

---

# **Blockchain-Lab**

V0.4

**AUSTRIAPRO**

**Dr. Christian Baumann**

**25.10.2018**

# Inhalt

---

- Phase 1 „classic“
- Phase 2 „Ethereum“ – smart contracts
- Phase 3 „MultiChain“
- Phase 4 ...

# Phase 1

---

- „classic“ (crypto coin based) blockchains
  - Look & Feel wie Bitcoin, Litecoin ... Client
  - „Hands on“
    - Installation & Betrieb wallet
    - “werte” transferieren (senden, empfangen)
    - Nachrichten signieren
  - Mining ausprobieren
    - Standalone, CPU, GPU
    - Über Miningpool
  - Weitere Tools kennenlernen
    - Blockexplorer
    - Paper-, Brain-wallets
  - Unterschied „CryptoCurrency – Blockchain“

# Classic crypto coin (am Beispiel C2coin)

- Wallet
  - Wallet für Windows:  
[http://www4.baumann.at/downloads/c2coin\\_Wallet\\_Windows-20141107.zip](http://www4.baumann.at/downloads/c2coin_Wallet_Windows-20141107.zip)
  - Kurzanleitung dazu:  
<http://www4.baumann.at/downloads/C2coin-Readme.txt>
- Mining
  - Mining mit GPUs: <http://www4.baumann.at/downloads/Mining-with-GPUs.txt>
  - Miningportal: <http://coinz.at:81/>
- Tools
  - Faucet (coins senden lassen) <http://coinz.at/c2coin/send.php>
  - Infoseite zum C2coin Netz: <http://coinz.at/c2coin/>
  - Einfacher Blockexplorer: <http://coinz.at/c2coin/be.php>
  - Walletgenerator: <http://coinz.at/walletgenerator/>

# Beispiel: C2coin - Wallet

The screenshot displays the C2coin wallet interface. The window title is "C2coin - Brieftasche". The menu bar includes "Datei", "Einstellungen", and "Hilfe". The navigation bar contains "Übersicht" (selected), "Überweisen", "Empfangen", "Transaktionen", and "Adressen".




**Brieftasche**

Kontostand: **3543518.60366691 C2C**

Unbestätigt: **0.00 C2C**

Unreif: **400.00 C2C**

**Letzte Transaktionen**

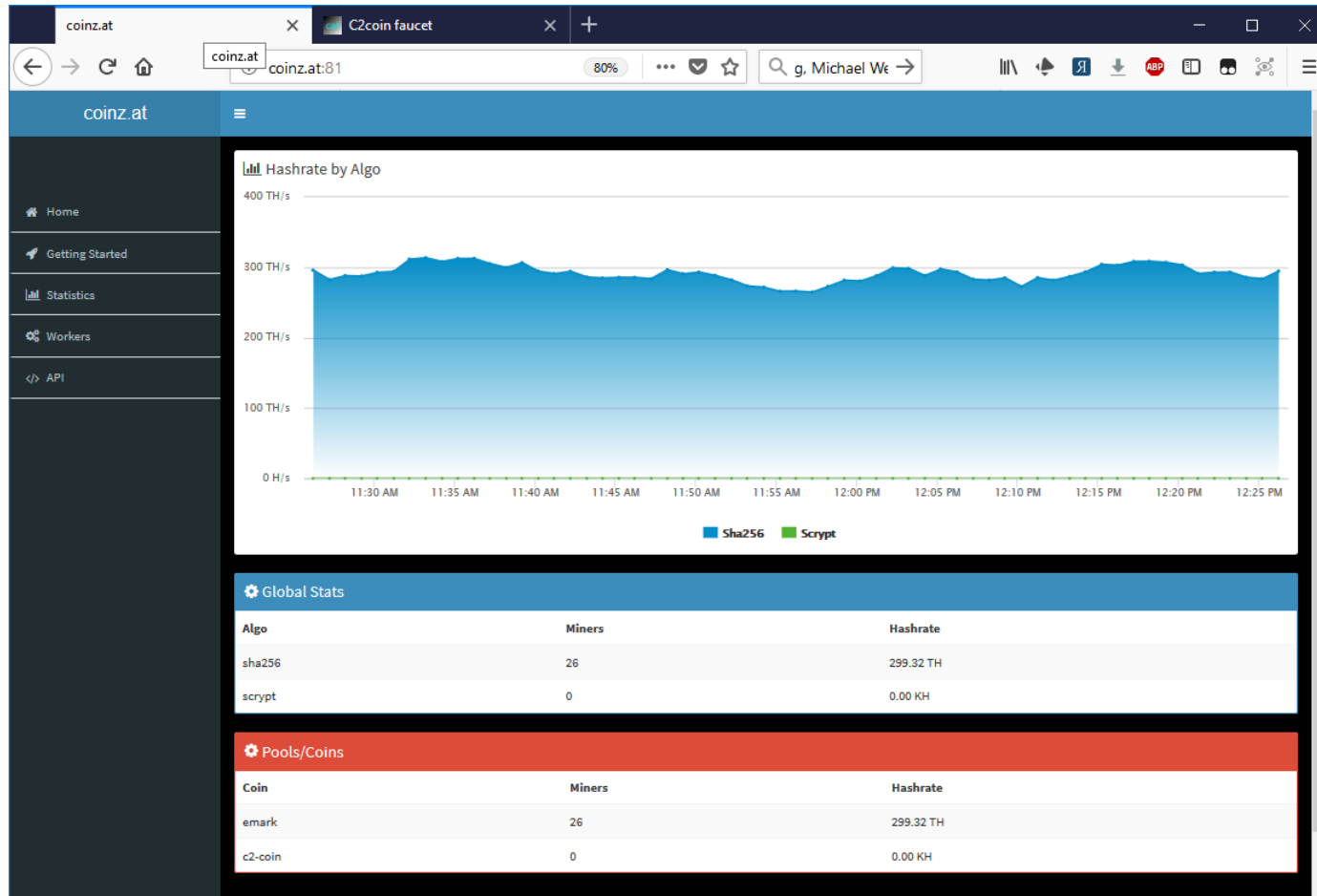
	06.11.2014 08:00	<b>[-1000.00 C2C]</b>
	Test wrong	
	11.04.2018 10:28	<b>[+200.00 C2C]</b>
	(CeMLhxNMjVYoEvgArAMpxQ3PTQcnw54fzG)	
	11.04.2018 10:27	<b>[+200.00 C2C]</b>
	(CX1MaJB42bgXy6eAHUev3A1UTCW5DpYZzK)	

