APPLIED COMPUTER SCIENCES

FFG Forschung wirkt.

FH JOANNEUM University of Applied Sciences

Web3 Security

FFG-Forum 2024

(https://picsart.com/)

11.09.2024
Wien, MQ-Libelle

DI(FH) Florian Temel, MSc MSc

FH JOANNEUM
University of Applied Sciences

Web 1.0/2.0/3

(https://de.wikipedia.org/wiki/Tim_Berners-Lee#/media/Datei:Sir_Tim_Berners-Lee.jpg)

- **Web 1.0**
  - static web – **read only**
  - 1990, Sir Tim Berners Lee
  - static HTML, low bandwidth

(https://ammunitiongroup.com/teams_pt/darcy-dinucci/)

- **Web 2.0**
  - dynamic/participative web – **read/write**
  - 1999, Darcy DiNucci
  - dynamic HTML, social media, multimedia contend

(Satoshi Nakamoto, Vitalik Buterin, Gavin Wood, wikipedia.com)

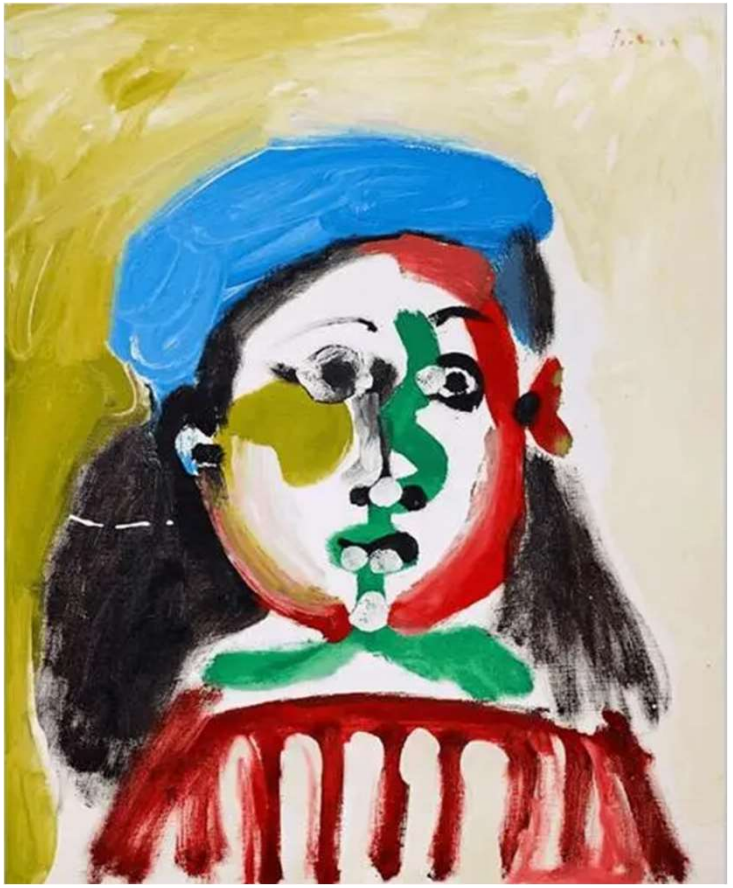
- **Web3**
  - semantic web – **read/write/own**
  - 2009, Satoshi Nakamoto, Bitcoin
  - 2014/2015, Vitalik Buterin, Gavin Wood, … Ethereum
  - Distributed ledger technologies (DLTs)

Web3 – use cases

- Bitcoin: Sound Money & Store of Value
- Ethereum: Smart Contracts

- Tokenization
- SSI, DAOs, DeFi, NFTs,…
- Automation of Business Processes
- New forms of commerce

- Web3 & DLTs
  - enable a new form of decentralized trust
  - disrupt inefficient 3rd parties' business models



Pablo Picasso's 1964 painting Fillette au béret
ARTEMUNDI

FFG Forschung wirkt.

