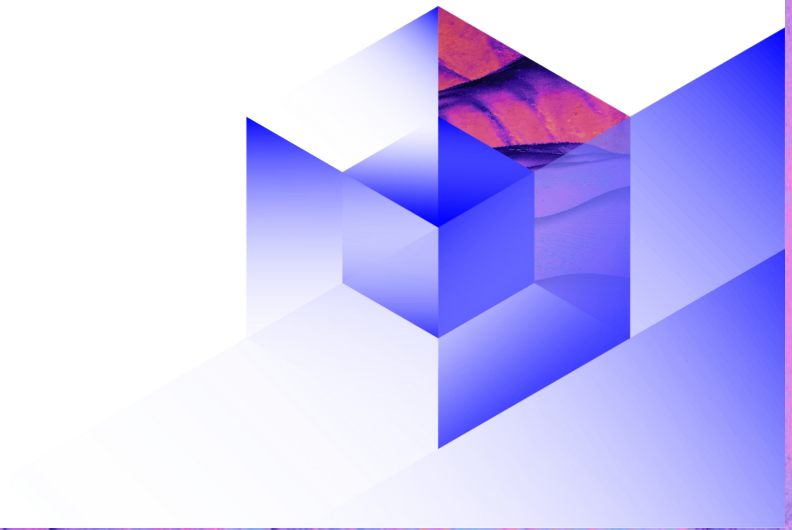
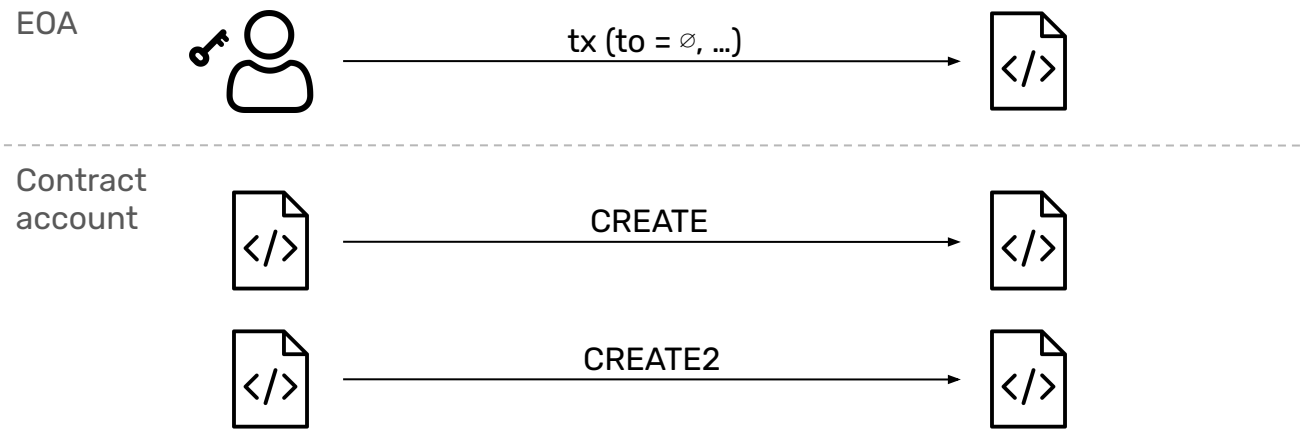
Things you didn't know about Contract Deployment

