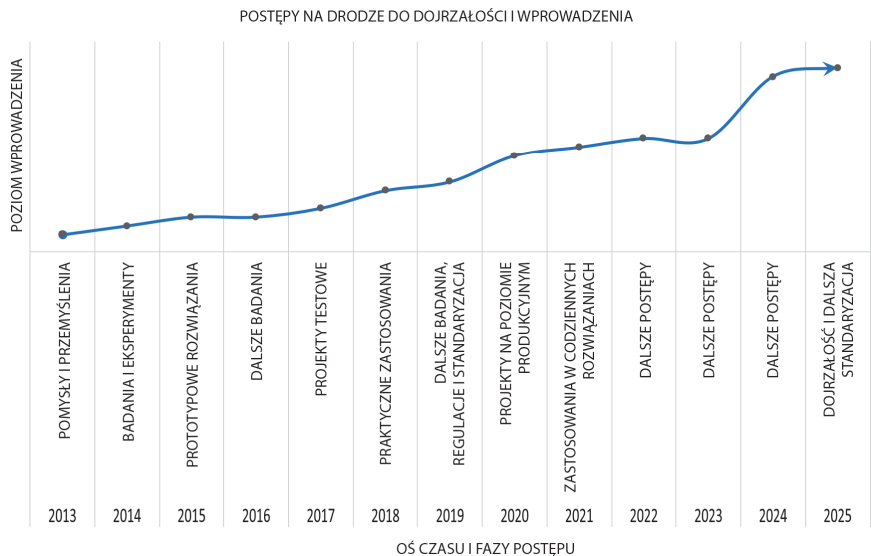


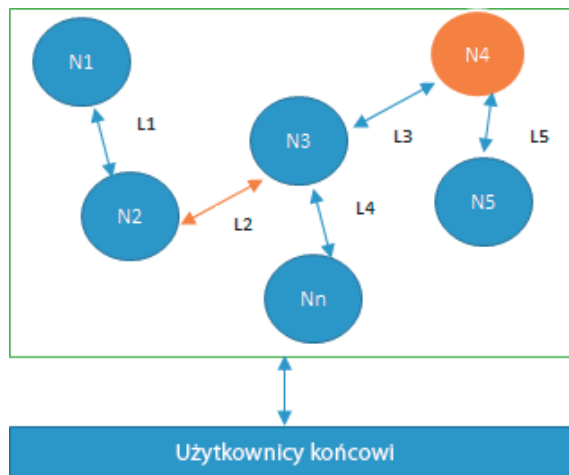
Rozdział 1. ABC łańcucha bloków



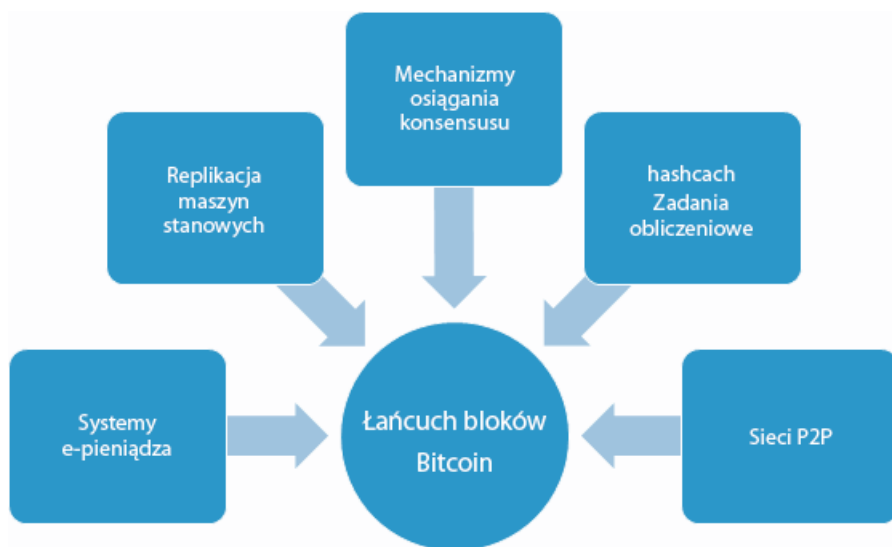
Rysunek 1.1. Wprowadzanie technologii łańcucha bloków i jej dojrzewanie



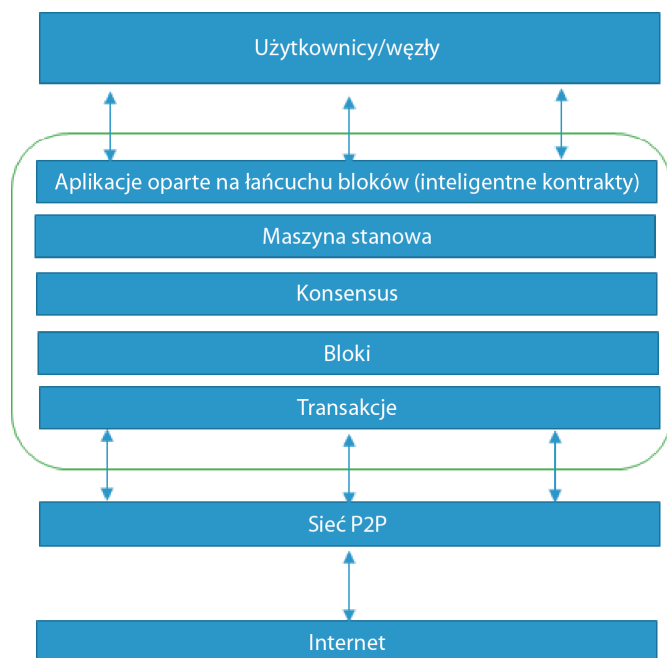
Rysunek 1.2. Liczba wyszukiwań słowa blockchain (czyli łańcuch bloków) w wyszukiwarce Google



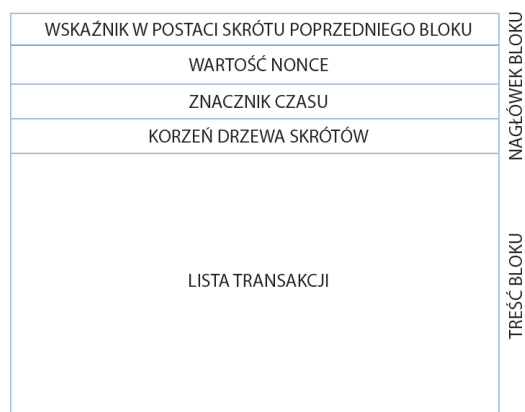
Rysunek 1.3. Projekt systemu rozproszonego: N4 to węzeł bizantyjski, L2 to uszkodzone lub powolne łącze sieciowe



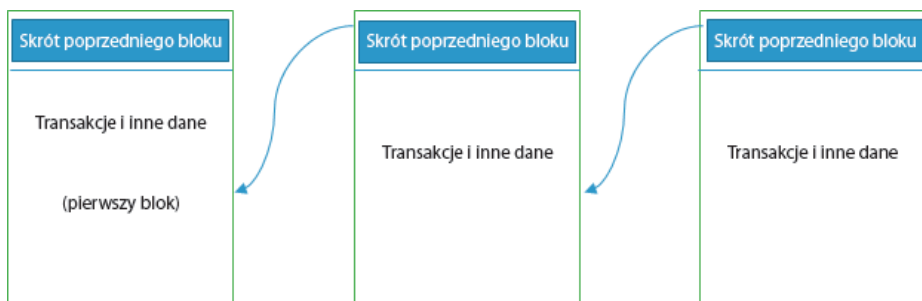
Rysunek 1.4. Różne idee wykorzystane do opracowania Bitcoina i łańcucha bloków



Rysunek 1.5. Obraz łańcucha bloków w kontekście sieci



Rysunek 1.6. Ogólna struktura bloku

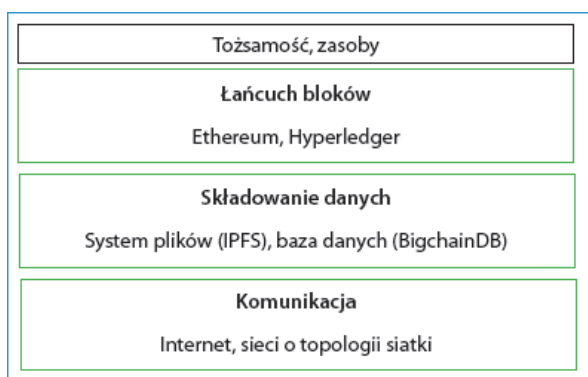


Rysunek 1.7. Ogólna struktura łańcucha bloków

Rozdział 2. Decentralizacja

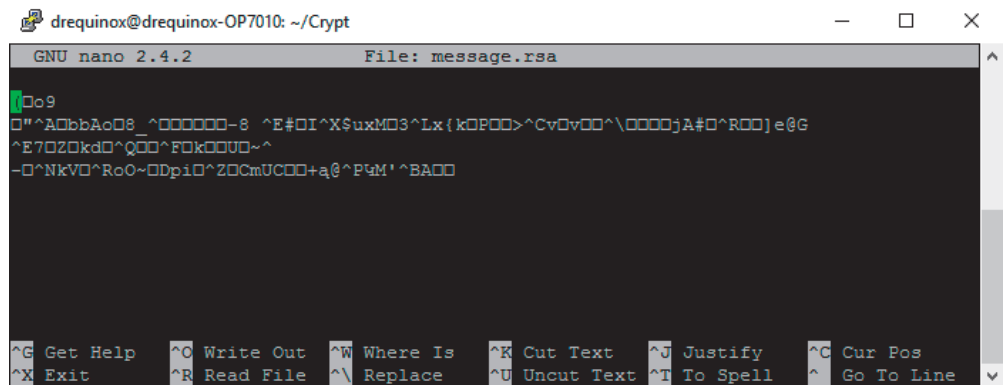


Rysunek 2.2. Poziom decentralizacji

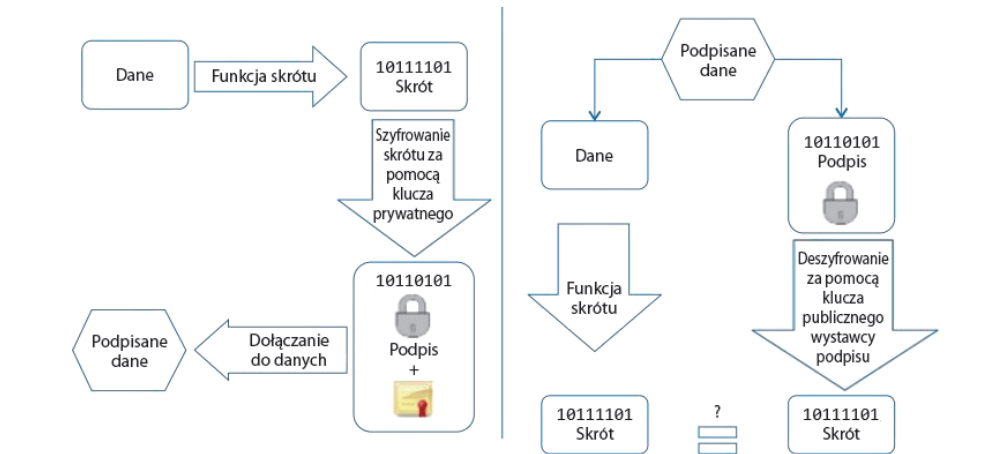


Rysunek 2.3. Zdecentralizowany ekosystem

Rozdział 4. Kryptografia klucza publicznego



Rysunek 4.8. Plik message.rsa zawierający niezrozumiałe (zaszyfrowane) dane



Rysunek 4.15. Tworzenie podpisu cyfrowego (po lewej) i proces sprawdzania podpisu (po prawej). Przykład tworzenia podpisów cyfrowych za pomocą RSA



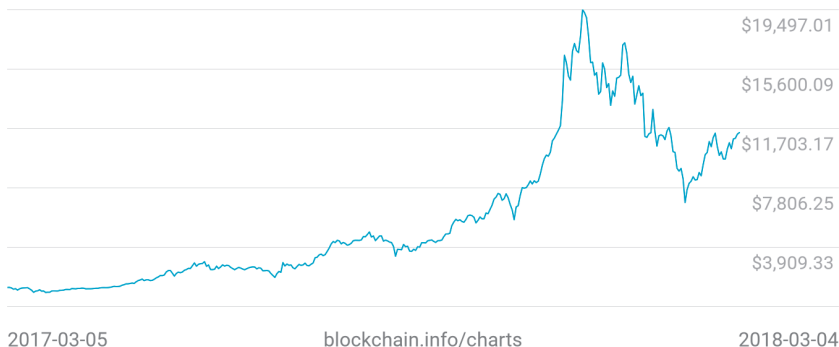
Rysunek 4.16. Zawartość pliku signature.bin

```
drequinox@drequinox-OP7010: ~/Crypt
drequinox$ openssl x509 -in ecccertificate.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1320520605335364006 (0xb74250f0fc159ea6)
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=GB, ST=Cambridge, O=Dr.Equinox!, OU=NA, CN=drequinox/emailAddress=drequinox@drequinox.com
        Validity
            Not Before: Sep 27 00:09:43 2016 GMT
            Not After : Sep 27 00:09:43 2017 GMT
        Subject: C=GB, ST=Cambridge, L=Cambridge, O=Dr.Equinox!, OU=NA, CN=drequinox/emailAddress=drequinox@drequinox.com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
            Public-Key: (256 bit)
                pub:
                    04:10:a2:92:e0:4e:3e:4c:04:c8:78:15:fc:a3:62:
                    7a:3e:12:a4:0d:ca:16:ad:73:d0:35:1a:3f:93:06:
                    3e:05:90:30:a5:7b:e5:c2:38:07:e4:b6:26:41:b5:
                    34:a9:4b:4f:33:b7:40:13:33:ac:6a:85:e6:7a:da:
                    81:fb:a7:0c:f9
                ASN1 OID: secp256k1
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                E1:68:E7:87:EE:E1:44:F0:70:71:76:4D:73:C6:15:14:F1:14:BE:F4
            X509v3 Authority Key Identifier:
                keyid:E1:68:E7:87:EE:E1:44:F0:70:71:76:4D:73:C6:15:14:F1:14:BE:F4
            X509v3 Basic Constraints:
                CA:TRUE
        Signature Algorithm: ecdsa-with-SHA256
            30:44:02:20:5e:ab:c9:85:f1:4f:e5:b1:05:e3:0f:ef:da:84:
            d7:d5:5f:c5:e9:20:be:c3:3c:34:b6:74:f4:a6:5e:11:3c:e0:
            02:20:65:b2:78:78:c7:80:ea:cf:a9:42:c4:ac:da:7b:cb:76:
            a0:15:62:0d:d0:89:f7:41:2a:03:9f:be:92:a7:2d:21
drequinox$
```

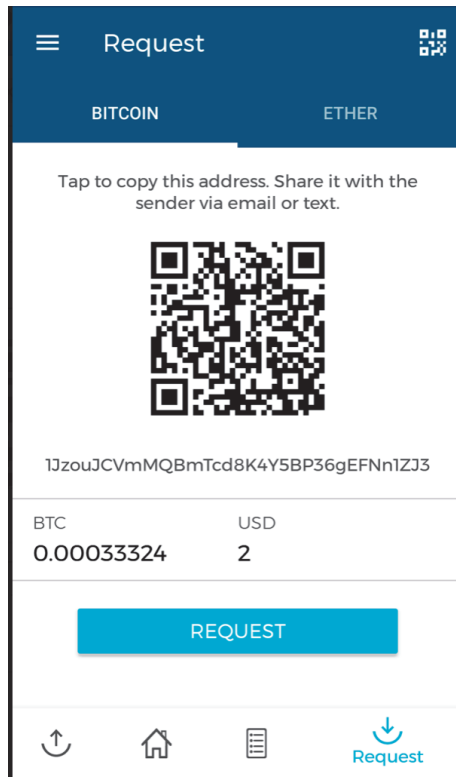
Rysunek 4.17. Certyfikat X509 wykorzystujący algorytmy ECDSA i SHA-256

Rozdział 5. Wprowadzenie do Bitcoina

Market Price (USD)
\$11,430.18



Rysunek 5.1. Ceny bitcoinów od marca 2017 r.



Rysunek 5.2. Żądanie płatności w bitcoinach (w portfelu Blockchain)



Rysunek 5.3. Kod QR reprezentujący płatność w bitcoinach

Bitcoin

Ether

From My Bitcoin Wallet

To 1JzouJCVmMQBmTcd8K4Y5BP36gEF...

BTC 0.00033324

GBP 1.53

Use total available minus fee: 0.00251933 BTC

Fee Regular

1+ hour

0.00010622 BTC (£0.49)

>

Continue

Rysunek 5.4. Wysyłanie bitcoinów za pomocą portfela Blockchain [138]

SENT

0.00043946 BTC

Value when sent: £2.00

Transaction fee: 0.00010622 BTC

Description

What's this for?

