

# **Einsatz und Vergleich verschiedener Blockchain-Technologien am Beispiel einer Glücksspielanwendung**

---

Masterarbeit von Dany Brossel

# Übersicht

- Projektidee
- Bitcoin
  - Grundlagen
  - Konzept
  - Umsetzung
- Ethereum
  - Grundlagen
  - Konzept
  - Umsetzung
- Fazit

# Projektidee

---

# Projektidee - Glücksspielanwendung

# Projektidee - Glücksspielanwendung

- Durch Einsatz von Blockchain-Technologie benötigtes Vertrauen reduzieren

# Projektidee - Glücksspielanwendung

- Durch Einsatz von Blockchain-Technologie benötigtes Vertrauen reduzieren
- Ziel: Auf Trusted Third Party verzichten

# Projektidee - Glücksspielanwendung

- Durch Einsatz von Blockchain-Technologie benötigtes Vertrauen reduzieren
- Ziel: Auf Trusted Third Party verzichten
- Glücksspielanwendung:
  - N Teilnehmer zahlen gleichen Betrag in Topf ein
  - 1 Teilnehmer wird zufällig ausgewählt und gewinnt

# Projektidee - Glücksspielanwendung

- Durch Einsatz von Blockchain-Technologie benötigtes Vertrauen reduzieren
- Ziel: Auf Trusted Third Party verzichten
- Glücksspielanwendung:
  - N Teilnehmer zahlen gleichen Betrag in Topf ein
  - 1 Teilnehmer wird zufällig ausgewählt und gewinnt
- Anforderungen:
  - Transparente Ein- und Auszahlungen
  - Gewinnerauswahl durch nachprüfbaren Zufallsfaktor
  - Faires Spiel



# Bitcoin

---



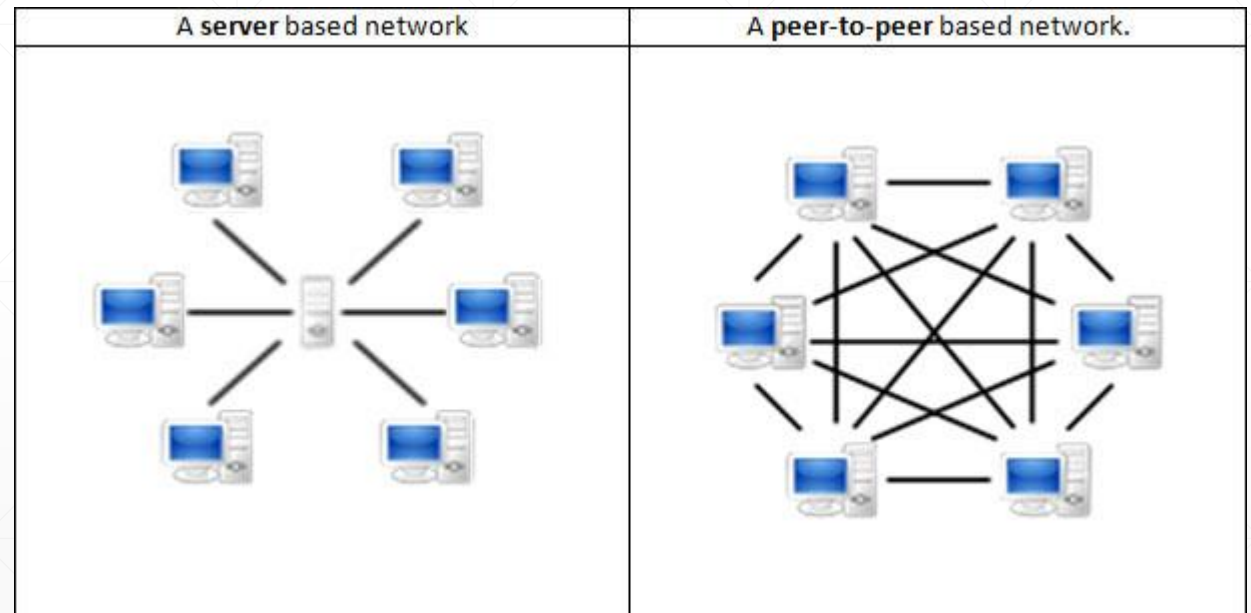
# Bitcoin - Grundlagen

# Bitcoin - Grundlagen

- Bitcoin ist die erste digitale, dezentral organisierte Währung

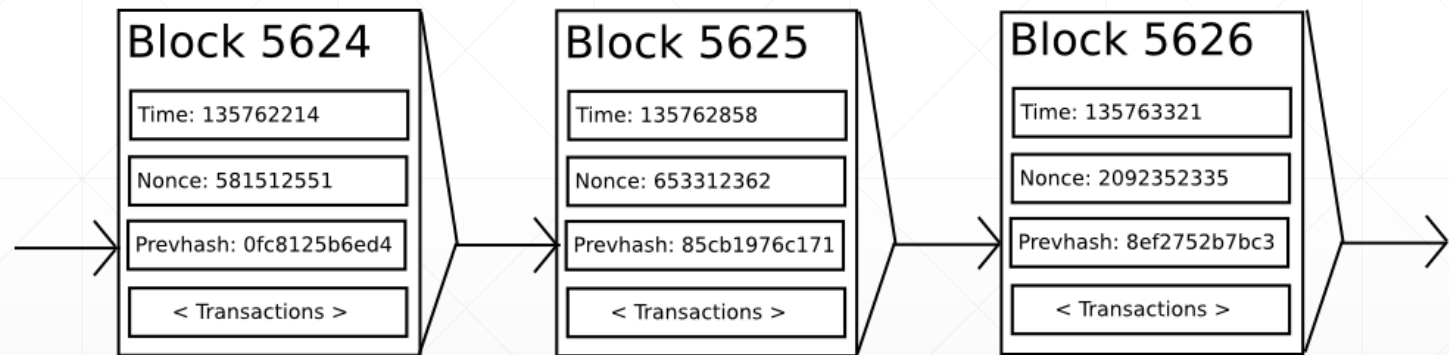
# Bitcoin - Grundlagen

- Bitcoin ist die erste digitale, dezentral organisierte Währung
- Bitcoin besteht aus:
  - Peer-to-Peer Netzwerk



# Bitcoin - Grundlagen

- Bitcoin ist die erste digitale, dezentral organisierte Währung
- Bitcoin besteht aus:
  - Peer-to-Peer Netzwerk
  - Blockchain



# Bitcoin - Grundlagen

- Bitcoin ist die erste digitale, dezentral organisierte Währung
- Bitcoin besteht aus:
  - Peer-to-Peer Netzwerk
  - Blockchain
  - Konsensregeln

## Konsensregeln:

Blockreward  
TXNs OK  
Blockgröße  
Blockzeit  
Blockhash < target  
...

# Bitcoin - Grundlagen

- Bitcoin ist die erste digitale, dezentral organisierte Währung
- Bitcoin besteht aus:
  - Peer-to-Peer Netzwerk
  - Blockchain
  - Konsensregeln

## Konsensregeln:

Blockreward  
TXNs OK  
Blockgröße  
Blockzeit  
Blockhash < target  
...

# Bitcoin - Grundlagen

- Bitcoin ist die erste digitale, dezentral organisierte Währung
- Bitcoin besteht aus:
  - Peer-to-Peer Netzwerk
  - Blockchain
  - Konsensregeln

## Konsensregeln:

Blockreward  
TXNs OK  
Blockgröße  
Blockzeit  
Blockhash < target  
...

Block 5626
Time: 135763321
Nonce: 2092352335
Prevhash: 8ef2752b7bc3
< Transactions >



# Bitcoin - Grundlagen

- Bitcoin ist die erste digitale, dezentral organisierte Währung
- Bitcoin besteht aus:
  - Peer-to-Peer Netzwerk
  - Blockchain
  - Konsensregeln

## Konsensregeln:

Blockreward  
TXNs OK  
Blockgröße  
Blockzeit  
Blockhash < target  
...

Block 5626
Time: 135763321
Nonce: 2092352335
Prevhash: 8ef2752b7bc3
< Transactions >

# Bitcoin - Grundlagen

- Bitcoin ist die erste digitale, dezentral organisierte Währung
- Bitcoin besteht aus:
  - Peer-to-Peer Netzwerk
  - Blockchain
  - Konsensregeln

## Konsensregeln:

Blockreward  
TXNs OK  
Blockgröße  
Blockzeit  
Blockhash < target  
...

Block 5626	
Time: 135763321	
Nonce: 2312755	
Prevhash: 8ef2752b7bc3	
< Transactions >	

# Bitcoin - Grundlagen

- Bitcoin ist die erste digitale, dezentral organisierte Währung
- Bitcoin besteht aus:
  - Peer-to-Peer Netzwerk
  - Blockchain
  - Konsensregeln
  - Proof-of-Work Algorithmus (Mining)



# Bitcoin - Systemzustand

# Bitcoin - Systemzustand

- Systemzustand = Kontobuch

# Bitcoin - Systemzustand

- Systemzustand = Kontobuch
- Wem (welcher Adresse) gehören wie viele Bitcoin?

# Bitcoin - Systemzustand

- Systemzustand = Kontobuch
- Wem (welcher Adresse) gehören wie viele Bitcoin?
- Systemzustand wird durch Transaktionen angepasst.

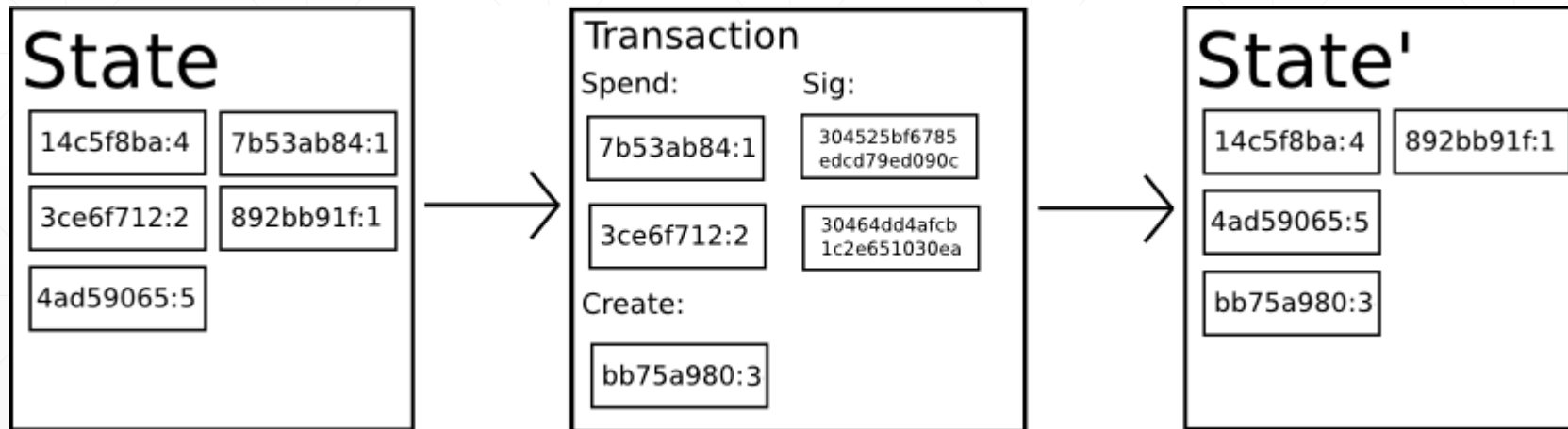
# Bitcoin - Systemzustand

- Systemzustand = Kontobuch
- Wem (welcher Adresse) gehören wie viele Bitcoin?
- Systemzustand wird durch Transaktionen angepasst.

