ALPS FORUM

LAW AND ECONOMICS FOUNDATION ST. GALLEN

BLOCKCHAIN

08. - 09. November 2018

Law and Economics Foundation St. Gallen

Institute of Public Finance, Fiscal Law and Law and Economics

University of St.Gallen

ALPS FORUM

LAW AND ECONOMICS FOUNDATION ST. GALLEN

Blockchain
Rekonstruktion am Beispiel Smart Contracts

Alps Forum, Flims, 8./9. November 2018

Rechtsanwältin Dr. Jana Essebier, Partnerin Vischer AG
jana.essebier@vischer.com

Jörn Erbguth, Dipl.-Inf., Dipl.-Jur.
Consultant Legal Tech, Blockchain, Smart Contracts und Datenschutz
joern@erbguth.ch +41 787256027

Law and Economics Foundation St.Gallen

Institute of Public Finance, Fiscal Law and Law and Economics
University of St.Gallen

ALPS FORUM
LAW AND ECONOMICS FOUNDATION ST. GALLEN

Agenda

Smart Contracts

- Wie funktioniert das technisch?
- Unterschied zu anderer Software
- Analyse eines Smart Contracts

Juristische Bewertung

- Pflichten
- Haftung für Fehler
- Durchsetzung von vertraglichen Ansprüchen

Aspekte der Smart Contracts auf einer Blockchain

1. Formulierung der Vertragsbedingungen als Computerprogramm

```
pragma solidity ^0.4.2;

contract Handel {
    string public Ware;
    uint public Preis;
    address public Verkaeufer;
    address public Kaeufer;
    bool public bezahlt;
    bool public geliefert;
    bool public abgewickelt;
    address constant post-0x12345671

function Angebot(string iWare, uint
{
    Verkaeufer=msg.sender;
    Ware=iWare;
    Preis=iPreis;
}

function Annahme() payable
{
    if(msg.value>=Preis)
    {
```

2. Automatische Vertragsausführung

3. Vereinbarung und sichere Ausführung auf einer Blockchain

Automatische Vertragsausführung

- Jeder Verkaufsautomat führt automatisiert Verträge aus
- Programmierung verborgen
- Verkäufer kann Programm unbemerkt manipulieren
- Keine sichere Protokollierung der Transaktion

Smart Contracts auf der Blockchain

- Kleine Programme
- Erhalten Nachrichten
- Wenn die Bedingungen erfüllt sind, werden Transaktionen durchgeführt

Solidity – Smart Contract Programmiersprache

- Objektorientiert
- Contracts sind die Klassen
- Contracts können Daten und Funktionen von anderen Contracts erben

Exkurs: Objektorientierte Programmierung

Klasse: Pferd

Methoden:
- Füttern
- Komm her
- Trab
- Schritt

Eigenschaften:
- Grösse
- Höchstgeschwindigkeit
- Aufenthaltsort
- Hungrig

Solidity – Smart Contract Programmiersprache

- Syntax ähnlich JavaScript
- Kompiliert in Bytecode, der dann ausgeführt wird
- Eigene und fremde Programme können sich gegenseitig aufrufen

Solidity – anders als übliche Programmiersprachen

- Ausführung von Programmen kostet Geld ("Gas")
- Ausführung wird abgebrochen, wenn nicht genug Gas mitgegeben wurde
- Es können eigene Tokens definiert werden
- Jedes Smart Contract Programm kann Ether transferieren

Ethereum – ein transparenter Weltcomputer

- Smart Contracts können nicht (direkt) geändert werden
- Smart Contracts werden auf allen Ethereum-Knoten identisch ausgeführt
- Ausführung lässt sich nicht rückgängig machen
- Ausführung ist öffentlich sichtbar

Angriff frei!

