smart contracts

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

spending the money of a utxo the easy story

- this is similar to a challenge response protocol
- txin of a transaction tx provides...
  - public key whose hash should match the address in txout
  - **signature** of a string X
- X is a string derived from...
  - tx where signatures are omitted
  - the destination address contained in referred txout

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

the reality: the conditions for unlocking funds can vary

- **only one subject can spend**
- anyone can spend
- nobody can spend (logging)
- M-of-N subjects should agree to spend
- one subject can spend after a certain amount of funds are accumulated (croudfunding)
- one (or many) can spend after a certain time
- etc…
- a combination of the above

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

scripts

- **locking** script (a.k.a. scriptPubKey)
  - associated with txout
  - states conditions to spend the output (a “question”)
    - usually it specifies the (hash of) a public key
- **unlocking** script (a.k.a. scriptSig)
  - associated with txin
  - should «match» the conditions of the corresponding txout (the “answer”)
    - usually it contains a signature
- the output of the unlocking script (answer) is used as input for the locking script (question)
  - essentially: (1) exec the unlocking script (2) exec the unlocking without resetting the stack (3) success if top of the stack is not zero and no operation failed
- executed as part of consensus checks

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

the language

- proprietary
- simple
- stack-based
- **no state**
- same execution on all nodes
- no iteration instructions
  - Turing incomplete

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

the language

- read and executed from left to right
- **constants** push themselves onto the stack
- arithmetic: ADD, SUB, …
- stack: DUP, DROP, ROT, 2DUP, …
- flow: IF, ELSE, ENDIF, VERIFY, RETURN, …
- crypto: HASH160, SHA1, CHECKSIG, CHECKMULTISIG …
- time: CHECKLOCKTIME,

https://en.bitcoin.it/wiki/Script

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

examples

- pay-to-public-key-hash (the “standard” one)

  unlock: <sig> <pubKey>

  lock: DUP HASH160 <pubKeyHash> EQUALVERIFY CHECKSIG

- anyone-can-spend

  unlock: (empty)

  lock: TRUE

- provably-unspendable, just to store data

  lock: RETURN <data max 80 bytes> (never considered an UTXO for efficiency)

- A or B can spend

  unlock: <sig> <A-or-BpubKey> <1 for A, 0 for B>

  lock: IF DUP HASH160 <ApubKeyHash>
  ELSE DUP HASH160 <BpubKeyHash> ENDIF
  EQUALVERIFY CHECKSIG

- freezing funds until a time in the future

  unlock: <sig> <pubKey>

  lock: <expiry time> CHECKLOCKTIMEVERIFY DROP
  DUP HASH160 <pubKeyHash> EQUALVERIFY CHECKSIG

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

smart contracts

- each one of these scripts is called *smart contract*
  - it is not a “legal contract”, it is just a script!
  - they may realize/support legal contracts
    - it might be recognized as a contract, if parties agree that “code is law”, since the execution is checked by consensus
- enable to use the bitcoin blockchain for other purposes:
  - colored coins
    - *tokens,* that are distinct from bitcoin, whose transactions are recorded in the bitcoin blockchain
    - obsoleted by the rising of the transaction fees
  - record of transaction for generic assets
  - settlement of off-chain transactions
    - so called “payment channels”, see the Lightning Network

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

bitcoin for smart contracts: limits

- high fees
- limited expressiveness
  - Turing incomplete
- slow
- the blockchain records any “state change”
  - unhandy for software execution

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

Ethereum

- Ethereum is targeted to smart contracts

	Bitcoin	Ethereum
Turing completeness	NO	**YES**
persistent values for scripts	not supported, complex, just UTXO, usually need external code	contracts accounts **can store variables**, easy to retrieve
blockchain contains	just transactions	**current status**
language	simple stack based	**high level language** compiled in a bytecode for the Ethereum Virtual Machine
block time	10 minutes	**20 seconds**
consensus	PoW	PoW->PoS?
block size limit	1MB	adjusted dynamically, no limit