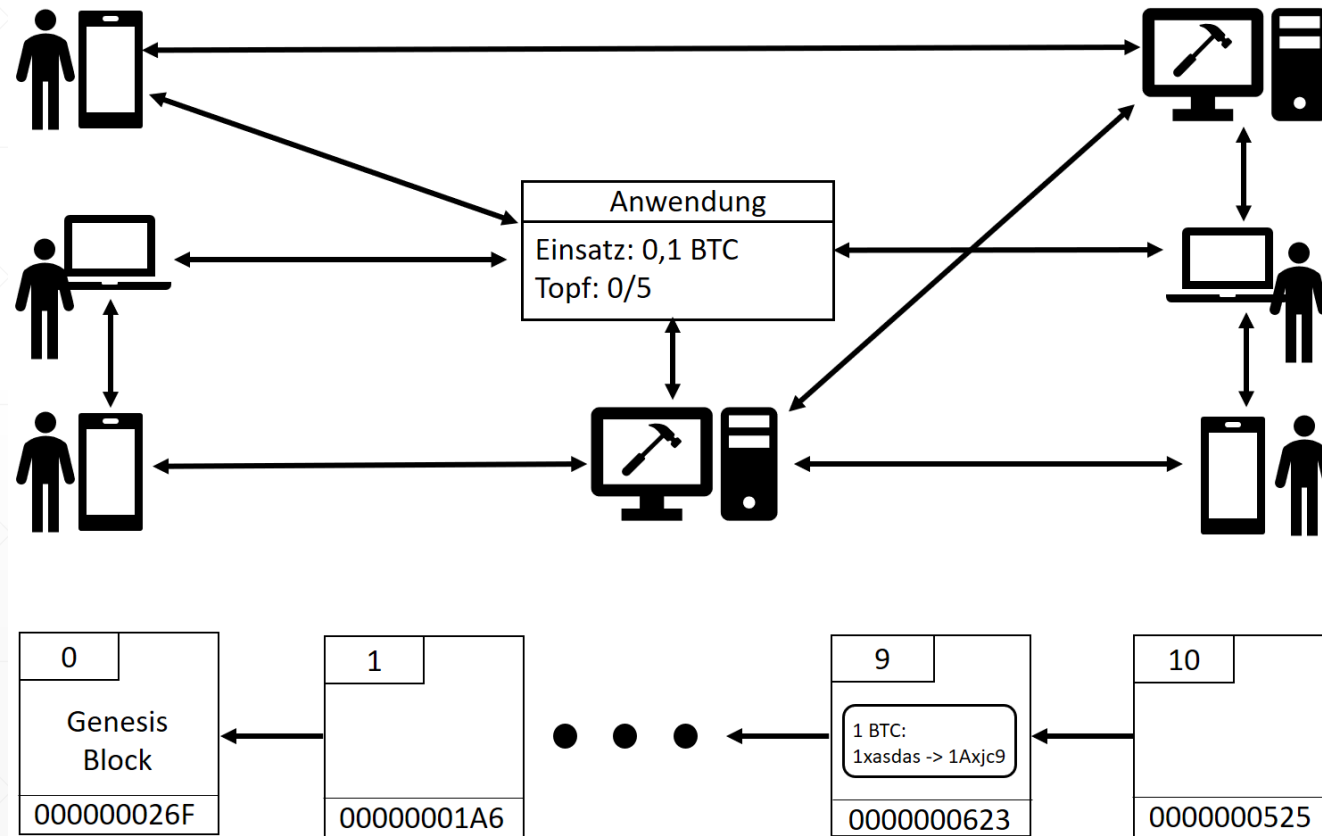


# Bitcoin - Systemzustand

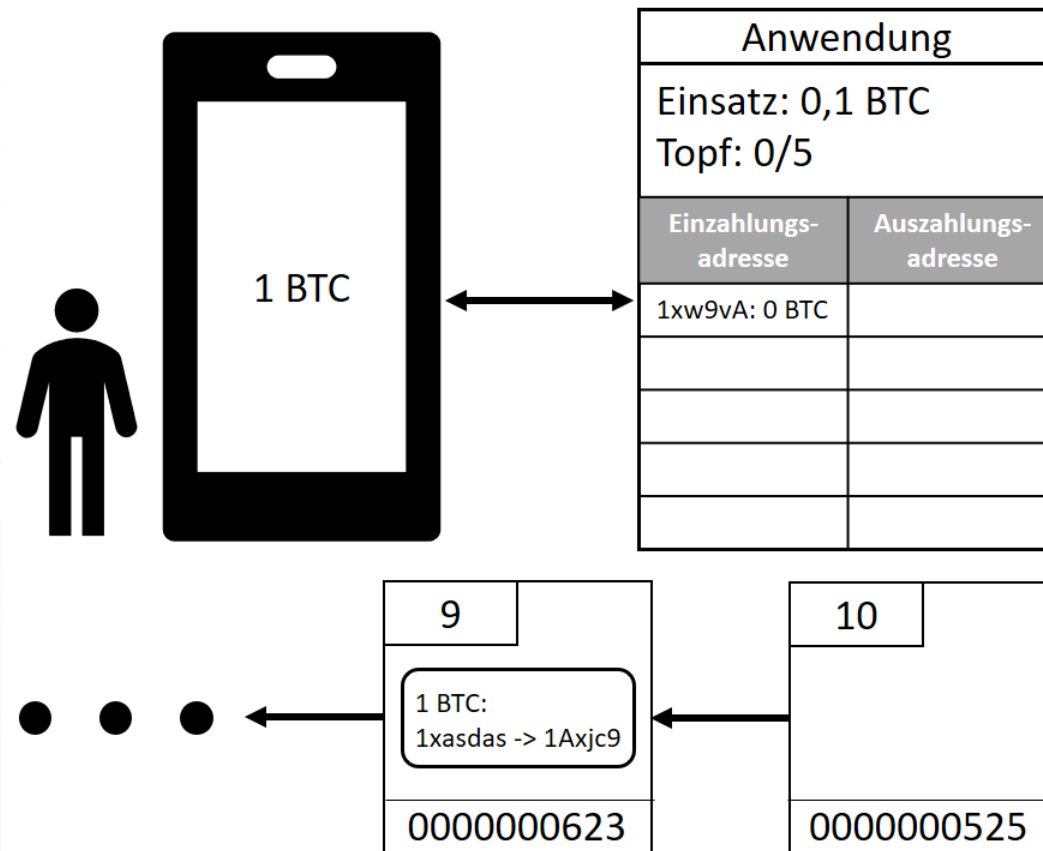
- Systemzustand = Kontobuch
- Wem (welcher Adresse) gehören wie viele Bitcoin?
- Systemzustand wird durch Transaktionen angepasst.



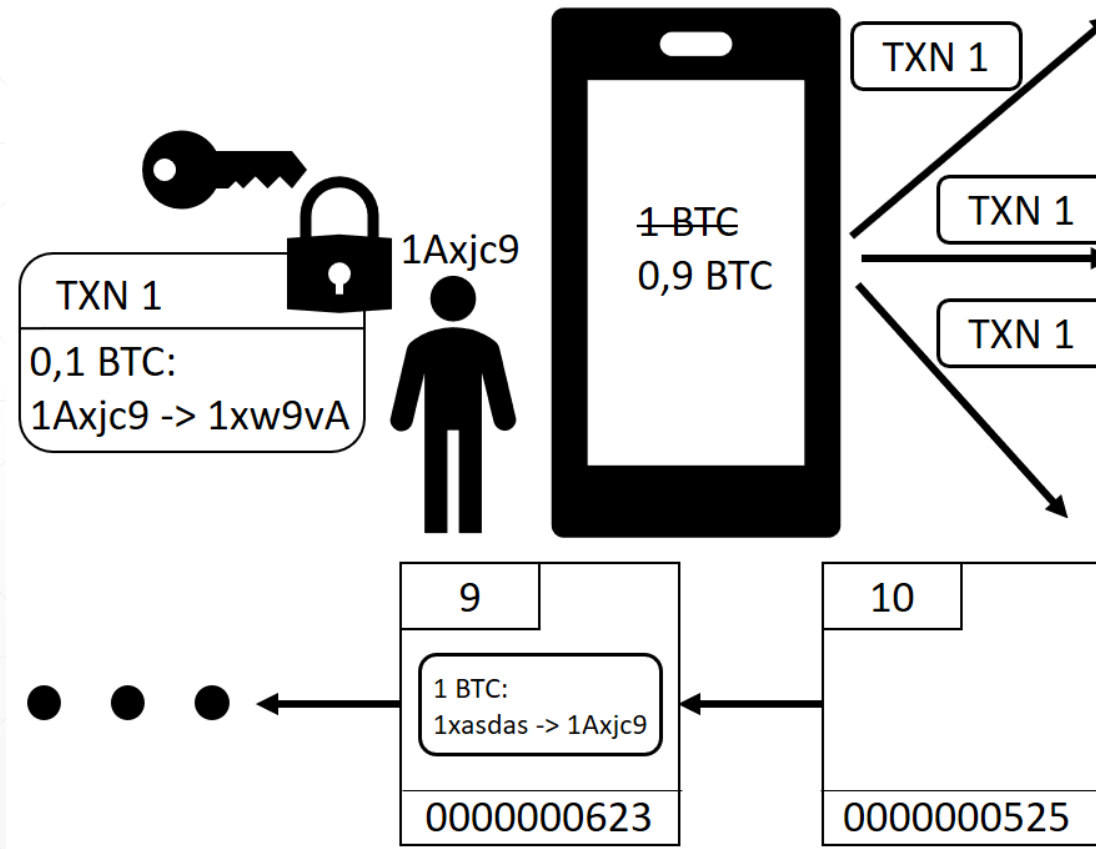
# Bitcoin - Konzept der Glücksspielanwendung



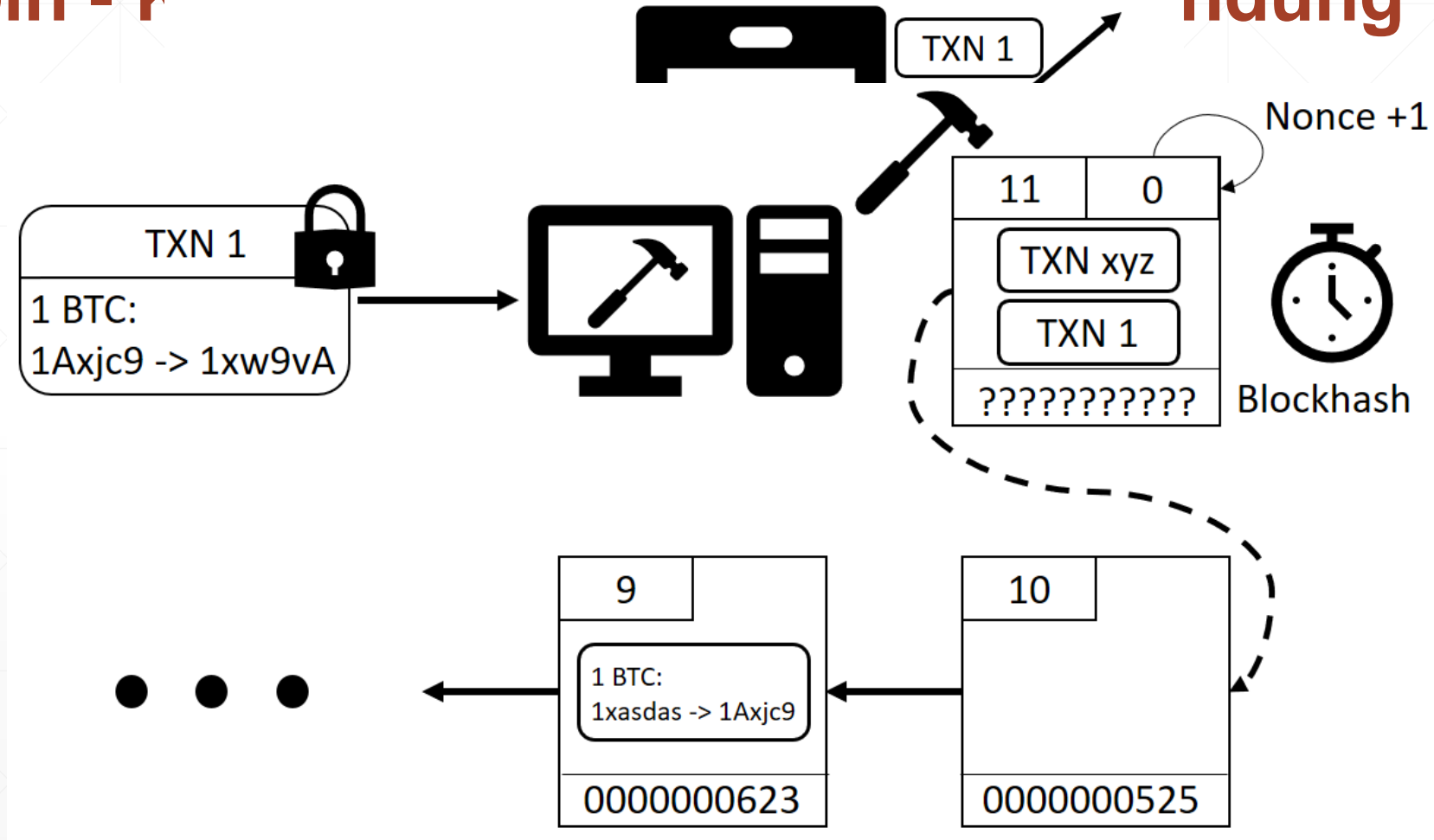
# Bitcoin - Konzept der Glücksspielanwendung



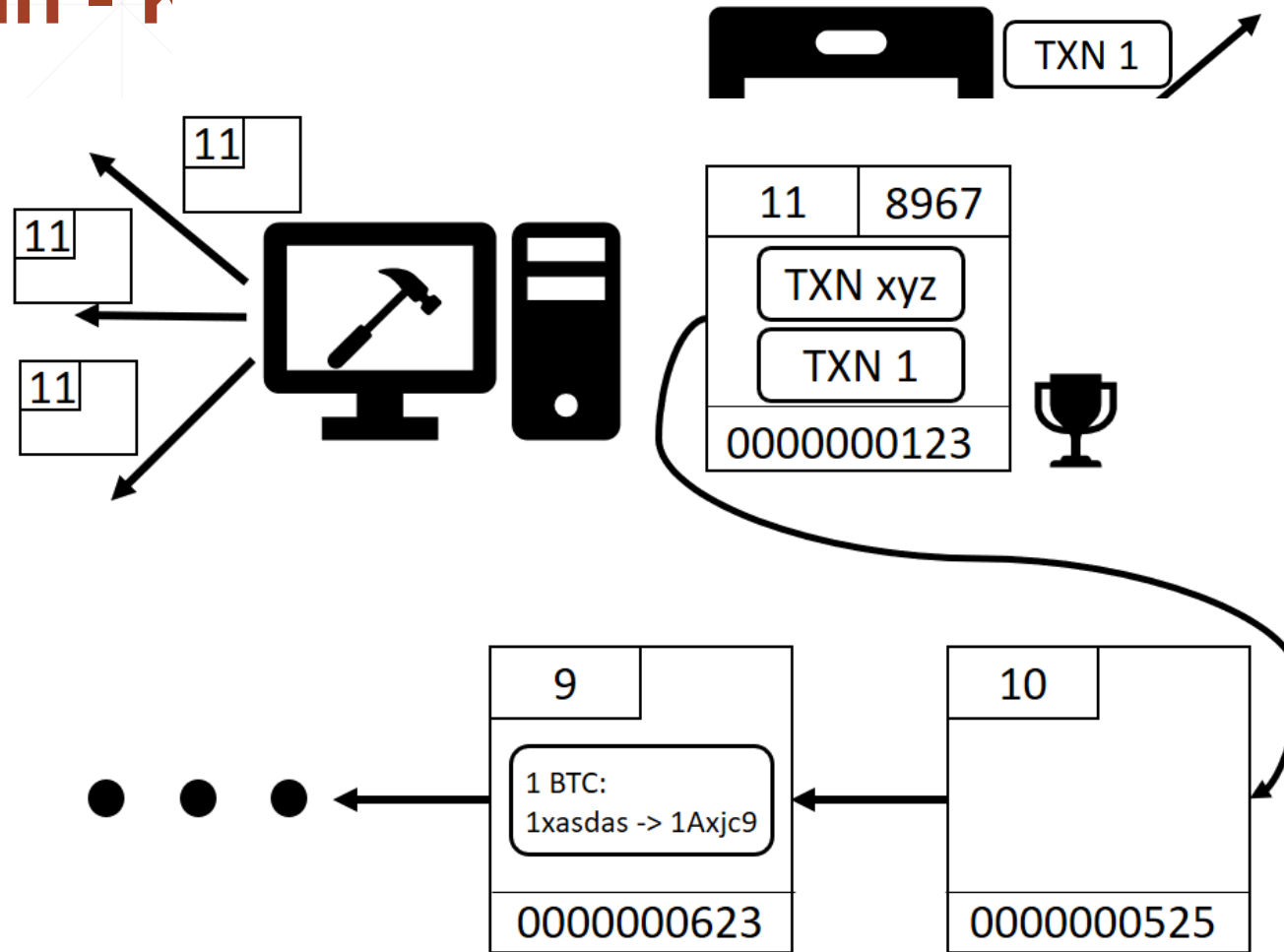
# Bitcoin - Konzept der Glücksspielanwendung



