

# Echte Transparenz bei Smart Contracts ?

---

Konferenz Smart Contracts – Schlaue Verträge

Albert-Ludwigs-Universität Freiburg, 6. Juli 2018

Jörn Erbguth, Diplom-Informatiker, Diplom-Jurist  
Legal Tech, Blockchain, Smart Contracts Consultant

[joern@erbguth.ch](mailto:joern@erbguth.ch) +41 787256027

# Ist ein Snackautomat transparent?

- Warenangebot direkt sichtbar
- Preise direkt sichtbar
- Funktionsweise klar verständlich

aber ...





# Ist ein Snackautomat transparent?

- Programmcode verborgen
- Aufsteller hat Kontrolle über Code
- Kein einsehbares Logging
- Nur Aufsteller kann Fehlfunktion beheben
- Vertrauen in Aufsteller erforderlich



# Transparenter Vertragsabschluss oder transparente Vertragsdurchführung?

---



**§ 307 Abs. 1 S. 2 BGB:** Eine unangemessene Benachteiligung kann sich auch daraus ergeben, dass die Bestimmung nicht klar und verständlich ist.



# Transparenz für die Vertragsdurchführung

Zimmerinformationen & Preis Ausstattung

## Hotel Adlon Kempinski Ber

Flughafenshuttle Barrierefrei

Unter den Linden 77, Mitte, 10117 Berlin, Deutschland



**100 % echte Bewertungen**  
Echte Bewertungen. Echte Aufenthalte. Echte Meinungen. [Weitere Informationen](#)

**9,3** **Hervorragend** · 3.533 Bewertungen ▾

Sauberkeit	9,5	Preis-Leistungs-Verhältnis	8,5
Komfort	9,5	Kostenfreies WLAN	9
Ausstattung	9,3	Lage	9,8
Hotelpersonal	9,4		

Bewertungen anzeigen: **Alle Bewertungen** ▾ **Alle Bewertungsergebnisse** ▾

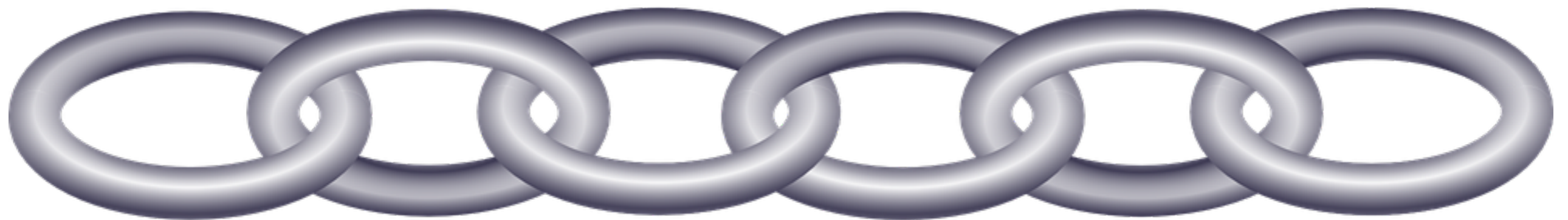
Bewertungen anzeigen auf:  Deutsch 930 Bewertungen  Englisch 442 Bewertungen  Chinesisch 14 Bewertungen [+](#)

Sortieren nach: **Empfehlungen** ▾

# Was bedeutet Transparenz bei Smart Contracts?

---

- Vertragscode einsehbar
- Vertragscode unveränderlich
- Ausführung genau des Vertragscodes