- Smart Contracts können jederzeit angegriffen werden
- Schwachstellen werden ausgenutzt
- Hacker erhält Zugriff auf Ether
- Keine Strafverfolgung
- Keine Rückerstattung der erbeuteten Coins

Smart Contract Bug blockiert 800 Mio $ (marketcap)

SECURITY All transfers of the $800M marketcap ICON (ICX) are completely disabled due to fatal bug in smart contract (self.CryptoCurrency)

eingereicht vor 4 Monate * von NotYourMothersDildo

https://etherscan.io/address/0xb5a5f22694352c15b00323844ad545abb2b11028

Earlier this morning, a smart contract bug was first discovered in Yggdrash (YEED) that allowed anyone **except** the contract creator to enable and disable token transfers for everyone.

A short while later the same bug was found in the Icon (ICX) smart contract. A few minutes ago, someone began spamming the contract with disable transfer transactions.

ICX is unable to be moved from any wallet at this point.

---

edit: And now Binance has suspended ICX withdrawls and deposits.

edit2: Binance has re-enabled the ICX wallet. Currently token transfers are enabled but may be disabled by the smart contract and anyone with the gas to send in the command.

edit3: looks like it was found first by these guys at 3:30pm PST according to their twitter

edit4: Icon team says issue is resolved. How? By them spamming enable transfer every minute. All it takes is one bad actor who wants to stop transfers and knows how to win a mining war and their fix will stop working.

Quelle: https://www.reddit.com/r/CryptoCurrency/comments/8rfm9w/all_transfers_of_the_800m_marketcap_icon_icx_are/

ICON – der Smart Contract

Etherscan
The Ethereum Block Explorer

LOGIN | Search by Address / Txhash / Block / Token / Ens | GO | Language

HOME | BLOCKCHAIN | TOKENS | RESOURCES | MORE

Contract 0xb5A5F22694352C15B00323844aD545ABb2B11028

Home / Accounts / Address

Etherscan - Sponsored slots available. Book your slot here!

Contract Overview

Balance:	0 Ether
Ether Value:	$0
Transactions:	318774 txns
Token Tracker:	ICON (ICX)

Misc: More Options

Address Watch:	Add To Watch List
Contract Creator:	0xe16fd9b95758fe8... at txn 0x882350251f87729...
Token Balance:	View ($35,550.84) 48

Transactions | Erc20 Token Txns | Code | Read Contract | Write Contract Beta | Events | Comments (28)

⚠ **Warning:** *The Compiled Contract might be susceptible to ExpExponentCleanup (medium/high-severity), NestedArrayFunctionCallDecoder (medium-severity), ZeroFunctionSelector (very low-severity), DelegateCallReturnValue (low-severity), ECRecoverMalformedInput (medium-severity), SkipEmptyStringLiteral (low-severity) SolidityCompiler Bugs.*

Contract Source Code Verified (Exact Match)

Contract Name:	IcxToken	Optimization Enabled:	Yes
Compiler Text:	v0.4.11+commit.68ef5810	Runs (Optimiser):	0

Contract Source Code </> Copy | Find Similar Contracts

```
1  pragma solidity ^0.4.11;
2
3  contract Migrations {
4    address public owner;
```