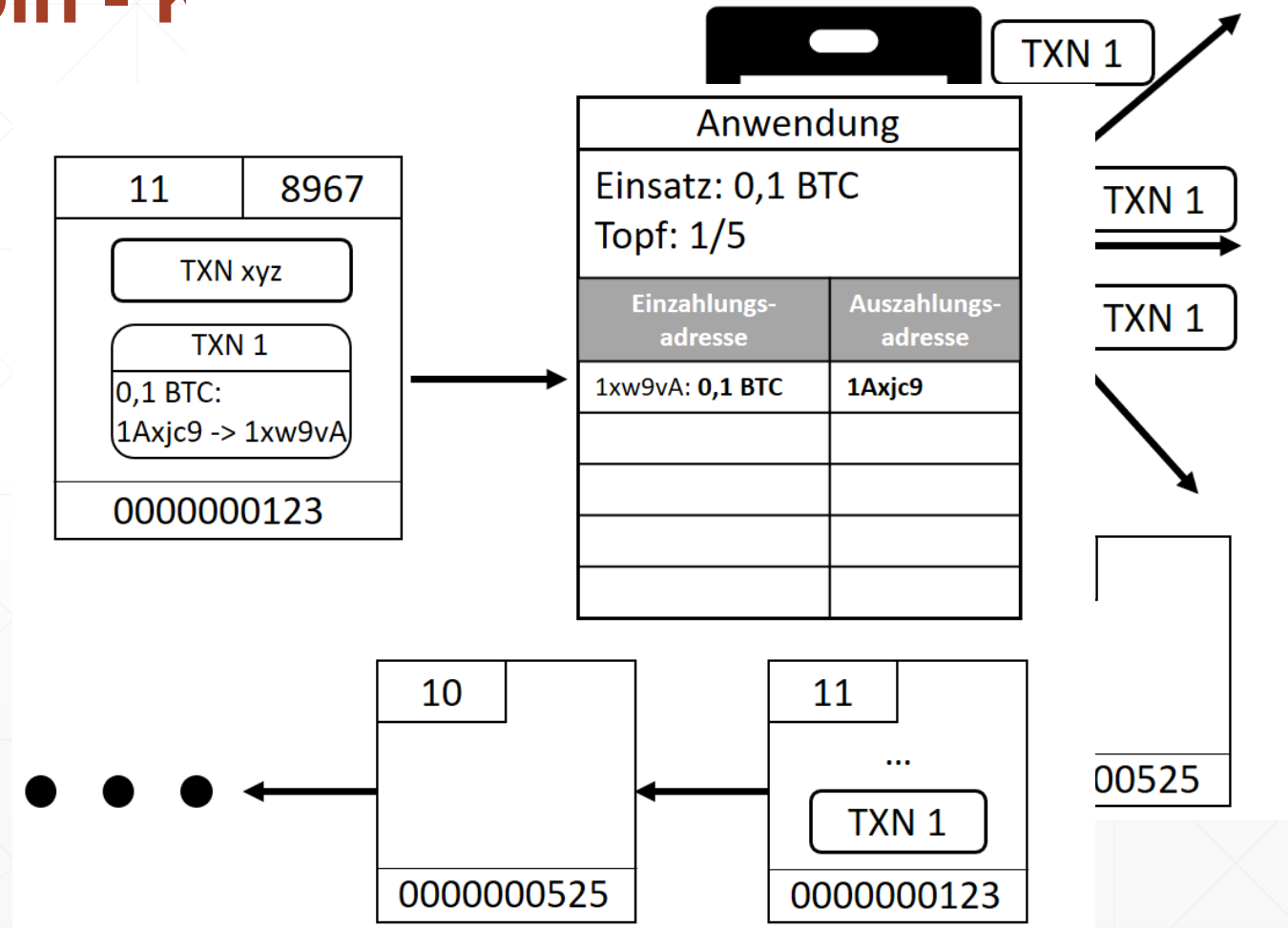
# Bitcoin - Konzept der Glücksspielanwendung



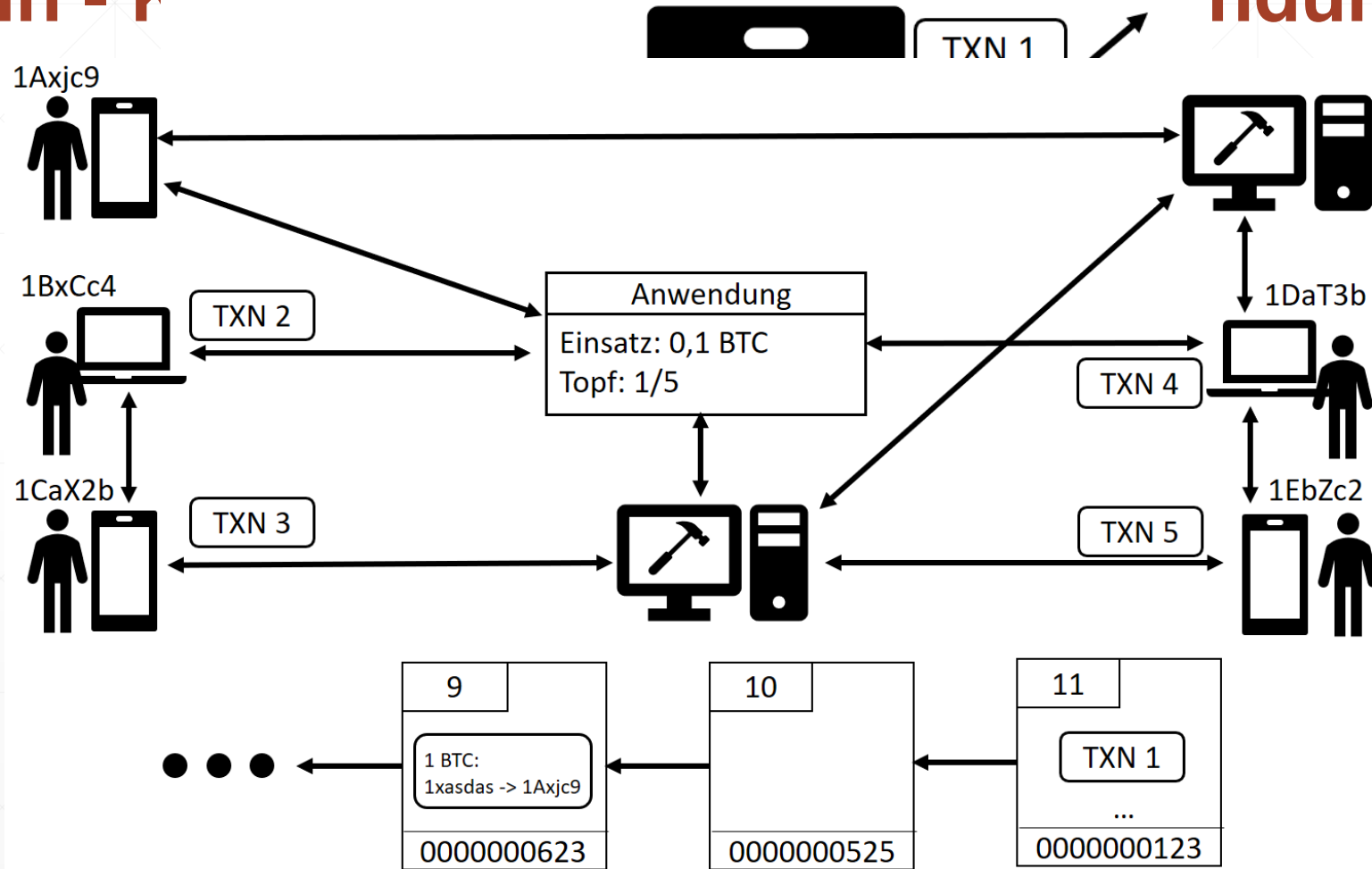
# Bitcoin - Konzept der Glücksspielanwendung



# Bitcoin - Konzept der Glücksspielanwendung



# Bitcoin - Konzept der Glücksspielanwendung





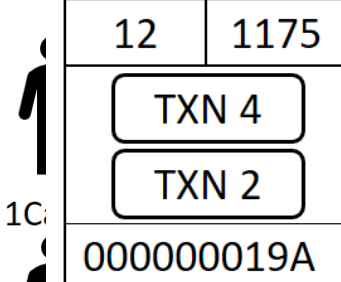
Bitcoin

1Axjc9



g

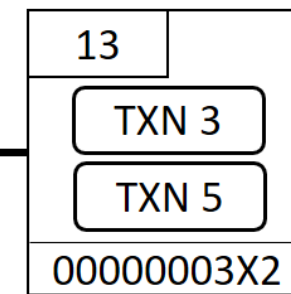
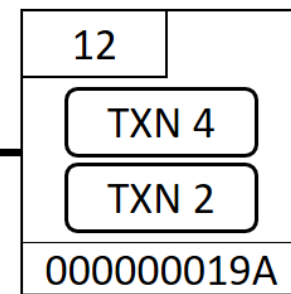
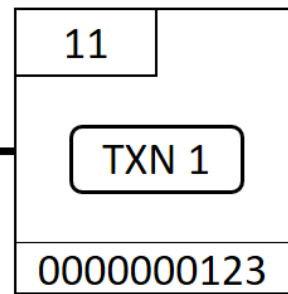
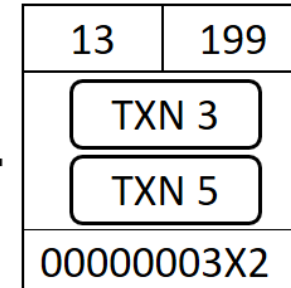
1B



