Reflections on Blockchain Security

Julian Martinez, Blockchain Advocate

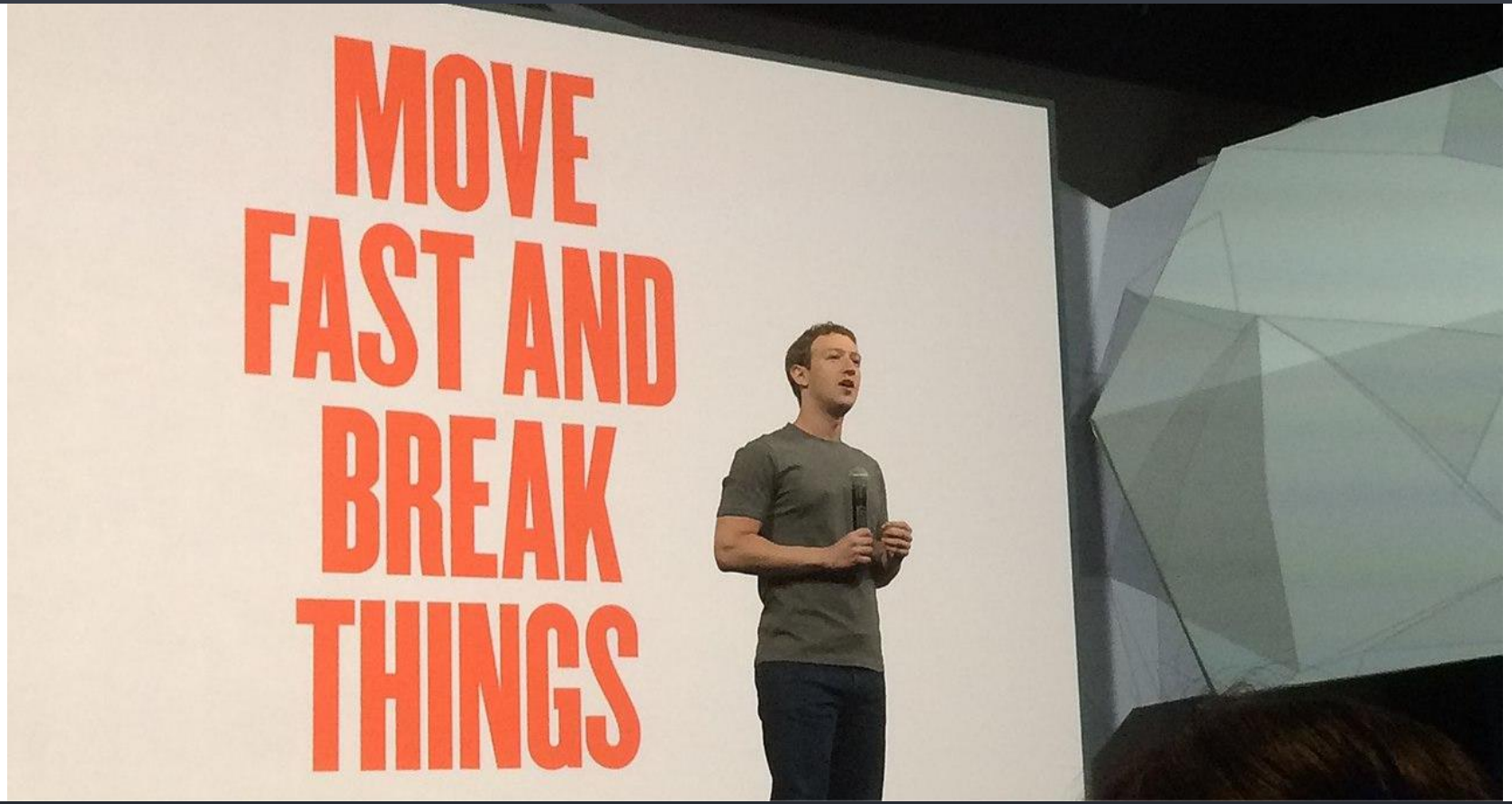
Quantstamp™

What are Smart Contracts?