In the bottom right corner, there is a small status indicator showing a green checkmark and a signal strength icon.

# Beispiel: C2coin – GPU Mining

```
c:\CryptoCoins\cudaminer-2014-02-28\x64\cudaminer.exe
[2018-04-11 10:33:10] 1 miner threads started, using 'scrypt' algorithm.
[2018-04-11 10:33:10] GPU #0: Quadro 600 with compute capability 2.1
[2018-04-11 10:33:10] GPU #0: interactive: 1, tex-cache: 0 , single-alloc: 0
[2018-04-11 10:33:10] GPU #0: 32 hashes / 4.0 MB per warp.
[2018-04-11 10:33:10] GPU #0: using launch configuration F2x16
[2018-04-11 10:33:10] GPU #0: Quadro 600, 20.75 khash/s
[2018-04-11 10:33:15] GPU #0: Quadro 600, 22.67 khash/s
[2018-04-11 10:33:20] GPU #0: Quadro 600, 22.57 khash/s
[2018-04-11 10:33:25] GPU #0: Quadro 600, 22.64 khash/s
[2018-04-11 10:33:30] GPU #0: Quadro 600, 22.64 khash/s
[2018-04-11 10:33:35] GPU #0: Quadro 600, 21.18 khash/s
[2018-04-11 10:33:40] GPU #0: Quadro 600, 21.84 khash/s
[2018-04-11 10:33:42] GPU #0: Quadro 600, 21.67 khash/s
[2018-04-11 10:33:43] accepted: 1/1 (100.00%), 21.67 khash/s (yay!!!)
[2018-04-11 10:33:48] GPU #0: Quadro 600, 22.31 khash/s
[2018-04-11 10:33:53] GPU #0: Quadro 600, 22.10 khash/s
[2018-04-11 10:33:58] GPU #0: Quadro 600, 22.14 khash/s
[2018-04-11 10:34:03] GPU #0: Quadro 600, 22.42 khash/s
[2018-04-11 10:34:08] GPU #0: Quadro 600, 22.61 khash/s
[2018-04-11 10:34:13] GPU #0: Quadro 600, 22.63 khash/s
[2018-04-11 10:34:17] GPU #0: Quadro 600, 22.29 khash/s
[2018-04-11 10:34:18] accepted: 2/2 (100.00%), 22.29 khash/s (yay!!!)
[2018-04-11 10:34:23] GPU #0: Quadro 600, 22.45 khash/s
[2018-04-11 10:34:28] GPU #0: Quadro 600, 22.10 khash/s
```