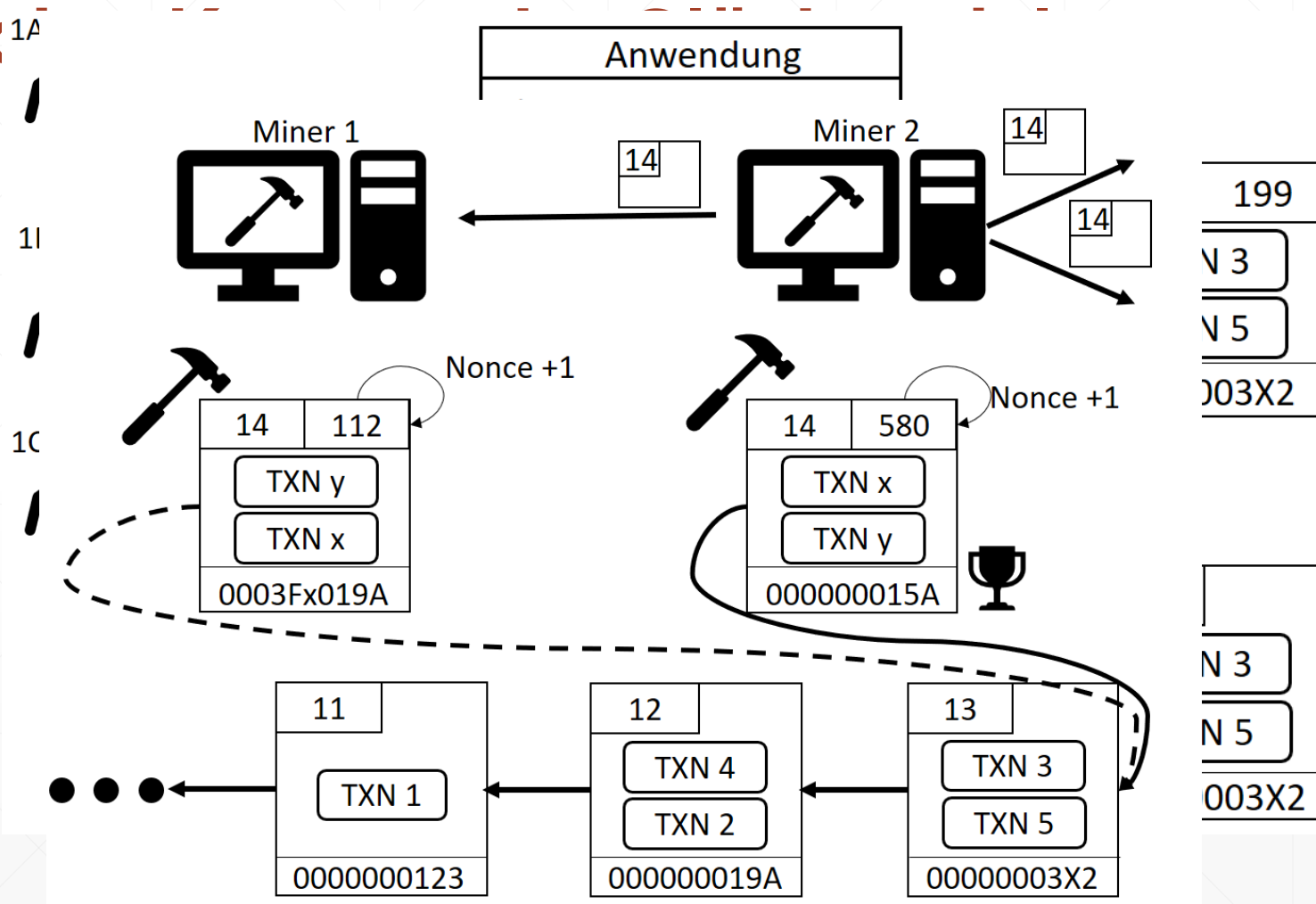
1C

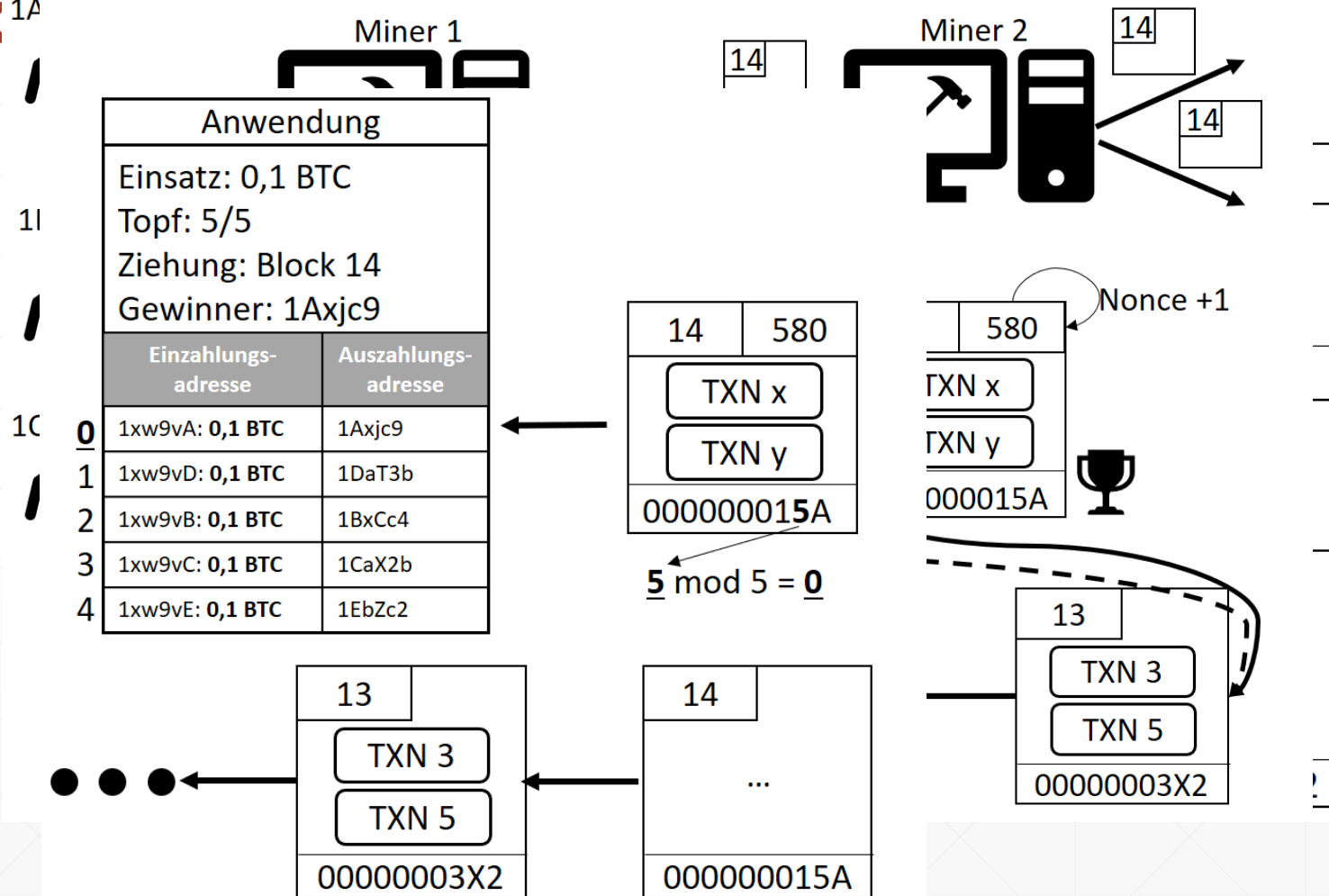


Anwendung	
Einsatz: 0,1 BTC Topf: 5/5	
Einzahlungs- adresse	Auszahlungs- adresse
1xw9vA: 0,1 BTC	1Axjc9
1xw9vD: 0,1 BTC	1DaT3b
1xw9vB: 0,1 BTC	1BxCc4
1xw9vC: 0,1 BTC	1CaX2b
1xw9vE: 0,1 BTC	1EbZc2