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

accounts

- in bitcoin the lock script states what should be provided to unlock funds
  - it is a feature of every UTXO
  - some standard scripts (P2PKH, 2-of-3, etc.)
  - potentially infinite kinds of UTXO
- in Ethereum just two kinds of accounts
  - Externally Owned Accounts (EOA)
  - contract accounts

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

accounts

	EOA	**contract**
associated keys	**yes**	**no**
balance	yes	yes
other persistent values/variables	no	yes, it also stores EVM bytecode
as a transaction sender…	• can send ETH • can call operations on a contract	• can send ETH • can call operations on another contract (in the same transaction)
as a transaction recipient…	• can receive ETH	• can receive ETH • always executes an operation (possibly the fallback one)

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

transactions fields

- (sender address)
- recipient address
- value (exchanged ETH)
- data
- nonce (increasing to avoid replay attack)
- gas price
- gas limit

- max fee = gas price * gas limit
  - actual fee depends on the executed code
  - if a tx run “out of gas”, it is reverted, but fee is taken anyway

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

contract lifecycle

- written in a high-level language
- compiled to EVM bytecode
- deployed
  - transaction sent to special address 0x0 and bytecode as data
- operations are called on the contract
  - as part of transactions, which may update its state
- cannot be deleted, but the contract can selfdestruct itself

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

a solidity example

- anyone can withdraw funds from this contract

```
1 // Our first contract is a faucet!
2 contract Faucet {
3
4     // Give out ether to anyone who asks
5     function withdraw(uint withdraw_amount) public {
6
7         // Limit withdrawal amount
8         require(withdraw_amount <= 10000000000000000);
9
10         // Send the amount to the address that requested it
11         msg.sender.transfer(withdraw_amount);
12     }
13
14     // Accept any incoming amount
15     function () public payable {}
16
17 }
```

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

```
4 contract owned {
5  address owner;
6  // Contract constructor: set owner
7  constructor() {
8   owner = msg.sender;
9  }
10  // Access control modifier
11  modifier onlyOwner {
12   require(msg.sender == owner,
13           "Only the contract owner can call this function");
14   _;
15  }
16 }
17
18 contract mortal is owned {
19  // Contract destructor
20  function destroy() public onlyOwner {
21   selfdestruct(owner);
22  }
23 }
24
25 contract Faucet is mortal {
26  event Withdrawal(address indexed to, uint amount);
27  event Deposit(address indexed from, uint amount);
28
29  // Give out ether to anyone who asks
30  function withdraw(uint withdraw_amount) public {
31   // Limit withdrawal amount
32   require(withdraw_amount <= 0.1 ether);
33   require(this.balance >= withdraw_amount,
34    "Insufficient balance in faucet for withdrawal request");
35   // Send the amount to the address that requested it
36   msg.sender.transfer(withdraw_amount);
37   emit Withdrawal(msg.sender, withdraw_amount);
38  }
39  // Accept any incoming amount
40  function () public payable {
41   emit Deposit(msg.sender, msg.value);
42  }
43 }
```

evolution

- state variables
- constructors
- inheritance
- custom modifiers
- assertions
- events