# Beispiel: Miningportal coinz.at



# Beispiel: C2coin – „Faucet“

**C2coin faucet**

**C2coin faucet**

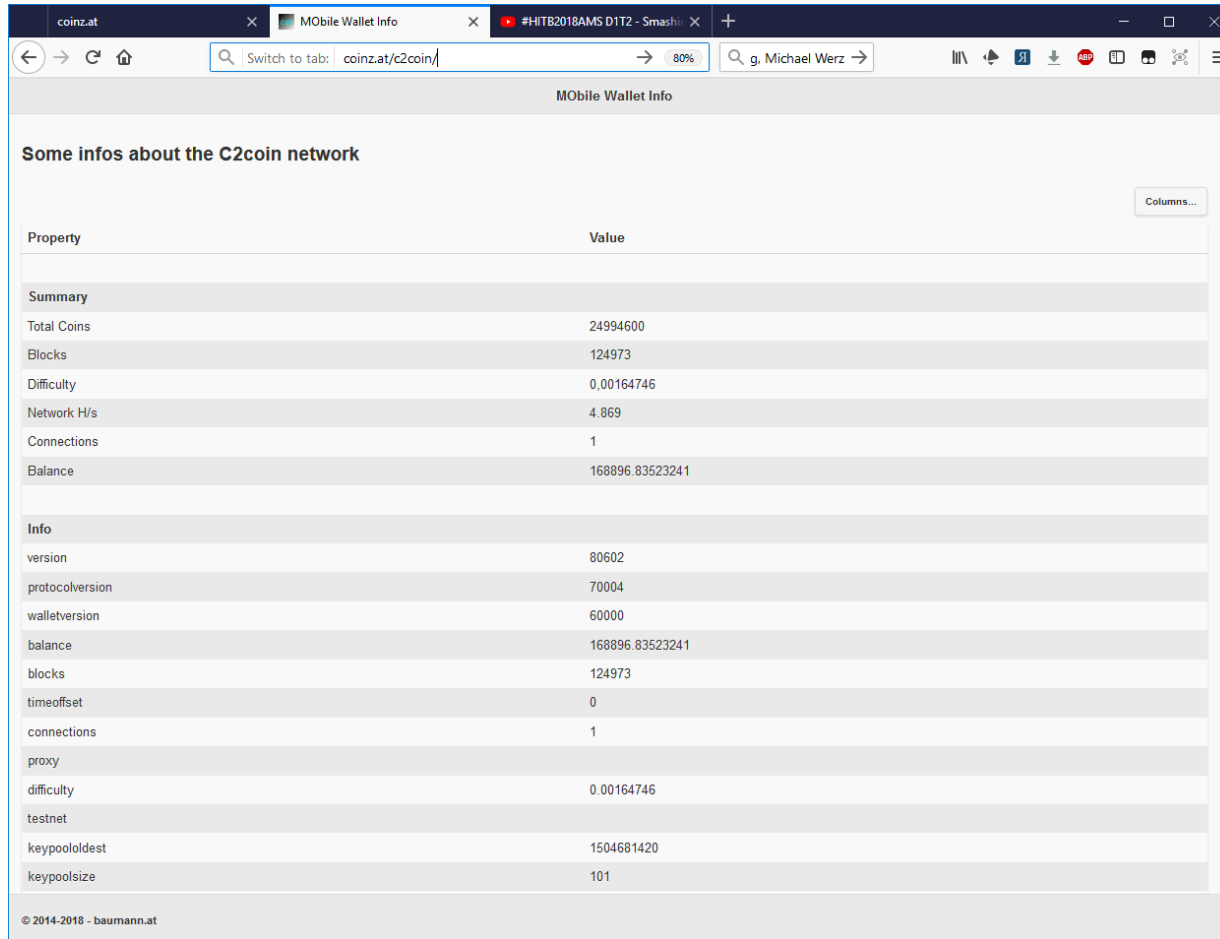
Enter a C2coin address to receive some coins, e.g. CMPiHHuwjSpf2fYpxrgMKsZFBrijSwEeSW:

C2coin address:

  
  
[Back](#)



# Beispiel: C2coin – Network Info



MOBILE WALLET INFO

Some infos about the C2coin network

Property	Value
<b>Summary</b>	
Total Coins	24994600
Blocks	124973
Difficulty	0.00164746
Network H/s	4.869
Connections	1
Balance	168896.83523241
<b>Info</b>	
version	80602
protocolversion	70004
walletversion	60000
balance	168896.83523241
blocks	124973
timeoffset	0
connections	1
proxy	
difficulty	0.00164746
testnet	
keypoololdest	1504681420
keypoolsize	101

© 2014-2018 - baumann.at

# Beispiel: C2coin – Block Explorer

**C2coin** block explorer

Connections: 1

Based on [RPC Ace](#) v0.6.7

Blocks: [124581](#)

Difficulty: 0.00024414 (= 0.00699 MH/s)

Net hashrate: 0.00018 MH/s (last 10 Blocks)


Net hashrate: 0.00009 MH/s (last 100 Blocks)