Theresa Wakonig



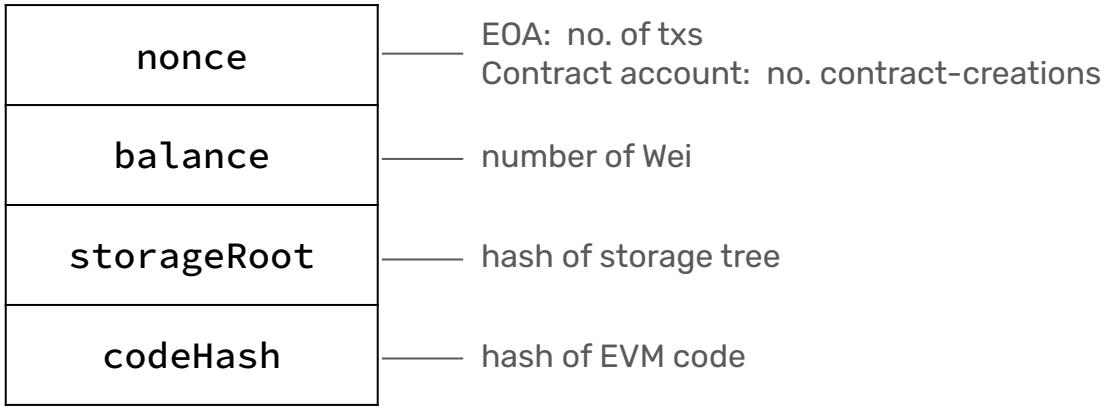
CHAINSECURITY

Contract Creation



What if we tried deploying at an address of an existing account?

Account State & Existence

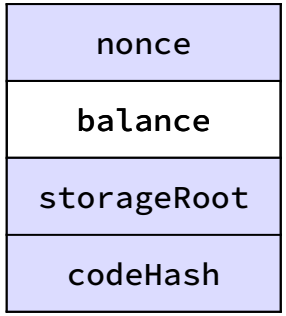


Implications on Contract Deployment

- **EIP-684:**
  Revert creation in case of collision

  nonce != 0: creation NOT allowed

  len(code) != 0: creation NOT allowed



- **EIP-7610:**
  Revert creation in case of non-empty storage

  storageRoot != 0: creation NOT allowed

  } contracts from *before* EIP-161

- balance **> 0**: creation allowed

EVM during Contract Construction

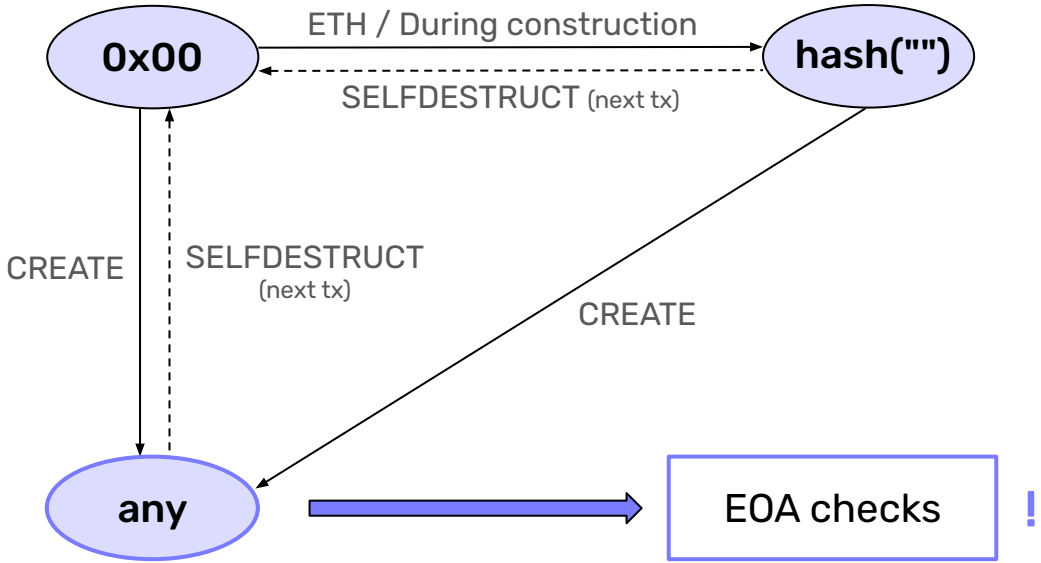
- Usually: `EXTCODESIZE(A) == CODESIZE` (executed by A)

- **During** contract construction …

opcode	output	opcode	output
`EXTCODESIZE`	0	`CODESIZE`	length of InitCode
`EXTCODECOPY`	0x00……0	`CODECOPY`	InitCode
`EXTCODEHASH`	0xc5d2…70 = hash("")		

!

Transitions: EXTCODEHASH of a Contract



... = value of EXTCODEHASH

Summary

- Contract account's nonce is incremented **before** constructor execution
- Can not create "on" existing contracts or EOAs
- Legacy contracts with non-zero storage, but zero nonce and code

- EXTCODEHASH transitions: **Try it out yourself!**

https://remix.ethereum.org/#gist=e082dcdc28be5ad51e47577fe9ef66d4

: : @chain_security