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 +41 787256027

Ist ein Snackautomat transparent?

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

aber …

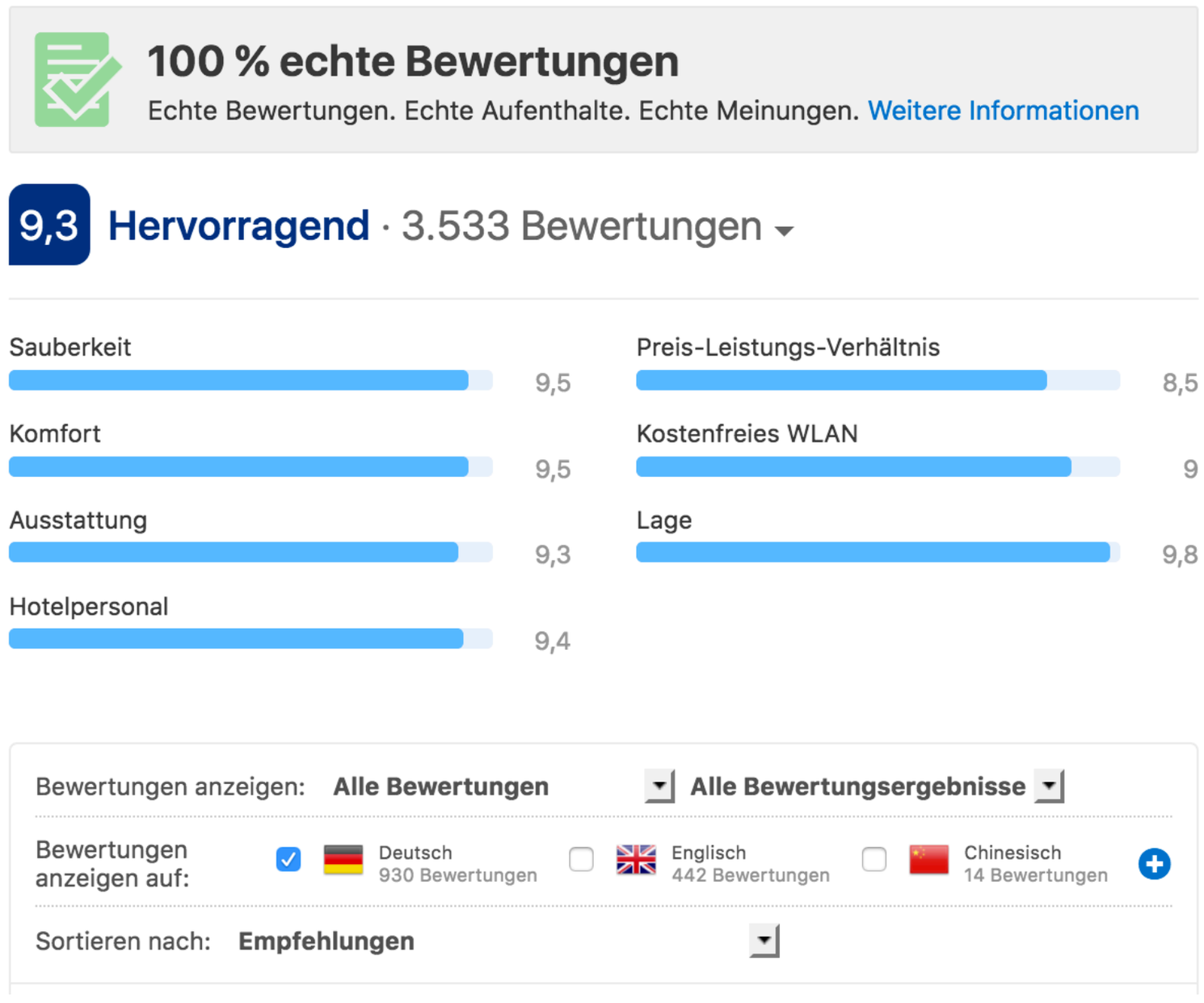
Ist ein Snackautomat transparent?

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

Transparenter Vertragsabschluss oder transparente Vertragsdurchführung?