Block	Hash	Difficulty	Time (UTC)	Tx# · Value out
124581	<a href="#">39687ae93816239f ...</a>	0.000244 (16)	08:34:13 11-Apr-2018	1 · 200
124580	<a href="#">8e64e92f50f9515d ...</a>	0.000244 (16)	08:33:40 11-Apr-2018	2 · 1600
124579	<a href="#">83eacb3d35a05e4d ...</a>	0.000244 (16)	08:28:07 11-Apr-2018	1 · 200
124578	<a href="#">f5919c1fbbad84a9 ...</a>	0.000244 (16)	08:27:52 11-Apr-2018	1 · 200
124577	<a href="#">82a7e682d9b6948a ...</a>	0.000244 (16)	08:26:13 11-Apr-2018	1 · 200
124576	<a href="#">5257148bc23a5a43 ...</a>	0.000244 (16)	08:25:48 11-Apr-2018	1 · 200
124575	<a href="#">9424957414d3afb9 ...</a>	0.000244 (16)	08:24:46 11-Apr-2018	1 · 200
124574	<a href="#">0b1ec7c761362250 ...</a>	0.000244 (16)	08:24:22 11-Apr-2018	1 · 200
124573	<a href="#">29cb0a1281644d7a ...</a>	0.000244 (16)	17:06:14 10-Apr-2018	2 · 800
124572	<a href="#">de0a3e49aea0e06d ...</a>	0.000244 (16)	16:09:52 10-Apr-2018	1 · 200
124571	<a href="#">e97a4b7d395b3df1 ...</a>	0.000244 (16)	16:07:06 10-Apr-2018	2 · 1400
124570	<a href="#">edfca9e2f7553be9 ...</a>	0.000244 (16)	15:58:39 10-Apr-2018	1 · 200

[< Newer](#)

[Older >](#)

# Beispiel: WalletGenerator


 **WalletGenerator.net**  
Universal Open Source Client-Side Wallet Generator

Choose currency :

Single Wallet | Paper Wallet | Bulk Wallet | Brain Wallet | Wallet Details | Support

Generate New Address Print


**Public Address**



**SHARE**

CGqCQCZeFXpjPxpj3sYK6pDXkSsnMKTE2mf

**Private Key (Wallet Import Format)**



**SECRET**

6F XuWRPeNo2Rhm7zKCZMr tDJzy5MMzWVu.fQAHNn2vSMtKudRi2E

**Step 0. Follow the security checklist recommendation**

First step is to **download** this website from [Github](#) and open the index.html file directly from your computer. It's just too easy to sneak some evil code in the 6000+ lines of javascript to leak your private key, and you don't want to see your fund stolen. Code version control make it much easier to cross-check what actually run. For extra security, **unplug your Internet access** while generating your wallet.

**Step 1. Generate new address**


Choose your currency and click on the "Generate new address" button.

**Step 2. Print the Paper Wallet**

Click the Paper Wallet tab and print the page on high quality setting. **Never save the page as a PDF file to print it later since a file is more likely to be hacked than a piece of paper.**

**Step 3. Fold the Paper Wallet**

Fold your new Paper wallet following the lines.



# Phase 2

---

- Ethereum based
  - Smart Contracts
  - Oracles
  - Tokens (vgl. ICOs)
- Lab: Ethereum Test-Chain (Private)
  - Bootnode
  - Node (mit On Demand Mining)
    - CPU Mining
- => Setup eigener Node
  - Anleitung siehe [https://blockchains.web-lab.at/austriapro/Ethereum-Testnet\\_20180528.pdf](https://blockchains.web-lab.at/austriapro/Ethereum-Testnet_20180528.pdf)