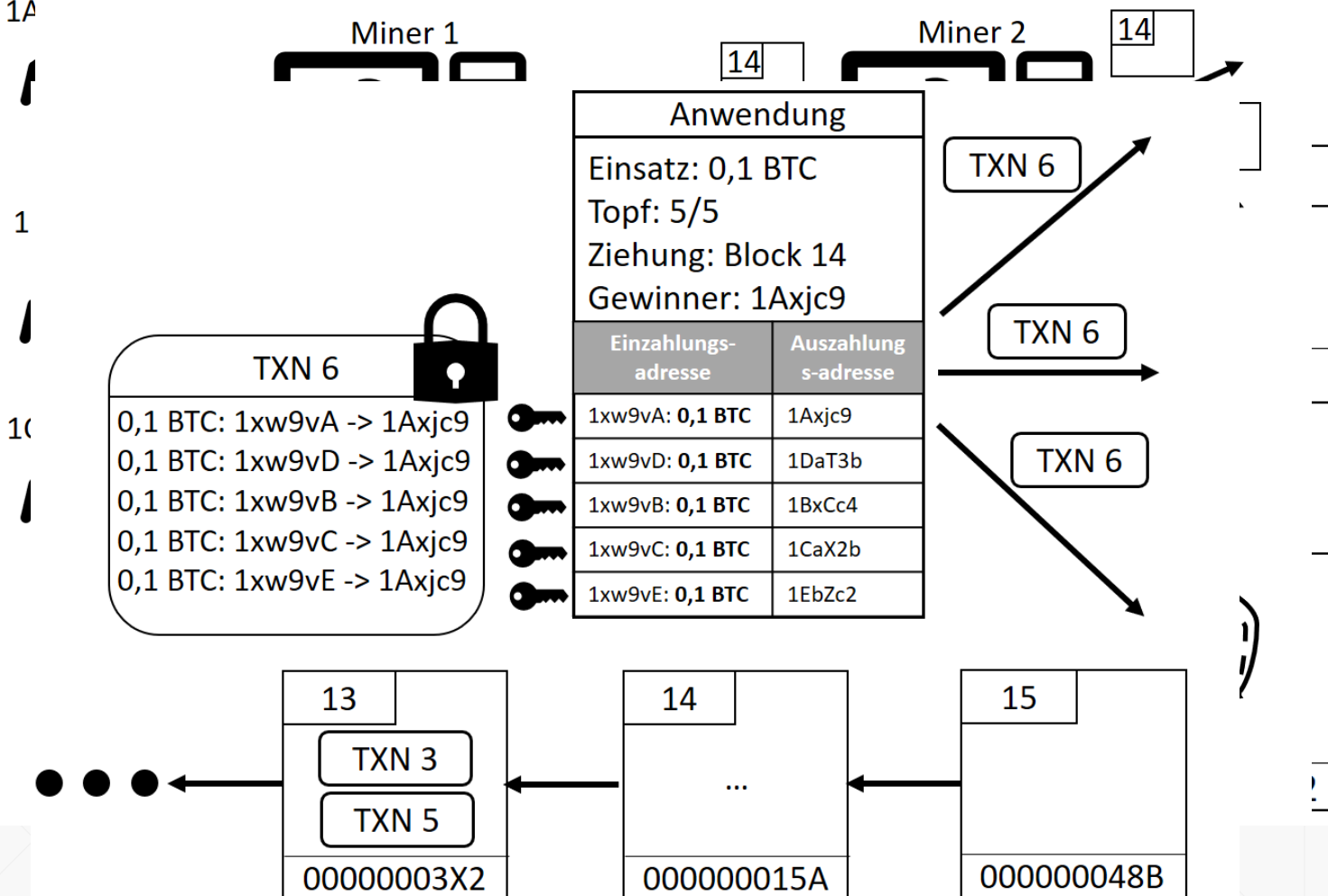


# Bitcoin

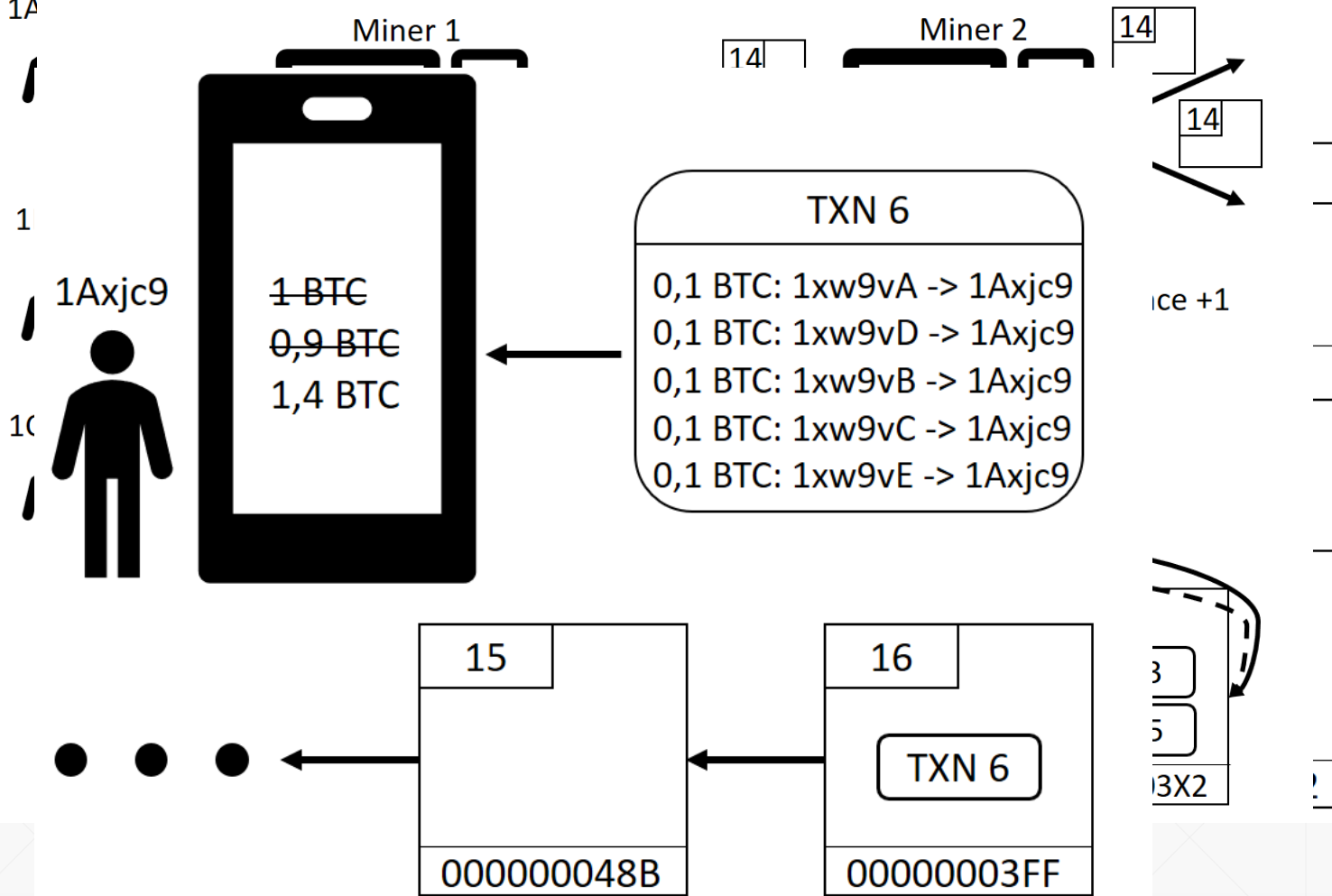




# Bitcoin



# Bitcoin



# Bitcoin - Umsetzung

# Bitcoin - Umsetzung



# Bitcoin - Umsetzung

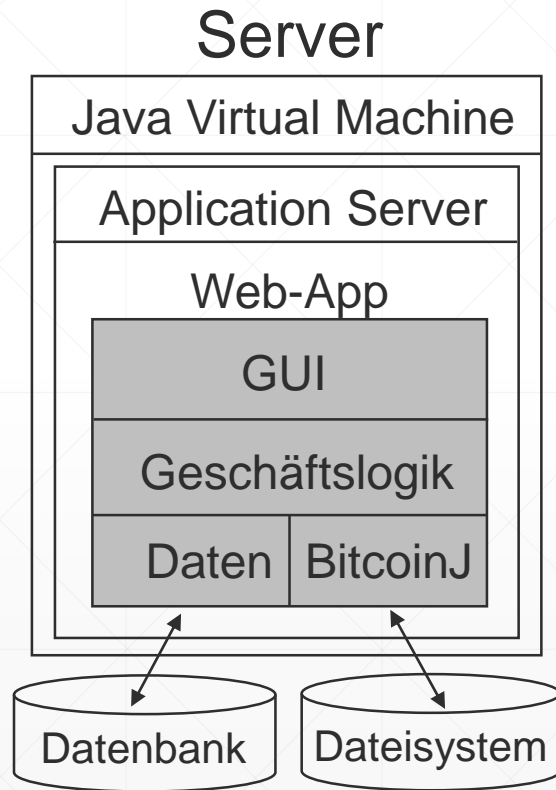




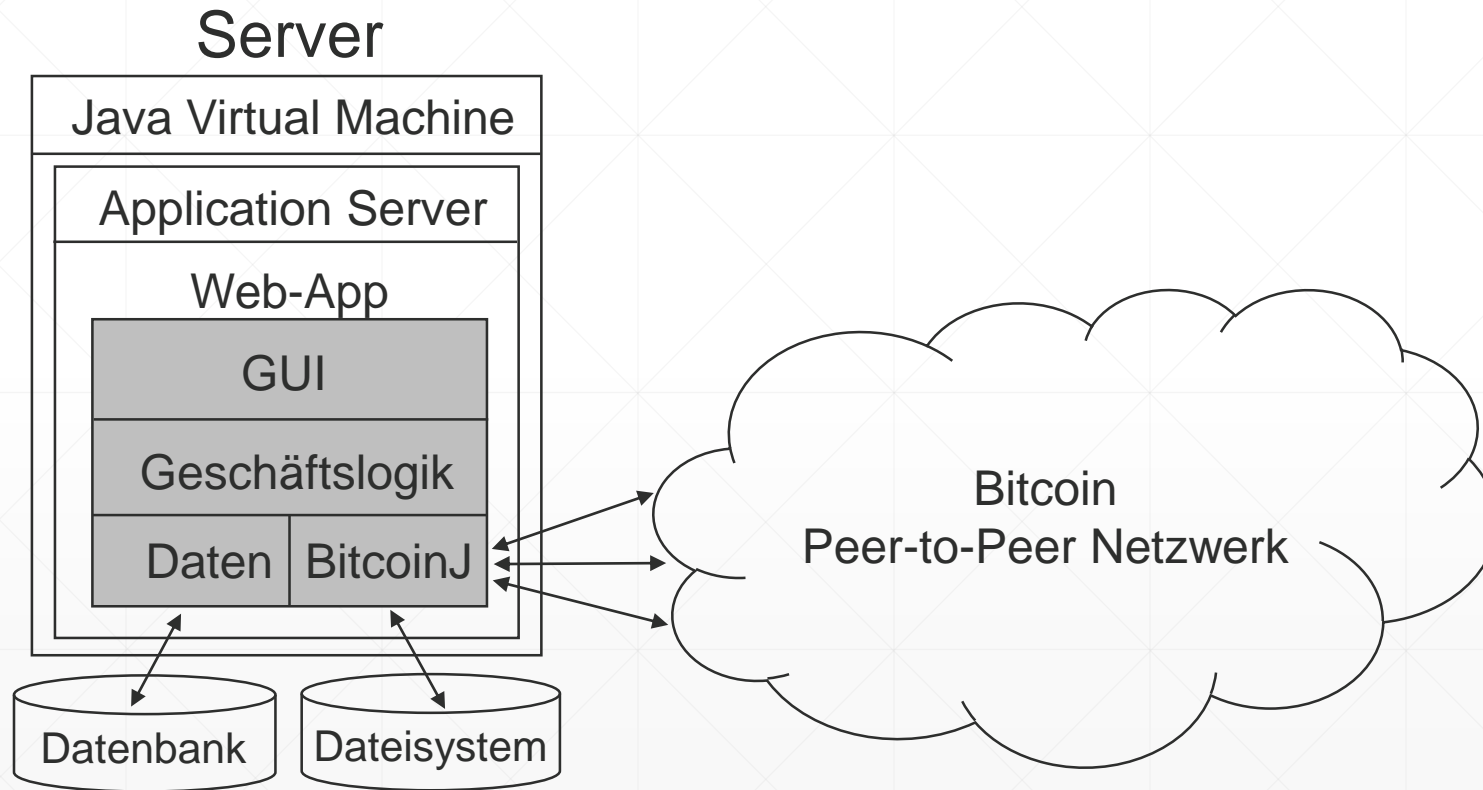
# Bitcoin - Umsetzung



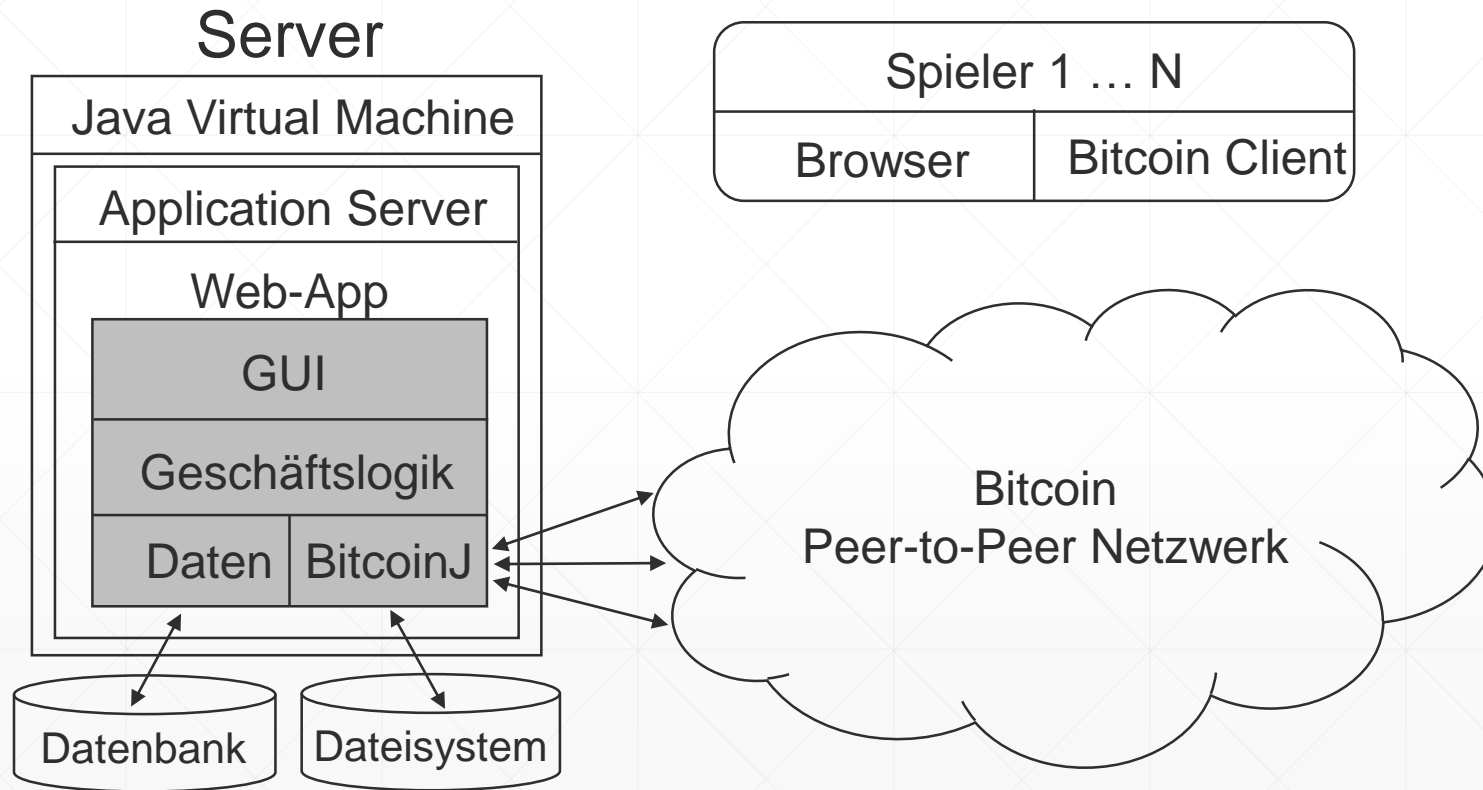
# Bitcoin - Umsetzung



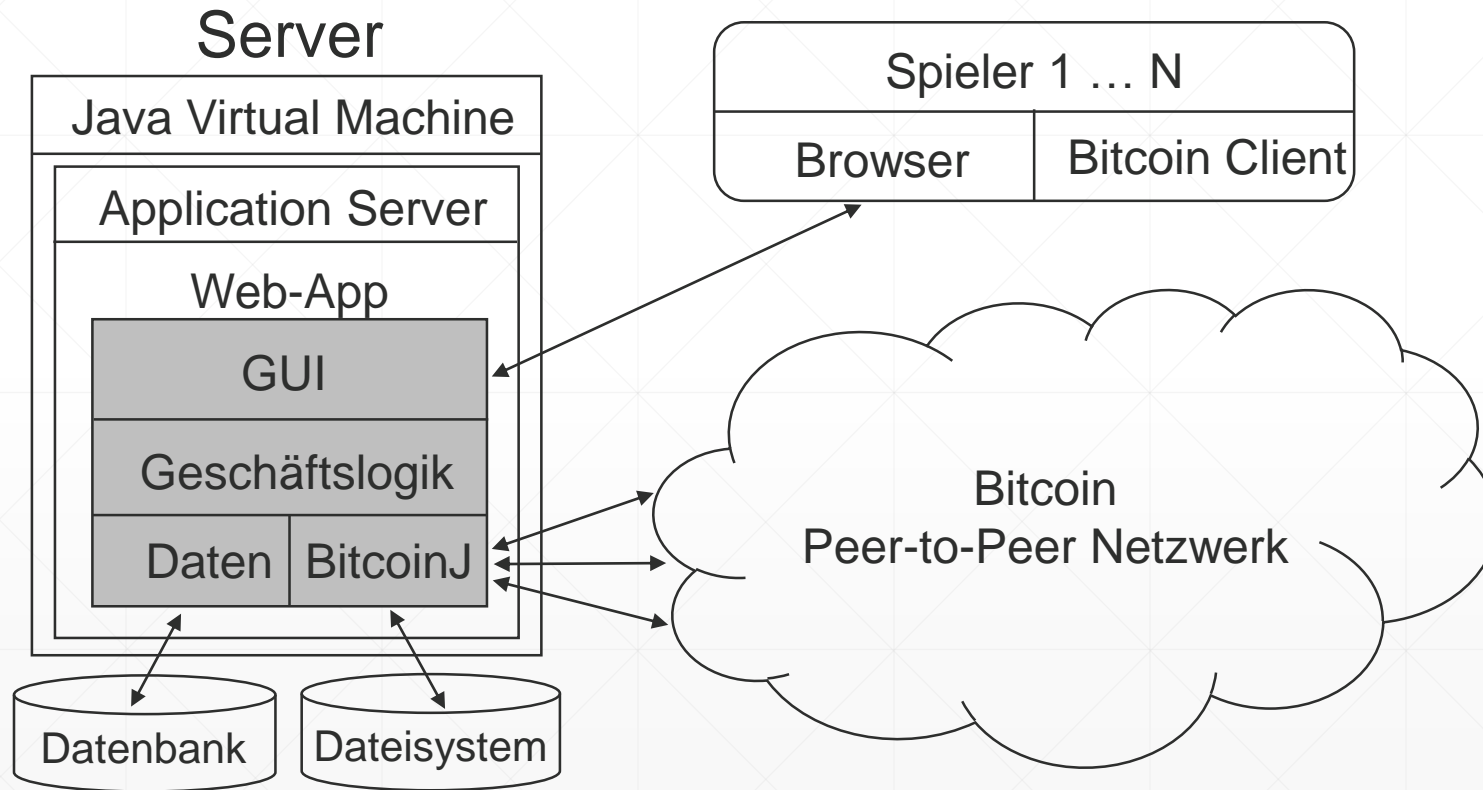
# Bitcoin - Umsetzung



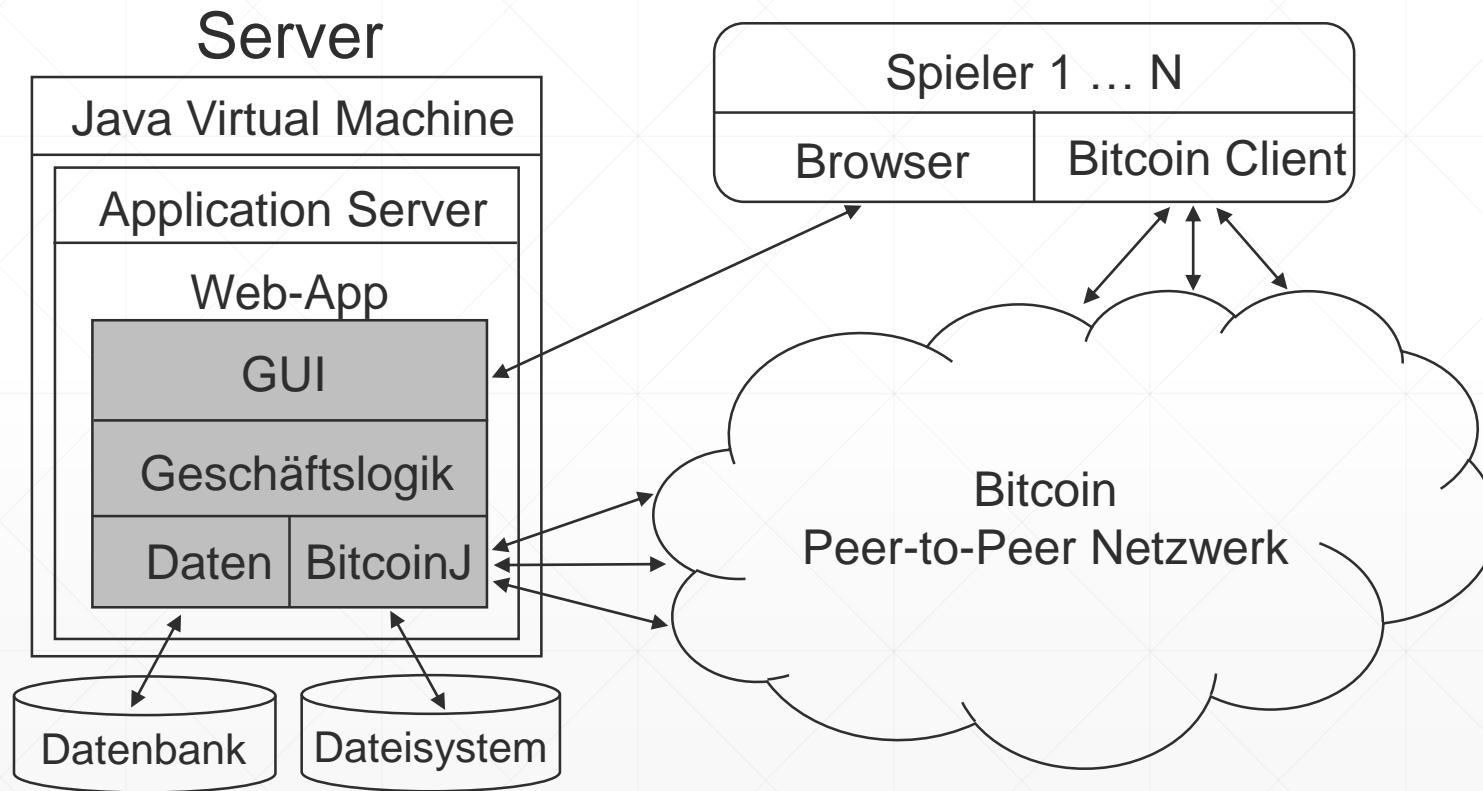
# Bitcoin - Umsetzung



# Bitcoin - Umsetzung




# Bitcoin - Umsetzung




# Bitcoin - Glücksspielanwendung

Block Height: 12878067186,8€ / BTCFr, 9 Mär 2018 19:04:19

 **Bitcoin Testnet**

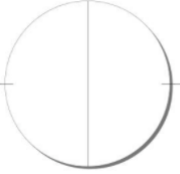
My deposits:

 Deposit address `muQrtRbvGLtyVGZWVZq6rryHmS1nmFu3Xk` received 0!

Pot open. Waiting for 2 more participants.

0.001 BTC / slot


open slot 2



open slot 1

Participants:  
No one joined this pot yet. You could be the first participant.

[Join Pot](#)



Send 100000 Satoshi to `muQrtRbvGLtyVGZWVZq6rryHmS1nmFu3Xk` to participate in the current pot.

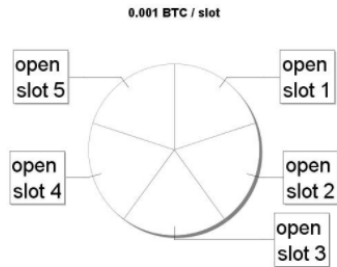
[Close](#)

# Bitcoin - Glücksspielanwendung

My deposits:

✓ Deposit address [muQrtRbvGLtyVGZWVZq6rryHmS1nmFu3Xk](#) received 100000! Payout address: [n31K7LM9gEsPKHUXmTirv64w46SDh7zSuz](#)

Pot open. Waiting for 5 more participants.



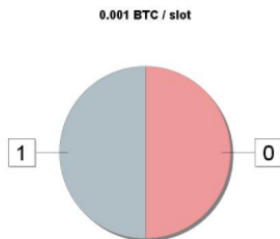
Participants:

No one joined this pot yet. You could be the first participant.

Join Pot

## Closed Pots

Pot closed. Waiting for block 1287811 to select the winner.



	Block Height	Block Hash
Payout	1287811	000000000000D7A2??06A?F??F2?45??0?6C2?2??1419??C2?8AA9??475
Closing	1287810	00000000a06c09f06dd471495a584688e6d4effe9192b9240154fab3c7abd46c

Participants:

✓ (0) : Deposit address [muQrtRbvGLtyVGZWVZq6rryHmS1nmFu3Xk](#) received 100000 Satoshi. Payout address: [n31K7LM9gEsPKHUXmTirv64w46SDh7zSuz](#)

✓ (1) : Deposit address [n4M9auRrATMBkAbY6X6xnGpxHkbvCdGYgC](#) received 100000 Satoshi. Payout address: [mznU6hNqaitg7psTFoVZCwFygAw7gbaM8w](#)





# Ethereum

---

# Ethereum - Grundlagen

# Ethereum - Grundlagen

- Ethereum ist genau wie Bitcoin ein **Peer-to-Peer Netzwerk**, das eine öffentliche **Blockchain** besitzt und einen **Systemzustand** verwaltet.

# Ethereum - Grundlagen

- Ethereum ist genau wie Bitcoin ein **Peer-to-Peer Netzwerk**, das eine öffentliche **Blockchain** besitzt und einen **Systemzustand** verwaltet.