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

simple things might be complex

- for example, multisignature

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

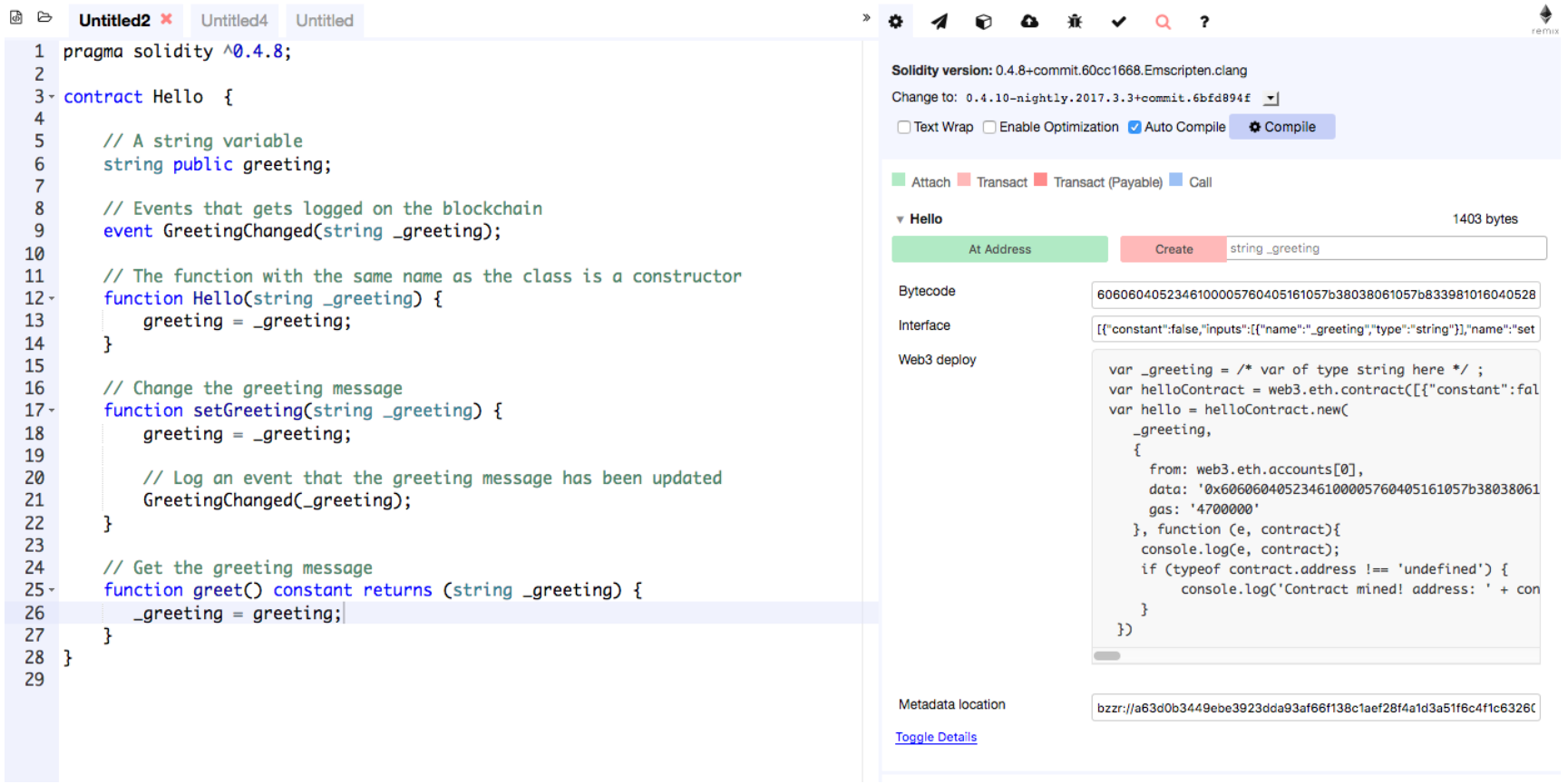
libraries

- libraries can be imported in a project as included code…
- …or from the blockchain!
  - …if you trust it!

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

remix

- a basic web based editor, emulator, debugger
- https://remix.ethereum.org



© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

contracts security

- contracts are usually not very long
- writing contracts is easy
- **writing secure contracts is difficult**
  - solidity/EVM semantic may be subtle
  - mistakes may cost a lot of money!

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

references

- A. M. Antonopoulos – Mastering Bitcoin
- A. M. Antonopoulos, G. Wood - Mastering Ethereum

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti

© 2018 maurizio pizzonia – sicurezza dei sistemi informatici e delle reti