To 1JzouJCVmMQBmTcd8K4Y5BP36gEFNn1Z33

From My Bitcoin Wallet

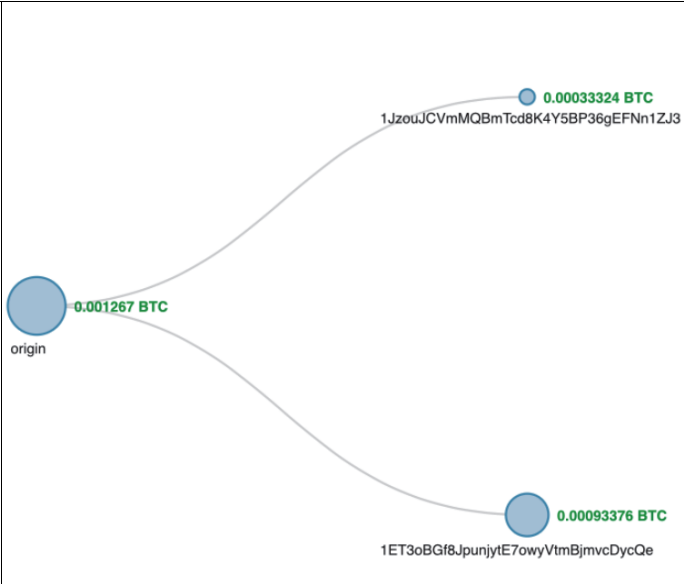
Date

October 29, 2017 @ 4:47pm

Status

Pending (0/3 Confirmations)

Rysunek 5.5. Przesłana transakcja



Rysunek 5.6. Wizualizacja przepływu środków w transakcji (z witryny Blockchain.info)

Transakcja [Zobacz informacje o transakcji bitcoin](#)

d28ca5a59b2239864eac1c96d3f1c23b747f0ded8f5af0161bae8a616b56a1d

1PL6gsm49xCFMvrXqgGcee5cdrG119GoWN

➡

1JzouJCVmMQBmTcd8K4Y5BP36gEFNn1ZJ3

1ET3oBGf8JpunjytE7owyVtmBjmvDycQe

0.00033324 BTC

0.00093376 BTC

0.001267 BTC

Podsumowanie		Przychody i wyjścia	
Rozmiar	226 (Bajtów)	Razem przychodów	0.00137322 BTC
Waga	904	Razem wychodzących	0.001267 BTC
Czas otrzymania	2017-10-29 16:51:42	Opląty	0.00010622 BTC
Zawarta w blokach	492229 (2017-10-29 16:51:42 + 0 minut)	Oplata za bajt	47 sat/B
Potwierdzeń	47715	Oplata za jednostkę wagi	11.75 sat/WU
Wizualizacja	Zobacz wykres drzewa	Szacunkowa ilość BTC w transakcji	0.00033324 BTC
		Skrypty	Pokaż skrypty & coinbase

Rysunek 5.7. Informacje o transakcji pobrane z witryny Blockchain.info



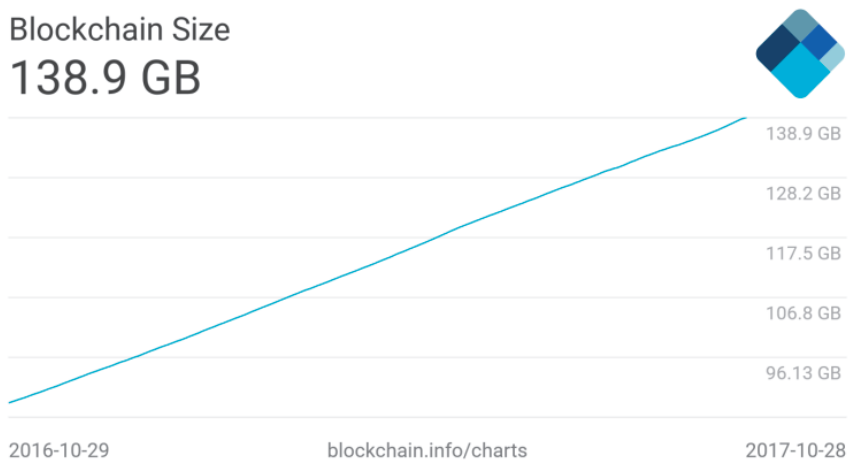
Rysunek 5.8. Hologram zabezpieczający na fizycznym bitcoinie Casascius z widocznym minikluczem i kodem QR



Rysunek 5.10. Klucz prywatny i adres Bitcoin w papierowym portfelu (za stroną: bitaddress.org)



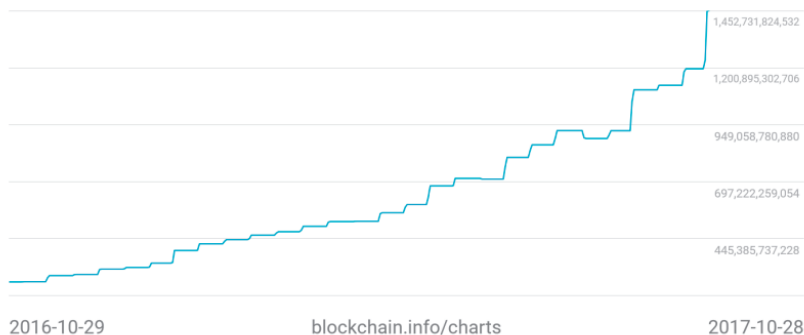
Rysunek 5.12. Adres vanity wygenerowany na stronie <https://bitcoinvanitygen.com/>



Rysunek 5.15. Aktualna wielkość łańcucha bloków na dzień 29.10.2017

Difficulty

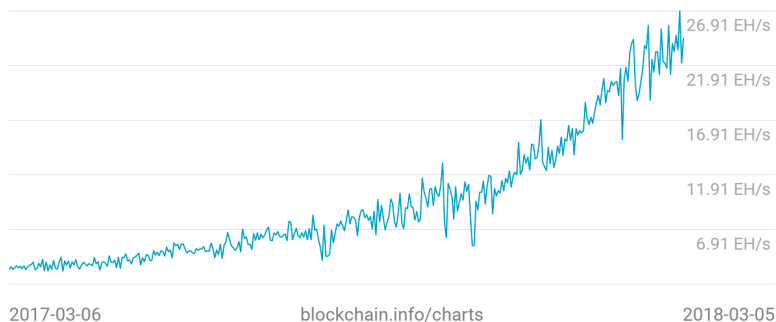
1,452,839,779,145



Rysunek 5.17. Trudność wydobywania bloków w ostatnim roku

Hash Rate

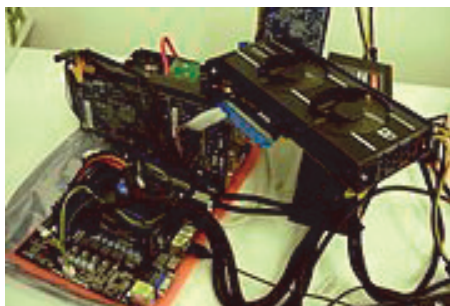
24.37 EH/s



Rysunek 5.18. Szybkość obliczania skrótów (mierzona w eksahashach) w okresie roku do marca 2018 r.



Rysunek 5.19. Zwykły procesor



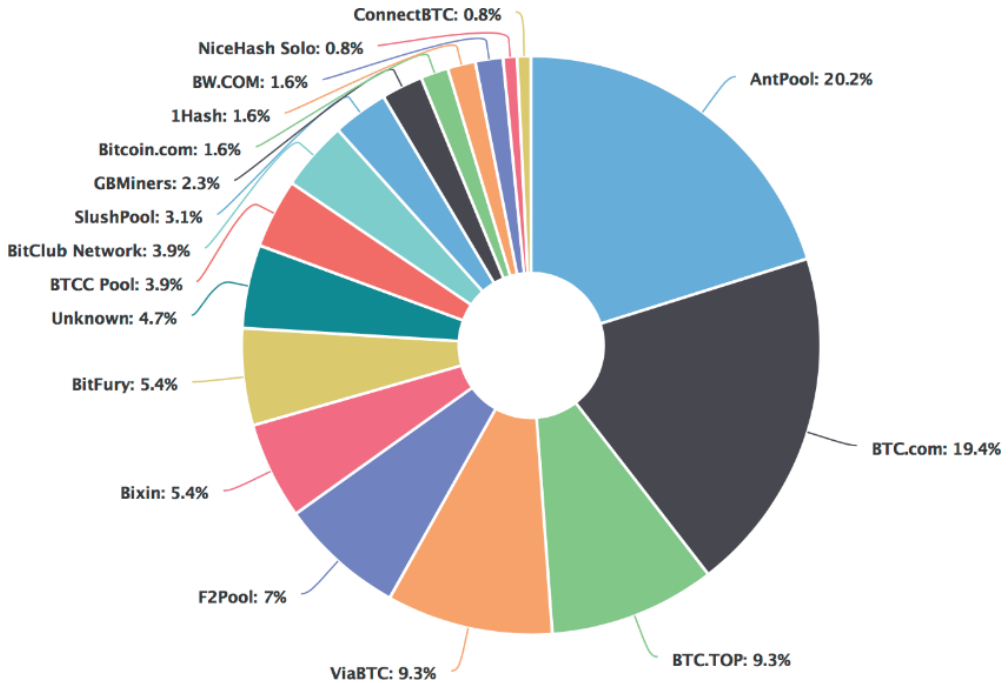
Rysunek 5.20. Procesor graficzny



Rysunek 5.21. Układ FPGA



Rysunek 5.22. Układy ASIC



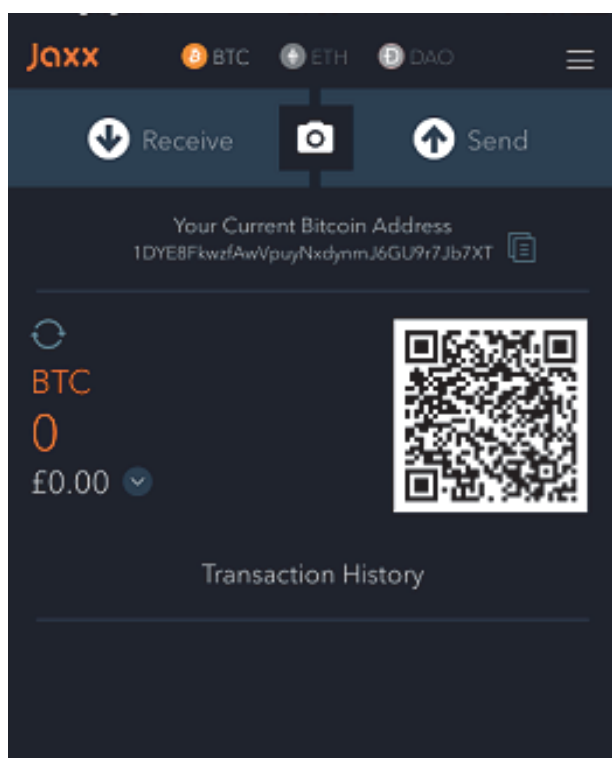
Rysunek 5.23. Kopalnie i ich moc obliczeniowa (szybkość obliczania skrótów) na dzień 28.10.2017.

Źródło: <https://blockchain.info/pools>

Rozdział 6. Sieć Bitcoina i płatności



Rysunek 6.5. Portfel Trezor



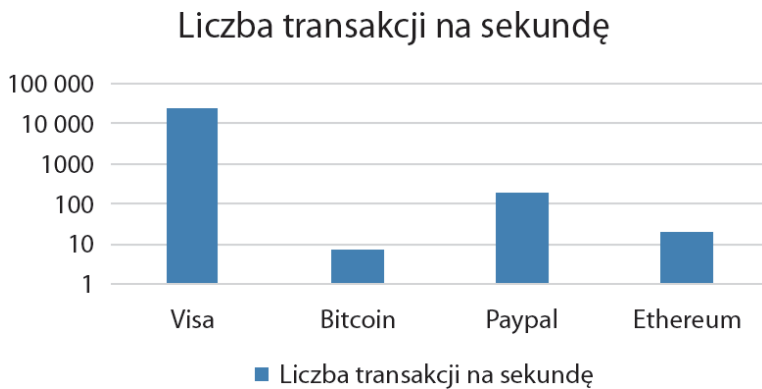
Rysunek 6.6. Portfel mobilny Jaxx



Rysunek 6.7. Logo informujące o akceptowaniu płatności w bitcoinach



Rysunek 6.8. Terminal kasowy firmy 34 Bytes



Rysunek 6.9. Szybkość przetwarzania transakcji w sieci Bitcoina i w innych sieciach (skala logarytmiczna)

BTC/USD
641.6617BTC/EUR
581.9899BTC/RUB
40000.69ETH/BTC
0.01870728ETH/USD
12.08170000ETHEUR
10.82830000LTC/USD
3.87650000LTC/EUR
3.4900LTC/BTC
0.00602549GHS/BTC
0.00010000

BTC/USD

Last price:
\$ 641.6617Daily change:
\$ -2.4695Today's open:
\$ 644.131224h volume:
฿393.23521389

Chart



Rysunek 6.10. Przykładowa giełda bitcoinów cex.io

Sell Orders

Total BTC available: 656.41831367

Price per BTC	BTC Amount	Total: (USD)
642.4085	฿0.20450000	\$ 131.38
642.4915	฿0.20910000	\$ 134.35
643.4470	฿0.05000000	\$ 32.18
643.4900	฿0.11944972	\$ 76.87
643.5000	฿1.85748652	\$ 1195.30
643.6500	฿3.00000000	\$ 1930.95
643.6999	฿0.13844181	\$ 89.12
643.7000	฿45.80000000	\$ 29481.46
643.7487	฿1.22995538	\$ 791.79

Buy Orders

Total USD available: 380739.41

Price per BTC	BTC Amount	Total: (USD)
641.6210	฿0.01390000	\$ 8.92
641.6201	฿0.23162780	\$ 148.62
641.6200	฿0.12050000	\$ 77.32
641.6117	฿1.83477084	\$ 1177.22
641.5584	฿0.30000000	\$ 192.47
641.5217	฿0.18180000	\$ 116.63
641.0217	฿0.10000000	\$ 64.11
640.5300	฿0.67323160	\$ 431.23
640.5000	฿0.40815400	\$ 261.43

Rysunek 6.11. Przykładowy arkusz zleceń bitcoinów na giełdzie cex.io

Rozdział 7. Klienci i interfejsy API Bitcoina

Download Bitcoin Core

Latest version: 0.15.0.1 



Download Bitcoin Core

Or choose your operating system



Windows
64 bit - 32 bit



Linux (tgz)
64 bit - 32 bit



Windows (zip)
64 bit - 32 bit



ARM Linux
64 bit - 32 bit



Mac OS X
dmg - tar.gz



Ubuntu (PPA)

[Verify release signatures](#)

[Download torrent](#) 

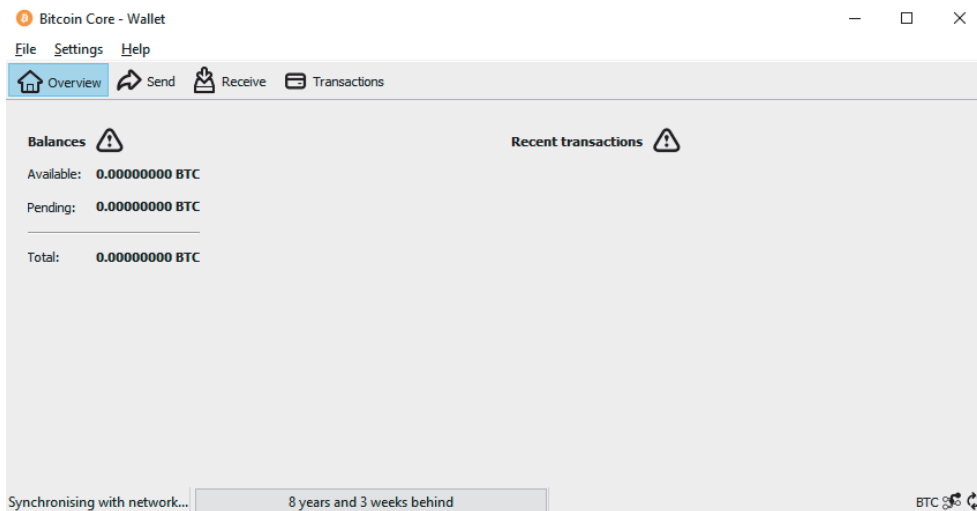
[Source code](#)

[Show version history](#)

Bitcoin Core Release Signing Keys

 [v0.8.6 - 0.9.2.1](#)  [v0.9.3 - 0.10.2](#)  [v0.11.0+](#)

Rysunek 7.1. Pobieranie klienta Bitcoin Core



Rysunek 7.2. Klient Bitcoin Core QT po instalacji, informujący, że łańcuch bloków nie jest zsynchronizowany

```
drequinox@drequinox-OP7010: ~  
drequinox@drequinox-OP7010:~$ sudo apt-add-repository ppa:bitcoin/bitcoin  
[sudo] password for drequinox:  
Stable Channel of bitcoin-qt and bitcoind for Ubuntu, and their dependencies  
More info: https://launchpad.net/~bitcoin/+archive/ubuntu/bitcoin  
Press [ENTER] to continue or ctrl-c to cancel adding it  
  
gpg: keyring `/tmp/tmpzsl4ltrx/secring.gpg' created  
gpg: keyring `/tmp/tmpzsl4ltrx/pubring.gpg' created  
gpg: requesting key 8842CE5E from hkp server keyserver.ubuntu.com  
gpg: /tmp/tmpzsl4ltrx/trustdb.gpg: trustdb created  
gpg: key 8842CE5E: public key "Launchpad PPA for Bitcoin" imported  
gpg: no ultimately trusted keys found  
gpg: Total number processed: 1  
gpg: imported: 1 (RSA: 1)  
OK  
drequinox@drequinox-OP7010:~$
```

Rysunek 7.3. Instalowanie Bitcoina

```
drequinox@drequinox-OP7010:~/bitcoin/regtest$ tail -f debug.log  
2016-10-16 15:43:55 AddToWallet d461efb162dd6958139a2ab5e4f9993f7bd51b1a4e3a80e5b77e472cd90dd6a new  
2016-10-16 15:43:55 CreateNewBlock(): total size 1000 txs: 0 fees: 0 sigops 400  
2016-10-16 15:43:55 UpdateTip: new best=97cf40299a37243dcedf63d26925cb590b8c5f27405289ef9204e53fefeb187 height=299 version=0x30000003 log2_work=9.22881  
87 tx=300 date='2016-10-16 15:44:27' progress=1.000000 cache=0.1MiB(299tx)  
2016-10-16 15:43:55 AddToWallet b88883e122c4f3aee6b53e402ed8faec916c570df2b154feb751c676235d70bf new  
2016-10-16 15:43:55 CreateNewBlock(): total size 1000 txs: 0 fees: 0 sigops 400  
2016-10-16 15:43:55 UpdateTip: new best=5c22d0b090b6f3fd978fbb14809d1d34ecccfe697a199d502beb1d88da43ad2 height=300 version=0x30000003 log2_work=9.23361  
97 tx=301 date='2016-10-16 15:44:28' progress=1.000000 cache=0.1MiB(300tx)  
2016-10-16 15:43:55 AddToWallet e315cb6863aed2d4477f6e6e5c0b7ace273140549d249b90b8793de0de0b8e1 new  
2016-10-16 15:43:55 CreateNewBlock(): total size 1000 txs: 0 fees: 0 sigops 400  
2016-10-16 15:43:55 UpdateTip: new best=7f9eeb78c0db34f374d426c95aab82c85810715574c0a87ec93218ab77ae9f5ae height=301 version=0x30000003 log2_work=9.23840  
47 tx=302 date='2016-10-16 15:44:28' progress=1.000000 cache=0.1MiB(301tx)  
2016-10-16 15:43:55 AddToWallet 428058e9e79f6962f8e126999efa4062dad2e63b253630d2e2ec086e7f5ac029 new
```

Rysunek 7.4. Komunikaty z dziennika debugowania Bitcoina

```
drequinox@drequinox-OP7010:~$ bitcoin-cli getinfo  
{  
  "version": 130000,  
  "protocolversion": 70014,  
  "walletversion": 130000,  
  "balance": 0.00000000,  
  "blocks": 433948,  
  "timeoffset": 0,  
  "connections": 8,  
  "proxy": "",  
  "difficulty": 258522748404.5154,  
  "testnet": false,  
  "keypoololdest": 1475534258,  
  "keypoolsize": 100,  
  "paytxfee": 0.00000000,  
  "relayfee": 0.00001000,  
  "errors": ""  
}  
drequinox@drequinox-OP7010:~$
```