Aus dem Quellcode generiert …

Contract ABI

Copy | Export ABI


```
":"unlockaddress","outputs":[{"name":"","type":"bool"}],"payable":false,"type":"function"},{"constant":false,"inputs":[{"name":"target","t
ype":"address"},{"name":"status","type":"bool"}],"name":"lockAddress","outputs":[],"payable":false,"type":"function"},{"constant":true,"in
puts":[],"name":"lock","outputs":[{"name":"","type":"bool"}],"payable":false,"type":"function"},{"inputs":[{"name":"initial_balance","type
":"uint256"},{"name":"wallet","type":"address"}],"payable":false,"type":"constructor"},{"anonymous":false,"inputs":[{"indexed":false,"name
":"burnAddress","type":"address"},{"indexed":false,"name":"amountOfTokens","type":"uint256"}],"name":"TokenBurned","type":"event"},{"anony
mous":false,"inputs":[],"name":"TokenTransfer","type":"event"},{"anonymous":false,"inputs":[{"indexed":false,"name":"lockaddress","type":"
address"},{"indexed":false,"name":"status","type":"bool"}],"name":"Locked","type":"event"},{"anonymous":false,"inputs":[{"indexed":false,"
name":"unlockedaddress","type":"address"},{"indexed":false,"name":"status","type":"bool"}],"name":"Unlocked","type":"event"},{"anonymous":
false,"inputs":[{"indexed":true,"name":"from","type":"address"},{"indexed":true,"name":"to","type":"address"},{"indexed":false,"name":"val
ue","type":"uint256"}],"name":"Transfer","type":"event"},{"anonymous":false,"inputs":[{"indexed":true,"name":"owner","type":"address"},{"i
ndexed":true,"name":"spender","type":"address"},{"indexed":false,"name":"value","type":"uint256"}],"name":"Approval","type":"event"}]
```


Contract Creation Code

Switch Back To Bytecodes View

```
PUSH4 0xffffffff
PUSH1 0xe0
PUSH1 0x02
EXP
PUSH1 0x00
CALLDATALOAD
DIV
AND
PUSH4 0x095ea7b3
DUP2
EQ
```