# Ethereum - Grundlagen

- Ethereum ist genau wie Bitcoin ein **Peer-to-Peer Netzwerk**, das eine öffentliche **Blockchain** besitzt und einen **Systemzustand** verwaltet.
- Dazu werden genau wie bei Bitcoin ein **Proof-of-Work Algorithmus** und **Konsensregeln** verwendet.

# Ethereum - Grundlagen

- Ethereum ist genau wie Bitcoin ein **Peer-to-Peer Netzwerk**, das eine öffentliche **Blockchain** besitzt und einen **Systemzustand** verwaltet.
- Dazu werden genau wie bei Bitcoin ein **Proof-of-Work Algorithmus** und **Konsensregeln** verwendet.
- Ethereum besitzt eine generalisierte Blockchain, die nicht nur Finanztransaktionen speichern kann, sondern auch **Smart Contracts**.  
**Smart Contracts**

# Ethereum - Grundlagen

- Ethereum ist genau wie Bitcoin ein **Peer-to-Peer Netzwerk**, das eine öffentliche **Blockchain** besitzt und einen **Systemzustand** verwaltet.
  - Dazu werden genau wie bei Bitcoin ein **Proof-of-Work Algorithmus** und **Konsensregeln** verwendet.
  - Ethereum besitzt eine generalisierte Blockchain, die nicht nur Finanztransaktionen speichern kann, sondern auch **Smart Contracts**.
- Smart Contracts**

# Ethereum - Grundlagen

- Ethereum ist genau wie Bitcoin ein **Peer-to-Peer Netzwerk**, das eine öffentliche **Blockchain** besitzt und einen **Systemzustand** verwaltet.
- Dazu werden genau wie bei Bitcoin ein **Proof-of-Work Algorithmus** und **Konsensregeln** verwendet.
- Ethereum besitzt eine generalisierte Blockchain, die nicht nur Finanztransaktionen speichern kann, sondern auch **Smart Contracts**.  
Smart Contracts



# Ethereum – Accounts & Smart Contracts

# Ethereum – Accounts & Smart Contracts

- Accounts:

# Ethereum – Accounts & Smart Contracts

- Accounts:
  - 20 Byte lange Adresse

# Ethereum – Accounts & Smart Contracts

- Accounts:
  - 20 Byte lange Adresse
  - Kontostand in Ether

# Ethereum – Accounts & Smart Contracts

- Accounts:
  - 20 Byte lange Adresse
  - Kontostand in Ether
  - Nonce-Wert

# Ethereum – Accounts & Smart Contracts

- Accounts:
  - 20 Byte lange Adresse
  - Kontostand in Ether
  - Nonce-Wert
  - Smart Contract Code (optional)

# Ethereum – Accounts & Smart Contracts

- Accounts:
  - 20 Byte lange Adresse
  - Kontostand in Ether
  - Nonce-Wert
  - Smart Contract Code (optional)
  - Speicherplatz (optional)

# Ethereum – Accounts & Smart Contracts

- Accounts:
  - 20 Byte lange Adresse
  - Kontostand in Ether
  - Nonce-Wert
  - Smart Contract Code (optional)
  - Speicherplatz (optional)
- Smart Contracts:



# Ethereum – Accounts & Smart Contracts

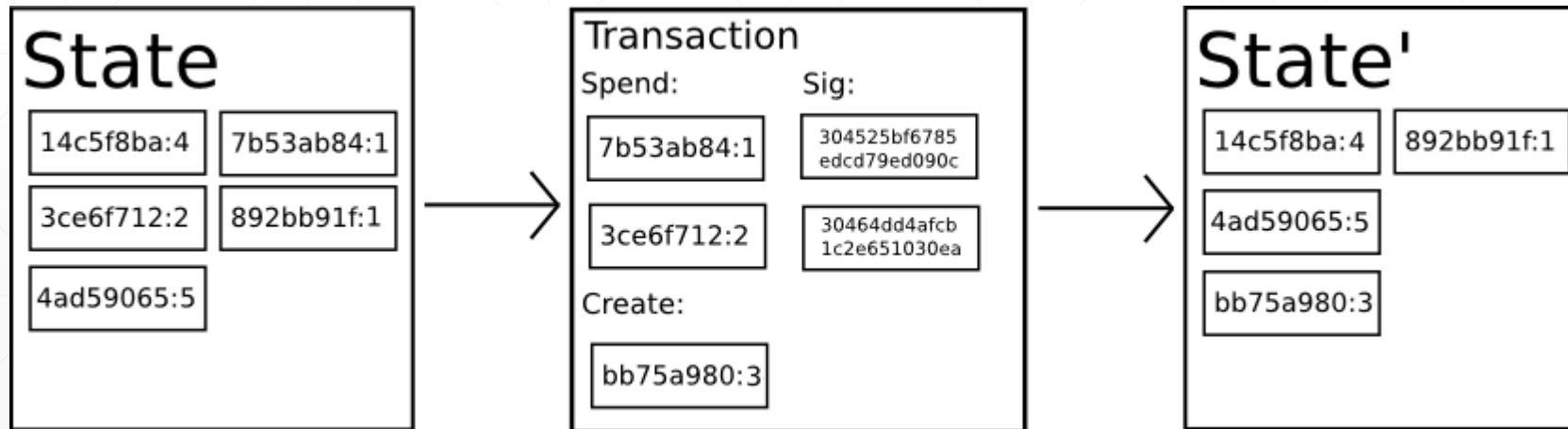
- Accounts:
  - 20 Byte lange Adresse
  - Kontostand in Ether
  - Nonce-Wert
  - Smart Contract Code (optional)
  - Speicherplatz (optional)
- Smart Contracts:
  - Programm Code in der Blockchain, der dezentral vom Netzwerk ausgeführt wird.

# Ethereum – Accounts & Smart Contracts

- Accounts:
  - 20 Byte lange Adresse
  - Kontostand in Ether
  - Nonce-Wert
  - Smart Contract Code (optional)
  - Speicherplatz (optional)
- Smart Contracts:
  - Programm Code in der Blockchain, der dezentral vom Netzwerk ausgeführt wird.
  - Verwaltet Zustand des zugehörigen Ethereum Accounts

# Bitcoin - Systemzustand (Wiederholung)

- Systemzustand = Kontobuch
- Wem (welcher Adresse) gehören wie viele Bitcoin?
- Systemzustand wird durch Transaktion verändert.



# Ethereum - Systemzustand

# Ethereum - Systemzustand

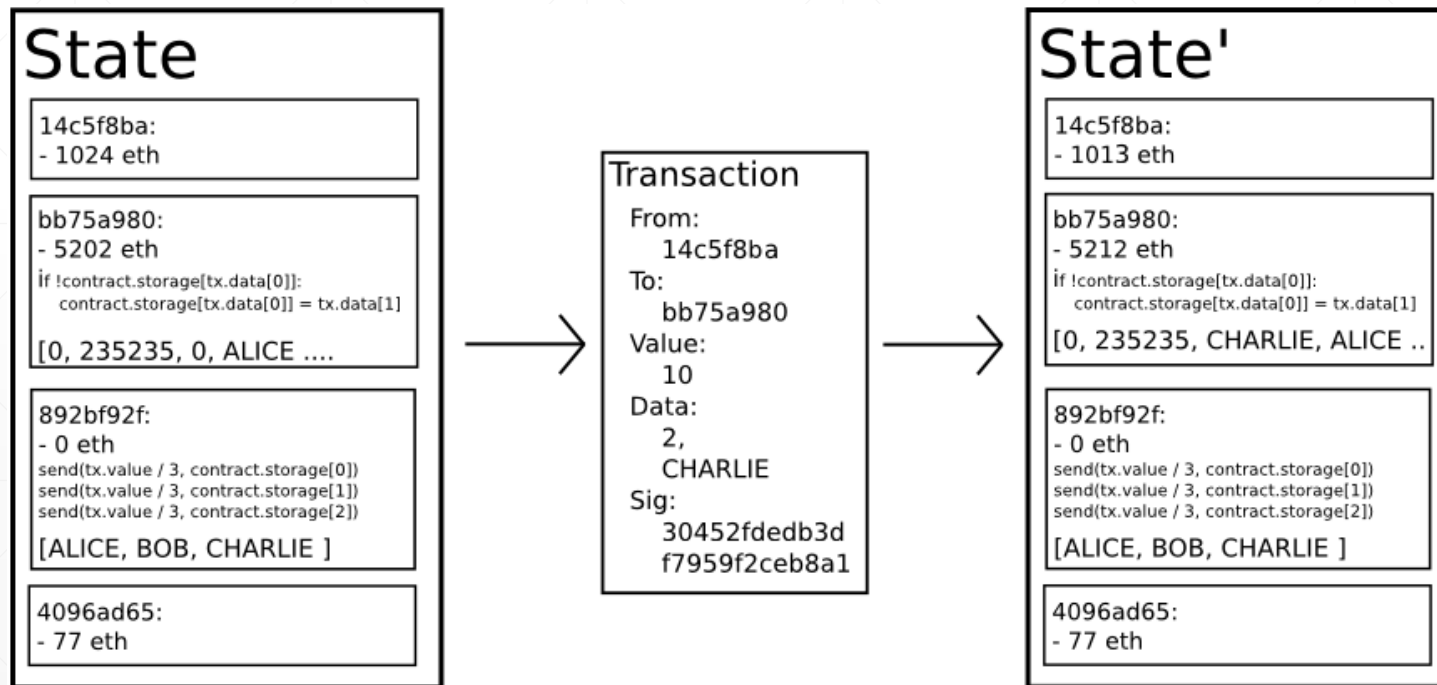
- Systemzustand = Zustand aller Ethereum Accounts

# Ethereum - Systemzustand

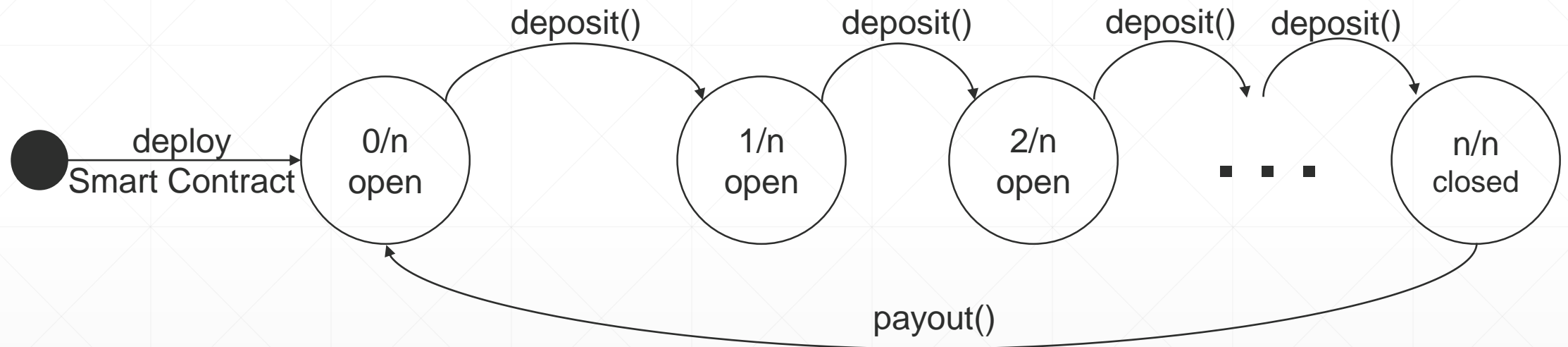
- Systemzustand = Zustand aller Ethereum Accounts
- Systemzustand wird durch Transaktionen verändert.

# Ethereum - Systemzustand

- Systemzustand = Zustand aller Ethereum Accounts
- Systemzustand wird durch Transaktionen verändert.



# Ethereum - Konzept





# Ethereum - Smart Contract

```
pragma solidity ^0.4.0;
contract TrustlessGambling {
    // constants
    uint8 public constant NBR_OF_SLOTS =3;
    uint public constant EXPECTED_POT_AMOUNT=1000;// WEI
    uint8 public constant PAYOUT_BLOCK_OFFSET =1;
    // pot values
    uint public nbrOfParticipants;
    address[NBR_OF_SLOTS] public depositAddresses;
    address[NBR_OF_SLOTS] public payoutAddresses;
    uint public closingBlockNumber;
    uint public payoutBlockNumber;
    bytes32 public payoutBlockHash;
    uint public winner; // 0 -> NBR_OF_SLOTS-1
    bool public potClosed;
    uint public nbrOfMissedPayouts;
    // constructor
    function TrustlessGambling() public {
        nbrOfParticipants = 0;
        potClosed = false;
        nbrOfMissedPayouts = 0;
    }
}
```

# Ethereum - Smart Contract

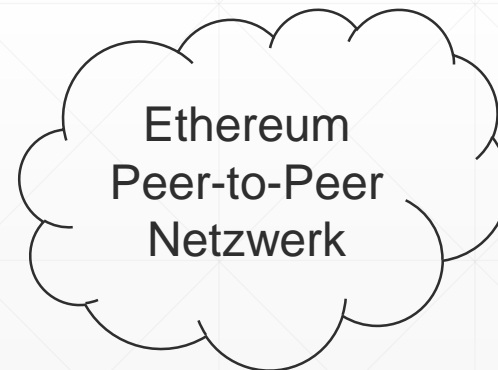
```
function deposit() payable public {
    deposit(msg.sender);
}
function deposit(address _payout) payable public {
    assert(!potClosed);
    assert(msg.value == EXPECTED_POT_AMOUNT);
    depositAddresses[nbrOfParticipants] = msg.sender;
    payoutAddresses[nbrOfParticipants] = _payout;
    nbrOfParticipants++;
    if (nbrOfParticipants == NBR_OF_SLOTS) {
        closingBlockNumber = block.number;
        payoutBlockNumber = closingBlockNumber +
            PAYOUT_BLOCK_OFFSET;
        potClosed = true;
    }
}
```