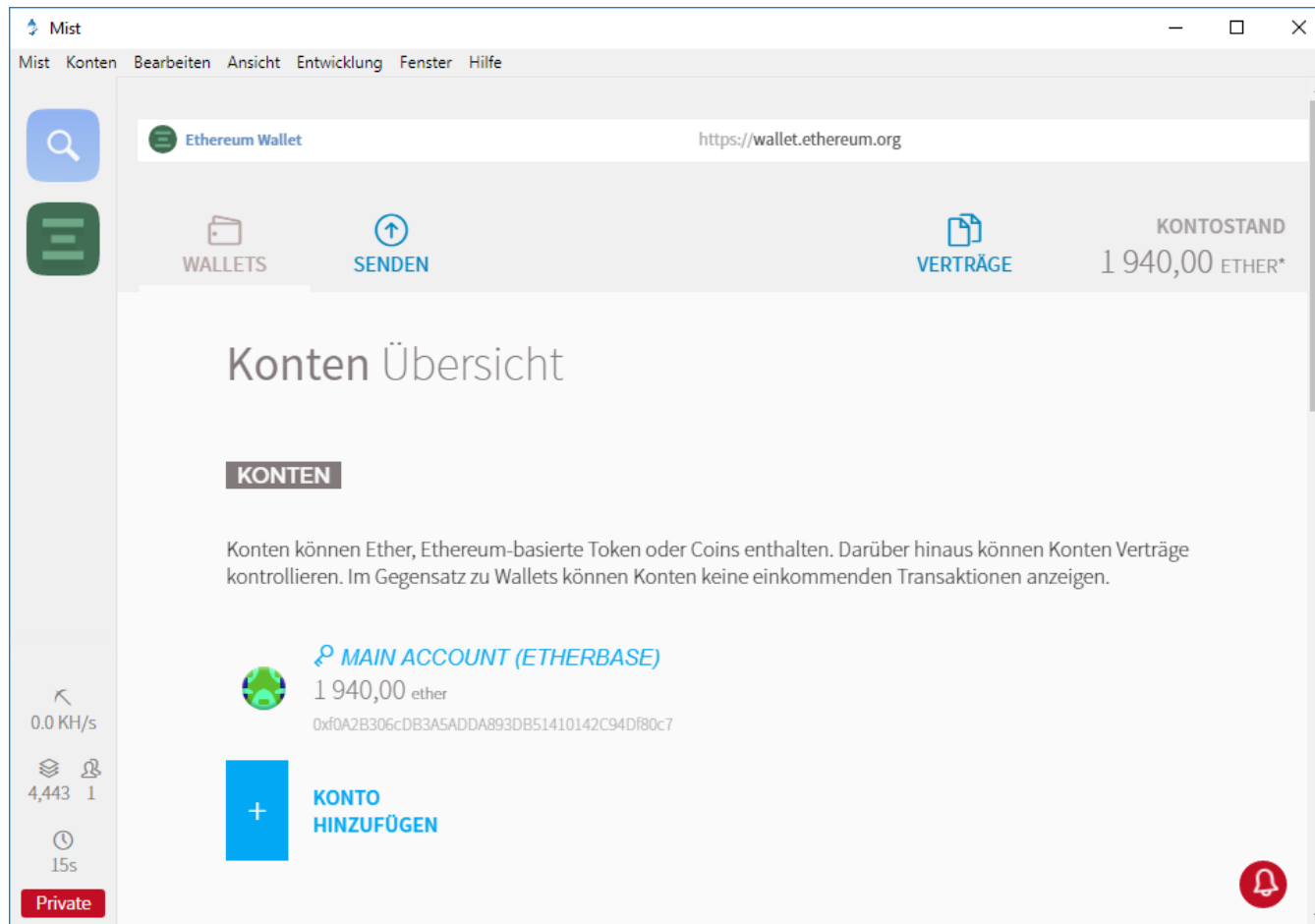
# Ethereum Test-Chain - console

```
C:\Windows\System32\cmd.exe - pc5_bn.cmd
WARN [04-11|10:38:51] Head state missing, repairing chain      number=3755 hash=c818a4...1b9c2d
INFO [04-11|10:38:51] Rewound blockchain to past state                    number=3602 hash=703b25...eb8bd4
INFO [04-11|10:38:51] Loaded most recent local header                          number=3755 hash=c818a4...1b9c2d td=2505735899
INFO [04-11|10:38:51] Loaded most recent local full block                      number=3602 hash=703b25...eb8bd4 td=2459503000
INFO [04-11|10:38:51] Loaded most recent local fast block                    number=3755 hash=c818a4...1b9c2d td=2505735899
INFO [04-11|10:38:51] Loaded local transaction journal                       transactions=0 dropped=0
INFO [04-11|10:38:51] Regenerated local transaction journal                 transactions=0 accounts=0
WARN [04-11|10:38:51] Blockchain not empty, fast sync disabled
INFO [04-11|10:38:51] Starting P2P networking
INFO [04-11|10:38:54] UDP listener up                                       self=enode://92f61c5ab4e4a999b05733ad68abdde9649351
1789fee25ed8ce2c4b7977e521081fdb6fab8d2575e1ef0e115a59d9c87fcfd5ba7ea2907cede2089c16cbb75@85.124.9.90:30332
INFO [04-11|10:38:54] RLPx listener up                                       self=enode://92f61c5ab4e4a999b05733ad68abdde9649351
1789fee25ed8ce2c4b7977e521081fdb6fab8d2575e1ef0e115a59d9c87fcfd5ba7ea2907cede2089c16cbb75@85.124.9.90:30332
INFO [04-11|10:38:55] HTTP endpoint opened                                  url=http://127.0.0.1:8000 cors=* vhosts=localhost
INFO [04-11|10:38:55] IPC endpoint opened                                   url=\\\\.\\pipe\\geth.ipc
Welcome to the Geth JavaScript console!

instance: Geth/c2eth-pc5/v1.8.3-stable-329ac18e/windows-amd64/go1.10
INFO [04-11|10:38:55] Etherbase automatically configured                   address=0x9159e7fc8a8639E812d9624868527703a40baA58
coinbase: 0x9159e7fc8a8639e812d9624868527703a40baa58
at block: 3602 (Mon, 09 Apr 2018 07:30:47 CEST)
  datadir: c:\CryptoCoins\c2eth-chain
  modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0

> INFO [04-11|10:39:05] Block synchronisation started
INFO [04-11|10:39:05] Imported new chain segment                          blocks=7 txs=0 mgas=0.000 elapsed=75.163ms mgasps=0
.000 number=3609 hash=88cd6e...3b69cc cache=4.95kB
INFO [04-11|10:39:05] Imported new chain segment                          blocks=29 txs=2 mgas=0.060 elapsed=81.251ms mgasps=
0.736 number=3638 hash=12c812...5dd0c6 cache=26.11kB
INFO [04-11|10:39:05] Imported new chain segment                          blocks=117 txs=8 mgas=0.234 elapsed=103.071ms mgasp
s=2.271 number=3755 hash=c818a4...1b9c2d cache=94.47kB
```