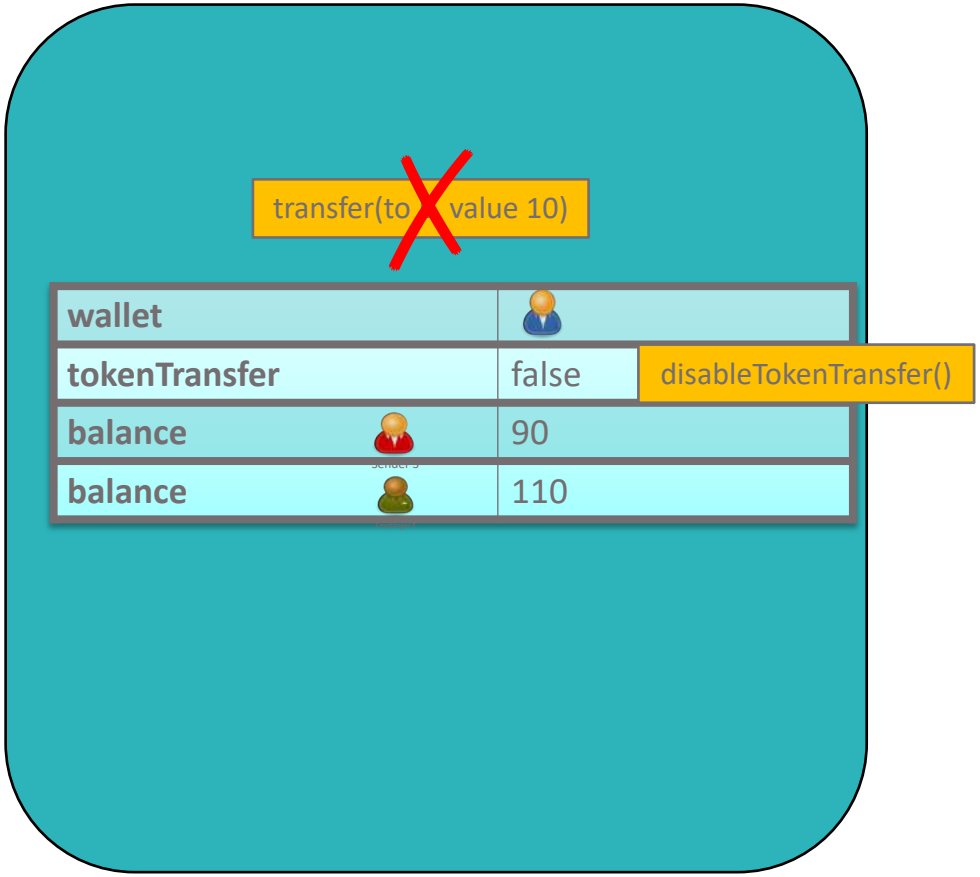
Contract Creation Code

Switch To Opcodes View


```
252519081900360200190f35b341561013f57fe5b61010160016a060020a03600435811690602435166044356104 7a565b604080519115158252519081900360200190f35b
341561017857fe5b61018061063f565b005b341561018a57fe5b61018060016a060020a036004351660243515156106865 65b005b34156101ad57fe5b6101b561070e565b6
0408051600160a060020a039092168252519081900360200190f35b34156101d957fe5b61010161071d565b604080519115158252519081900360200190f35b34156101fd57
fe5b61018060043561072b565b005b341561021257fe5b610125600160a060020a036004351661082d565b604080519182525190819003602001 90f35b341561024057fe5b6
101b561084c565b60408051600160a060020a039092168252519081900360200190f35b341561026c57fe5b61010160016a060020a036004351660243561086156 5b604080
5191151582525190819003602001 90f35b341561029f57fe5b61010160016a060020a036004351661099c565b604080519115158252519081900360200190f35b34156102c
f57fe5b6101256109b1565b604080519182525190819003602001 90f35b34156102f157fe5b610125600160a060020a036004358116906024351661 09b7565b604080519182
525190819003602001 90f35b341561032557fe5b6101806109e4565b005b341561033757fe5b610101600160a060020a036004351661 0a27565b604080519115158252519 08
1900360200190f35b341561036757fe5b61018060016a060020a036004351660243515156 10a3c565b005b341561038a57fe5b610101610ae6565b604080519115158252 51
9081900360200190f35b600154600090610100900460ff1615156103e257600160a060020a033316600090815260026020526040902054 60ff1615156103e25760006000fd5
b5b600160a060020a033316600090815260036020526040902054 60ff161561040a5760006000fd5b600160a060020a033381166000818152600560209081526040808320 94
```

Was macht der ICON-Smart Contract?

ICON Smart Contract Entwickler D



Wallet W

Sender S

Empfänger E

ICON – Transfer von Coins

```
187     function transfer( address to, uint value)
188     isTokenTransfer
189     checkLock
190     returns (bool success) {
191
192         require( _balances[msg.sender] >= value );
193
194         _balances[msg.sender] = _balances[msg.sender].sub(value);
195         _balances[to] = _balances[to].add(value);
196         Transfer( msg.sender, to, value );
197         return true;
198     }
```

isTokenTransfer

Contract Source Code </>

```
41      bool public tokenTransfer;
42      address public owner;
43      mapping( address => bool ) public unlockaddress;
44      mapping( address => bool ) public lockaddress;
45
46      event Locked(address lockaddress,bool status);
47      event Unlocked(address unlockedaddress, bool status);
48
49
50      // if Token transfer
51      modifier isTokenTransfer {
52          // if token transfer is not allow
53          if(!tokenTransfer) {
54              require(unlockaddress[msg.sender]);
55          }
56          _;
57      }
58
59      // This modifier check whether the contract should be in a locked
60      // or unlocked state, then acts and updates accordingly if
61      // necessary
62      modifier checkLock {
63          if (lockaddress[msg.sender]) {
64              throw;
65          }
```