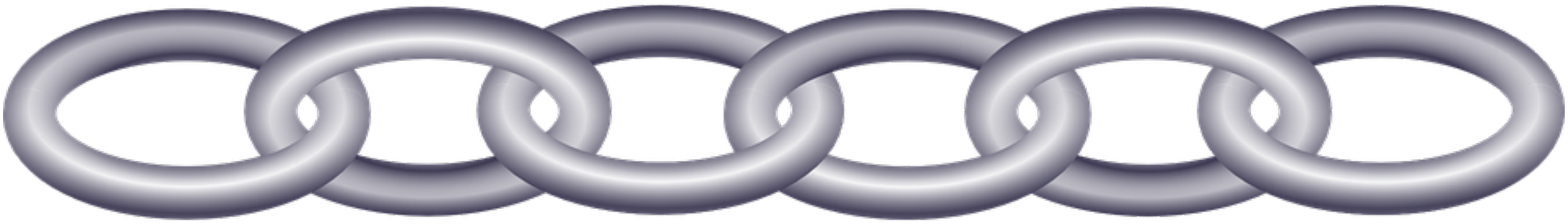
§ 307 Abs. 1 S. 2 BGB: Eine unangemessene Benachteiligung kann sich auch daraus ergeben, dass die Bestimmung nicht klar und verständlich ist.

Transparenz für die Vertragsdurchführung



Was bedeutet Transparenz bei Smart Contracts?

- Vertragscode einsehbar
- Vertragscode unveränderlich
- Ausführung genau des Vertragscodes



Quellcode des Vertrags

TokenCard-ICO

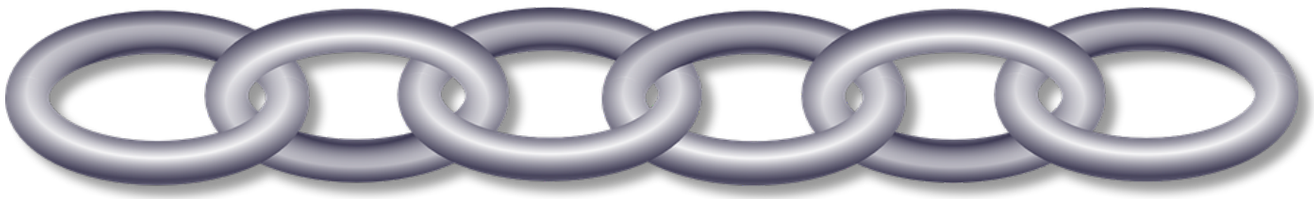
0x49EdF201c1E139282643d5e7C6fB0C7219Ad1db7

```
pragma solidity >=0.4.4;

contract Sale {
    uint public startTime;
    uint public stopTime;
    uint public target;
    uint public raised;
    uint public collected;
    uint public numContributors;
    mapping(address => uint) public balances;

    function buyTokens(address _a, uint _eth, uint _time) returns (uint);
    function getTokens(address holder) constant returns (uint);
    function getRefund(address holder) constant returns (uint);
    function getSoldTokens() constant returns (uint);
    function getOwnerEth() constant returns (uint);
    function tokensPerEth() constant returns (uint);
    function isActive(uint time) constant returns (bool);
    function isComplete(uint time) constant returns (bool);
}

contract Constants {
    uint DECIMALS = 8;
}

```

Quellcode nicht auf der Blockchain

```
pragma solidity >=0.4.4;

contract Sale {
    uint public startTime;
    uint public stopTime;
    uint public target;
    uint public raised;
    uint public collected;
    uint public numContributors;
    mapping(address => uint) public balances;

    function buyTokens(address _a, uint _eth, uint _time) returns (uint);
    function getTokens(address holder) constant returns (uint);
    function getRefund(address holder) constant returns (uint);
    function getSoldTokens() constant returns (uint);
    function getOwnerEth() constant returns (uint);
    function tokensPerEth() constant returns (uint);
    function isActive(uint time) constant returns (bool);
    function isComplete(uint time) constant returns (bool);
}

contract Constants {
    uint DECIMALS = 8;
}
```