# Ethereum - Smart Contract

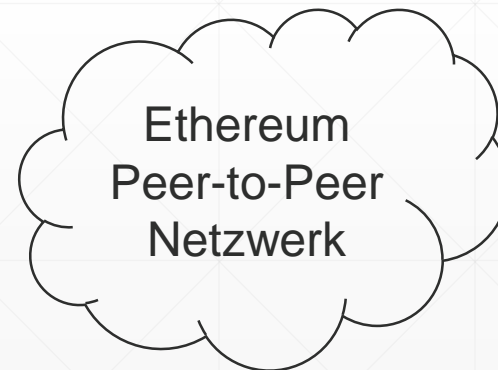
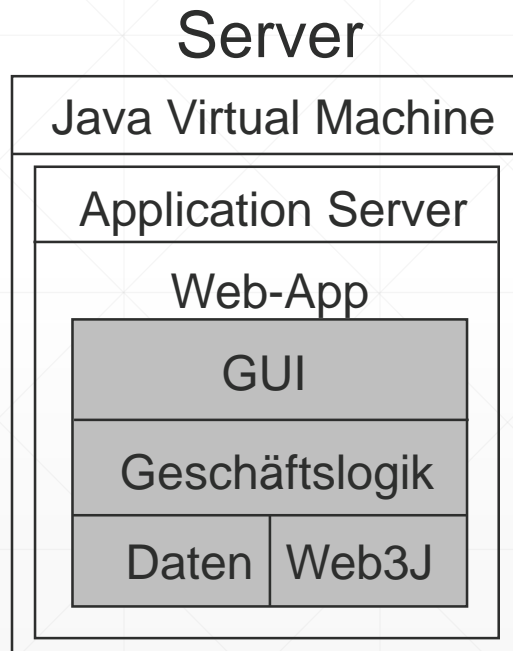
```
function payout() public{
    assert(potClosed);
    assert(block.number>payoutBlockNumber);
    payoutBlockHash = block.blockhash(payoutBlockNumber);
    if(payoutBlockHash == 0){
        nbrOfMissedPayouts++;
    } else {
        winner = uint256(payoutBlockHash) % NBR_OF_SLOTS;
        address winnerAddress = payoutAddresses[winner];
        uint amount= EXPECTED_POT_AMOUNT*NBR_OF_SLOTS;
        amount +=
            EXPECTED_POT_AMOUNT*NBR_OF_SLOTS*nbrOfMissedPayouts;
        winnerAddress.transfer(amount); // send pot amount to
            winner
        nbrOfMissedPayouts = 0;
    }
    potClosed = false;
    nbrOfParticipants=0;
}
```