Rysunek 7.5. Przykładowe wywołanie instrukcji getinfo za pomocą interfejsu bitcoin-cli. Ten sam format można wykorzystać do wywoływania innych poleceń

```

drequinox@drequinox-OP7010:~$ bitcoin-cli -testnet help | more
== Blockchain ==
getbestblockhash
getblock "hash" ( verbose )
getblockchaininfo
getblockcount
getblockhash index
getblockheader "hash" ( verbose )
getchaintips
getdifficulty
getmempoolancestors txid (verbose)
getmempooldescendants txid (verbose)
getmempoolentry txid
getmempoolinfo
getrawmempool ( verbose )
gettxout "txid" n ( includemempool )
gettxoutproof ["txid",...] ( blockhash )
gettxoutsetinfo
verifychain ( checklevel numblocks )
verifytxoutproof "proof"

== Control ==
getinfo
help ( "command" )
stop

```

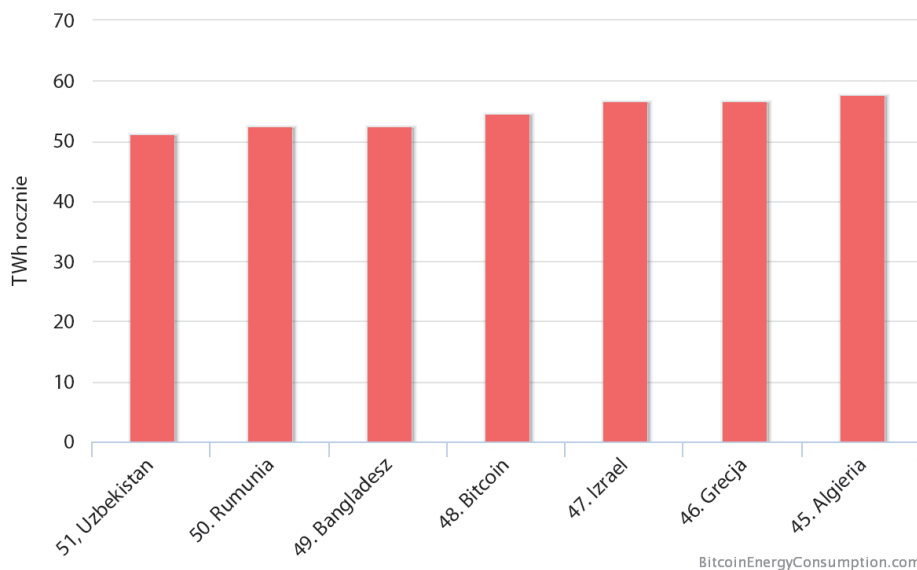
Rysunek 7.6. Używanie interfejsu bitcoin-cli do sieci testnet. Pokazano tu tylko kilka pierwszych wierszy danych wyjściowych. Rzeczywista lista zawiera wiele poleceń

Rozdział 8. Inne kryptowaluty



Rysunek 8.1. Ten wykres pokazuje, że w czasie, gdy powstaje ta książka, łączna kapitalizacja rynku alternatywnych kryptowalut przekracza 200 miliardów dolarów

Wykres zużycia energii według państw






Rysunek 8.2. Zużycie energii według państw



Rysunek 8.6. Poziom trudności w Namecoinie od grudnia 2016 r.
(za: <https://bitinfocharts.com/comparison/difficulty-nmc.html>)

Instant Rate 1 BTC = 3114.84374999 NMC

Deposit Min 0.00000300 BTC	Deposit Max 0.14532464 BTC	Liquidity 00000
-------------------------------	-------------------------------	--------------------

NFgrujLsjwRGWtRFj25RNfUqUucjs9Fsgb

14Koadj8xLpAeKDFke8qVWX5ETeU81amxH

☒ I agree to Terms

Miner Fee: NMC

Start Transaction



Rysunek 8.7. Wymiana bitcoinów na namecoiny

Order ID: 164b3f96-b73c-4fb9-a7b4-82e194d21263



Bookmark

Your Namecoin was sent.

See it on the blockchain

Deposit Received

Exchange Complete




Order Details

 Deposit

Send up to 0.14532464

Email receipt
Submit

1KTB9Uuq6KeTqQrgUGrxXqnYdYDmz2aRcU

 Receive

NFgrujLsjwRGWtRFj25RNfUqUucjs9Fsgb

Final Rate
1 BTC = 3114.84374999 NMC

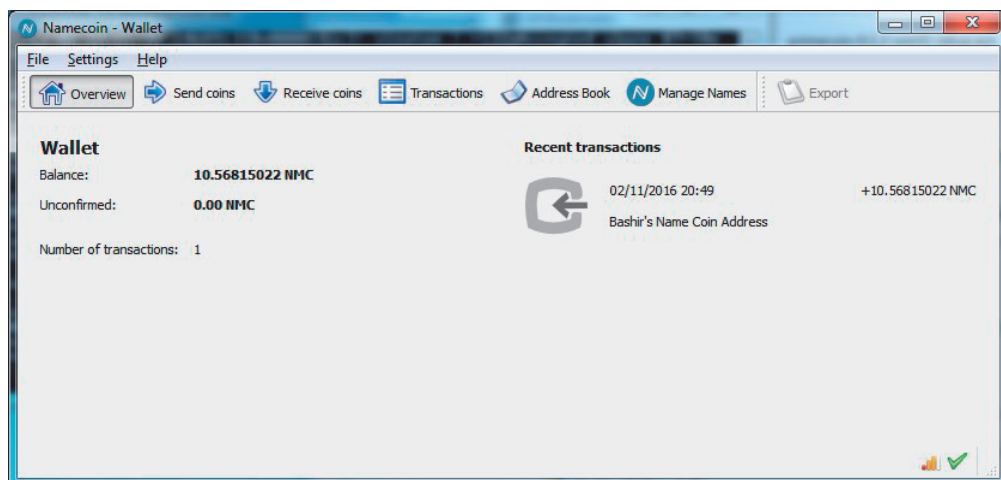
Share



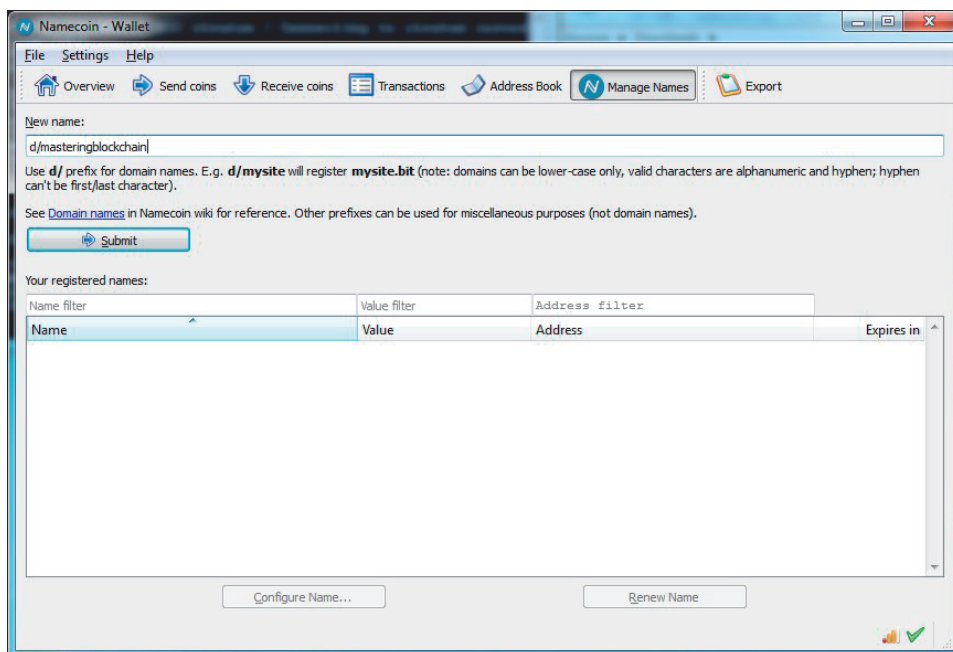

Type
Quick

Liquidity
00000

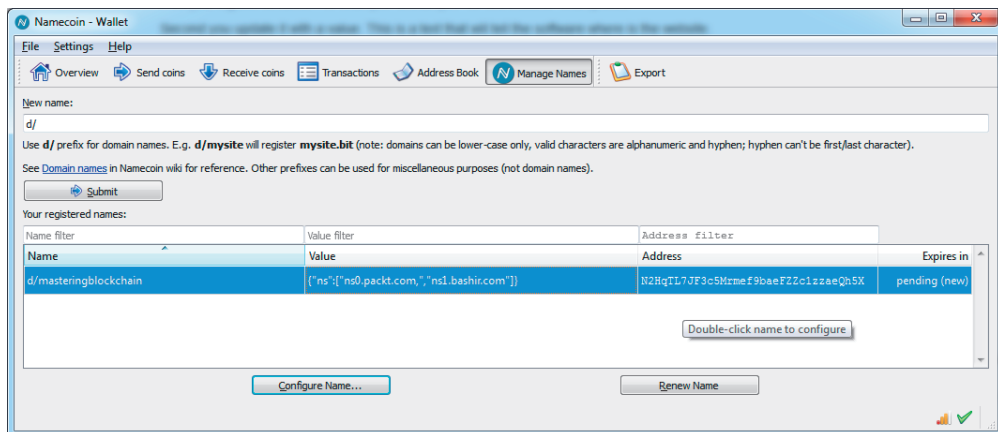
Rysunek 8.8. Powiadomienie o dostarczeniu namecoinów



Rysunek 8.9. Portfel Namecoina



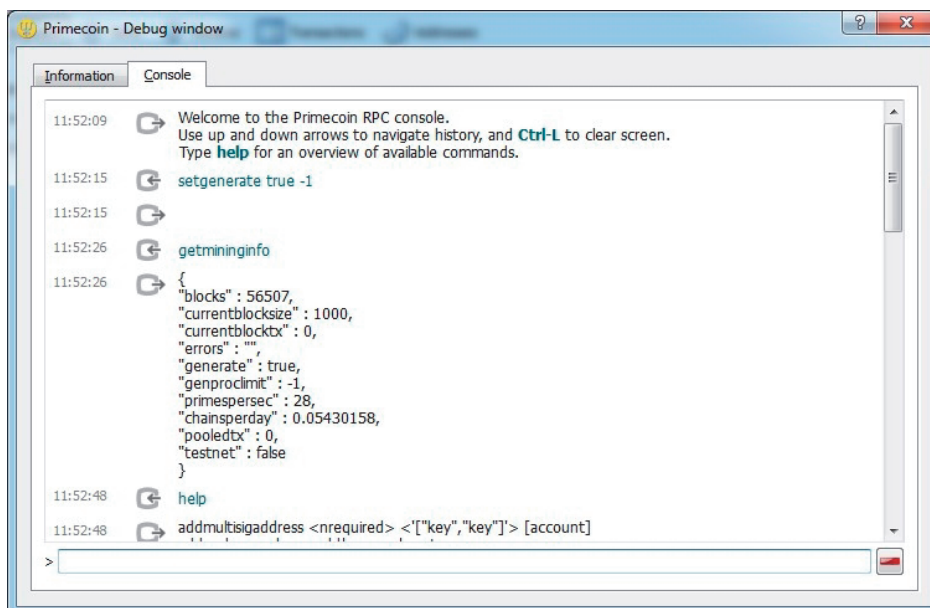
Rysunek 8.10. Portfel Namecoina — konfigurowanie nazwy domeny



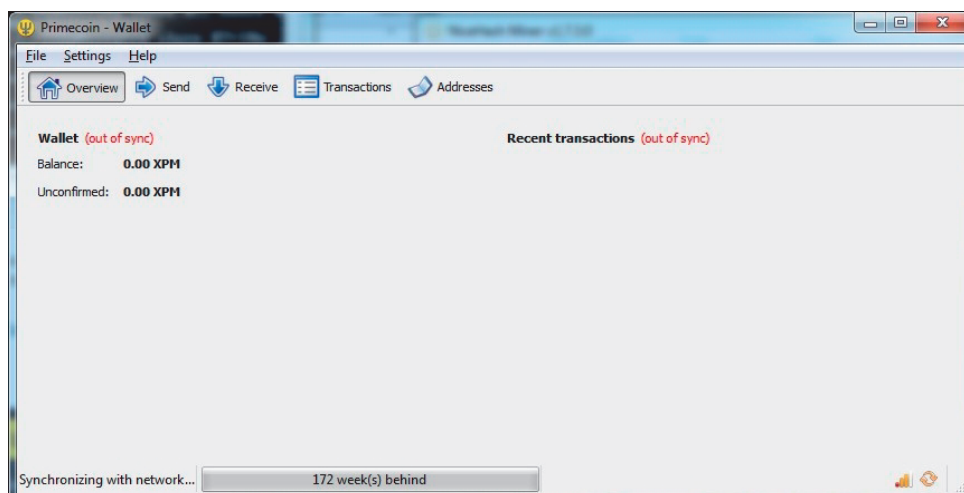
Rysunek 8.11. Portfel Namecoina — wyświetlanie zarejestrowanej nazwy



Rysunek 8.14. Wykres ze statystykami na temat Primecoina; źródło danych: <https://coinmarketcap.com/currencies/primecoin/>



Rysunek 8.15. Wydobywanie primecoinów



Rysunek 8.16. Oprogramowanie portfela Primecoina synchronizujące się z siecią



Rysunek 8.17. Wartość rynkowa i cena zcashów

```
drequinox@drequinox-OP7010:~$ git clone https://github.com/zcash/zcash.git
Cloning into 'zcash'...
remote: Counting objects: 56593, done.
remote: Total 56593 (delta 0), reused 0 (delta 0), pack-reused 56593
Receiving objects: 100% (56593/56593), 42.78 MiB | 2.11 MiB/s, done.
Resolving deltas: 100% (43020/43020), done.
Checking connectivity... done.
drequinox@drequinox-OP7010:~$ cd zcash/
drequinox@drequinox-OP7010:~/zcash$ git checkout v1.0.0
Note: checking out 'v1.0.0'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by performing another checkout.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -b with the checkout command again. Example:

  git checkout -b <new-branch-name>

HEAD is now at 1feaeefa... Update network magics for 1.0.0
```

Rysunek 8.18. Klonowanie repozytorium Zcasha z serwisu Git

```

drequinox@drequinox-OP7010:~/zcash$ ./zcutil/fetch-params.sh
Zcash - fetch-params.sh

This script will fetch the Zcash zkSNARK parameters and verify their
integrity with sha256sum.

The parameters are currently just under 911MB in size, so plan accordingly
for your bandwidth constraints. If the files are already present and
have the correct sha256sum, no networking is used.

Creating params directory. For details about this directory, see:
/home/drequinox/.zcash-params/README

Retrieving: https://z.cash/downloads/sprout-proving.key
--2016-10-28 21:46:21-- https://z.cash/downloads/sprout-proving.key
Resolving z.cash (z.cash)... 104.236.171.172
Connecting to z.cash (z.cash)|104.236.171.172|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://s3.amazonaws.com/zcashfinalmpc/sprout-proving.key [following]
--2016-10-28 21:46:22-- https://s3.amazonaws.com/zcashfinalmpc/sprout-proving.key
Resolving s3.amazonaws.com (s3.amazonaws.com)... 54.231.40.114
Connecting to s3.amazonaws.com (s3.amazonaws.com)|54.231.40.114|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 910173851 (868M) [application/octet-stream]
Saving to: '/home/drequinox/.zcash-params/sprout-proving.key.dl'

  OK ..... 3% 2.71M 5m8s
32768K ..... 7% 3.58M 4m20s
65536K ..... 11% 2.53M 4m28s
98304K ..... 14% 1.75M 4m59s
131072K .....

```

Rysunek 8.19. Pobieranie parametrów dowodów ZK-SNARK w trakcie konfigurowania Zcasha

```

drequinox@drequinox-OP7010:~/zcash/src$ ./zcash-cli getinfo
{
  "version" : 1000050,
  "protocolversion" : 170002,
  "walletversion" : 60000,
  "balance" : 0.00000000,
  "blocks" : 601,
  "timeoffset" : 0,
  "connections" : 0,
  "proxy" : "",
  "difficulty" : 13748.56014152,
  "testnet" : false,
  "keypoololdest" : 1477688856,
  "keypoolsize" : 101,
  "paytxfee" : 0.00000000,
  "relayfee" : 0.00005000,
  "errors" : "WARNING: abnormally high number of blocks generated, 190 blocks received in the last 4 hours (96 expected)"
}
drequinox@drequinox-OP7010:~/zcash/src$ █

```

Rysunek 8.20. Zrzut ilustrujący dane wyjściowe instrukcji getinfo

```
equihash@equinox-0P761G1:~/nheqminer/nheqminer/build$ ./nheqminer -l eu -u 1PL6gsm49xCFWxrXqgCceSdcrl119GoWN.worker1 -t 6 --od 0
```

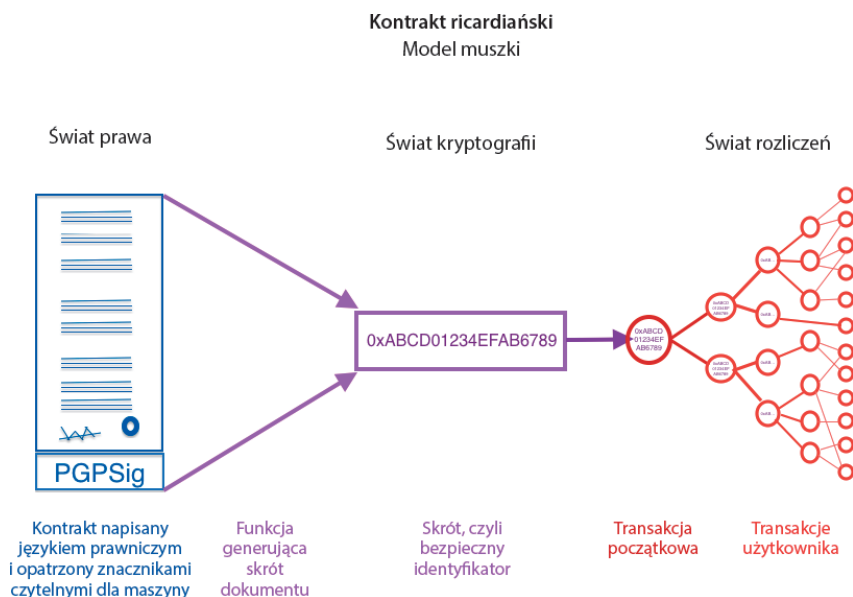
Thanks to Ccash developers for providing most of the code
Special thanks to tromp for providing optimized CPU equihash solver