# Ethereum Test-Chain - „Mist“ - Wallet



# Ethereum Test-Chain - Smart Contract

The screenshot displays the Mist Ethereum wallet interface. At the top, the window title is "Mist" and the menu bar includes "Mist", "Konten", "Bearbeiten", "Ansicht", "Entwicklung", "Fenster", and "Hilfe". The main content area shows the "Ethereum Wallet" with the URL "https://wallet.ethereum.org" and the account address "0x0995f5620c11ccf765dd0fe2188500ecf9aeaae4". Below this, there are tabs for "WALLETS", "SENDEN", and "VERTRÄGE". The "VERTRÄGE" tab is active, showing a balance of "2 025,00 ETHER\*" and a specific contract "SMARTCONTRACT1" with a balance of "0,00 ETHER\*". A blue button labeled "SCHLIESSE VERTRAGSINFORMATIONEN" is visible. Below this, there are two main sections: "VERTRAG AUSLESEN" and "IN VERTRAG SCHREIBEN". The "VERTRAG AUSLESEN" section has a "Name" field containing "Baumann Test - 28.5.2018" and a "Sum" field containing "42". The "IN VERTRAG SCHREIBEN" section has a "Select function" dropdown menu with "Add" selected, a "value - 256 bits unsigned integer" field containing "1234", and an "Execute from" field. On the left sidebar, there is a search icon, a menu icon, and network status information: "0.0 KH/s", "4,460" nodes, and "23s" sync time. A "Private" button is at the bottom left of the sidebar.

# News

---

- => 19.9.2018



# Smart Contract - Code

```
pragma solidity ^0.4.18;

contract MyContract {
    string public name;
    uint256 public sum;

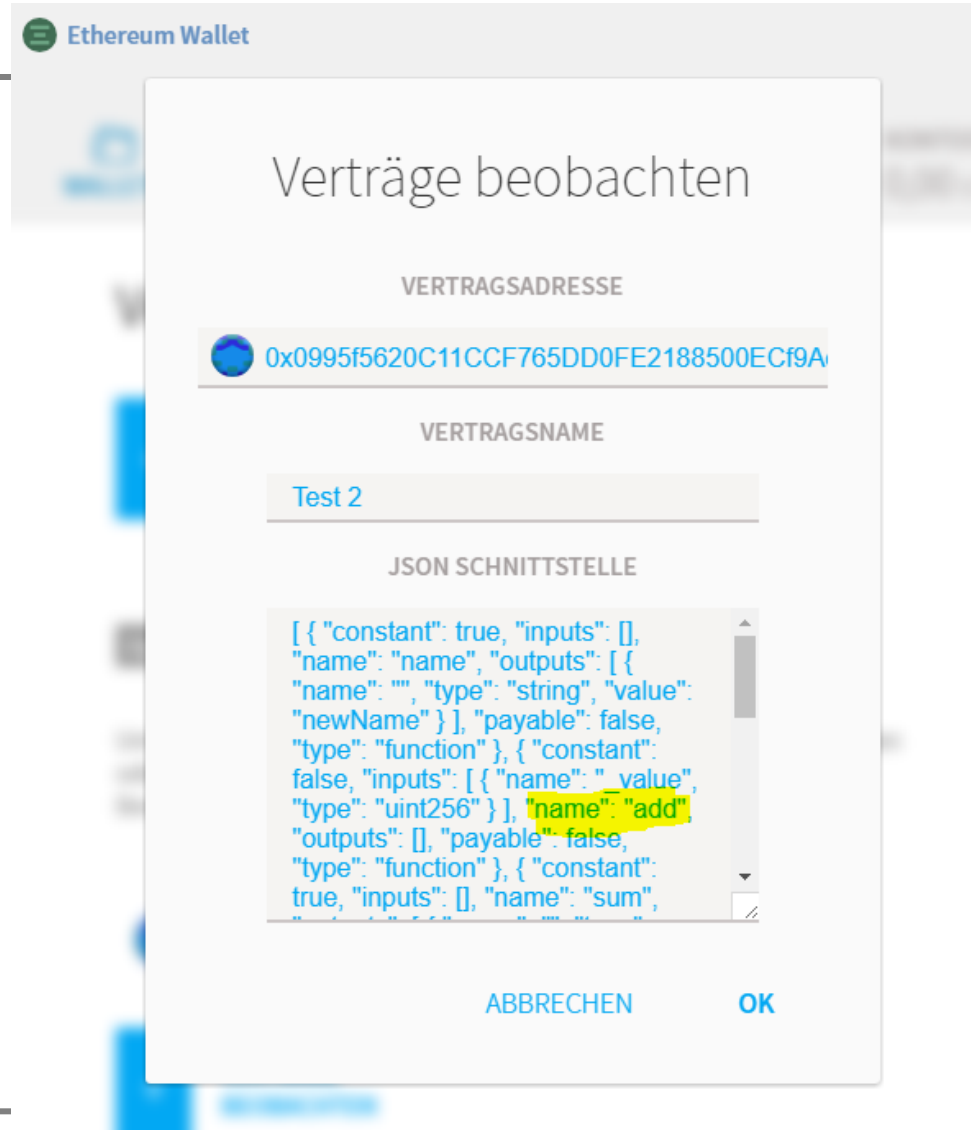
    constructor(uint256 psum, string pname) {
        sum = psum;
        name = pname;
    }

    function add(uint256 _value) {
        sum += _value;
    }

    function setName(string _name) {
        name = _name;
    }
}
```