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


```
6060604052341561000c57fe5b5b600180546101010060a860020a031916610100336000160a060020a0316908102919091179091556005805460016a060020a031916821790556
00f80546201000060b060020a0319166201000090920291909117905555b5b61234b80610073600039600f3006060604052361561023557636fffffff60e060020a6000350416
6307cbe8ab81146102465780631440fa6d7146102745780631561773ca146102925780631a6af7b7146102b05780631c1bc850146102d2578063379ba3b7146102f05780633fe3f
427146103145780633443f95dc1461034157806348b17b6414610353578063634a6d029214610377578063e71d92d1461039557806353cea153146103a75780635ab827f6146103
cc57806367f8a8b8146103ee5780636a092e791461040f5780636c530ee314610433578063e1e063f1461045557806371c1d19614610483578063e6379ba5097146104a85780637
a08339d146104ba57806384d24226146104cf5780638d03b102146104fd5780638da5cb5b1461052157806338ff591b41461054d57806392eefe9b1461056257806398e54c5514
6105805780639aa93c8146105925780639c492b9e146105b4578063a015cb10146105d6578063a6f9dae1146105eb578063a8af232b14610609578063ae90b2131461061b578
063b4ba9e1114610647578063b5f522f71461066b578063bab8fe401461069a578063cbdd69b5146106bc578063cd5681d5146106de578063cf007460146107055780631d0e30d
40805191151582525190819003602001 90f35b341561052957fe5b6105316114b1565b60408051600160a060020a0390921682525190819003602001 90f35b341561055557fe5
b610244600435611 4c5565b005b341561056a57fe5b610244600160a060020a0360043516611 4e7565b005b34156105857fe5b610244611551565b005b341561059a57fe5b61
026261158c565b60408051918252519081900360200190f35b34156105bc57fe5b610262611593565b60408051918252519081900360200190f35b34156105de57fe5b6102446
00435611599565b005b34156105f357fe5b610244600160a060020a0360043516611655565b005b341561061157fe5b610244611696565b005b341561062357fe5b6105316117
0e565b60408051600160a060020a0390921682525190819003602001 90f35b341561064f57fe5b610244600160a060020a0360043581169060243516611 71d565b005b3415610
67357fe5b6105316004356118b4565b60408051600160a060020a0390921682525190819003602001 90f35b34156106a257fe5b6102626118e6565b60408051918252519081900
0360200190f35b34156106c457fe5b6102626118f7565b60408051918252519081900360200190f35b34156106e657fe5b610300604356119 8c565b60408051918252519081900360200190a
```

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 reetrant 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
```

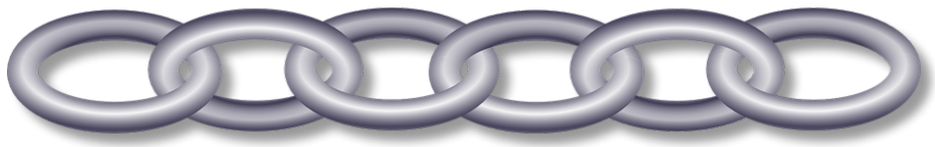
Quellcode

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

```
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 (DB193): Potential reetrant 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
```

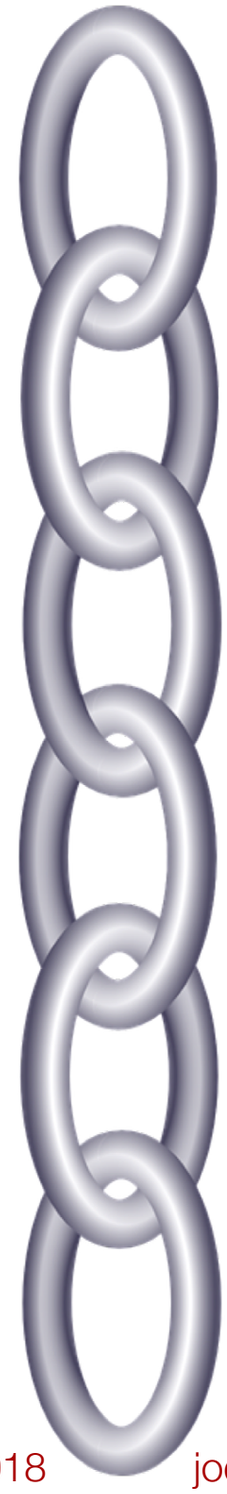
```
pragma solidity >=0.4.4;