Setting log level to 2

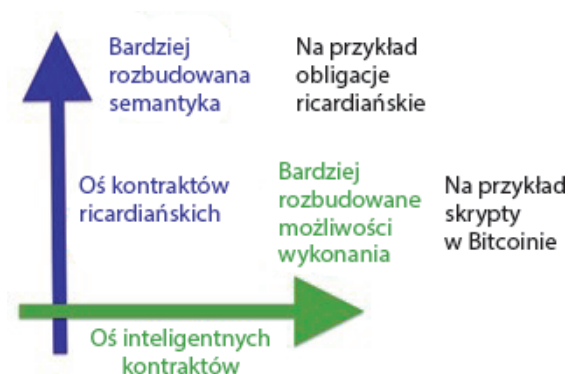
```
[09:28:53][ex00007f51009cd700] stratum | Connecting to stratum server equihash.eu.nicehash.com:3357
[09:28:53][ex00007f51009cd700] stratum | Connected
[09:28:53][ex00007f51009cd700] stratum | Starting miner
[09:28:53][ex00007f50fa7cf700] miner#1 | Starting thread #1
[09:28:53][ex00007f50fb7cf700] miner#0 | Starting thread #0
[09:28:53][ex00007f50f8fca700] miner#5 | Starting thread #5
[09:28:53][ex00007f50fa7cd700] miner#2 | Starting thread #2
[09:28:53][ex00007f50f97cb700] miner#4 | Starting thread #4
[09:28:53][ex00007f50f9fcc700] miner#3 | Starting thread #3
[09:28:54][ex00007f51009cd700] stratum | Subscribed to stratum server
[09:28:54][ex00007f51009cd700] miner | Extranonce is 5000e5b00000000000000000000000005000e5b9ab
[09:28:54][ex00007f51009cd700] stratum | Authorized worker 1PL6gsm49xCFWxrXqgCceSdcrl119GoWN.worker1
[09:28:54][ex00007f51009cd700] stratum | Target set to 01c1e1e000000000000000000000000000000000000000000000000000000000
[09:28:54][ex00007f51009cd700] stratum | Received new job #000000329b82d287
[09:28:54][ex00007f50fa7cf700] stratum | Submitting share #4, nonce 0200000000000000000000000000000000
[09:28:55][ex00007f51009cd700] stratum | Accepted share #4
[09:28:55][ex00007f51009cd700] stratum | Ignoring non-clean job #000000329b82d2cc
[09:28:57][ex00007f50fafce700] stratum | Submitting share #5, nonce 0100000000000000000000000000000001
[09:28:57][ex00007f51009cd700] stratum | Accepted share #5
[09:28:59][ex00007f50f97cb700] stratum | Submitting share #6, nonce 0400000000000000000000000000000005
```

[illegible]

Rozdział 9. Inteligentne kontrakty

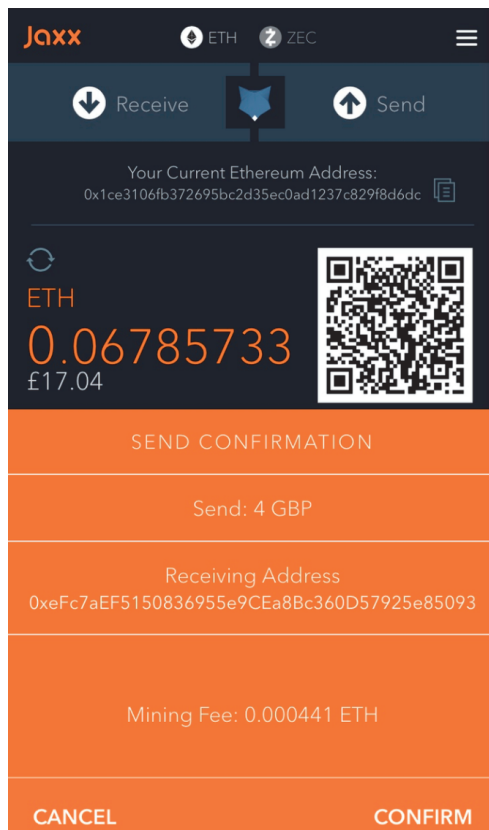


Rysunek 9.1. Kontrakty ricardiańskie, model muszki





Rysunek 9.2. Rysunek pokazujący, że kwestie semantyki i wykonywania są niezależne od siebie (za lanem Griggem). Ilustrację zmodyfikowano, aby na osiach pokazać inne rodzaje kontraktów

Rozdział 10. ABC łańcucha bloków Ethereum



Rysunek 10.3. Przesyłanie przelewu środków od Bashira w portfelu Jaxx

Transaction

RECEIVED£4.02

Value when received: £4.02

DescriptionWhat's this for?

ToOxefc7aef5150836955e9cea8bc360d57925e85093

FromOx1ce3106fb372695bc2d35ec0ad1237c829f8d6dc

DateNovember 18, 2017 @ 1:25pm

StatusConfirmed

VIEW ON ETHERSCAN.IO

Rysunek 10.4. Transakcja w portfelu łańcucha bloków należącym do Irshad

TxHash:
0xc63dce6747e1640abd63ee63027c3352aed8cdb92b6a02ae25225666e171009e

TxReceipt Status:
Success

Block Height:
4576084 (20583 block confirmations)

TimeStamp:
3 days 7 hrs ago (Nov-18-2017 01:25:54 PM +UTC)

From:
0x1ce3106fb372695bc2d35ec0ad1237c829f8d6dc

To:
0xefc7aef5150836955e9cea8bc360d57925e85093

Value:
0.015927244142974896 Ether (\$5.82)

Gas Limit:
21000

Gas Used By Txn:
21000

Gas Price:
0.000000021 Ether (21 Gwei)

Actual Tx Cost/Fee:
0.000441 Ether (\$0.16)

Cumulative Gas Used:
156148

Nonce:
1

Rysunek 10.5. Eksplorator bloków z łańcucha bloków Ethereum

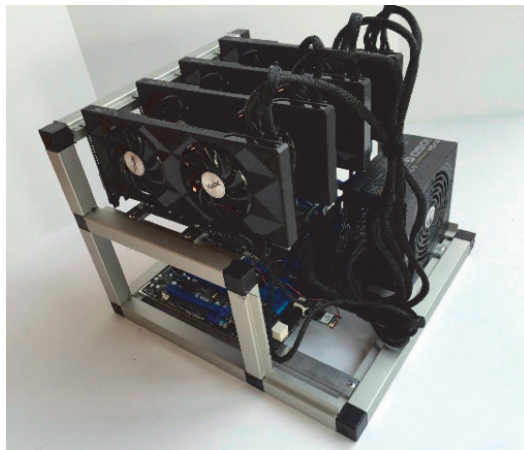
Rozdział 11. Jeszcze o Ethereum

```
drequinox@drequinox-OP7010:~$ ethminer -G
[OPENCL]:No OpenCL platforms found
No GPU device with sufficient memory was found. Can't GPU mine. Remove the -G argument
drequinox@drequinox-OP7010:~$
```

Rysunek 11.3. Błąd zwracany w sytuacji, gdy nie można znaleźć odpowiednich kart graficznych

```
drequinox@drequinox-OP7010:~$ ethminer -M -C
  ◊ 22:43:30.560 ethminer #00004000...
Benchmarking on platform: 8-thread CPU
Preparing DAG...
  ◻ 22:43:30.561 miner0 Loading full DAG of seedhash: #00000000...
Warming up...
Trial 1... 0
Trial 2... DAG 22:43:38.310 miner0 Generating DAG file. Progress: 0 %
0
Trial 3... 0
Trial 4... DAG 22:43:45.336 miner0 Generating DAG file. Progress: 1 %
0
```

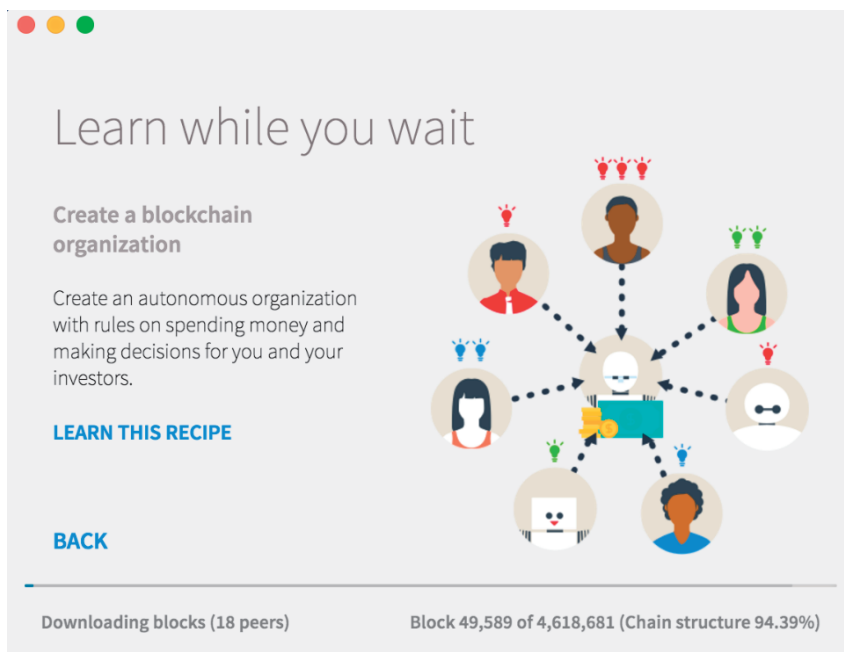
Rysunek 11.4. Testy porównawcze z użyciem zwykłych procesorów



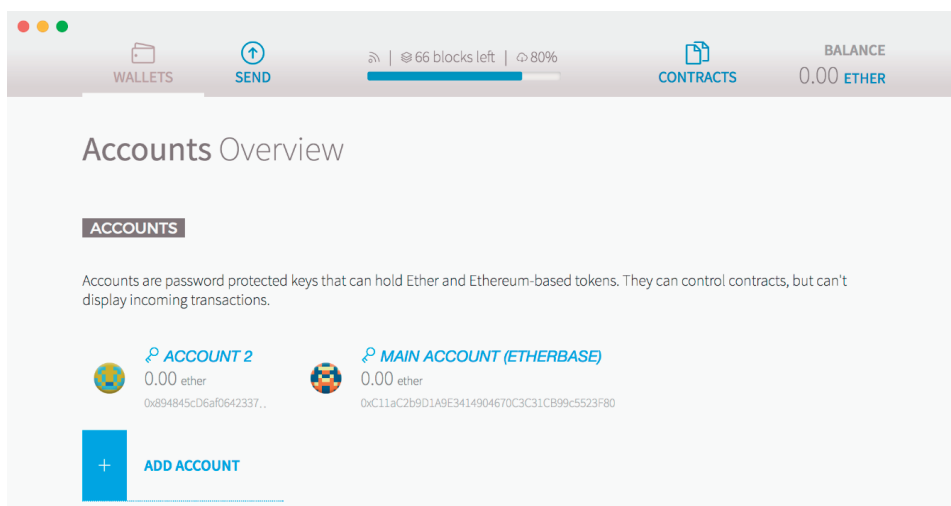
Rysunek 11.5. Koparka Ethereum wystawiona na sprzedaż w serwisie eBay

```
drequinox@drequinox-OP7010:~$ ethminer -C -F http://ethereumpool.co/?miner=0.1@0x024a20cc5feba7f3dc3776075b3e60c20eb1459c@DrEquinox
miner 23:50:52.046 ethminer Getting work package...
```

Rysunek 11.6. Zrzut z programu Ethminer



Rysunek 11.7. Przeglądarka Mist w trakcie uruchamiania i synchronizowania się z siecią mainnet



Rysunek 11.8. Przeglądarka Mist

```

drequinox@drequinox-OF7010:~$ geth attach
Welcome to the Geth JavaScript console!

instance: Parity/v1.4.4-beta-a68d52c-20161118/x86_64-linux-gnu/rustc1.13.0
coinbase: 0x0000000000000000000000000000000000000000000000000000000000000000
at block: 2718377 (Tue, 29 Nov 2016 22:52:52 GMT)
modules: eth:1.0 net:1.0 parity:1.0 parity_accounts:1.0 personal:1.0 rpc:1.0 traces:1.0 web3:1.0
>

```

Rysunek 11.10. Klient Geth

Shifty
Ethereum Wallet Accounts Edit View Develop Window Help

Send **0.02568731** Bitcoin to
15jfoneg8N5HKk9F2qdEha3oPmyBJprTzQ

It will be converted into 2 Ether, and sent to
0xdf482f1e3fbb7716e2868786b3afede1c1fb37f

Deposit Address 15jfoneg8N5HKk9F2qdEha3oPmyBJprTzQ 9:28 until expiration

Awaiting Deposit Awaiting Exchange Complete

Destination
0xdf482f1e3fbb7716e2868786b3afede1c1fb37f

Deposit Limit 2.0463 BTC	Exchange Rate 1 BTC = 78.24876631 ETH	Deposit Minimum 0.0002535 BTC	Deposit Maximum 6.82104743 BTC
-----------------------------	--	----------------------------------	-----------------------------------

Powered by ShapeShift.io

Rysunek 11.11. Wymiana bitcoinów na ethery

```
drequisno@drequinox-OP7010: /opt
drequisno@drequinox-OP7010:/opt$ bash <(curl https://get.parity.io -Lk)
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 154 100 154 0 0 429 0 --:--:-- --:--:-- --:--:-- 430
100 154 100 154 0 0 211 0 --:--:-- --:--:-- --:--:-- 9625
100 12876 100 12876 0 0 11824 0 0:00:01 0:00:01 --:--:-- 11824
==> Checking OS dependencies
✓ Ubuntu, but version not supported
✓ curl
✓ apt-get
✓ sudo
Found all dependencies (3/3)
==> OK, let's install Parity now!
==> Last chance! Sure you want to install this software? [Y/n] Y

==> Installing Parity build dependencies
==> Verifying installation
✓ apt-get
==> Installing parity
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 5449k 100 5449k 0 0 648k 0 0:00:08 0:00:08 --:--:-- 812k
(Reading database ... 227048 files and directories currently installed.)
Preparing to unpack /tmp/parity.deb ...
Unpacking parity (1.4.4) over (1.4.4) ...
Setting up parity (1.4.4) ...
==> Parity has been installed

==> Netstats Would you like to download, install and configure a Netstats client?
WARNING: This will need a secret and reconfigure any existing node/NPM installation you have. [Y/n] Y
Installing netstats
Please enter the netstats secret: a38e1e50b1b82fa
Please enter your instance name: Dr.Equisno!
Please enter your contact details (optional):

## Installing the NodeSource Node.js v0.12 repo...
```

Rysunek 11.12. Instalowanie klienta Parity

```
drequisno@drequinox-OP7010: /opt
[PM2] Spawning PM2 daemon with pm2_home=/home/drequisno/.pm2
[PM2] PM2 Successfully daemonized
[PM2][WARN] Applications node-app not running, starting...
[PM2] App [node-app] launched (1 instances)

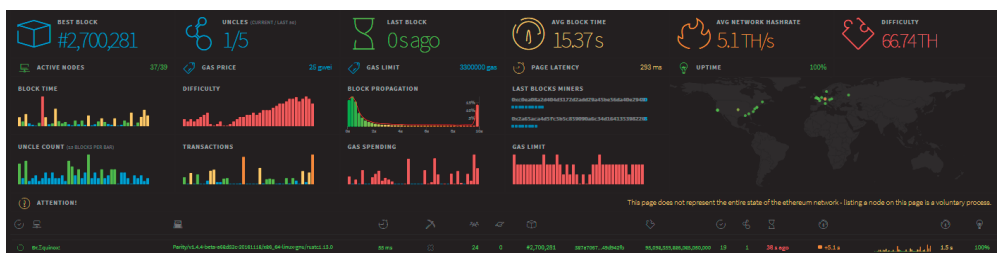
App name id mode pid status restart uptime cpu mem watching
node-app 0 fork 6018 online 0 0s 13% 18.2 MB disabled

Use 'pm2 show <id/name>' to get more details about an app

==> All done
==> Next steps
==> Run 'parity -j' to start the Parity Ethereum client.

drequisno@drequinox-OP7010:/opt$
```

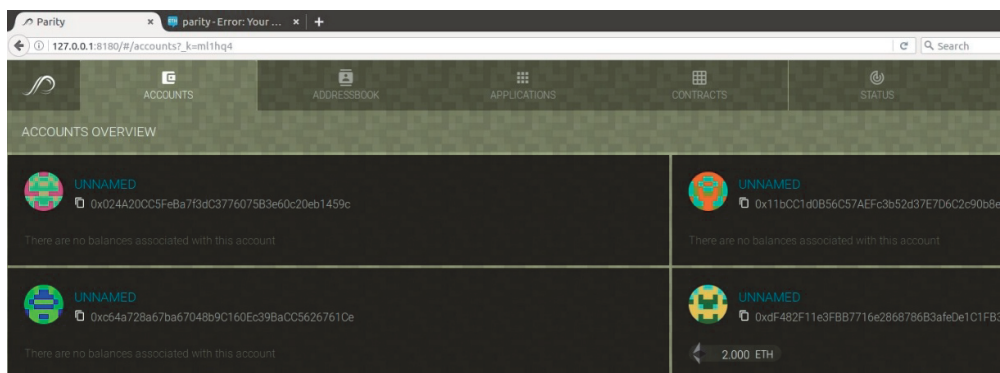
Rysunek 11.13. Uruchamianie klienta Parity



Rysunek 11.14. Statystyki na temat sieci Ethereum w witrynie ethstats.net

○ Bootnode-SG	Geth/v1.8.1-stable/linux-amd64/go1.7	123 ms	✖	510
○ Bootnode-IE	Geth/v1.8.1-stable/linux-amd64/go1.7	43 ms	✖	499
○ sphinxRust	Parity//v1.8.11-stable-21522f86-20180227/x86_64-linux-gnu/rustc1.24.1	46 ms	✖	328
○ Bootnode-NORCAL	Geth/v1.8.1-stable/linux-amd64/go1.10	36 ms	✖	256
○ Zetabit2	Parity//v1.8.10-stable-78acefd-20180219/x86_64-linux-gnu/rustc1.24.0	50 ms	✖	239
○ FunFair-01	Geth/v1.8.2-stable-b8b9f7f4/linux-amd64/go1.9.4	60 ms	✖	239
○ Bootnode-AU	Geth/v1.8.1-stable/linux-amd64/go1.7	100 ms	✖	232
○ Bootnode-BR	Geth/v1.8.2-stable/linux-amd64/go1.10	59 ms	✖	229
○ ethpool.maxhash.org (US)	Parity//v1.8.9-stable-1952d05-20180201/x86_64-linux-gnu/rustc1.23.0	8 ms	0 KH/s	199
○ CIMS FARM CRYPTO. INVEST.	Geth/v1.8.2-stable-b8b9f7f4/linux-amd64/go1.9.4	4 ms	✖	161

Rysunek 11.15. Klienci wymienione na stronie <https://ethstats.net/>



Rysunek 11.16. Interfejs użytkownika klienta Parity

Ether Historical Market Capitalization Chart (USD)

Source: Etherscan.io

Click and drag in the plot area to zoom in



Rysunek 11.18. Wartość rynkowa etherów w przeszłości (źródło: etherscan.io)