# Quellcode des Vertrags



0x49EdF201c1E139282643d5e7C6fB0C7219Ad1db7

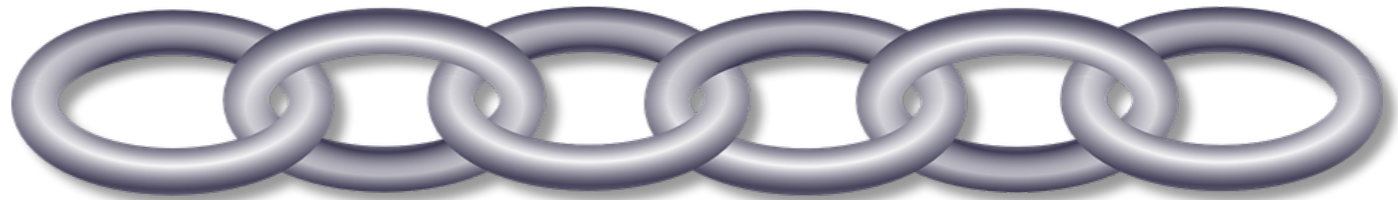
```
1 pragma solidity >=0.4.4;
2
3 contract Sale {
4     uint public startTime;
5     uint public stopTime;
6     uint public target;
7     uint public raised;
8     uint public collected;
9     uint public numContributors;
10    mapping(address => uint) public balances;
11
12    function buyTokens(address _a, uint _eth, uint _time) returns (uint);
13    function getTokens(address holder) constant returns (uint);
14    function getRefund(address holder) constant returns (uint);
15    function getSoldTokens() constant returns (uint);
16    function getOwnerEth() constant returns (uint);
17    function tokensPerEth() constant returns (uint);
18    function isActive(uint time) constant returns (bool);
19    function isComplete(uint time) constant returns (bool);
20 }
21
22 contract Constants {
23     uint DECIMALS = 8;
24 }
25
```

# Quellcode nicht auf der Blockchain

```
1 pragma solidity >=0.4.4;
2
3 contract Sale {
4     uint public startTime;
5     uint public stopTime;
6     uint public target;
7     uint public raised;
8     uint public collected;
9     uint public numContributors;
10    mapping(address => uint) public balances;
11
12    function buyTokens(address _a, uint _eth, uint _time) returns (uint);
13    function getTokens(address holder) constant returns (uint);
14    function getRefund(address holder) constant returns (uint);
15    function getSoldTokens() constant returns (uint);
16    function getOwnerEth() constant returns (uint);
17    function tokensPerEth() constant returns (uint);
18    function isActive(uint time) constant returns (bool);
19    function isComplete(uint time) constant returns (bool);
20 }
21
22 contract Constants {
23     uint DECIMALS = 8;
24 }
25
```



Objectcode  
Bytecode





# Objectcode

---

PUSH1 0x60  
PUSH1 0x40  
MSTORE  
CALLDATASIZE  
ISZERO  
PUSH2 0x0235  
JUMPI  
PUSH4 0xffffffff  
PUSH1 0xe0  
PUSH1 0x02  
EXP  
PUSH1 0x00  
CALLDATALOAD  
DIV  
AND  
PUSH4 0x07cbe8ab  
DUP2  
EQ  
PUSH2 0x0246  
JUMPI  
DUP1  
PUSH4 0x144fa6d7  
EQ  
PUSH2 0x0274  
JUMPI  
DUP1  
PUSH4 0x156773ca  
EQ  
PUSH2 0x0292  
JUMPI  
DUP1  
PUSH4 0x1a6af7b7  
EQ  
PUSH2 0x02b0  
JUMPI  
DUP1  
PUSH4 0x1c1bc850

EQ  
PUSH2 0x02d2  
JUMPI  
DUP1  
PUSH4 0x379ba3b7  
EQ  
PUSH2 0x02f0  
JUMPI  
DUP1  
PUSH4 0x3fe3f427  
EQ  
PUSH2 0x0314  
JUMPI  
DUP1  
PUSH4 0x443f95dc  
EQ  
PUSH2 0x0341  
JUMPI  
DUP1  
PUSH4 0x48b17b64  
EQ  
PUSH2 0x0353  
JUMPI  
DUP1  
PUSH4 0x4a6d0292  
EQ  
PUSH2 0x0377  
JUMPI  
DUP1  
PUSH4 0x4e71d92d  
EQ  
PUSH2 0x0395  
JUMPI  
DUP1  
PUSH4 0x53cea153  
EQ  
PUSH2 0x03a7

JUMPI  
DUP1  
PUSH4 0x5ab827f6  
EQ  
PUSH2 0x03cc  
JUMPI  
DUP1  
PUSH4 0x67f8a8b8  
EQ  
PUSH2 0x03ee  
JUMPI  
DUP1  
PUSH4 0x6a092e79  
EQ  
PUSH2 0x040f  
JUMPI  
DUP1  
PUSH4 0x6c530ee3  
EQ  
PUSH2 0x0433  
JUMPI  
DUP1  
PUSH4 0x6e1e063f  
EQ  
PUSH2 0x0455  
JUMPI  
DUP1  
PUSH4 0x71c1d196  
EQ  
PUSH2 0x0483  
JUMPI  
DUP1  
PUSH4 0x79ba5097  
EQ  
PUSH2 0x04a8  
JUMPI  
DUP1