# Ethereum - Umsetzung

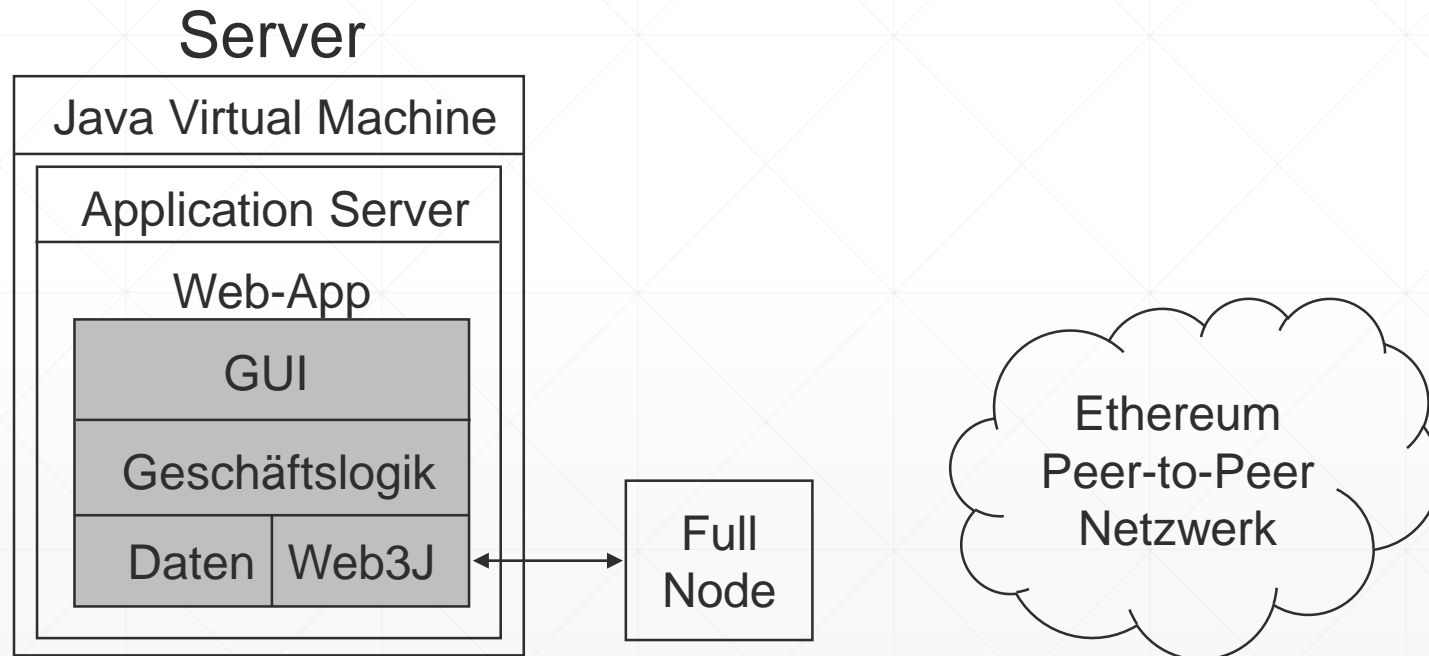
# Ethereum - Umsetzung



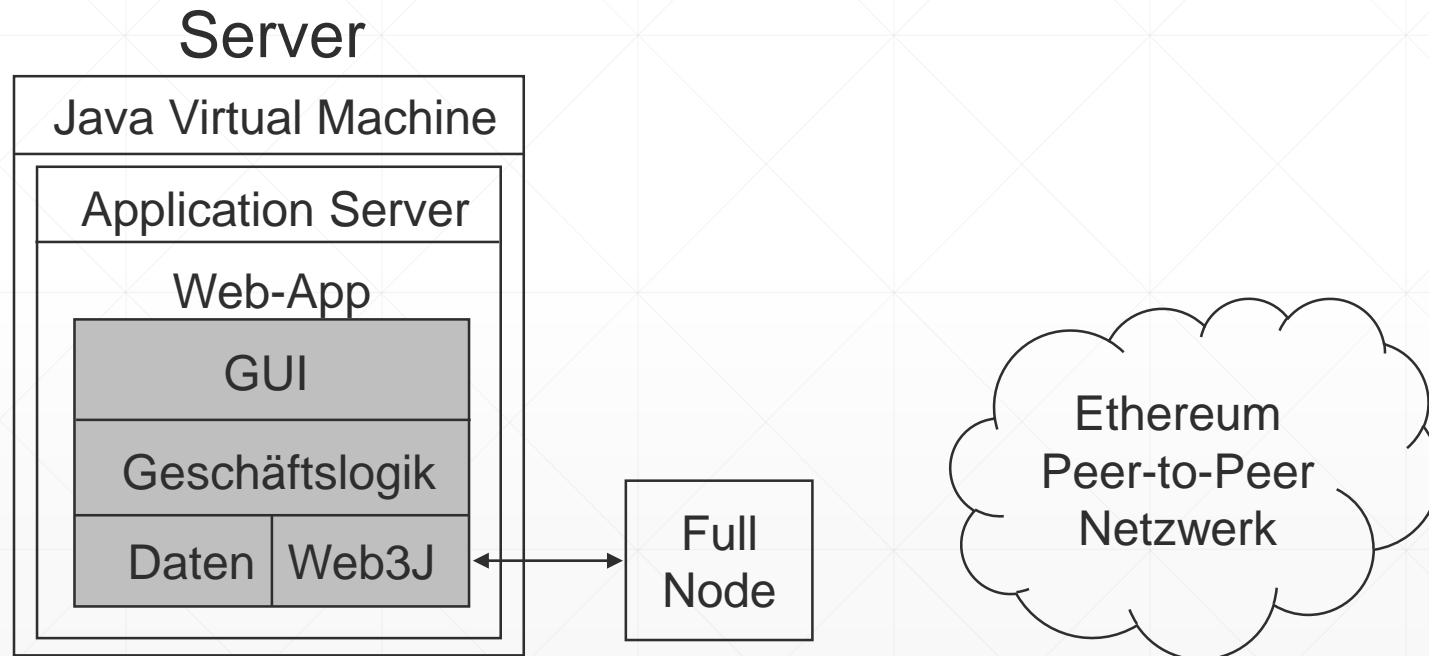
# Ethereum - Umsetzung



# Ethereum - Umsetzung

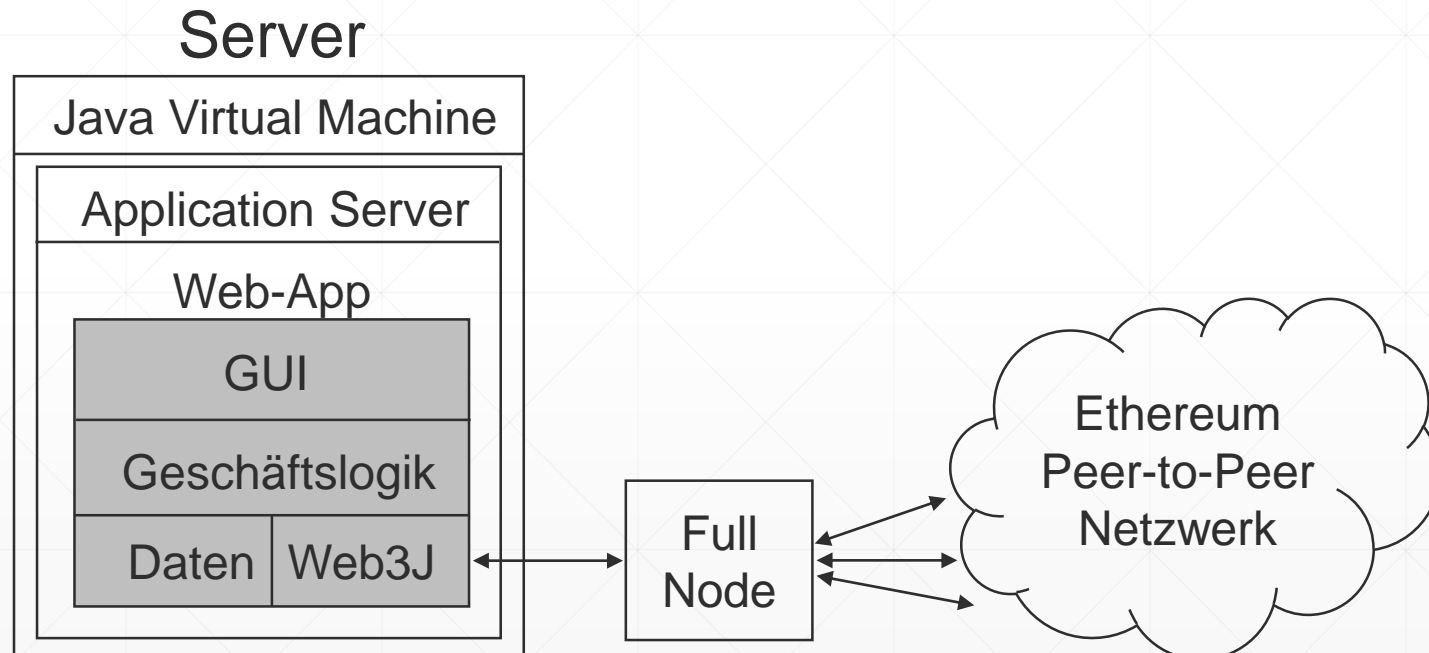


# Ethereum - Umsetzung

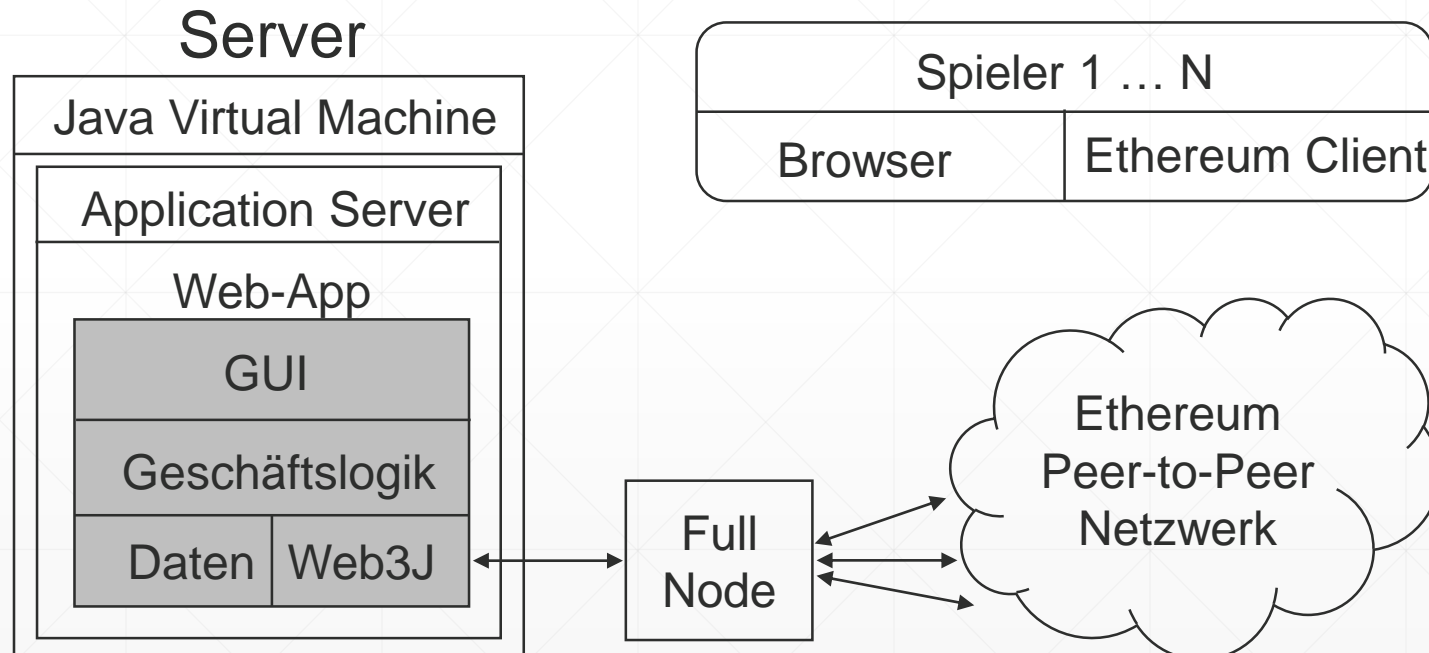




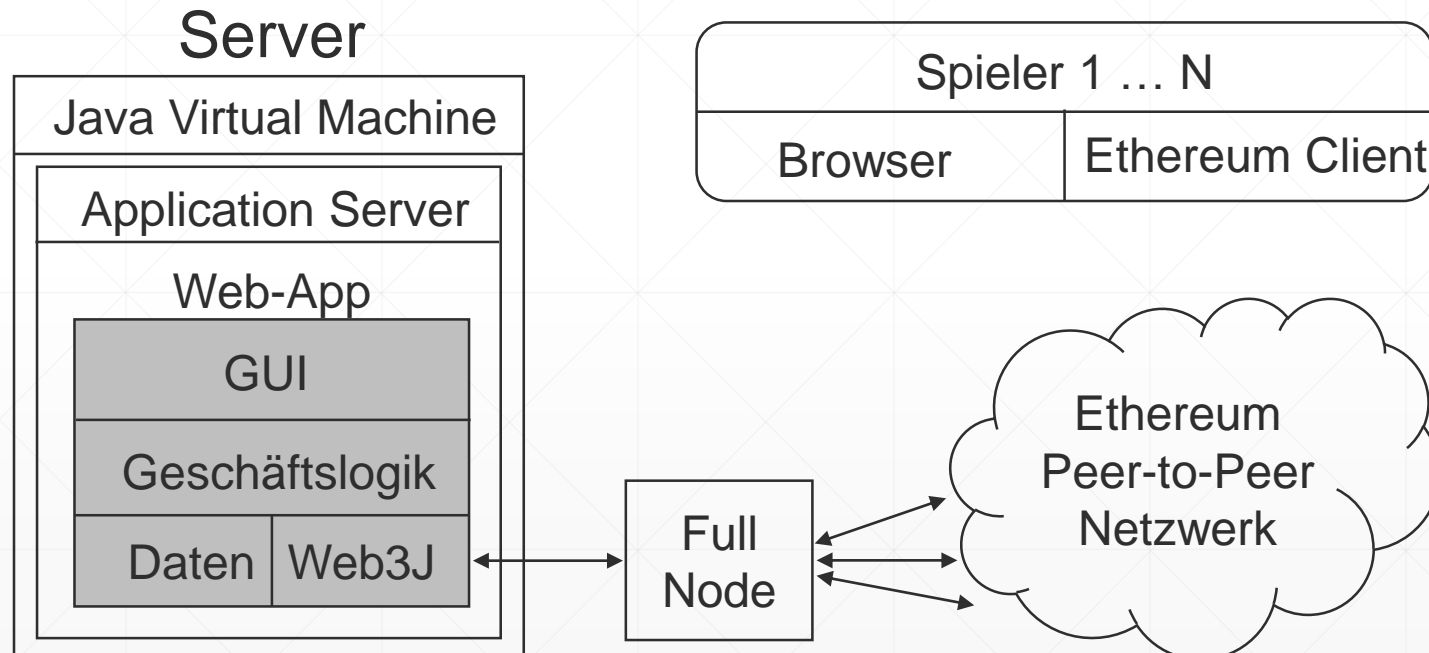
# Ethereum - Umsetzung



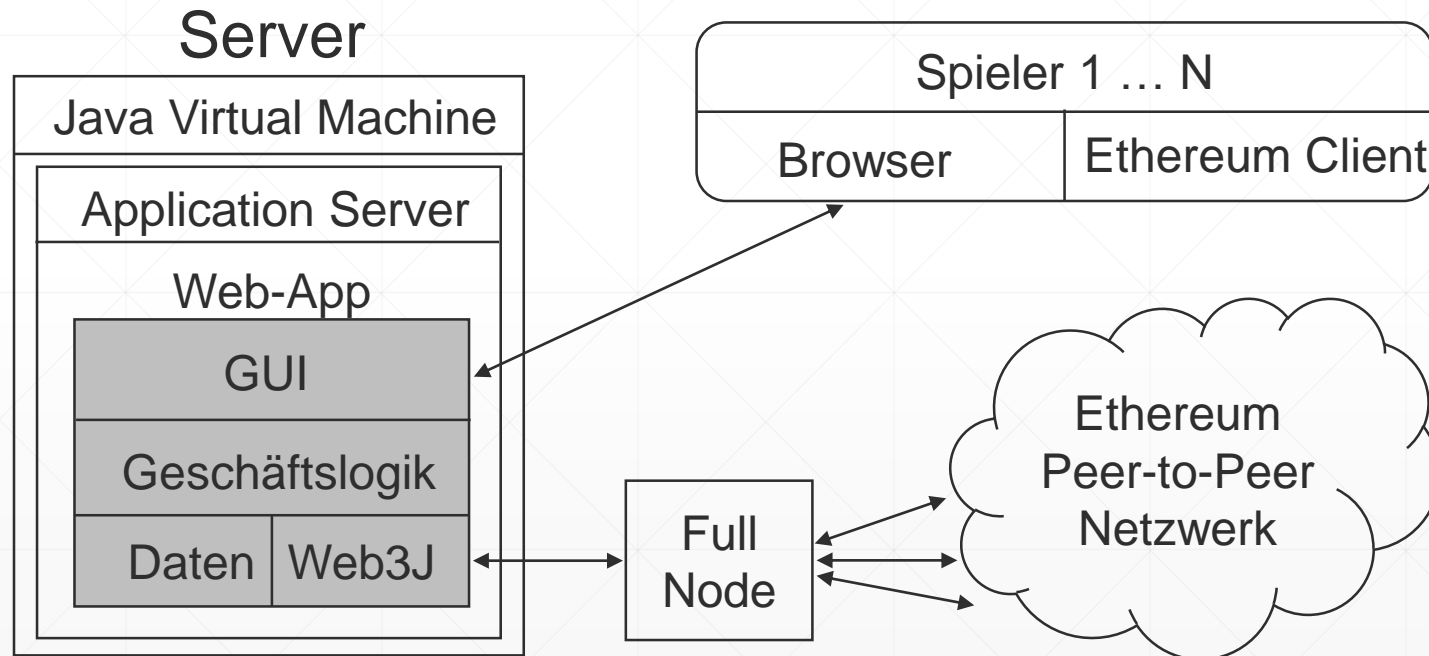
# Ethereum - Umsetzung



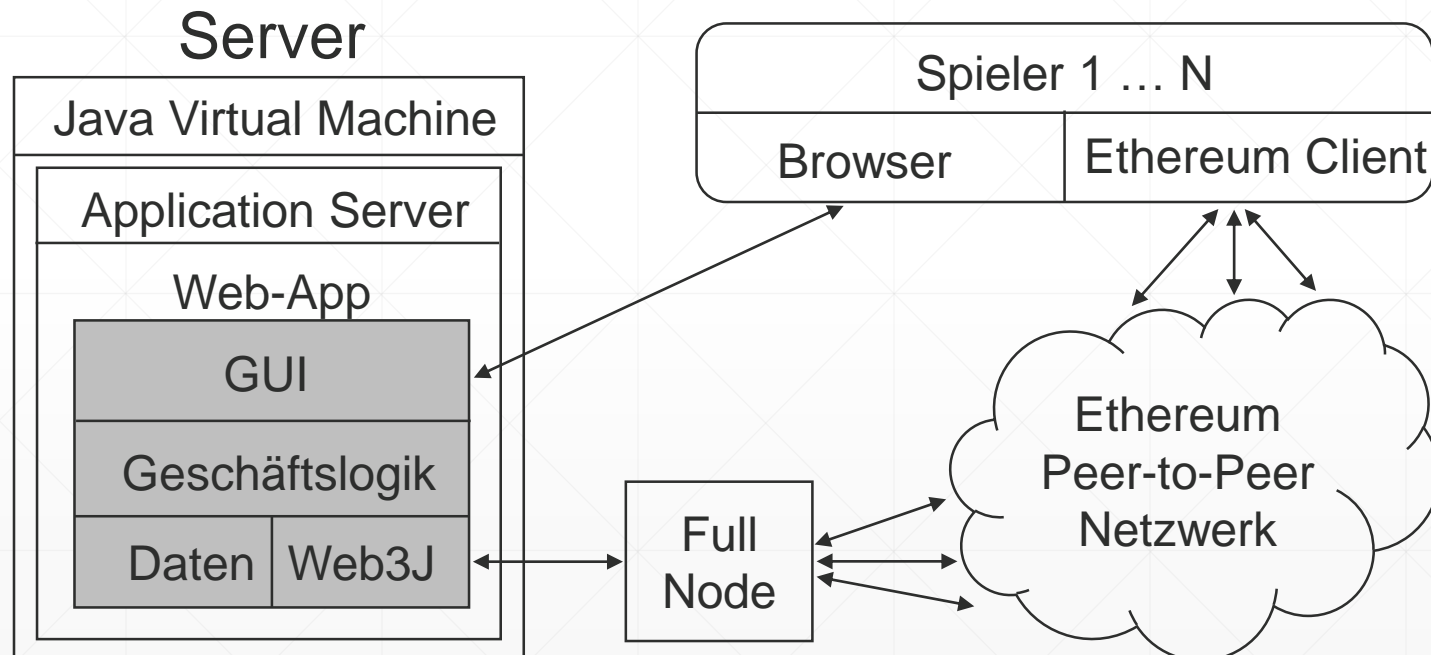
# Ethereum - Umsetzung



# Ethereum - Umsetzung




# Ethereum - Umsetzung

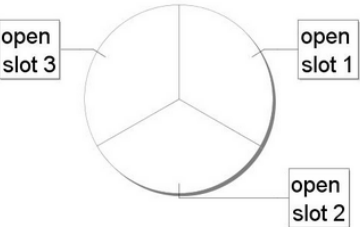


# Ethereum - Glücksspielanwendung

Block Height: 1903061 563,65€ / ETH Fr, 9 Mär 2018 18:19:12

 **Ethereum Rinkeby Testnet**


1000 WEI / slot



Participants:

No one joined this pot yet. You could be the first participant.

Join Pot



Send 1000 WEI to [0x9b04da87b9bedafae8f02c53bb5e290dce0cf2d](#) to participate in the current pot.


Smart contract ABI:

```
[{"constant":true,"inputs":[],"name":"_message","outputs":[{"name":"","type":"string"}],"payable":false,"stateMutability":"view","type":"function"}, {"constant":true,"inputs":[{"name":"","type":"uint256"}],"name":"depositAddresses","outputs":[{"name":"","type":"address"}],"payable":false,"stateMutability":"view","type":"function"}, {"constant":true,"inputs":[],"name":"NBR_OF_SLOTS","outputs":[{"name":"","type":"uint8"}],"payable":false,"stateMutability":"view","type":"function"}, {"constant":true,"inputs":[],"name":"closingBlockNumber","outputs":[]}]
```

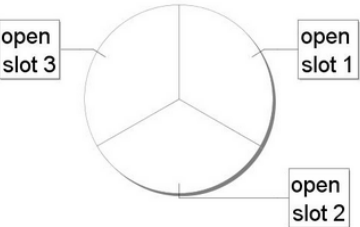
Close

# Ethereum - Glücksspielanwendung

Block Height: 1903061 563,65€ / ETH Fr, 9 Mär 2018 18:19:12

 **Ethereum Rinkeby Testnet**


1000 WEI / slot



Participants:

No one joined this pot yet. You could be the first participant.

Join Pot




Send 1000 WEI to [0x9b04da87b9bedafae8f02c53bb5e290dce0cf2d](#) to participate in the current pot.

Smart contract ABI:

```
[{"constant":true,"inputs":[],"name":"_message","outputs":[{"name":"","type":"string"}],"payable":false,"stateMutability":"view","type":"function"}, {"constant":true,"inputs":[{"name":"","type":"uint256"}],"name":"depositAddresses","outputs":[{"name":"","type":"address"}],"payable":false,"stateMutability":"view","type":"function"}, {"constant":true,"inputs":[],"name":"NBR_OF_SLOTS","outputs":[{"name":"","type":"uint8"}],"payable":false,"stateMutability":"view","type":"function"}, {"constant":true,"inputs":[],"name":"closingBlockNumber","outputs":[]}]
```

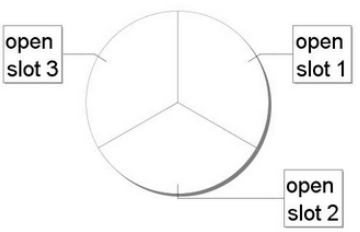
Close

# Ethereum - Glücksspielanwendung

 **Ethereum Rinkeby Testnet**

Pot open. Waiting for 3 more participants.

1000 WEI / slot



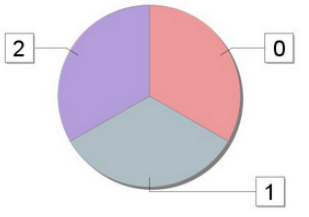
[Participants:](#)  
No one joined this pot yet. You could be the first participant.

[Join Pot](#)

**Closed Pots**

Pot closed. Winner is 0x2201f3919589b519135ce977cc0906c9481069b2. Payout done.

1000 WEI / slot



Winner calculation: `uint(0x93e821543246d870d52c564de2c07fcaeeffad45ed6a91d038ddd5061ba3e3e) modulo 3 = (1)` (hover for explanations)

	Block Height	Block Hash
Payout	1909338	0x93e821543246d870d52c564de2c07fcaeeffad45ed6a91d038ddd5061ba3e3e
Closing	1909337	0x55e137d546ea48c5c15941f671818978a4ddf38d20d65293832e352fbd98adc

[Participants:](#)

- ✔ (0) Smart contract received 1000 WEI from address 0x2201f3919589b519135ce977cc0906c9481069b2.  
Payout address: 0x2201f3919589b519135ce977cc0906c9481069b2
- ✔ (1) Smart contract received 1000 WEI from address 0x2201f3919589b519135ce977cc0906c9481069b2.  
Payout address: 0x83ddd477852f6f9493d8cfa0f895e44ef2eac20e
- ✔ (2) Smart contract received 1000 WEI from address 0x2201f3919589b519135ce977cc0906c9481069b2.  
Payout address: 0x83ddd477852f6f9493d8cfa0f895e44ef2eac20e



# Fazit

---

# Fazit

- Durch Ethereum vollständig auf Trusted Third Party verzichtet
- Einsatz von Blockchain:
  - Nur für wenige Anwendungsfälle sinnvoll
  - Bringt viele Nachteile mit
- Zukunft ungewiss
- Sehr viel Innovation auf dem Gebiet
  - Proof-of-Stake
  - Second Layer Solutions
  - ...

# Abbildungsverzeichnis

- Alle nicht auf dieser Folie angegebenen Abbildungen entstammen der Ausarbeitung:  
<https://github.com/ossel/master-thesis/blob/master/Thesis/Thesis.pdf>
- Bitcoin Logo:  
<https://upload.wikimedia.org/wikipedia/commons/thumb/4/46/Bitcoin.svg/1000px-Bitcoin.svg.png>
- Antminer S9i:  
<https://shop.bitmain.com/product/detail?pid=00020180612110232223Y3T9dchY0685>
- BTC Mining:  
<https://coindoo.com/wp-content/uploads/2018/01/bitcoin-mining-55745096-1024x740.jpg>
- Ethereum Logo:  
[https://www.ethereum.org/images/logos/ETHEREUM-ICON\\_Black\\_small.png](https://www.ethereum.org/images/logos/ETHEREUM-ICON_Black_small.png)