Rozdział 12. Środowisko programistyczne Ethereum

```
linrad@requinox-0P7010:~$ geth --testnet
I1204 16:03:32.759208 cmd/utils/flags.go:613] WARNING: No etherbase set and no accounts found as default
I1204 16:03:32.759415 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/linrad/.ethereum/testnet/geth/chaindata
I1204 16:03:32.807292 ethdb/database.go:176] closed db:/home/linrad/.ethereum/testnet/geth/chaindata
I1204 16:03:32.807589 node/node.go:175] Instance: Geth/v1.5.2-stable-c8695209/linux/go1.7.3
I1204 16:03:32.807603 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/linrad/.ethereum/testnet/geth/chaindata
I1204 16:03:32.814016 eth/backend.go:280] Successfully wrote custom genesis block: 0cd786a2425d16f152c658316c423e6ce1181e15c3295826d7c99
04cba9ce303
I1204 16:03:32.814076 eth/db_upgrade.go:346] upgrading db log bloom bins
I1204 16:03:32.814112 eth/db_upgrade.go:354] upgrade completed in 36.513µs
I1204 16:03:32.814128 eth/backend.go:193] Protocol Versions: [63 62], Network Id: 2
I1204 16:03:32.814363 core/blockchain.go:214] Last header: #0 [0cd786a2_] TD=131072
I1204 16:03:32.814375 core/blockchain.go:215] Last block: #0 [0cd786a2_] TD=131072
I1204 16:03:32.814382 core/blockchain.go:216] Fast block: #0 [0cd786a2_] TD=131072
I1204 16:03:32.814840 p2p/server.go:336] Starting Server
I1204 16:03:37.983847 p2p/discover/udp.go:217] Listening, enode://fa838ec3fee8a26d75755b5f7cbdd80efacc4a98b521acd5a23aea5465b794c84aff
e70ec3324d2095768a2122a25e87cf97bd369895ace9f4ef868eaf180[:]:30303
I1204 16:03:37.983968 p2p/server.go:604] listening on [::]:30303
I1204 16:03:37.984963 node/node.go:340] IPC endpoint opened: /home/linrad/.ethereum/testnet/geth.ipc
I1204 16:04:17.984169 eth/downloader/downloader.go:326] Block synchronisation started
```

Rysunek 12.1. Dane wyjściowe z polecenia nawiązania połączenia z siecią testową Ethereum w kliencie geth

Rysunek 12.2. Inicjowanie sieci prywatnej

Rysunek 12.3. Uruchamianie klienta geth dla sieci prywatnej

Rysunek 12.5. Generowanie acyklicznego grafu skierowanego

Rysunek 12.6. Dane wyjściowe w procesie wydobywania bloków

Rysunek 12.7. Dostępne obiekty

```

> personal.
personal._requestManager personal.getListAccounts personal.lockAccount personal.sign
personal.constructor personal.importRawKey personal.newAccount personal.unlockAccount
personal.ecRecover personal.listAccounts personal.sendTransaction
> net.
net._requestManager net.getListening net.getVersion net.peerCount
net.constructor net.getPeerCount net.listening net.version

```

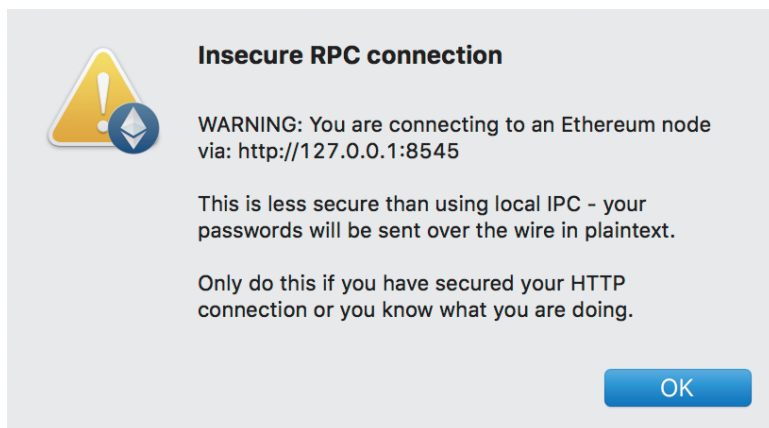
Rysunek 12.8. Dostępne metody

```

> net;
{
  listening: true,
  peerCount: 0,
  version: "786",
  getListening: function(callback),
  getPeerCount: function(callback),
  getVersion: function(callback)
}
>

```

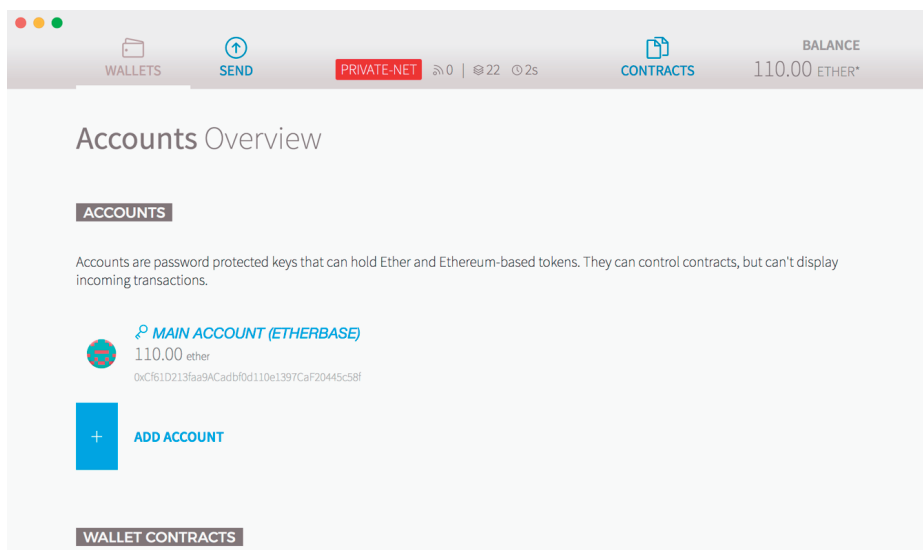
Rysunek 12.9. Lista metod



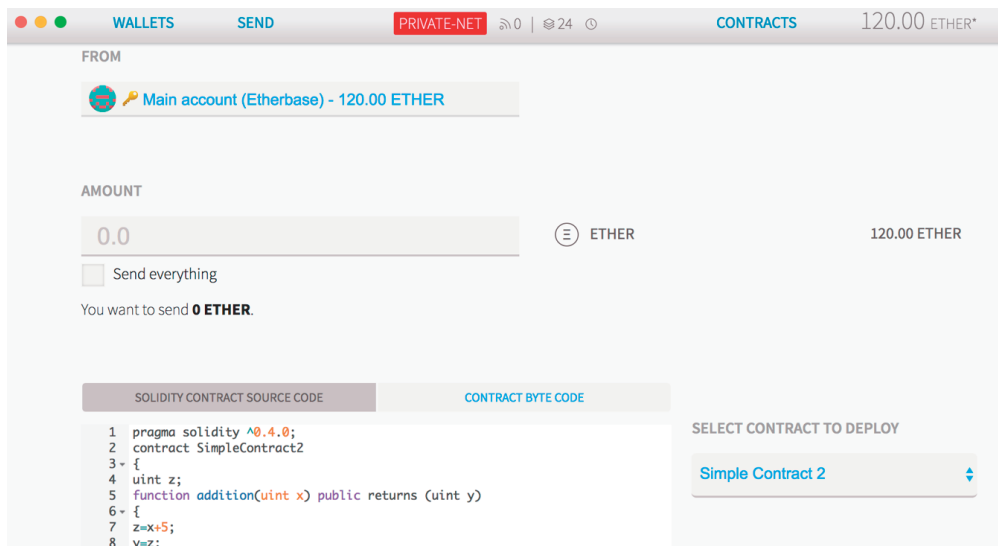
Rysunek 12.10. Niezabezpieczone połączenie RPC

```
imran@drequinox-OP7010: /opt/Ethereum Wallet
imran@drequinox-OP7010: /opt/Ethereum Wallet$ ./Ethereum\ Wallet --rpc /home/imran/.ethereum/privatenet/geth.ipc
[2016-12-06 07:58:08.706] [INFO] main - Running in production mode: true
[2016-12-06 07:58:08.706] [INFO] main - Starting in Wallet mode
[2016-12-06 07:58:08.868] [INFO] Db - Loading db: /home/imran/.config/Ethereum Wallet/mist.lokidb
[2016-12-06 07:58:08.947] [INFO] Windows - Creating commonly-used windows
[2016-12-06 07:58:08.948] [INFO] Windows - Create secondary window: loading, owner: notset
[2016-12-06 07:58:09.612] [INFO] updateChecker - Check for update...
[2016-12-06 07:58:11.373] [INFO] Windows - Create primary window: main, owner: notset
[2016-12-06 07:58:11.385] [INFO] Windows - Create primary window: splash, owner: notset
[2016-12-06 07:58:11.989] [INFO] ipcCommunicator - Backend language set to: en-GB
[2016-12-06 07:58:13.362] [INFO] (ui: splash) - Web3 already initialized, re-using provider.
[2016-12-06 07:58:13.362] [INFO] ClientBinaryManager - Initializing...
[2016-12-06 07:58:13.363] [INFO] ClientBinaryManager - Resolving path to Eth client binary ...
[2016-12-06 07:58:13.363] [INFO] ClientBinaryManager - Eth client binary path: /opt/Ethereum Wallet/nodes/eth/linux-x64/eth
[2016-12-06 07:58:13.663] [INFO] ClientBinaryManager - Initializing...
[2016-12-06 07:58:13.664] [INFO] ClientBinaryManager - Resolving platform...
[2016-12-06 07:58:13.664] [INFO] ClientBinaryManager - Calculating possible clients...
[2016-12-06 07:58:13.667] [INFO] ClientBinaryManager - 1 possible clients.
[2016-12-06 07:58:13.667] [INFO] ClientBinaryManager - Verifying status of all 1 possible clients...
[2016-12-06 07:58:13.669] [INFO] ClientBinaryManager - Verify Geth status ...
[2016-12-06 07:58:13.691] [INFO] ClientBinaryManager - Checking for Geth sanity check ...
[2016-12-06 07:58:13.693] [INFO] ClientBinaryManager - Checking sanity for Geth ...
[2016-12-06 07:58:13.764] [INFO] Sockets/node-ipc - Connect to {"path":"/home/imran/.ethereum/privatenet/geth.ipc"}
[2016-12-06 07:58:13.768] [INFO] Sockets/node-ipc - Connected!
[2016-12-06 07:58:13.769] [INFO] NodeSync - Ethereum node connected, re-start sync
[2016-12-06 07:58:13.770] [INFO] NodeSync - Starting sync loop
[2016-12-06 07:58:13.771] [INFO] Sockets/7 - Connect to {"path":"/home/imran/.ethereum/privatenet/geth.ipc"}
[2016-12-06 07:58:13.772] [INFO] main - Connected via IPC to node.
[2016-12-06 07:58:13.801] [INFO] Sockets/7 - Connected!
[2016-12-06 07:58:13.818] [INFO] (ui: splash) - network is privatenet
[2016-12-06 07:58:14.939] [INFO] updateChecker - App is up-to-date.
```

Rysunek 12.11. Uruchamianie portfela Ethereum łączącego się z prywatną siecią za pomocą komunikacji IPC



Rysunek 12.12. Przeglądarka Mist w sieci prywatnej



Rysunek 12.13. Dodawanie kontraktu w przeglądarce Mist


```
explorer — node • npm TERM_PROGRAM=Apple_Terminal SHELL=/bin/bash — 121x34
node-uuid@1.4.0
pauth-sign@0.8.2
qs@3.1.0
stringstream@0.0.5
tough-cookie@2.3.3
punycode@1.4.1
tunnel-agent@0.4.3
saucelabs@1.0.1
https-proxy-agent@1.0.0
agent-base@2.1.1
semver@5.0.0
extend@3.0.1
selenium-webdriver@2.47.0
tmp@0.0.24
ws@0.8.1
bufferutil@1.2.1
bindings@1.2.1
options@0.0.4
ultron@1.0.2
utf-8-validate@1.2.2
nan@2.4.0
xml2js@0.4.4
sax@0.6.1
xmlbuilder@9.0.4
source-map-support@0.2.10
source-map@0.1.0
shelljs@0.2.6

> EthereumExplorer@0.1.0 start /Users/drequinox/explorer
> http-server ./app -a localhost -p 8000 -c-1

Starting up http-server, serving ./app on port: 8000
Hit CTRL-C to stop the server
```

Rysunek 12.18. Serwer HTTP eksploratora Ethereum

localhost:8000/#/block/661

Ether Block Explorer

Block View information about an Ethereum Block

0x6162c67e07fec9347cbb98e85396d6bef3839995c623d5f5e0a5a5572977933b

21 Confirmations

615461 Gas Used

Summary	
Block Number	661
Received Time	1481094979
Difficulty	179724
Nonce	0x301cef8bdc816721

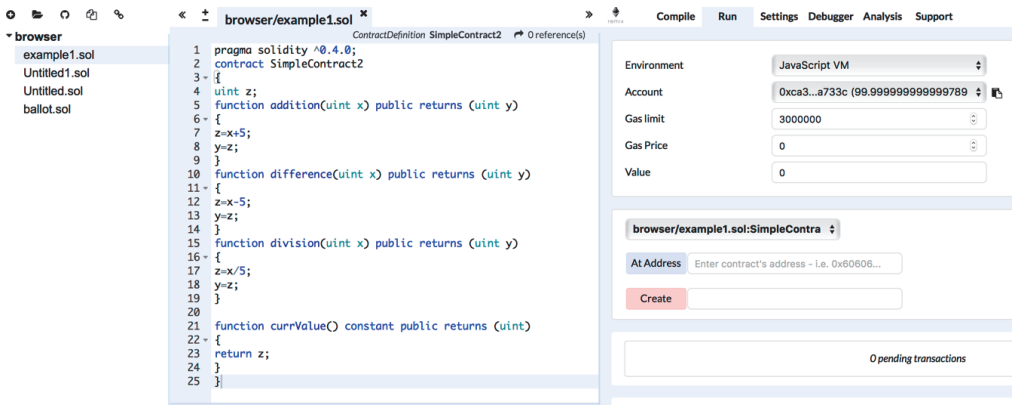
Rysunek 12.19. Eksplorator bloków

Allow Access to Geth and Refresh the Page

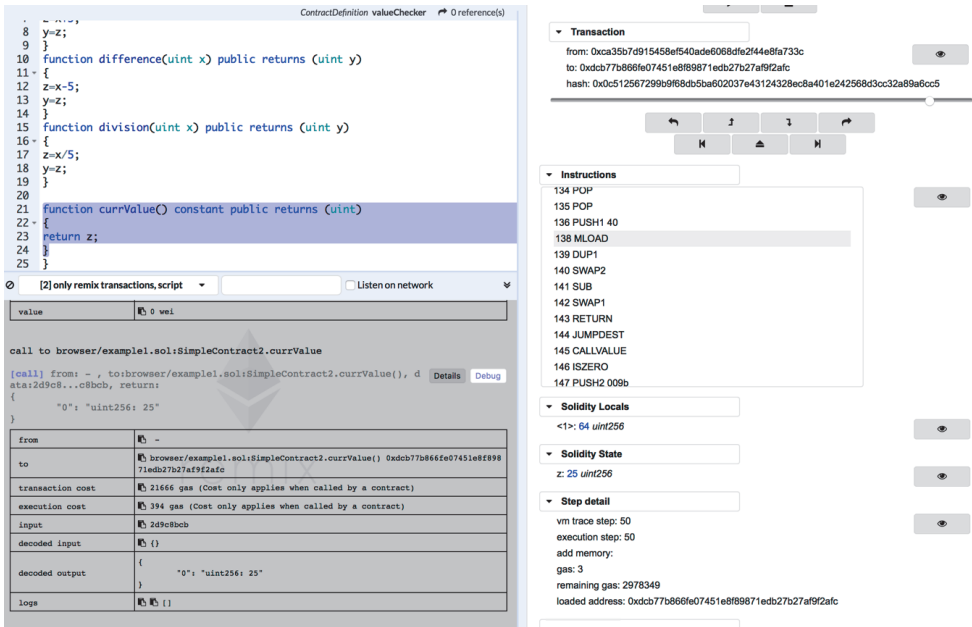
```
geth --rpc --rpccorsdomain "http://192.168.0.17:9900"
```

Rysunek 12.20. Komunikat o błędzie

Rozdział 13. Narzędzia i platformy programistyczne



Rysunek 13.5. Środowisko IDE Remix



Rysunek 13.6. Debugowanie w środowisku IDE Remix

▼ Instructions

134 POP
135 POP
136 PUSH1 40
138 MLOAD
139 DUP1
140 SWAP2
141 SUB
142 SWAP1
143 RETURN
144 JUMPDEST
145 CALLVALUE
146 ISZERO
147 PUSH2 009b

▼ Solidity Locals

<1>: 64 uint256

▼ Solidity State

z: 25 uint256

▼ Step detail

vm trace step: 50
execution step: 50
add memory:
gas: 3
remaining gas: 2978349
loaded address: 0xdcdb77b866fe07451e8f89871edb27b27af9f2afc

👁

👁

👁

👁

Rysunek 13.7. Debugger w środowisku Remix

ACCOUNTS BLOCKS TRANSACTIONS LOGS

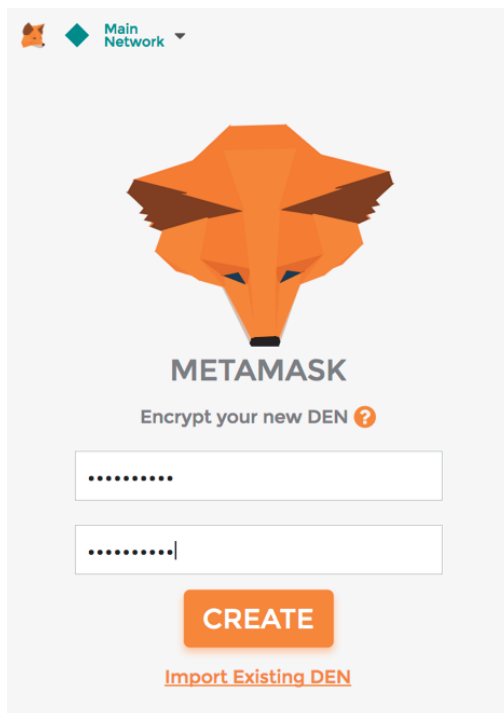
SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK0GAS PRICE20000000000GAS LIMIT6721975NETWORK ID5777RPC SERVERHTTP://127.0.0.1:7545MINING STATUSAUTOMINING

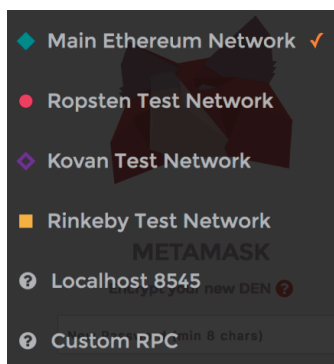
MNEMONICcandy maple cake sugar pudding cream honey rich smooth crumble sweet treatHD PATHm/44'/60'/0'/0/account_index