# Smart Contract – „Beobachten“

- „Installieren“ in eigener Umgebung (Wallet)
- Adresse und Schnittstelle müssen bekannt sein



# Smart Contract - Nutzung

- Aufrufen von definierten Funktionen
- Übergabe von Parameter/n
- Bezahlen der Gebühr ("Gas")
- <http://blockchains.web-lab.at/austriapro/MyContract1.js>

**Vertrag Auslesen**



Name  
Baumann Test 18.9.2018

Sum  
42

**In Vertrag Schreiben**

Select function  
Add ▾

*\_value - 256 bits unsigned integer*  
1

Execute from  
  Account 1 - 5

**AUSFÜHREN**

# Phase 3 - MultiChain

---

- MultiChain - Node
  - Installiert im Lab
  - Web-GUI
- Demo
- Setup eigener Node
- Next Steps

# MultiChain Web-GUI

---

- Node hat kein GUI
  - API Schnittstelle (RPC über https/JSON)
  - => Web-GUI
- <https://blockchains.web-lab.at/austriapro/multichain/>
- Credentials (s.a. Mailing)

# MultiChain Web-GUI

The screenshot displays the MultiChain Web-GUI interface for the AustriaPro Lab node. The browser address bar shows the URL: <https://blockchains.web-lab.at/austriapro/multichain/>. The page title is "MultiChain – AustriaPro Lab (node: ap)".

The interface includes a navigation menu with the following items: Node, Permissions, Asset: Issue | Update, Send, Stream: Create | Publish, View, Blocks, Infos, and a help icon (?).

**This Node**

Name	apro-lab-1
Description	MultiChain apro-lab-1
Version	2.0 alpha 3
Protocol	20003
Node address	apro-lab-1@88.99.145.156:7177
Blocks	128
Peers	1

**Addresses**

Label	ap@fra – <a href="#">change label</a>
Address	1Nvs6cxwXn9K1CQM5Ak7d7aSkwEhyyGcsPzmvV
Permissions	connect, send, receive, issue, create, mine, admin, activate – <a href="#">change</a>

[Get new address](#)

**Connected Nodes**

Node IP address	85.124.9.90
Version/Subver	70002 /MultiChain:0.2.0.3/
Handshake address	1bYr6FsUCYgEZdMj8DT7cdB5Yzw2E8zpNRuv2
Latency	0.130 sec
Connection Time	2018-09-19 07:35:08 GMT
Send: Last / Size	2018-09-19 08:46:19 GMT / 0.07 MB
Recv: Last / Size	2018-09-19 08:46:19 GMT / 0.06 MB

- **Infos**
  - Node, Permissions, Infos, Help
- **Assets**
  - Issue
  - Update
  - Send
- **Streams**
  - Create
  - Publish
  - View
- **Blocks**

# MultiChain Setup Node

---

- Download, Infos, Tutorials ...
  - <https://www.multichain.com/>
  - Aktuell Version 2.0 alpha 4
- In Verzeichnis entpacken
  - oder selbst compilieren ;-)
- Erster Start
  - `multichaind apro-lab-1@88.99.145.156:7177`
  - public key wird angezeigt
  - => an uns senden => Freigabe
- Start
  - `multichaind apro-lab-1`

# MultiChain Next Steps

---

- Sie
  - Node installieren
  - Eigene Entwicklungen?
    - Web-GUI
    - API
  - Basis: <https://github.com/MultiChain>
- Wir
  - Weitere Demos: Wünsche/Vorschläge?
    - (Notarization, Messdaten, Zertifikate ...)
  - Sourcecode auf Labs-Homepage und/oder
  - <https://github.com/austriapro>



# News - 24.10.2018

---

- Notarization (Proof Of Existence)
  - Demo unter Nutzung der „apro-lab-1“ MultiChain
- Demos (Anders Brownworth)
  - Blockchain Demo
  - Public/Private Keys & Signing
- Ausblick / Phase 4
  - “etwas weniger technisch”
  - Blockchain 3.0?