# Bytecode

```
6060604052341561000c57fe5b5b6001805461010060a860020a03191661010033600160a060020a03169081029190911790915560058054600160a060020a031916821790556
00f80546201000060b060020a031916620100009092029190911790555b5b61234b806100736000396000f300606060405236156102355763fffffffff60e060020a6000350416
6307cbe8ab8114610246578063144fa6d714610274578063156773ca146102925780631a6af7b7146102b05780631c1bc850146102d2578063379ba3b7146102f05780633fe3f
42714610314578063443f95dc1461034157806348b17b64146103535780634a6d0292146103775780634e71d92d1461039557806353cea153146103a75780635ab827f6146103
cc57806367f8a8b8146103ee5780636a092e791461040f5780636c530ee3146104335780636e1e063f1461045557806371c1d1961461048357806379ba5097146104a85780637
a08339d146104ba57806384d24226146104cf5780638d03b102146104fd5780638da5cb5b146105215780638ff591b41461054d57806392ee9b1461056257806398e54c5514
61058057806399aa93c8146105925780639c492b9e146105b4578063a015cb10146105d6578063a6f9dae1146105eb578063a8af232b14610609578063ae90b2131461061b578
063b4ba9e1114610647578063b5f522f71461066b578063bab8fe401461069a578063cbdd69b5146106bc578063cd5681d5146106de578063cf00746014610705578063d0e30d
4080519115158252519081900360200190f35b341561052957fe5b6105316114b1565b60408051600160a060020a039092168252519081900360200190f35b341561055557fe5
b6102446004356114c5565b005b341561056a57fe5b610244600160a060020a03600435166114e7565b005b341561058857fe5b610244611551565b005b341561059a57fe5b61
026261158c565b60408051918252519081900360200190f35b34156105bc57fe5b610262611593565b60408051918252519081900360200190f35b34156105de57fe5b6102446
00435611599565b005b34156105f357fe5b610244600160a060020a036004351661165565b005b341561061157fe5b610244611696565b005b341561062357fe5b6105316117
0e565b60408051600160a060020a039092168252519081900360200190f35b341561064f57fe5b610244600160a060020a036004358116906024351661171d565b005b3415610
67357fe5b6105316004356118b4565b60408051600160a060020a039092168252519081900360200190f35b34156106a257fe5b6102626118e6565b6040805191825251908190
0360200190f35b34156106c457fe5b6102626118f7565b60408051918252519081900360200190f35b34156106e657fe5b61030060043561198c565b604080519115158252519
081900360200190f35b341561070d57fe5b610262600160a060020a03600435166119a1565b60408051918252519081900360200190f35b610244610871565b005b3415610745
57fe5b6102446004356119b3565b005b6102446119d7565b005b341561076457fe5b610262611a1d565b60408051918252519081900360200190f35b341561078657fe5b61026
2611a23565b60408051918252519081900360200190f35b34156107a857fe5b610244611a41565b005b34156107ba57fe5b610244600160a060020a0360043516602435604435
611a9d565b005b34156107de57fe5b610244600160a060020a0360043516602435611b80565b005b34156107ff57fe5b610262611d08565b60408051918252519081900360200
190f35b341561082157fe5b610531611d9d565b60408051600160a060020a039092168252519081900360200190f35b341561084d57fe5b610531611dac565b60408051600160
a060020a039092168252519081900360200190f35b600f5460009060ff16156108855760006000fd5b61088f3334611dbb565b50600160a060020a03331660008181526009602
0908152604091829020805434808201909255835191825292519293927fc30df14cb928081d7587d26c00adb1c5483c8049cc0456e2d2e8e226dfb7c920929181900390910190
a25b5b50565b600b6020526000908152604090205481565b60015433600160a060020a0390811661010090920416146109225760006000fd5b600354600160a060020a0316156
109395760006000fd5b60038054600160a060020a031916600160a060020a0383161790555b5b50565b60015433600160a060020a03908116610100909204161461097a576000
6000fd5b600154600f54620100009004600160a060020a0390811661010090920416146109a2576108eb565b600f805475ffffffffffffffffffffffffffffffffffffffff000
0191662010000600160a060020a038416021790555b5b50565b60015460009060ff16156109ed57506000546109f0565b50425b5b90565b60015433600160a060020a03908116
6101009092041614610a155760006000fd5b600f5460ff1615610a265760006000fd5b60058054600160a060020a031916600160a060020a0383161790555b5b5b50565b60006
006610a53611a23565b81548110610a5d57fe5b906000526020600020900160005b9054906101000a9004600160a060020a0316600160a060020a03166382afd23b610a936109
d6565b6000604051602001526040518263ffffffff1660e060020a02815260040180828152602001915050602060405180830381600087803b1515610ad157fe5b60325a03f11
515610ade57fe5b5050604051519150505b90565b600f54600090819060ff1615610b015760006000fd5b60015433600160a060020a039081166101009092041614610b225760
006000fd5b6000610b2c611a23565b1115610b385760006000fd5b6000838152600a602052604090205460ff1615610b555760006000fd5b6000838152600a602090815260408
08320805460ff19166001179055600160a060020a0389168352600b909152902054610b8f9086611f28565b600160a060020a0387166000908152600b60205260408120919091
55600680549091908110610bba57fe5b906000526020600020900160005b9054906101000a9004600160a060020a0316600160a060020a031663cbdd69b560006040516020015
26040518163ffffffff1660e060020a028152600401809050602060405180830381600087803b1515610c1f57fe5b60325a03f11515610c2c57fe5b5050604051519250610c3e
9050611336565b610c488684611f50565b811515610c5157fe5b6003546040805160e060020a6340c10f19028152600160a060020a038c8116600483015294909304602484018
1905290519094509216916340c10f199160448082019260009290919082900301818387803b1515610cab57fe5b60325a03f11515610cb857fe5b505060408051868152602081
018890528082018690529051600160a060020a03808a1693508a16917f15910e5cea9f22af6be011580707d2135bf1a23bf888657249f6e887af70a1fc919081900360600190a
```