ADDRESS0x627306090abaB3A6e1400e9345bC60c78a8BEf57	BALANCE100.00 ETH	TX COUNT0	INDEX0	🔗
ADDRESS0xf17f52151EbEF6C7334FAD080c5704D77216b732	BALANCE100.00 ETH	TX COUNT0	INDEX1	🔗
ADDRESS0xC5fdf4076b8F3A5357c5E395ab970B5B54098Fef	BALANCE100.00 ETH	TX COUNT0	INDEX2	🔗
ADDRESS0x821aEa9a577a9b44299B9c15c88cf3087F3b5544	BALANCE100.00 ETH	TX COUNT0	INDEX3	🔗
ADDRESS0xd1d4e623D10F9FBA5Db95830F7d3839406C6AF2	BALANCE100.00 ETH	TX COUNT0	INDEX4	🔗

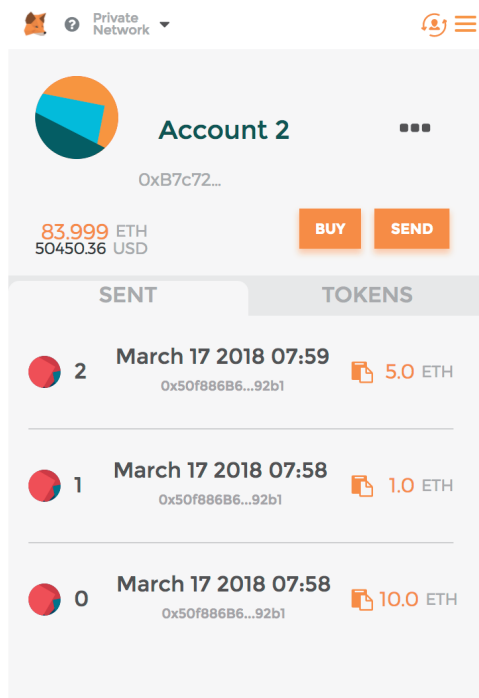
Rysunek 13.9. Ganache — osobisty łańcuch bloków Ethereum



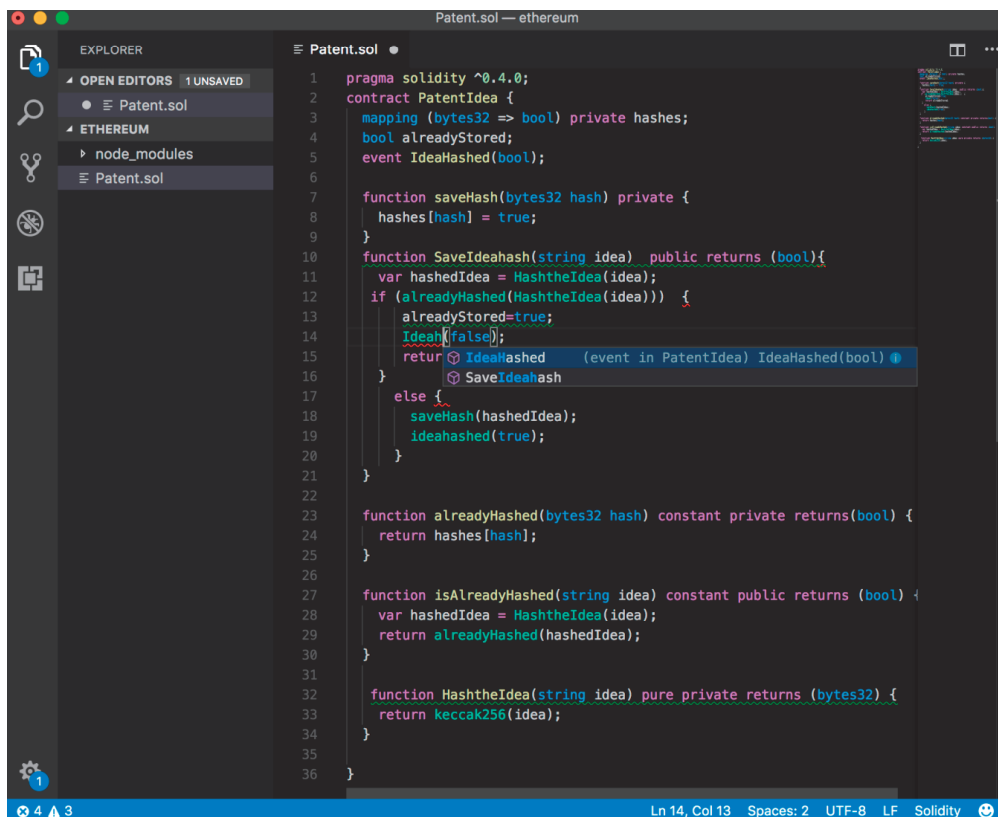
Rysunek 13.10. MetaMask



Rysunek 13.11. Sieci Ethereum widoczne w interfejsie użytkownika narzędzia MetaMask



Rysunek 13.12. Konta i podgląd transakcji w narzędziu MetaMask



Rysunek 13.14. Edytor Visual Studio Code

```

1  pragma solidity ^0.4.0; // Określa wersję kompilatora.
2  /*
3   To prosty kontrakt do sprawdzania wartości. Sprawdza
4   podaną wartość i zwraca wartość logiczną na podstawie
5   przetworzenia wyrażenia warunkowego.
6   */
7  import "dev.oracize.it/api.sol";
8  contract valuechecker {
9      uint price=10;
10     //Jest to deklaracja zmiennej price inicjowanej wartością 10.
11     event valueEvent(bool returnValue)
12     function Matcher (uint8 x) returns (bool)
13     {
14         if ( x >= price )
15         {
16             valueEvent(true);
17             return true;
18         }
19     }
20 }

```

Rysunek 13.16. Przykładowy program w języku Solidity widoczny w środowisku IDE Remix

Rozdział 14. Wprowadzenie do Web3

```
> web3.version
{
  api: "0.15.3",
  ethereum: "0x3f",
  network: "786",
  node: "Geth/v1.5.2-stable-c8695209/linux/go1.7.3",
  whisper: undefined,
  getEthereum: function(callback),
  getNetwork: function(callback),
  getNode: function(callback),
  getWhisper: function(callback)
}
```

Rysunek 14.1. Używanie biblioteki Web3 za pomocą klienta geth



The image shows the Remix IDE interface. On the left, a code editor displays Solidity code for a contract named `valueChecker`. The code includes a pragma statement for Solidity 0.4.0, a contract definition, a `uint` variable `price` set to 10, an event `valueEvent`, and a `Matcher` function that returns a boolean based on a comparison of `x` and `price`. On the right, the compilation panel is visible, showing the `valueChecker` contract selected in a dropdown menu. Above the dropdown are buttons for 'Start to compile' and 'Auto compile' (which is checked). Below the dropdown are buttons for 'Details' and 'Publish on Swarm'. At the bottom of the panel, a green box indicates the current contract being compiled is `valueChecker`.

```
1 pragma solidity ^0.4.0;
2 contract valueChecker
3 {
4     uint price=10;
5     event valueEvent(bool returnValue);
6     function Matcher (uint8 x) public returns (bool)
7 {
8     {
9         if (x>=price){valueEvent(true);
10         return true;
11     }
12 }
```

Rysunek 14.2. Kod w środowisku Remix



Copy value to clipboard

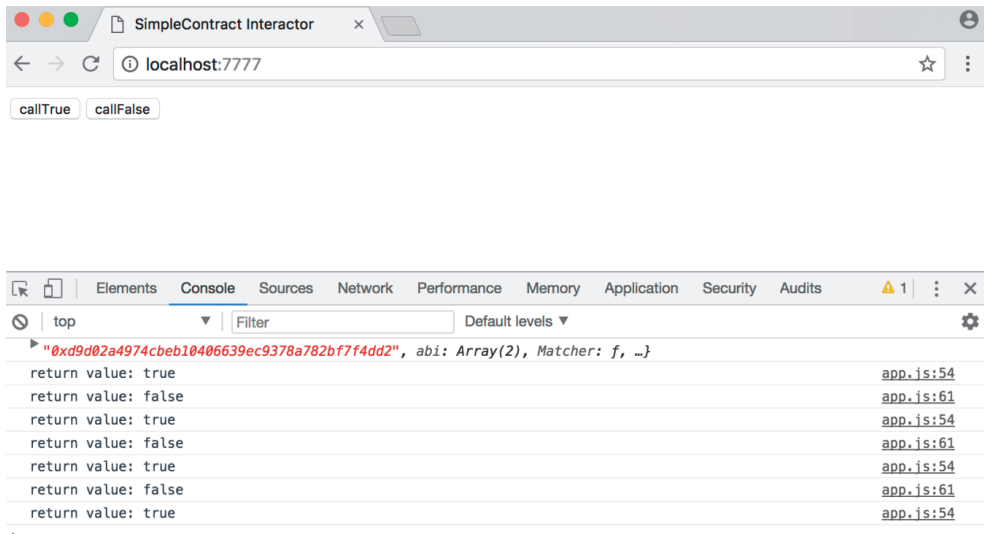
```
var valuecheckerContract = web3.eth.contract([{"constant":false,"inputs":[{"name":"x","type":"uint8"}],"name":"Matcher","outputs":[{"name":"","type":"bool"}],"payable":false,"stateMutability":"nonpayable","type":"function"}, {"anonymous":false,"inputs":[{"indexed":false,"name":"returnValue","type":"bool"}],"name":"valueEvent","type":"event"}]);
var valuechecker = valuecheckerContract.new(
{
  from: web3.eth.accounts[0],
  data: '0x6060604052600a600055341561001457600080fd5b6101038061002
36000396000f300606060405260043610603f576000357c01000000000000000000
00000000000000000000000000000000000000000000000000900463fffffffff168063f9d55e2114604
4575b600080fd5b3415604e57600080fd5b6065600480803560ff1690602001909190
5050607f565b604051808215151515815260200191505060405180910390f35b60008
0548260ff1610151560d1577f3eb1a229ff7995457774a4bd31ef7b13b6f4491ad1eb
b8961af120b8b4b6239c6001604051808215151515815260200191505060405180910
390a16001905060d2565b5b9190505600a165627a7a723058205b1d9d0f31b39806b7
782fdb9360af93d5b5f66a36f6f4023ee1aa9ca12782b70029',
  gas: '4700000'
}, function (e, contract){
  console.log(e, contract);
  if (typeof contract.address !== 'undefined') {
    console.log('Contract mined! address: ' + contract.address +
' transactionHash: ' + contract.transactionHash);
  }
})
```

```

> valuechecker.
valuechecker.Matcher
valuechecker._eth
valuechecker.abi
valuechecker.abi
valuechecker.address
valuechecker.allEvents
valuechecker.constructor
valuechecker.transactionHash
valuechecker.valueEvent
[
  {
    constant: false,
    inputs: [
      {
        name: "x",
        type: "uint8"
      }
    ],
    name: "Matcher",
    outputs: [
      {
        name: "",
        type: "bool"
      }
    ],
    payable: false,
    stateMutability: "nonpayable",
    type: "function"
  },
  {
    anonymous: false,
    inputs: [
      {
        indexed: false,
        name: "returnValue",
        type: "bool"
      }
    ],
    name: "valueEvent",
    type: "event"
  }
]
> valuechecker.address
"0xbd663c5136155cb6d7ed55446888271dcd5092bc"
>

```

Rysunek 14.5. Atrybuty kontraktu valuechecker



Rysunek 14.7. Interakcja z kontraktem

Ganache

SERVER

ACCOUNTS & KEYS

CHAIN

ADVANCED

CANCEL

RESTART

SERVER

HOSTNAME

127.0.0.1

The server will accept RPC connections on the following host and port.

PORT NUMBER

7545

NETWORK ID

5777

Internal blockchain identifier of Ganache server.

AUTOMINE

Process transactions instantaneously.

Rysunek 14.8. Ustawienia narzędzia Ganache

ACCOUNTS

BLOCKS

TRANSACTIONS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK

11

GAS PRICE

20000000000

GAS LIMIT

6721975

NETWORK ID

5777

RPC SERVER

HTTP://127.0.0.1:7545

MINING STATUS

AUTOMINING

TX HASH

0xd5050afb739a27fba97e027707af14e6e07077227a11a1035d352647a3f644aa

CONTRACT CALL

FROM ADDRESS

0x627306090abab3a6e1400e9345bc60c78a8bef57

TO CONTRACT ADDRESS

0x2c2b9c9a4a25e24b174f26114e8926a9f2128fe4

GAS USED

26981

VALUE

0

TX HASH

0xc9f8eb7e12b2cd33d73c8ed5858157eb7181ea262b19677a081e5e014ce1

CONTRACT CREATION

FROM ADDRESS

0x627306090abab3a6e1400e9345bc60c78a8bef57

CREATED CONTRACT ADDRESS

0xaa588d3737b611bafd7bd713445b314bd453a5c8

GAS USED

332608

VALUE

0

TX HASH

0x4d1f4c386d0b213c154ce5587aa6f625b1c70ff374f4ca0053a82db1074e8765

CONTRACT CREATION

FROM ADDRESS

0x627306090abab3a6e1400e9345bc60c78a8bef57

CREATED CONTRACT ADDRESS

0xfb88de099e13ced21f80a7a1e49f8caecf10df6

GAS USED

99662

VALUE

0

TX HASH

0x9b51540f5a7d75a8fc920e3e5e4ec66792ba31fd006bd176901f0e6347af2dba

CONTRACT CALL

FROM ADDRESS

0x627306090abab3a6e1400e9345bc60c78a8bef57

TO CONTRACT ADDRESS

0x2c2b9c9a4a25e24b174f26114e8926a9f2128fe4

GAS USED

41981

VALUE

0

TX HASH

0x54ac3fff035594cb4f3244ca0115fd206e9bce0a6e19b4964e67fb792e4c4991

CONTRACT CREATION

FROM ADDRESS

0x627306090abab3a6e1400e9345bc60c78a8bef57

CREATED CONTRACT ADDRESS

0x2c2b9c9a4a25e24b174f26114e8926a9f2128fe4

GAS USED

269607

VALUE

0

Rysunek 14.10. Transakcje wyświetlone w Ganache

ACCOUNTS

BLOCKS

TRANSACTIONS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK
11

GAS PRICE
20000000000

GAS LIMIT
6721975

NETWORK ID
5777

RPC SERVER
HTTP://127.0.0.1:7545

MINING STATUS
AUTOMINING

MNEMONIC

candy maple cake sugar pudding cream honey rich smooth crumble sweet treat

HD PATH

m/44'/60'/0'/0/account_index

ADDRESS

0x627306090abaB3A6e1400e9345bC60c78a8BEf57

BALANCE

99.84 ETH

TX COUNT

11

INDEX

0

ADDRESS

0xf17f52151EbEf6C7334FAD080c5704D77216b732

BALANCE

100.00 ETH

TX COUNT

0

INDEX

1

ADDRESS

0xC5fdf4076b8F3A5357c5E395ab970B5B54098FeF

BALANCE

100.00 ETH

TX COUNT

0

INDEX

2

ADDRESS

0x821aEa9a577a9b44299B9c15c88cf3087F3b5544

BALANCE

100.00 ETH

TX COUNT

0

INDEX

3

ADDRESS

0x0d1d4e623D10F9FBA5Db95830F7d3839406C6AF2

BALANCE

100.00 ETH

TX COUNT

0

INDEX

4

Rysunek 14.11. Wyświetlanie kont w Ganache

```
> truffle-init-webpack@0.0.2 dev /Users/drequinox/dapp1
> webpack-dev-server

Project is running at http://localhost:8080/
webpack output is served from /
Hash: 157d6514272a12586aba
Version: webpack 2.7.0
Time: 6702ms

   Asset      Size  Chunks             Chunk Names
  app.js    1.65 MB               0 [emitted] [big]  main
  index.html 925 bytes               0 [emitted]

chunk {0} app.js (main) 1.63 MB [entry] [rendered]
   [71] ./app/javascripts/app.js 3.64 kB {0} [built]
   [72] (webpack)-dev-server/client?http://localhost:8080 7.95 kB {0} [built]
   [73] ./build/contracts/MetaCoin.json 23.8 kB {0} [built]
  [111] ./~/loglevel/lib/loglevel.js 7.86 kB {0} [built]
  [117] ./~/quyrstring-es3/index.js 127 bytes {0} [built]
  [119] ./~/strip-ansi/index.js 161 bytes {0} [built]
  [122] ./app/stylesheets/app.css 905 bytes {0} [built]
  [163] ./~/truffle-contract/index.js 2.64 kB {0} [built]
  [197] ./~/url/url.js 23.3 kB {0} [built]
  [199] ./~/web3/index.js 193 bytes {0} [built]
  [233] (webpack)-dev-server/client/overlay.js 3.73 kB {0} [built]
  [234] (webpack)-dev-server/client/socket.js 1.05 kB {0} [built]
  [235] (webpack)/hot nonrecursive ^\.\/log$ 160 bytes {0} [built]
  [236] (webpack)/hot/emitter.js 77 bytes {0} [built]
  [237] multi (webpack)-dev-server/client?http://localhost:8080 ./app/javascripts/app.js 40 bytes {0} [built]
        + 223 hidden modules
webpack: Compiled successfully.
```

Rysunek 14.12. Uruchamianie pakietu Webpack

MetaCoin Example Truffle Dapp

You have 8680 META

Send MetaCoin

Amount:

To Address:

Send MetaCoin

Rysunek 14.13. Fronton przykładowej aplikacji MetaCoin

ACCOUNTS

BLOCKS

TRANSACTIONS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK

42

GAS PRICE

20000000000

GAS LIMIT

6721975

NETWORK ID

5777

RPC SERVER

HTTP://127.0.0.1:7545

MINING STATUS

AUTOMINING

TX HASH

0xb24064b090e15ec13949252cb24ce2a4e7f73ffbeed2405f9cce89020301530c

CONTRACT CALL

FROM ADDRESS

0x627306090abab3a6e1400e9345bc60c78a8bef57

TO CONTRACT ADDRESS

0xf25186b5081ff5ce73482ad761db0eb0d25abfbf

GAS USED

35960

VALUE

0

TX HASH

0x5df0cff3c7a13c9f75b00d74b49fc0207e19da0c97e1c208244395f5892ac37

CONTRACT CALL

FROM ADDRESS

0x627306090abab3a6e1400e9345bc60c78a8bef57

TO CONTRACT ADDRESS

0xf25186b5081ff5ce73482ad761db0eb0d25abfbf

GAS USED

35960

VALUE

0

TX HASH

0xc3a646e853c72433a60585c51fde547ef3bf9d728f5403962fc2e23e12e660c8

CONTRACT CALL

FROM ADDRESS

0x627306090abab3a6e1400e9345bc60c78a8bef57

TO CONTRACT ADDRESS

0xf25186b5081ff5ce73482ad761db0eb0d25abfbf

GAS USED

35960

VALUE

0

Rysunek 14.14. Szczegółowe informacje o transakcjach w Ganache

```
drequinox@drequinox-OP7010:~/testdapp$ truffle console
truffle (default) >
```

Rysunek 14.15. Konsola platformy Truffle

Rysunek 14.20. Udostępnianie dwóch metod

Rysunek 14.21. Wywołanie funkcji SaveIdeaHash

Rysunek 14.22. Dzienniki

[illegible]

Rysunek 14.26. Wywoływanie metod dodanego kontraktu w konsoli platformy Truffle

```

amran@requinox-OP7010:~$ ipfs cat /ipfs/QmYwAPJzv5CZsnA62Ss3Xf2nemtYgPpHdWEz79oJWnPBdG/readme
Hello and Welcome to IPFS!

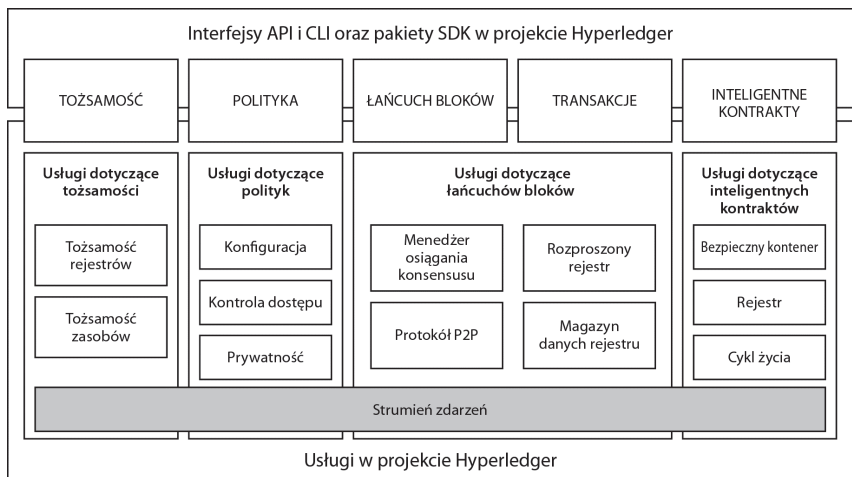
IPFS

If you're seeing this, you have successfully installed
IPFS and are now interfacing with the ipfs merkledag!