# Usecase - Proof Of Existence

---

- Elektronische Dokumente
  - kopierbar, veränderbar
  - Beweis für Authentizität in realen Welt aufwändig & teuer
- => Notarization („Proof of existence“)
- Beweis, dass ein (elektronisches) Dokument existiert (hat)
  - zu einem bestimmten Zeitpunkt
  - in einer bestimmten Form

# Usecase - Proof Of Existence

## Proof Of Existence (Notarization)

Create Verify

Proof Of Existence - Create

Detaillierte Beschreibung in Deutsch siehe <https://www4.baumann.at/proof-of-existence-auf-basis-blockchain/>.

Notarization ("Proof Of Existence") is the process of storing a hash value of a document ("fingerprint") in a blockchain. The existence and integrity of the document at a certain time can be proven later.

To create a PoE choose a file you want to certify. The file is NOT uploaded to the server, the hash is calculated from your browser locally. Optionally you can enter a remark and choose, if the filename should also be included in the remark.

Select File:

Calculated Hash (SHA256): 60e9b7c8c131703b2d074f6519eec0a13981188ebec92ffb909b2654f4e71b53

Filename: AustriaPro-Blockchain-eDay2018\_V1.ppt

Remarks (optional):

Options:  Include filename

Submit

Proof of Existence successfully published to Blockchain. PLEASE KEEP THIS INFORMATION!

Transaction: 8b7a3f43b3efdb20e94c83c54fe7fb92a4274e9a68fff5ee09d12a3ab5a7d7cf  
Hash: 60e9b7c8c131703b2d074f6519eec0a13981188ebec92ffb909b2654f4e71b53

Additional information:  
Service/Publisher <https://blockchains.web-lab.at/poe/>  
Filename: AustriaPro-Blockchain-eDay2018\_V1.ppt

### Verifying Transaction

Transaction found 8b7a3f43b3efdb20e94c83c54fe7fb92a4274e9a68fff5ee09d12a3ab5a7d7cf

TxID: 8b7a3f43b3efdb20e94c83c54fe7fb92a4274e9a68fff5ee09d12a3ab5a7d7cf  
Hash:  
Data: Service/Publisher <https://blockchains.web-lab.at/poe/>  
Filename: AustriaPro-Blockchain-eDay2018\_V1.ppt  
Time: 2018-04-11 08:13:06 GMT

Blockhash: 00d74fe91b6e2ae4c64bd43c109aba9f3fc5382f7e00f413348784ac0a78f9bb  
Blocktime: 2018-04-11 08:13:06 GMT  
Confirmations: 5

- Beweis
  - Hashwert + Zeitstempel
  - (optional Zusatzinfos)
- Identifikation
  - Hashwert oder
  - TransaktionsID

# Blockchain Demo

Blockchain Demo

Hash

Block

Blockchain

Distributed

Tokens

Coinbase

## SHA256 Hash

Data:

Hash:

## Block

Block: # 1

Nonce:

Data:

Hash:

## Blockchain

Block: # 1

Nonce:

Data:

Prev:

Hash:

Block: # 2

Nonce:

Data:

Prev:

Hash:



# Blockchain 3.0?

---

- 3.0:
  - Schneller, skalierbarer ...
  - Ökonomischer ...
  - Smart contracts ...
- Digital Assets „integriert“
- Waves Plattform
  - „Blockchain for the people“
  - <https://wavesplatform.com/>
- => Obsnetwork
  - „Blockchain for the real world“
  - <https://Obsnetwork.com/>

# Waves / Obsnetwork

---

- Plattform für digitale Geschäftsmodelle
  - Fund Raising
  - Loyalty
  - Tracking/Tracing
  - Supply Chain
  - ...
- Digital Assets („Tokens“) integriert
  - issue, store, manage, trade
- Decentralized Exchange
- Gateways zu Krypto und Fiat-Währungen

# Waves / Obsnetwork – im Lab

---

- Testnet in AustriaPro Lab
  - Client: tbd
  - Node für API Tests: tbd
- Testnet Obs
  - <https://client.testnet-0bsnetwork.com>
  - <https://node1.testnet-0bsnetwork.com>
  - <https://explorer.testnet-0bsnetwork.com>
- Waves
  - <https://wavesplatform.com/>



# Startseite Lab

---

- <https://blockchains.web-lab.at/austriapro/>

## Phase 2: Ethereum based (smart contracts)

### Privates Ethereum Test-Netz

- [Setup-Anleitung](#)
- [Smart Contracts - Beispiel 1](#)

## Phase 3: Multichain

### Node AustriaPro Lab

- [Web-GUI](#)
- [Proof Of Existence - Demo](#)

## Demos

- [Blockchain Demo - By Anders Brownworth](#)
- [Public/Private Keys & Signing - By Anders Brownworth](#)

# Kontakt

---

AUSTRIAPRO

<http://www.austriapro.at>  
[austriapro@wko.at](mailto:austriapro@wko.at)

DI Dr. Christian Baumann  
[c.baumann@baumann.at](mailto:c.baumann@baumann.at)  
+43 664 43 24 243