# Quellcodetransparenz

---

- Quellcode befindet sich nicht auf der Blockchain
- Kompilierter Quellcode kaum lesbar
- Tools zum Abgleich des Quellcodes mit dem kompilierten Objektcode auf der Blockchain

# Quellcode oder Dekompilierung

```
contract SendBalance {
    mapping ( address => uint ) userBalances ;
    bool withdrawn = false ;

    function getBalance (address u) constant returns ( uint ){
        return userBalances [u];
    }

    function addToBalance () {
        userBalances[msg.sender] += msg.value ;
    }

    function withdrawBalance (){
        if (!(msg.sender.call.gas(0x1111).value (
            userBalances [msg . sender ]))){ throw ; }
        userBalances [msg.sender ] = 0;
    }
}
```

Attempting to parse ABI definition...  
Success.

```
Hash: 0x5FD8C710
function withdrawBalance() {
    if (msg.sender.call.gas(4369).value(store[msg.sender])) {
        store[msg.sender] = 0x0;
    }
}
```

L3 (D8193): Potential reentrant vulnerability found.

LOC: 5

Hash: 0xC0E317FB

```
function addToBalance() {
    store[msg.sender] = store[msg.sender] + msg.value;
    return;
}
```

LOC: 4

Hash: 0xF8B2CB4F

```
function getBalance(address) {
    return store[arg_4];
}
```

LOC: 3



# Quellcode

Quellcode	Nicht auf der Blockchain	Verständlich für Programmierer
Dekompilierter Quellcode	Aus der Blockchain generierbar	Schwerer verständlich
Objectcode	Auf der Blockchain	Kaum verständlich
Bytecode	Auf der Blockchain	unverständlich

```
1 pragma solidity >=0.4.4;
2
3 contract Sale {
4     uint public startTime;
5     uint public stopTime;
6     uint public target;
7     uint public raised;
8     uint public collected;
9     uint public numContributors;
10    mapping(address => uint) public balances;
11
12    function buyTokens(address _a, uint _eth, uint _time) returns (uint);
13    function getTokens(address holder) constant returns (uint);
14    function getRefund(address holder) constant returns (uint);
15    function getSoldTokens() constant returns (uint);
16    function getOwnerEth() constant returns (uint);
17    function tokensPerEth() constant returns (uint);
18    function isActive(uint time) constant returns (bool);
19    function isComplete(uint time) constant returns (bool);
20 }
21
22 contract Constants {
23     uint DECIMALS = 8;
24 }
25
```

```
Attempting to parse ABI definition...
Success.

Hash: 0x5F08C710
function withdrawBalance() {
  if (msg.sender.call.gas(4369).value(store[msg.sender])) {
    store[msg.sender] = 0x0;
  }
}

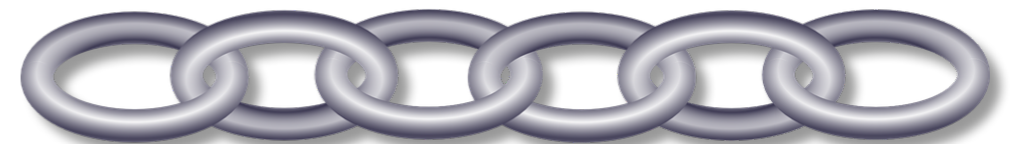
L3 (0B193): Potential reentrant vulnerability found.

LOC: 5
Hash: 0xC0E317FB
function addToBalance() {
  store[msg.sender] = store[msg.sender] + msg.value;
  return;
}

LOC: 4
Hash: 0xFBB2CB4F
function getBalance(address) {
  return store[arg_0];
}

LOC: 3
```