tokenTransfer
Transfers ermöglichen oder blockieren

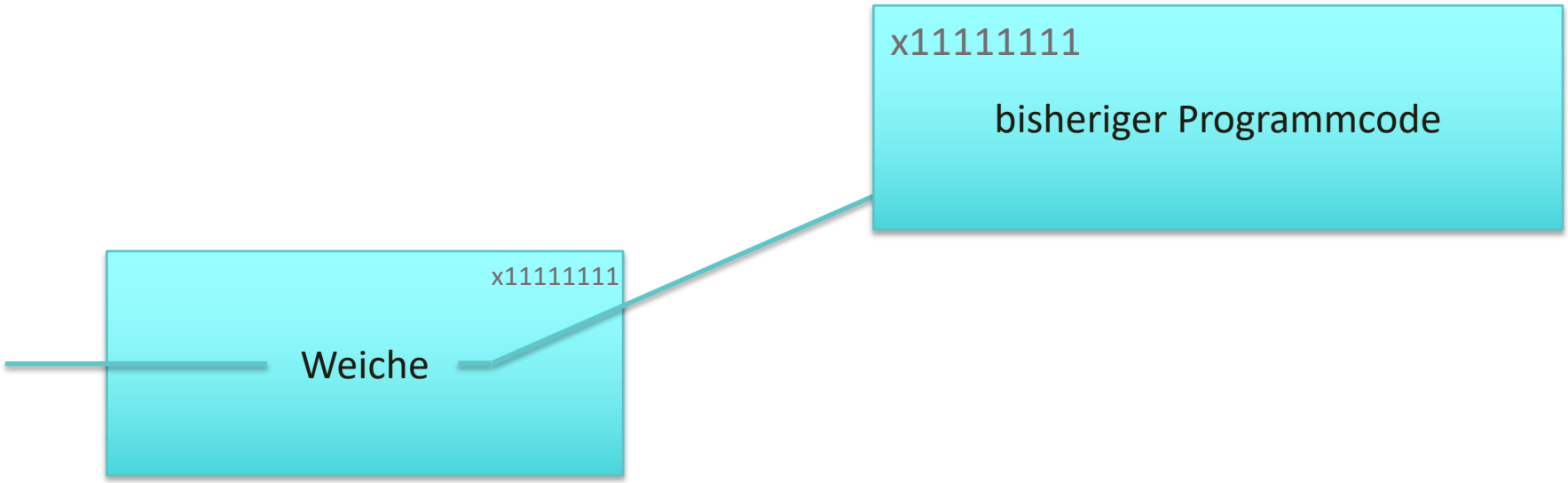
```
function enableTokenTransfer()
external
onlyFromWallet {
    tokenTransfer = true;
    TokenTransfer();
}

function disableTokenTransfer()
external
onlyFromWallet {
    tokenTransfer = false;
    TokenTransfer();
}
```

```
modifier onlyFromWallet {
    require(msg.sender != walletAddress);
    _;
}
```

