технологије са традиционалним базама

Карактеристика	Традиционалне базе података	<i>Blockchain</i>
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

🗑 Collections

+

☰

⋮

📁 Environments

🕒 History

🧩

⌵ Diplomski

GET hello_world

GET print blockchain

POST mine

GET get transactions

GET post transaction

GET public_key

GET balance

➤ MiniZanzibar

🔗 Overview

GET print blockchai

GET balance

GET public_key

POST post tranasac

POST mine

GET get transactio

+

⌵

🗑 No environment

⌵

📄

🔗 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
	Key	Value	Description	

Body

Cookies

Headers (3)

Test Results

🌐 Status: 200 OK Time: 5 ms Size: 123 B

📄 Save as example

⋮

Pretty

Raw

Preview

Visualize

JSON

⌵

🔗

1

2

3

```
{
  "balance": 500
}
```

📄

🔍

📄 Online

🔍 Find and replace

📄 Console

🔗 Postbot

📄 Runner

🔗 Start Proxy

📄 Cookies

🔗 Vault

🗑 Trash

⌵

⌵

🔍 Search

🌐

📄

🔗

🔗

ENG

🔗

🔗

🔗

20:15

22.8.2024.

🔗

📄

⋮

←

→

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 trasanaction

GET public_key

GET balance

➤ MiniZanzibar

Overview

GET print blockchai

GET balance

GET public_key

POST post trasanac

POST mine

GET get transactio

+

▼

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
	Key	Value	Description	

Body

Cookies

Headers (3)

Test Results

Status: 200 OK

Time: 5 ms

Size: 191 B

Save as example

⋮

Pretty

Raw

Preview

Visualize

JSON

▼

🔗

```
1 {
2   "public_key": "02d96b436e3717e87c97503a854546c30a85f7cf049076ba9a87cc1d1637e7bb42"
3 }
```

📄

🌐 Online

🔍 Find and replace

📄 Console

🔗 Postbot

🏃 Runner

🔄 Start Proxy

🔒 Cookies

🔒 Vault

🗑️ Trash

🔗

🔗

🖱️

🔍 Search

🌸

🏠

🏆

🔧

⬆️

☁️

ENG

🔊

🔌

20:15

22.8.2024.

🔔

👤

⋮

←

→

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 transaction

GET public_key

GET balance

MiniZanzibar

Overview

GET print blockchai

GET balance

GET public_key

POST post tranasac

POST mine

GET get transactio

+

⋮

No environment

📄

Diplomski / post transaction

Save

Share

POST

http://localhost:8888/transaction

Send

Params

Authorization

Headers (9)

Body

Scripts

Tests

Settings

Cookies

Beautify

none

form-data

x-www-form-urlencoded

raw

binary

GraphQL

JSON

1

2

3

4

1

2

3

4

Body

Cookies

Headers (3)

Test Results

Status: 201 Created

Time: 14 ms

Size: 662 B

Save as example

Pretty

Raw

Preview

Visualize

JSON

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

⌨️ Online

🔍 Find and replace

📄 Console

🔗 Postbot

🏃 Runner

🌐 Start Proxy

🍪 Cookies

🔒 Vault

🗑️ Trash

🔍

🔍 Search

🏠

🎮

🏆

🔪

🔍

🏠

☁️

ENG

🔊

🔌

20:16

22.8.2024.

🔔

👤

⋮

←

→

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 transaction

GET public_key

GET balance

MiniZanzibar

🔗 Overview

GET print blockchai

GET balance

GET public_key

POST post tranasac

POST mine

GET get transactio

+

⌵

No environment

📄

🔗 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
	Key	Value	Description	

Body

Cookies

Headers (2)

Test Results

🌐 Status: 200 OK Time: 45 ms Size: 75 B

📄 Save as example

⋮

Pretty

Raw

Preview

Visualize

Text

⌵

🔄

1

📄 Online 🔍 Find and replace 📄 Console

🔄 Postbot 📄 Runner 🔄 Start Proxy 📄 Cookies 📄 Vault 🗑 Trash

🖱️ 🔍 Search 🌸 🏠 🏆 🛠

⬆️ ☁️ ENG 📶 🔊 🔋 20:17 22.8.2024. 📢 🧑‍🚀

⋮

←

→

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

NewImport

Collections

+

⋮

⋮

Environments

⋮

History

⌚

⋮

Diplomski

GET hello_world

GET print blockchain

POST mine

GET get transactions

GET post transaction

GET public_key

GET balance

> MiniZanzibar

Overview

GET print blockchai

GET balance

GET public_key

POST post tranasac

POST mine

GET get transactio

+

▾

No environment ▾

HTTP

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
	Key	Value	Description		

Body

Cookies

Headers (3)

Test Results

Status: 200 OK

Time: 6 ms

Size: 123 B

Save as example

⋮

Pretty

Raw

Preview

Visualize

JSON ▾

1

2

3

```
{  "balance": 600}
```

📄 Online

🔍 Find and replace

📄 Console

🔗 Postbot

🏃 Runner

🌐 Start Proxy

🍪 Cookies

🔒 Vault

🗑️ Trash

⌵

🔍 Search

20:18

22.8.2024.

⌵

← → 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

🕒

📁

Overview

GET print blockchai

GET balance

GET public_key

POST post tranasac

POST mine

GET get transactio

+

▾

No environment ▾

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
	Key	Value	Description		

Body

Cookies

Headers (3)

Test Results

Status: 200 OK Time: 6 ms Size: 123 B Save as example ⋮

Pretty

Raw

Preview

Visualize

JSON ▾

1

2

3

```
{
  "balance": 450
}
```

MiniZanzibar

Online

🔍 Find and replace

📄 Console

Postbot

Runner

Start Proxy

Cookies

Vault

Trash

🔍

🔍 Search

ENG

20:18

22.8.2024.



Хвала на пажњи