```

Rysunek 14.28. Instalowanie systemu IPFS

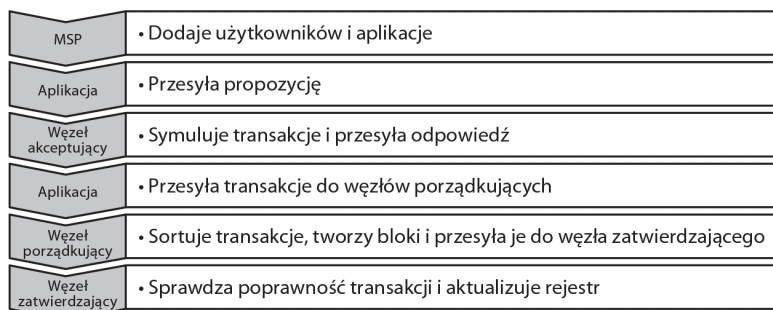
Rozdział 15. Hyperledger



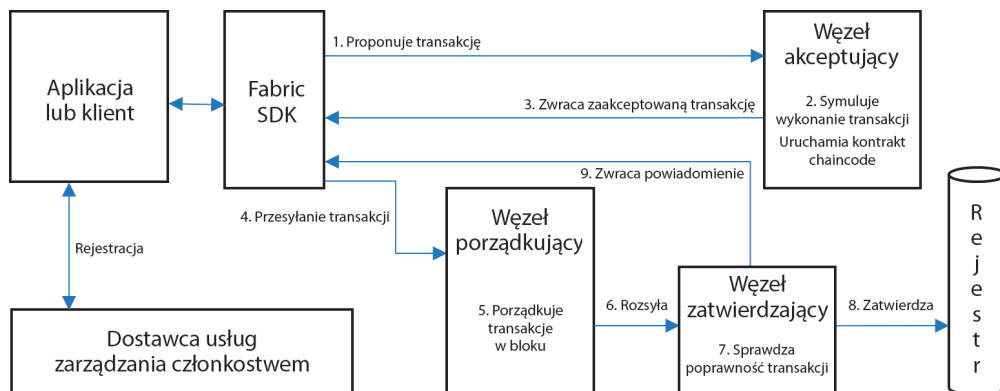
Rysunek 15.1. Architektura wzorcowa. Źródło: dokument na temat projektu Hyperledger



Rysunek 15.6. Proces osiągnięcia konsensusu



Rysunek 15.7. Cykl życia transakcji



Rysunek 15.8. Architektura procesu obsługi transakcji

```

drequinox@drequinox-OP7010:~/project$ git clone https://github.com/IntelLeder/sawtooth-core.git
Cloning into 'sawtooth-core'...
remote: Counting objects: 12527, done.
remote: Compressing objects: 100% (964/964), done.
remote: Total 12527 (delta 452), reused 0 (delta 0), pack-reused 11515
Receiving objects: 100% (12527/12527), 9.26 MiB | 1.76 MiB/s, done.
Resolving deltas: 100% (8131/8131), done.
Checking connectivity... done.
  
```

Rysunek 15.11. Klonowanie projektu Sawtooth z serwisu GitHub

```

drequinox@drequinox-OP7010:~/project/sawtooth-core/tools$ vagrant up
Could not determine vagrant user.
VAGRANT_BOX = ubuntu/xenial64
VAGRANT_FORWARD_PORTS = true
VAGRANT_MEMORY = 2048
VAGRANT_CPUS = 2
Proxyconf plugin not found
Install: vagrant plugin install vagrant-proxyconf
Bringing machine 'default' up with 'virtualbox' provider...
==> default: Box 'ubuntu/xenial64' could not be found. Attempting to find and install...
    default: Box Provider: virtualbox
    default: Box Version: >= 0
==> default: Loading metadata for box 'ubuntu/xenial64'
    default: URL: https://atlas.hashicorp.com/ubuntu/xenial64
==> default: Adding box 'ubuntu/xenial64' (v20161221.0.0) for provider: virtualbox
    default: Downloading: https://atlas.hashicorp.com/ubuntu/boxes/xenial64/versions/20161221.0.0/providers/virtualbox.bo
x
    default: Progress: 1% (Rate: 1709k/s, Estimated time remaining: 0:04:04)
  
```

Rysunek 15.12. Wykonywanie polecenia vagrant up

```

ubuntu@ubuntu-xenial:/project/sawtooth-core$ /project/sawtooth-core/docs/source/tutorial/genesis.sh
writing file: /home/ubuntu/sawtooth/keys/base000.wif
writing file: /home/ubuntu/sawtooth/keys/base000.addr
  
```

Rysunek 15.13. Generowanie bloku początkowego i kluczy

```

ubuntu@ubuntu-xenial:/project/sawtooth-core$ ./bin/txnvalidator -v -F ledger.transaction.integer_key --config /home/ubuntu/sawtooth/v0.json
[22:08:22 INFO validator_cli] validator started with arguments: ['./bin/txnvalidator', '-v', '-F', 'ledger.transaction.integer_key', '--config', '/home/ubuntu/sawtooth/v0.json']
[22:08:22 INFO validator_cli] read signing key from /home/ubuntu/sawtooth/keys/base000.wif
[22:08:24 WARNING validator_cli] validator pid is 10937
[22:08:24 INFO gossip_core] listening on IPv4Address(UDP, '0.0.0.0', 33713)
[22:08:24 INFO global_store_manager] create blockstore from file /home/ubuntu/sawtooth/data/base000_state.dbm with flag c
[22:08:24 INFO validator] set administration node to None
[22:08:24 INFO validator] starting ledger base000 with id 1K5RNedZ at network address ('127.0.0.1', 33713)
[22:08:24 INFO web_api] listen for HTTP requests on (ip='localhost', port=8800)
[22:08:24 INFO validator_cli] adding transaction family: ledger.transaction.integer_key
[22:08:24 INFO journal_core] restore ledger state from persistence
[22:08:24 INFO global_store_manager] add block 60af3ec894fa1cb0 to the queue for loading
[22:08:24 INFO global_store_manager] load block 60af3ec894fa1cb0 from storage
[22:08:24 INFO journal_core] commit head: 60af3ec894fa1cb0
[22:08:26 INFO validator] ledger connections using RandomWalk topology
[22:08:26 INFO random_walk] initiate random walk topology update
[22:08:29 INFO validator] ledger initialization complete
[22:08:29 INFO journal_core] process initial transactions and blocks
[22:08:29 INFO validator] register endpoint 1K5RNedZ with name base000
[22:08:29 INFO journal_core] build transaction block to extend 60af3ec8 with 1 transactions
[22:08:29 INFO wait_timer] wait timer created; TIMER, 5.00, 33.69, HE2QNJWGI2DCN3Q

```

Rysunek 15.14. Uruchamianie mechanizmu sprawdzania poprawności transakcji

```

ubuntu@ubuntu-xenial:/project/sawtooth-core$ ./bin/mktclient --name market --keyfile validator/keys/mkt.wif
//UNKNOWN> help

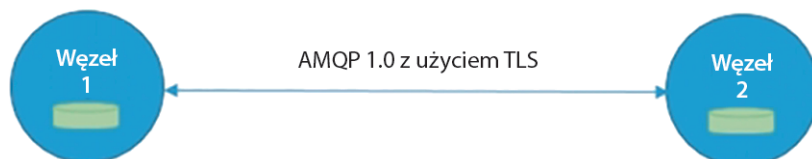
Documented commands (type help <topic>):
=====
EOF      dump      exit      liability  selloffer tokenstore
account  echo      help      map        session  waitforcommit
asset    exchange holding  offers    sleep
assettype exchangeoffer holdings participant state

Miscellaneous help topics:
=====
symbols  names

//UNKNOWN> participant reg --name market --description "the market"
transaction ff652e63dadeaf32 submitted
//market>

```

Rysunek 15.15. Klient market utworzony na potrzeby rodziny transakcji Marketplace



Rysunek 15.17. Dwa węzły komunikujące się w sieci Corda

Rozdział 16. Inne łańcuchy bloków

```

drequinox@drequinox-OP7010:~/Downloads$ ./pact
pact> 1234
1234
pact> (+ 1 2)
3
pact> (if (= (+ 1 2) 3) "OK" "ERROR")
(interactive):1:31: error: unexpected
EOF, expected: ")", ";", "{",
Boolean false, Boolean true,
Decimal literal, Integer literal,
String literal, Symbol literal,
list literal, pact, sexp, space
(if (= (+ 1 2) 3) "OK" "ERROR")<EOF>
^
pact> (if (= (+ 1 2) 3) "OK" "ERROR")
"OK"
pact>

```

Rysunek 16.2. Środowisko REPL języka Pact; widoczne są tu przykładowe polecenia i komunikat o błędzie

```

1 ;Rozpoczynanie transakcji o opcjonalnej nazwie.
2 ▾ (begin-tx) 'testTransaction
3 ;Podawanie danych transakcji w formacie JSON z typami języka Pact.
4 (env-data { "keyset": { "keys": [ "admin" ], "pred": "keys-any" }})
5 ;Definiowanie keyset jako nazwy powiązanej ze zbiorem kluczy.
6 (define-keyset 'admin-keyset (read-keyset "keyset"))
7 ;Podawanie kluczy na potrzeby podpisywania transakcji.
8 (env-keys [ "admin" ])
9 ;Definiowanie modułu za pomocą składni (module NAZWA KLUCZE [DOKUMENT] DEFINICJE ...)
10 (module additionModule 'admin-keyset
11 ;Definiowanie funkcji przyjmującej trzy argumenty: x y z.
12 (defun addition (x y z) (+ x (+ y z))))
13 ;Zatwierdzanie transakcji.
14 (commit-tx)
15 ;Używanie funkcji addition.
16 (use 'additionModule)
17 ;Uruchomienie funkcji addition i sformatowanie wyniku.
18 (format "Wynik: {}" [(addition 100 200 300)])

```

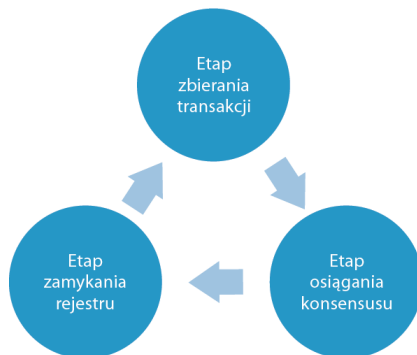
Rysunek 16.3. Przykładowy kod w języku Pact

```

""
""
"testTransaction"
"Setting transaction data"
"Keyset defined"
"Setting transaction keys"
"Loaded module \"additionModule\", hash
\"08a0de7383896b88e7287ed869bb0f405c8d7e7371404916c41330addbf3bab0eccecc3fa92bd3f
742e25beb60cd9022fef411a039c5fd1107266e69f4eccb2c7\"""
""
""
"Using \"additionModule\""
"Wynik: 600"

```

Rysunek 16.4. Dane wyjściowe kodu



Rysunek 16.5. Etapy protokołu osiągnięcia konsensusu w systemie Ripple

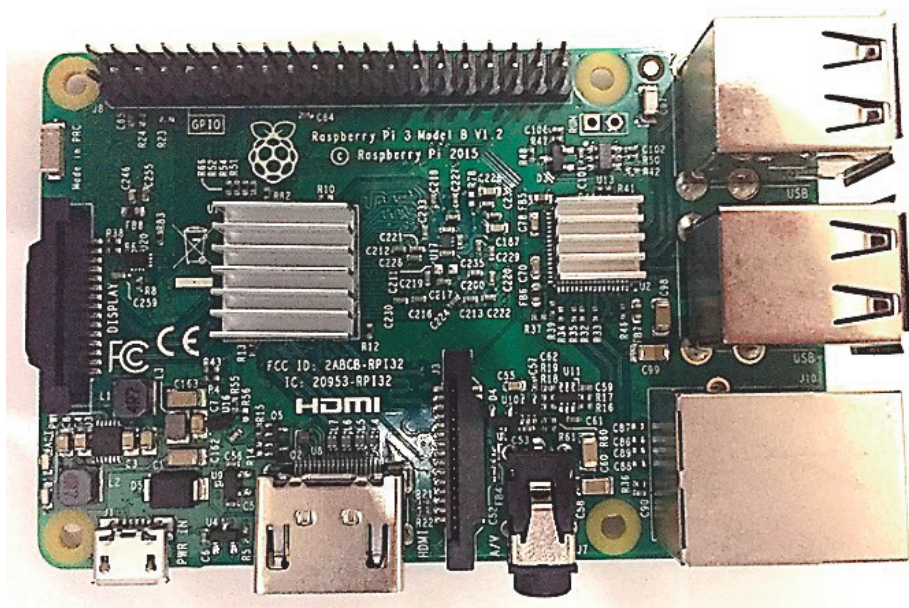
Rozdział 17. Łańcuch bloków — poza świat walut



Rysunek 17.1. Typowa sieć internetu rzeczy (źródło: IBM)



Rysunek 17.4. Model bezpośredniej komunikacji opartej na łańcuchu bloków (źródło: IBM)



Rysunek 17.5. Raspberry Pi Model B

```
pi@raspberrypi: ~  
File Edit Tabs Help  
pi@raspberrypi:~$ uname -a  
Linux raspberrypi 4.4.34-v7+ #930 SMP Wed Nov 23 15:20:41 GMT 2016 armv7l GNU/Linux  
pi@raspberrypi:~$
```

Rysunek 17.6. Architektura Raspberry Pi

```
pi@raspberrypi:~/geth-linux-arm7-1.5.6-2a609af5$ ./geth init genesis.json  
I0110 23:37:15.744795 cmd/utlits/flags.go:612] WARNING: No etherbase set and no accounts found as default  
I0110 23:37:15.745283 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/pi/.ethereum/geth/chaindata  
I0110 23:37:15.794383 ethdb/database.go:176] closed db:/home/pi/.ethereum/geth/chaindata  
I0110 23:37:15.794723 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/pi/.ethereum/geth/chaindata  
I0110 23:37:15.923300 core/genesis.go:193] Genesis block already in chain. Writing canonical number  
I0110 23:37:15.923895 cmd/geth/chaincmd.go:131] successfully wrote genesis block and/or chain rule set: f2b2ffed01907a845a01d1dea21e5a  
ec021e8e6b5ec9ffcc82df
```

Rysunek 17.7. Inicjowanie bloku początkowego

```
pi@raspberrypi:~/ethereum$ cat static-nodes.json  
[  
  "enode://44352ede5b9e792e437c1c0431c1578ce3676a87e1f588434aff1299d30325c233c8d426fc57a25380481c8a36fb957a25380481c8a36fb3be2787375e932fb4885885f6452f6efa77f@192.168.0.19:30301"  
]
```

Rysunek 17.8. Konfigurowanie węzłów statycznych

```
> admin.nodeInfo  
{  
  enode: "enode://44352ede5b9e792e437c1c0431c1578ce3676a87e1f588434aff1299d30325c233c8d426fc57a25380481c8a36fb957a25380481c8a36fb3be2787375e932fb4885885f6452f6efa77f@192.168.0.19:30301",  
  id: "44352ede5b9e792e437c1c0431c1578ce3676a87e1f588434aff1299d30325c233c8d426fc57a25380481c8a36fb3be2787375e932fb4885885f6452f6efa77f",  
}
```

Rysunek 17.9. Instrukcja nodeInfo w kliencie Geth

```
lmaran@drequinox-0P7010:~$ geth --datadir .ethereum/privatenet/ --networkid 786 --maxpeers 5 --rpc --rpccorsdomain "*" --port 30301 --identity "drequinox"  
I0110 23:26:46.032878 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/lmaran/.ethereum/privatenet/geth/chaindata  
I0110 23:26:46.072986 ethdb/database.go:176] closed db:/home/lmaran/.ethereum/privatenet/geth/chaindata  
I0110 23:26:46.073243 node/node.go:175] instance: Geth/drequinox/v1.5.2-stable-c8695209/linux/go1.7.3  
I0110 23:26:46.073258 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/lmaran/.ethereum/privatenet/geth/chaindata  
I0110 23:26:46.082654 eth/backend.go:193] Protocol Versions: [63 62], Network Id: 786  
I0110 23:26:46.083188 core/blockchain.go:214] Last header: #7991 [999c534f...] TD=11652654509  
I0110 23:26:46.083203 core/blockchain.go:215] Last block: #7991 [999c534f...] TD=11652654509  
I0110 23:26:46.083210 core/blockchain.go:216] Fast block: #7991 [999c534f...] TD=11652654509  
I0110 23:26:46.083929 p2p/server.go:336] Starting Server  
I0110 23:26:48.239776 p2p/discover/udp.go:217] Listening, enode://44352ede5b9e792e437c1c0431c1578ce3676a87e1f588434aff1299d30325c233c8d426fc57a25380481c8a36fb3be2787375e932fb4885885f6452f6efa77f@192.168.0.19:30301  
I0110 23:26:48.239893 p2p/server.go:604] Listening on [::]:30301  
I0110 23:26:48.240913 node/node.go:340] IPC endpoint opened: /home/lmaran/.ethereum/privatenet/geth.ipc  
I0110 23:26:48.241212 node/node.go:410] HTTP endpoint opened: http://localhost:9001  
I0110 23:42:58.206205 eth/backend.go:479] Automatic pregeneration of ethash DAG ON (ethash dir: /home/lmaran/.ethash)  
I0110 23:42:58.206217 miner/miner.go:136] Starting mining operation (CPU=8 TOT=9)
```