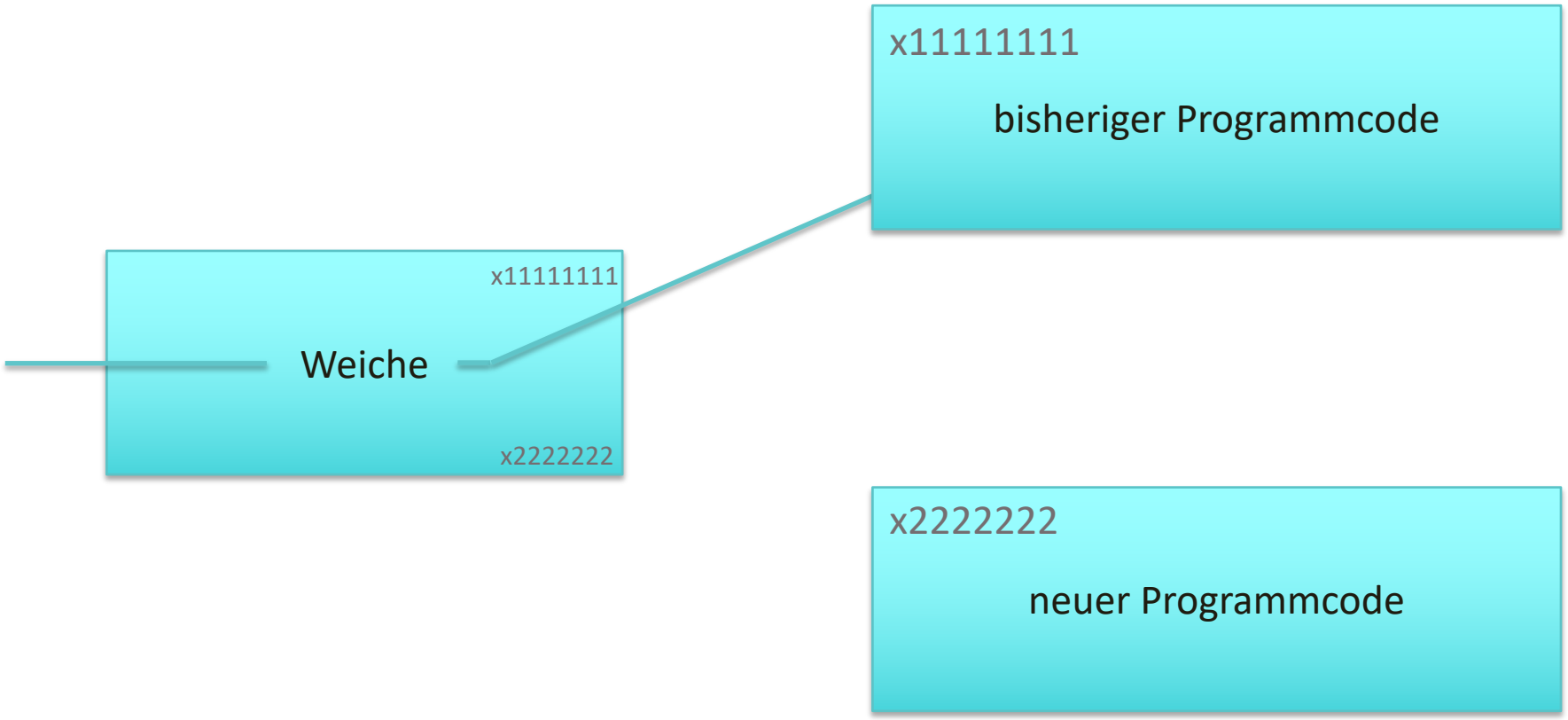
Nur walletAddress darf blockieren

```
// ICON ICX Token
/// @author DongOk Ryu - <pop@theloop.co.kr>
contract IcxToken is ERC20, Lockable {
    using SafeMath for uint;

    mapping( address => uint ) _balances;
    mapping( address => mapping( address => uint ) ) _approvals;
    uint _supply;
    address public walletAddress;

    //event TokenMint(address newTokenHolder, uint amountOfTokens);
    event TokenBurned(address burnAddress, uint amountOfTokens);
    event TokenTransfer();

    modifier onlyFromWallet {
        require(msg.sender != walletAddress);
        _;
    }

    function IcxToken( uint initial_balance, address wallet) {
        require(wallet != 0);
        require(initial_balance != 0);
        _balances[msg.sender] = initial_balance;
        _supply = initial_balance;
        walletAddress = wallet;
    }