FH JOANNEUM University of Applied Sciences

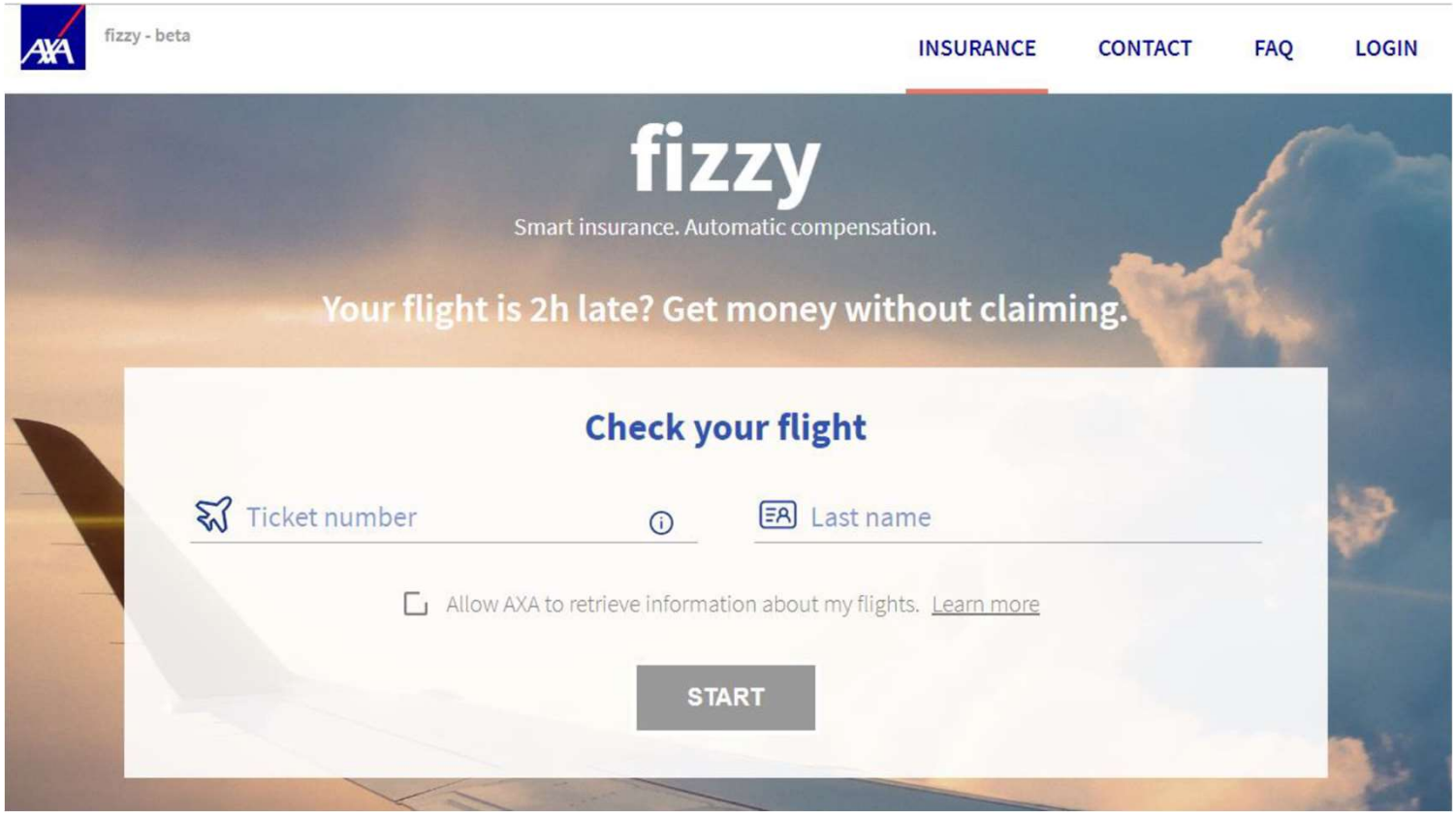
Web3 Attack Surface

- User
- Wallets
- Smart Contracts
- Infrastructure
- Economic Attacks
- Geopolitical/Legal Attacks/Bans
- Supply Chain Attacks
- Community Attacks/Forks
- Centralization
- …

ethereum classic

ethereum

Smart Contract Example



(https://fizzy.axa/, 2017)

Smart Contract Top 10 Threats

Top 10

- SC01:2023 - Reentrancy Attacks
- SC02:2023 - Integer Overflow and Underflow
- SC03:2023 - Timestamp Dependence
- SC04:2023 - Access Control Vulnerabilities
- SC05:2023 - Front-running Attacks
- SC06:2023 - Denial of Service (DoS) Attacks
- SC07:2023 - Logic Errors
- SC08:2023 - Insecure Randomness
- SC09:2023 - Gas Limit Vulnerabilities
- SC10:2023 - Unchecked External Calls