Rysunek 17.10. Uruchamianie klienta Geth w pierwszym węźle

```

pi@raspberrypi:~/geth-linux-arn7-1.5.6-2a609af5 $ ./geth --networkid 786 --maxpeers 5 --rpc --rpcapi web3,eth,debug,personal,net --
--ppccorsdonatin "*" --port 30302 --identity "raspberrypi"
I0110 23:38:04.654374 cmd/util/flags.go:612] WARNING: No etherbase set and no accounts found as default
I0110 23:38:04.654776 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/pi/.ethereum/geth/chaindata
I0110 23:38:04.693111 ethdb/database.go:176] closed db:/home/pi/.ethereum/geth/chaindata
I0110 23:38:04.696937 node/node.go:176] instance: Geth/raspberrypi/v1.5.6-stable-2a609af5/linux/go1.7.4
I0110 23:38:04.697042 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/pi/.ethereum/geth/chaindata
I0110 23:38:04.847835 eth/backend.go:191] Protocol Versions: [63 62], Network Id: 786
I0110 23:38:04.849753 eth/backend.go:219] Chain config: {ChainID: 0 Homestead: <nil> DAO: <nil> DAOsupport: false EIP150: <nil> EIP1
P158: <nil>}
I0110 23:38:04.857847 core/blockchain.go:216] Last header: #2668 [6776ef24..] TD=708187563
I0110 23:38:04.858174 core/blockchain.go:217] Last block: #2668 [6776ef24..] TD=708187563
I0110 23:38:04.858349 core/blockchain.go:218] Fast block: #2668 [6776ef24..] TD=708187563
I0110 23:38:04.866705 p2p/server.go:340] Starting Server
I0110 23:38:10.223170 p2p/discover/udp.go:227] Listening, enode://98ba36ecea7ff011803d634da45752abd2510f20a62f23427afc3f280017bc134
b195ac6ed59c3b01ca2a3f14638a52697a1bb1bf967fc84274086.15.44.209:30302
I0110 23:38:10.224031 p2p/server.go:608] Listening on [::]:30302
I0110 23:38:10.233788 node/node.go:341] IPC endpoint opened: /home/pi/.ethereum/geth.ipc
I0110 23:38:10.237027 node/node.go:411] HTTP endpoint opened: http://localhost:9002
I0110 23:38:20.225637 eth/downloader/downloader.go:326] Block synchronisation started
I0110 23:38:49.583631 core/blockchain.go:1067] imported 1 blocks, 0 txs ( 0.000 Mg/s). #2669 [76077955
I0110 23:38:49.622191 core/blockchain.go:1067] imported 5 blocks, 0 txs ( 0.000 Mg/s). #2674 [76077955

```

Rysunek 17.11. Klient Geth w Raspberry Pi

```

> admin.peers
[[
  caps: ["eth/62", "eth/63"],
  id: "44352ede5b9e792e437c1c0431c1578ce3676a87e1f588434aff1299d30325c233c8d426fc57a25380481c8a36fb3be2787375e932f
b4885885f6452f6efa77f",
  name: "Geth/drequisinox/v1.5.2-stable-c8695209/linux/go1.7.3",
  network: {
    localAddress: "192.168.0.21:56550",
    remoteAddress: "192.168.0.19:30301"
  },
  protocols: {
    eth: {
      difficulty: 11719415397,
      head: "0x2d32c90b4c9dacea9a109b0ae52c1ebf511915bb618a2d3c55a80a63852e89f6",
      version: 63
    }
  }
]}

```

Rysunek 17.12. Polecenie admin.peers w konsoli klienta geth w Raspberry Pi

```

> admin.peers
[[
  caps: ["eth/62", "eth/63"],
  id: "98ba36ecea7ff011803d634da45752abd2510f20a62f23427afc3f280017bc134833dd5ba400bb195ac6ed59c3b01
ca2a3f14638a52697a1bb1bf967fc84274",
  name: "Geth/raspberrypi/v1.5.6-stable-2a609af5/linux/go1.7.4",
  network: {
    localAddress: "192.168.0.19:30301",
    remoteAddress: "192.168.0.21:56512"
  },
  protocols: {
    eth: {
      difficulty: 11700366137,
      head: "0x1188f58b4900a1d771d333141ea9400d78400bb8e561494ab436519ae64e1e34",
      version: 63
    }
  }
]}

```

Rysunek 17.13. Polecenie admin.peers w konsoli klienta geth uruchomione w innym węźle

```

pi@raspberrypi:~/testled $ curl -sL https://deb.nodesource.com/setup_7.x | sudo -E bash -
## Installing the NodeSource Node.js v7.x repo...

## Populating apt-get cache...

+ apt-get update
Get:1 http://archive.raspberrypi.org jessie InRelease [22.9 kB]

```

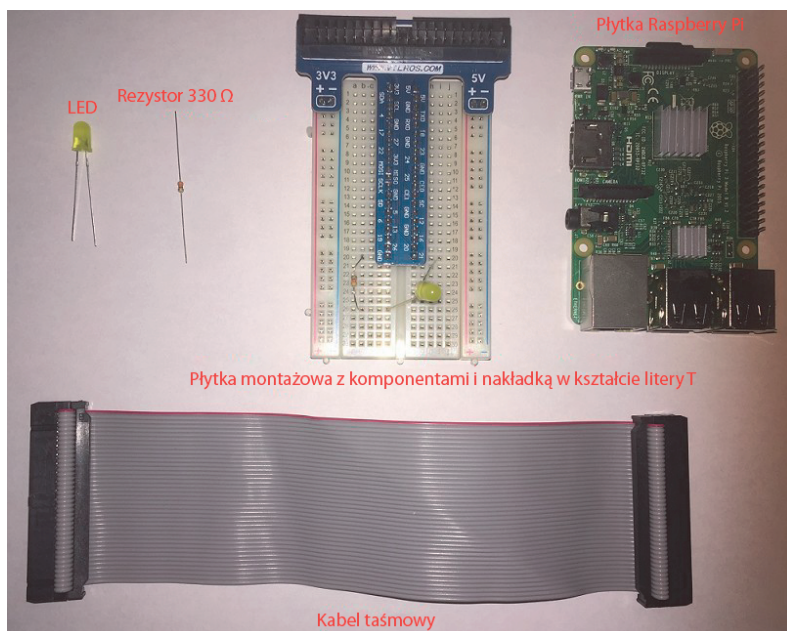
Rysunek 17.14. Instalowanie środowiska Node.js

```
pi@raspberrypi:~/testled $ npm -v
4.0.5
pi@raspberrypi:~/testled $ node -v
v7.4.0
pi@raspberrypi:~/testled $
```

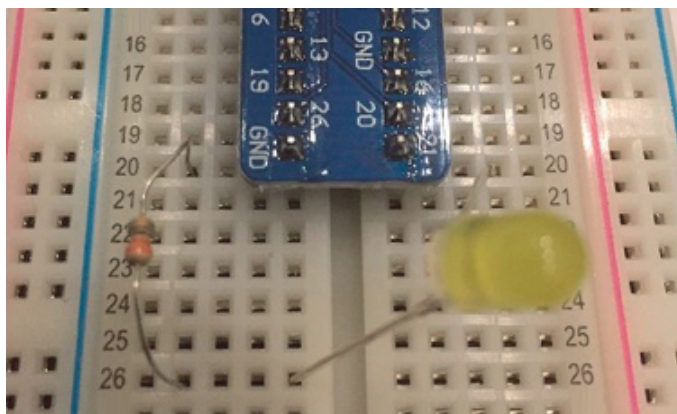
Rysunek 17.15. Sprawdzanie zainstalowanych wersji narzędzi Node.js i npm

```
pi@raspberrypi:~/testled $ npm install web3
testled@1.0.0 /home/pi/testled
└─ web3@0.18.0
   └─ bignumber.js@2.0.7 (git+https://github.com/debris/bignumber.js.git#94d7146671b9719e00a09c29b01a691bc85048c2)
npm WARN testled@1.0.0 No repository field.
pi@raspberrypi:~/testled $
```

Rysunek 17.16. Instalowanie pakietu web3 za pomocą narzędzia npm



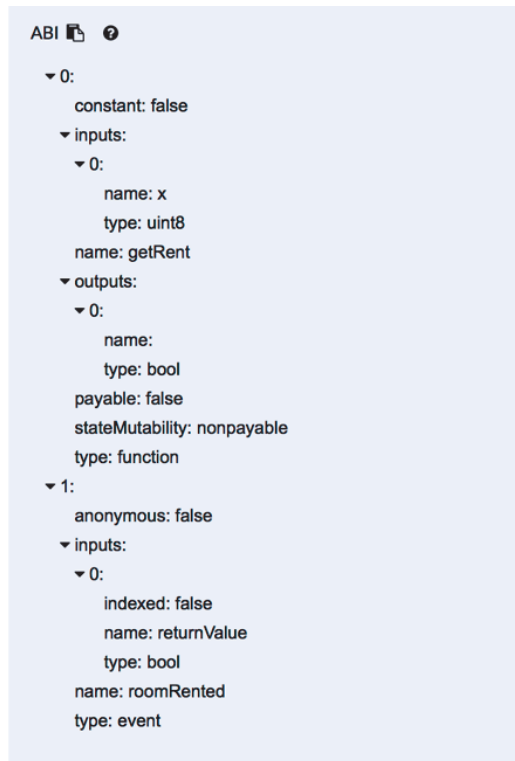
Rysunek 17.18. Potrzebne komponenty



Rysunek 17.19. Podłączenia komponentów na płytce montażowej

```
1 pragma solidity ^0.4.0;
2 contract simpleIOT {
3     uint roomrent = 10;
4     event roomRented(bool returnValue);
5     function getRent (uint8 x) public returns (bool) {
6         if (x==roomrent) {
7             roomRented(true);
8             return true;
9         }
10    }
11 }
```

Rysunek 17.20. Kod w języku Solidity dla prostego urządzenia dla internetu rzeczy



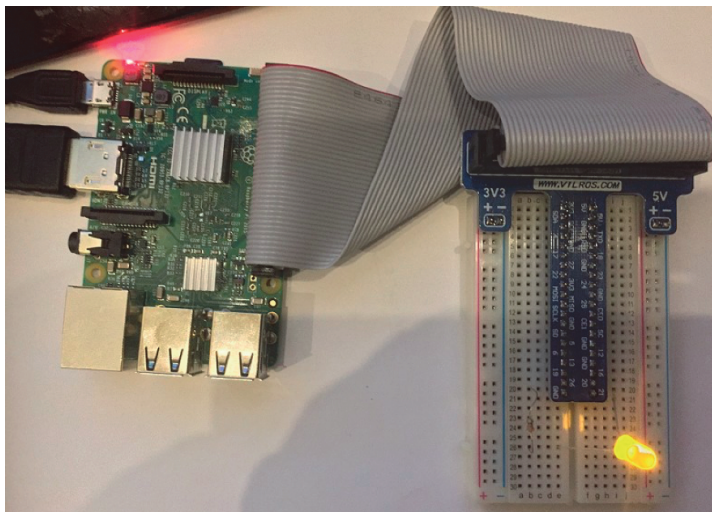
Rysunek 17.21. Interfejs ABI w środowisku IDE Remix

```
imran@drequinox-OP7010:~/iotcontract$ truffle migrate --reset
Running migration: 1_initial_migration.js
  Deploying Migrations...
  Migrations: 0xdd8a88072aa4ff49b62c25d6f6f2207b731aee76
Saving successful migration to network...
Saving artifacts...
Running migration: 2_deploy_contracts.js
  Deploying simpleIoT...
  simpleIoT: 0x151ce17c28b20ce554e0d944deb30e0447fbf78d
Saving successful migration to network...
Saving artifacts...
```

Rysunek 17.24. Dodawanie kontraktu za pomocą narzędzia Truffle

```
[truffle(development)> simpleiot.getRent(10)
'0x71f550949a4c5168af7b9f7f84fada99bccc20a123779642e5e8c0c0127266ee'
```

Rysunek 17.25. Interakcja z kontraktem



Rysunek 17.26. Raspberry Pi sterujące diodą LED

Rozdział 18. Skalowalność i inne problemy

Security

- ✓ Transaction origin: Warn if tx.origin is used
- ✓ Check effects: Avoid potential reentrancy bugs
- ✓ Inline assembly: Use of Inline Assembly
- ✓ Block timestamp: Semantics maybe unclear
- ✓ Low level calls: Semantics maybe unclear
- ✓ Block.blockhash usage: Semantics maybe unclear
- ✓ Selfdestruct: Be aware of caller contracts.

Gas & Economy

- ✓ Gas costs: Warn if the gas requirements of functions are too high.
- ✓ This on local calls: Invocation of local functions via this

Miscellaneous

- ✓ Constant functions: Check for potentially constant functions
- ✓ Similar variable names: Check if variable names are too similar
- ✓ no return: Function with return type is not returning
- ✓ Guard Conditions: Use require and appropriately

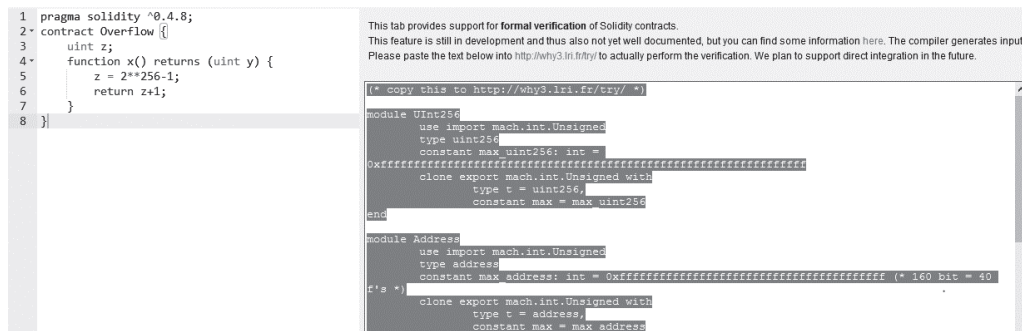
Run

☐ Auto run

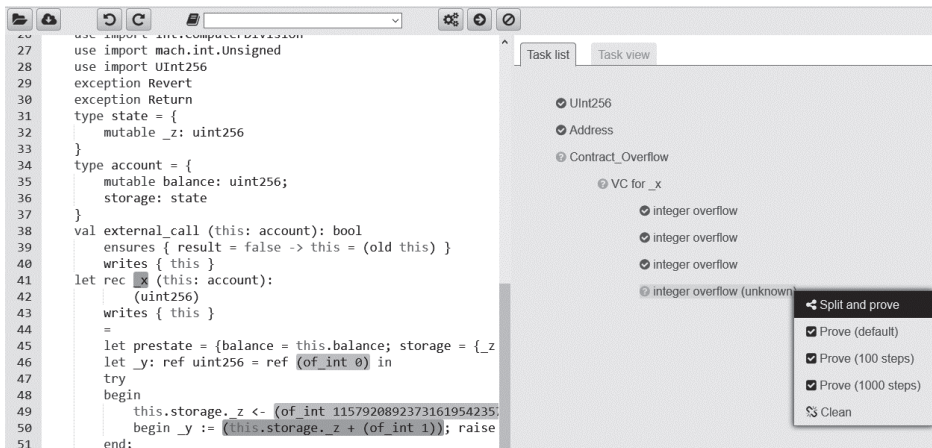
Potential Violation of Checks-Effects-Interaction pattern in `Fund.withdraw()`: Could potentially lead to re-entrancy vulnerability.

[more](#)

Rysunek 18.2. Opcje analiz w środowisku IDE Remix



Rysunek 18.3. Internetowy kompilator kodu w języku Solidity oferujący formalne sprawdzanie poprawności



Rysunek 18.4. Why3

```

1 pragma solidity ^0.4.0;
2 contract Fund {
3   mapping(address => uint) shares;
4   function withdraw() public {
5     if (msg.sender.call.value(shares[msg.sender]))()
6       shares[msg.sender] = 0;
7   }
8 }

```

Rysunek 18.5. Kontrakt z błędem związanym z ponownym wywołaniem kodu. Źródło: dokumentacja języka Solidity

```
root@fa9ef6ac8455:/home/oyente/oyente
(venv)root@fa9ef6ac8455:/home/oyente/oyente# python oyente.py a1.sol
Contract Fund:
Running, please wait...
===== Results =====
CallStack Attack: False
THIS IS A CALLLLLLLLLLL
{'path condition': '[iv >= 0, init_Is >= Iv, init_Ia >= 0, If(Id_0/
26959946667150639794667015087019630673637144422540572481103610249216 ==
1020253707,
1,
0) !=
0, Not(iv != 0)], 'Is': Is, 'Iv': Iv, 'some_var_1': some_var_1, 'Id_0': Id
_0, 'Ia_store_some_var_1': Ia_store_some_var_1, 'Ia': Ia}

This is the global state
{'Ia': {'some_var_1': 0}, 'niu_1': 3L, 'balance': {'Ia': init_Ia + Iv, 'Is
': init_Is + Iv}}
(64: 96, 0: Is & 1461501637330902918203684832716283019655932542975, 32: 0)

CALL params

Is & 1461501637330902918203684832716283019655932542975

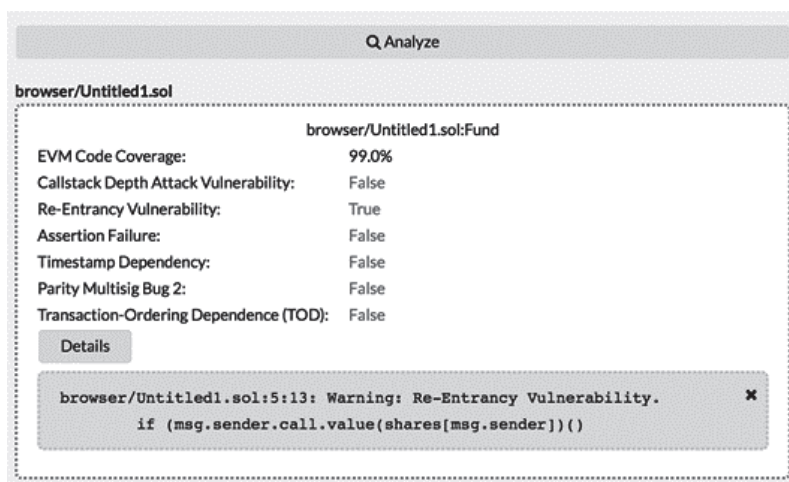
Ia_store_some_var_1

>>>>> New PC: []

Reentrancy_bug? True

Added True
Concurrency Bug: False
Time Dependency: False
Reentrancy bug exists: True
===== Analysis Completed =====
(venv)root@fa9ef6ac8455:/home/oyente/oyente#
```

Rysunek 18.6. Narzędzie Oyente wykrywające błędy w języku Solidity



Rysunek 18.7. Analiza w narzędziu Oyente