```

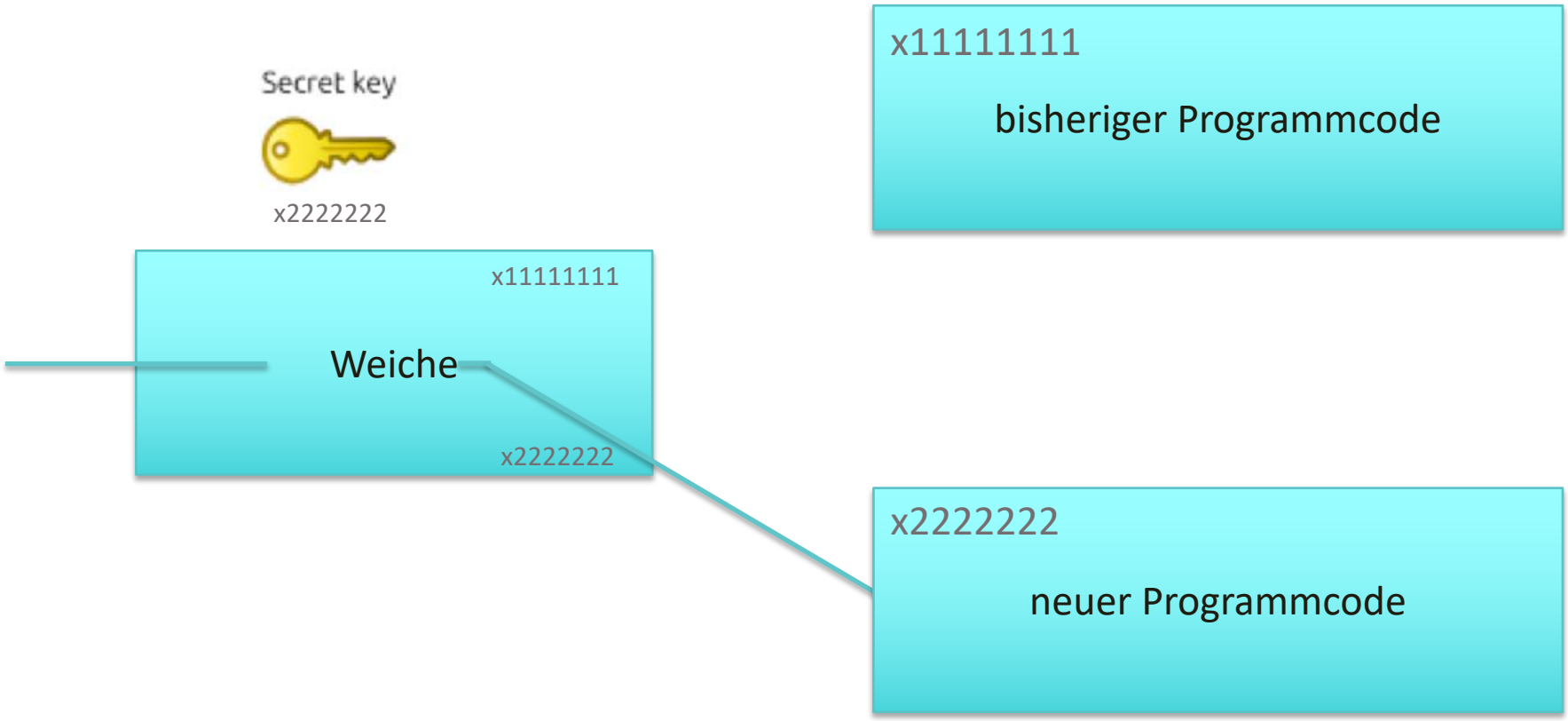
Updates für Smart Contracts?



Updates für Smart Contracts?



Updates für Smart Contracts?



Was bedeutet eine Update-Weiche?

+ Bugs können behoben werden

- Kein Vertrauen in die unveränderliche Ausführung des Smart Contracts

Update-Weiche erfordert Governance um Gefahr des Missbrauchs zu reduzieren!

Lösungsansätze

- Sicherere Programmiersprachen
- Frameworks, die die Programmierung kapseln
- Automatisierung des Auditing / Testings
- Integration mit Dispute Resolution

Viele neue Fragen für Juristen

- Welches Recht ist überhaupt anwendbar?
- Sind Smart Contracts überhaupt Verträge? Sollte ein schriftlicher Rahmenvertrag geschlossen werden?
- Wer ist mein Anspruchsgegner? Was für Ansprüche habe ich?
- Wo liegen die Grenzen für Haftungsbeschränkungen in der Praxis?
- (…)

Vielen Dank für Ihre Aufmerksamkeit!

Fragen, Diskussion