contract Sale {
    uint public startTime;
    uint public stopTime;
    uint public target;
    uint public raised;
    uint public collected;
    uint public numContributors;
    mapping(address => uint) public balances;

    function buyTokens(address _a, uint _eth, uint _time) returns (uint);
    function getTokens(address holder) constant returns (uint);
    function getRefund(address holder) constant returns (uint);
    function getSoldTokens() constant returns (uint);
    function getOwnerEth() constant returns (uint);
    function tokensPerEth() constant returns (uint);
    function isActive(uint time) constant returns (bool);
    function isComplete(uint time) constant returns (bool);
}

contract Constants {
    uint DECIMALS = 8;
}
```

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

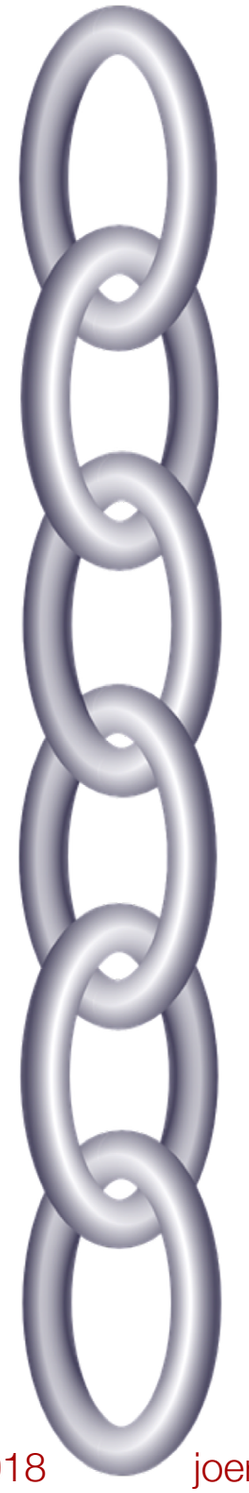
TxHash	Block	Age	From		To	Value	[TxFee]
0x1ebc95710a4aa9…	4874434	178 days 11 hrs ago	0x20f72f8ce1fe6036…	IN	TokenCard-ICO	0.8 Ether	0.00105
0xf1993e3fca10207…	4337275	274 days 2 hrs ago	0x2ff4d83d13fb20b…	IN	TokenCard-ICO	0 Ether	0.000305488
0x0b4f0236b49791…	4336072	274 days 12 hrs ago	0x2ff4d83d13fb20b…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

Transparenz durch Nachvollziehbarkeit

TxHash:	0xd48877804b8ac70e534dca0bacc9dfe791d4161b2d84a695bf3b4d7769c7cd04
Block Height:	3673180 (2239603 block confirmations)
TimeStamp:	423 days 5 hrs ago (May-08-2017 07:13:42 PM +UTC)
From:	0x000f372e3e45ada03456aef3b90c545ff2b7329c
To:	Contract 0x49edf201c1e139282643d5e7c6fb0c7219ad1db7 (TokenCard-ICO)
Token Transfered:	From 0x49edf201c1e1392…To 0x00de5f818693eb… for 29,446.6972444 ($2,989,193.13) DGD
Value:	0 Ether ($0.00)
Gas Limit:	940000
Gas Used By Txn:	45280
Gas Price:	0.00000002 Ether (20 Gwei)
Actual Tx Cost/Fee:	0.0009056 Ether ($0.42)
Nonce & {Position}:	779 | {4}
Input Data:	Function: transferTokens(address _token, address _to) MethodID: 0x6a092e79 [0]: 000000000000000000000000e0b7927c4af23765cb51314a0e0521a9645f0e2a [1]: 000000000000000000000000de5f818693eb9a0b38f78866c43d1ff67218a4 View Input As Decode Input Data

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 ?