The DAO

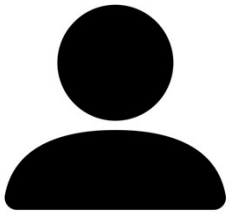
Company type	Decentralized autonomous organization
Industry	Cryptocurrency software venture capital fund
Founded	2016
Area served	Global[1]
Key people	Stephan Tual, Simon Jentzsch, Christoph Jentzsch
Total assets	ETH 11.5 million[2]
Owners	+18 000 stakeholders[3]
Number of employees	0 (automated)[4]

(https://en.wikipedia.org/wiki/The_DAO)

- OWASP Smart Contract top 10:
  - https://owasp.org/www-project-smart-contract-top-10/

Smart Contract Example

1.) Deposit 1 ETH



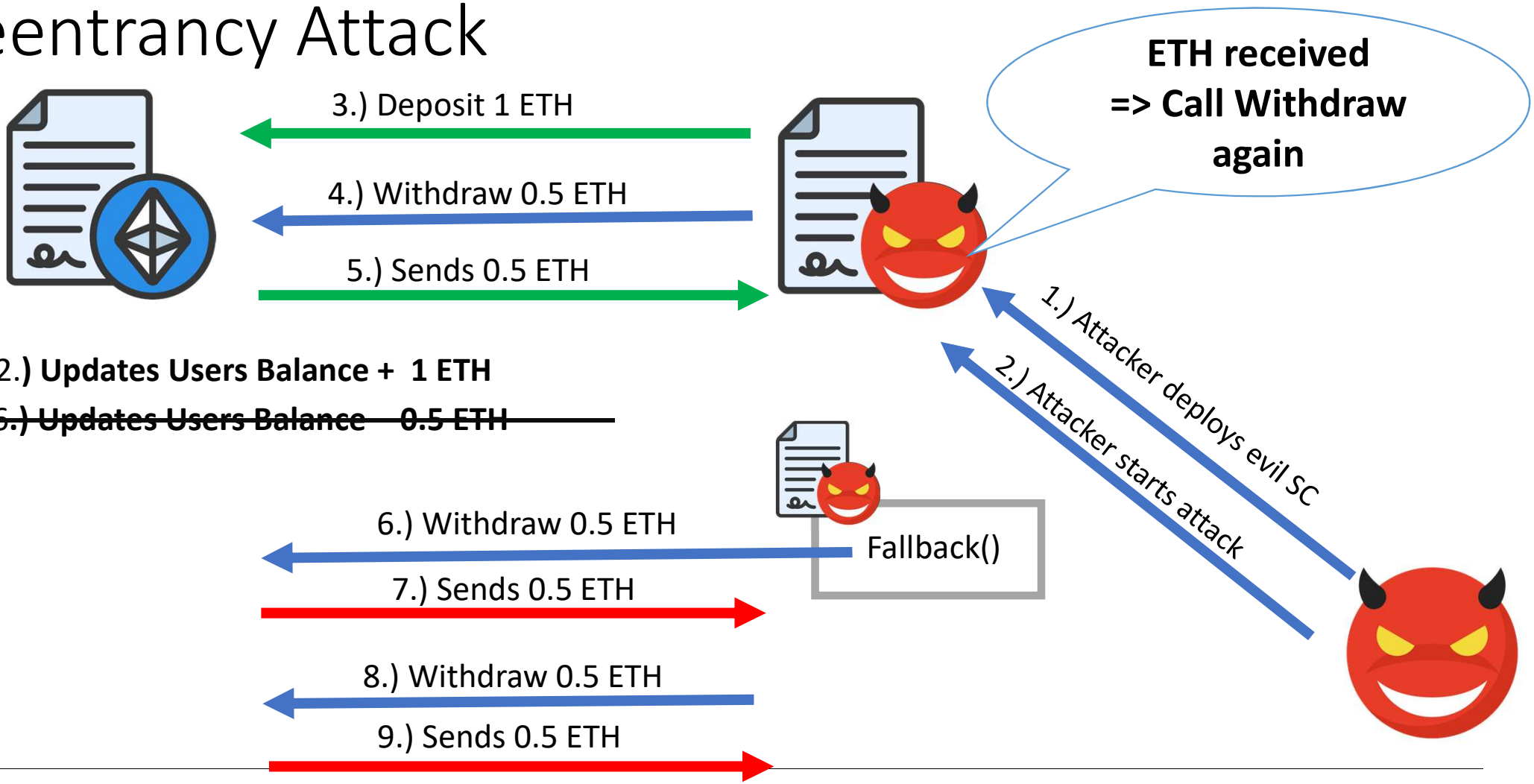
2.) Updates Users Balance + 1ETH

3.) Withdraw 0.5 ETH

4.) Sends 0.5 ETH to User

5.) Updates Users Balance – 0.5 ETH

Reentrancy Attack



..... continue until SC is empty

Reentrancy Mitigation

- Reentrancy Guards (OpenZeppelin)
- Checks, Effects, Interaction (CEI)
- Gas Limits
- Pull Payment

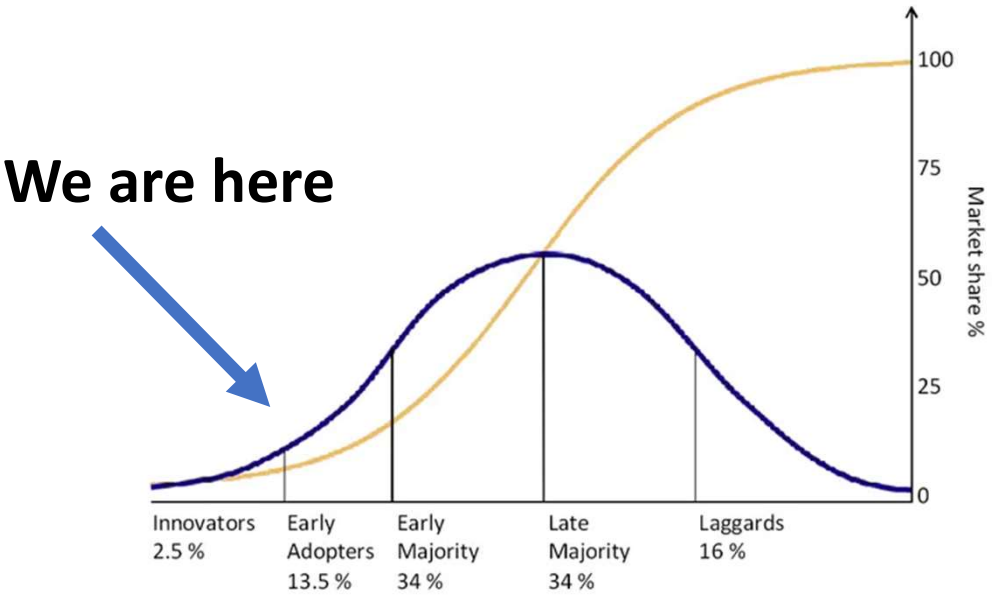
```
contract Reentrant {
  bool private lock;
  mapping (address => ulnt256) public userBalances;
  utnt256 public totalsupply;
  //SCT_ITALIA

  modifier nonReentrant() {
    require( !lock);
    lock = true;
    _;
    lock = false;
  //SCT_ITALIA
  }
  function withdrawAll() external nonReentrant {
    utnt256 balance = userBalances (msg. sender];
    require(balance > 0, "Insufficient balance");
    totalsupply -= balance;
    (bool done, ) = msg.sender.call{value: balance}("");
    require(done, "Failed to send Ether");
    userBalances(msg. sender] = 0;
  }
}
```

(https://smartcontract.tips/articoli/understanding-the-threat-of-read-only-reentrancy-attacks-on-yoursmart-contracts/)

Outlook & Challenges

- Number of Web3 Users
  - ~= 460 Million Bitcoin addresses
  - only about 37 % economical relevant
  - ~ 2 – 5 % global adoption

- Security Challenges
  - Complex interconnected systems
  - Vulnerability management
  - Governance & maintenance
  - User education



https://medium.com/@mcasey0827/speculative-bitcoin-adoption-price-theory-2eed48ecf7da

FFG Forschung wirkt.

FH JOANNEUM University of Applied Sciences

Thank you for your attention!

Contact:
florian.temel5@fh-joanneum.at