Opcode  
Bytecode



# Weniger Softwarefehler

---

- Formale Verifizierung von Code
- Automatisierte Analysetools
- Entwicklung weniger fehleranfälliger Programmiersprachen





# Transparenz durch Nachvollziehbarkeit

Latest 25 txns from a total Of [2864 transactions](#)



TxHash	Block	Age	From		To	Value	[TxFee]
<a href="#">0x1ebc95710a4aa9...</a>	<a href="#">4874434</a>	178 days 11 hrs ago	<a href="#">0x20f72f8ce1fe6036...</a>		TokenCard-ICO	0.8 Ether	0.00105
<a href="#">0xf1993e3fca10207...</a>	<a href="#">4337275</a>	274 days 2 hrs ago	<a href="#">0x2ff4d83d13fb20b...</a>		TokenCard-ICO	0 Ether	0.000305488
<a href="#">0x0b4f0236b49791...</a>	<a href="#">4336072</a>	274 days 12 hrs ago	<a href="#">0x2ff4d83d13fb20b...</a>		TokenCard-ICO	0 Ether	0.000358032
<a href="#">0x42bdfbd48d23be...</a>	<a href="#">4084710</a>	342 days 16 hrs ago	<a href="#">0xbc8428b4aec8dc...</a>		TokenCard-ICO	0 Ether	0.0021
<a href="#">0xdc3a56a3df0550...</a>	<a href="#">4084698</a>	342 days 16 hrs ago	<a href="#">0xbc8428b4aec8dc...</a>		TokenCard-ICO	0 Ether	0.0021
<a href="#">0xc473245debc816...</a>	<a href="#">3737706</a>	411 days 12 hrs ago	<a href="#">0x00db2b9178f83b...</a>		TokenCard-ICO	0 Ether	0.01
<a href="#">0x8ca753f9ae07d51...</a>	<a href="#">3734934</a>	412 days 57 mins ago	<a href="#">0x000f372e3e45ada...</a>		TokenCard-ICO	0 Ether	0.001224909
<a href="#">0x29284caf5849c52...</a>	<a href="#">3734933</a>	412 days 58 mins ago	<a href="#">0x000f372e3e45ada...</a>		TokenCard-ICO	0 Ether	0.000606669
<a href="#">0x1f27dc934a14c71...</a>	<a href="#">3722913</a>	414 days 6 hrs ago	<a href="#">0x51e07ebffb63c57...</a>		TokenCard-ICO	0.1 Ether	0.002268
<a href="#">0x0022630ab31c60...</a>	<a href="#">3722896</a>	414 days 6 hrs ago	<a href="#">0x51e07ebffb63c57...</a>		TokenCard-ICO	0.1 Ether	0.012519
<a href="#">0x9da1ac841b60a3...</a>	<a href="#">3692621</a>	419 days 18 hrs ago	<a href="#">0x483280195a600e...</a>		TokenCard-ICO	1 Ether	0.009584913
<a href="#">0xd48877804b8ac7...</a>	<a href="#">3673180</a>	423 days 5 hrs ago	<a href="#">0x000f372e3e45ada...</a>		TokenCard-ICO	0 Ether	0.0009056





# Weitere Aspekte der Transparenz bei Smart Contracts

---

- Identifikation des Vertragspartners
- Transparente Governance



# Transparenz bei Smart Contracts

---

- Transparenz der Vertragsvereinbarung
- Transparenz der Vertragsdurchführung
- Toolbasierte Transparenz
  - Decompiler
  - Analysetools
  - Blockchainexplorer
- Identifikation der Vertragspartner
- Transparente Governance



Vielen Dank für Ihre Aufmerksamkeit

---

Fragen ?