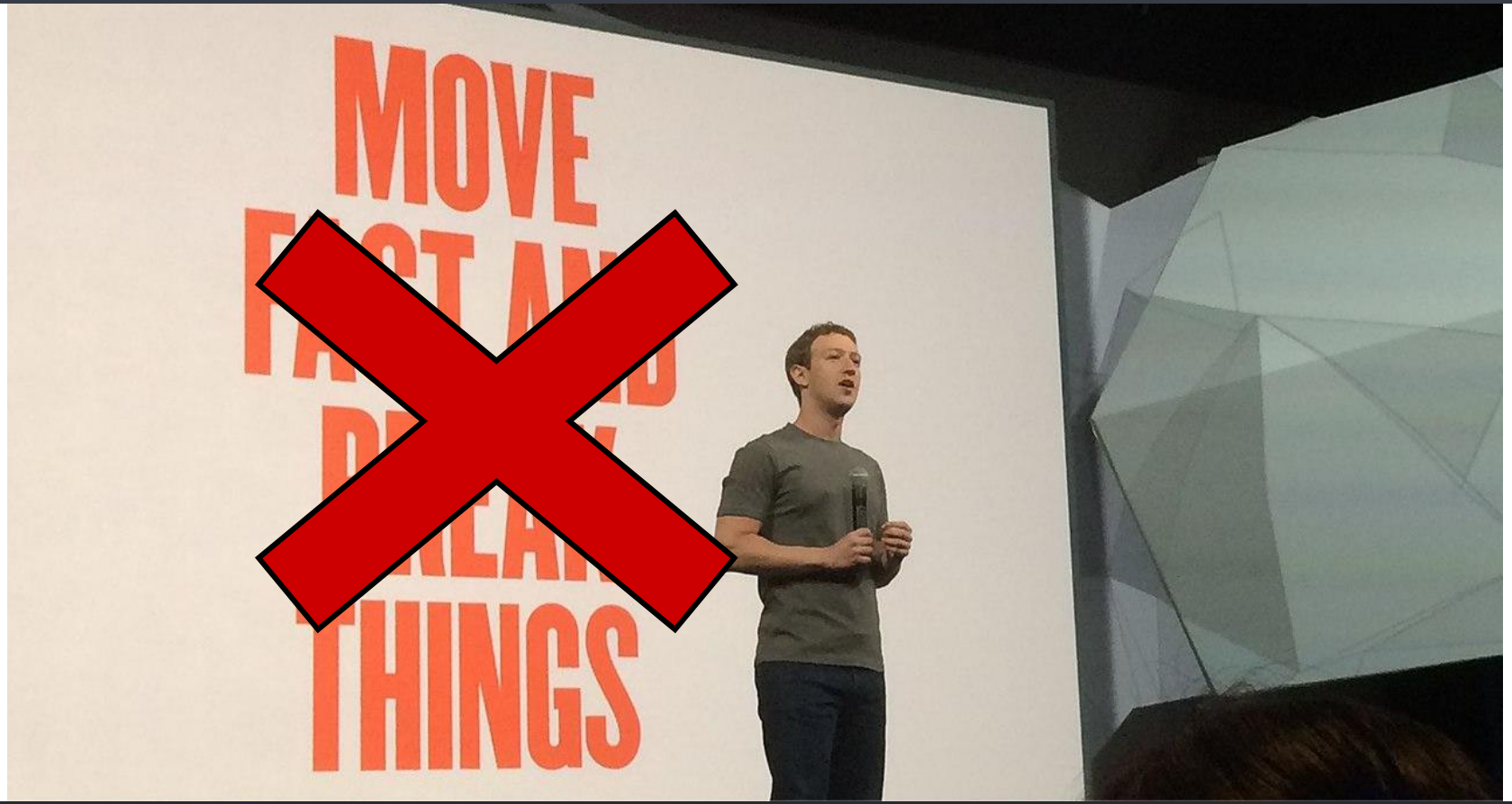
- Public and immutable programs
- Hold and transfer value
- Over 250 million USD worth of assets lost or stolen

```
1.  function withdraw() {
2.      if (balances[msg.sender] > 0
3.          && bankBalance > 0){
4.          msg.sender.call.value(balances[msg.sender])
5.          bankBalance -= balances[msg.sender];
6.          balances[msg.sender] = 0;
7.      }
8.  }
```

Traditional Web Development

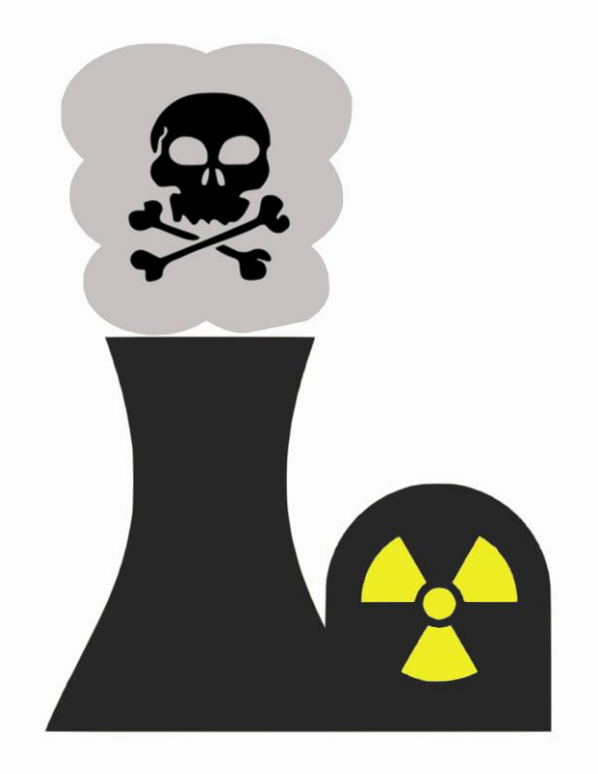


Traditional Web Development



Safety and Security Critical Workflow

- Safety and security critical workflow
  - Aviation
  - Nuclear power plants
  - Gov defense organizations
- What does this mean for smart contract development?

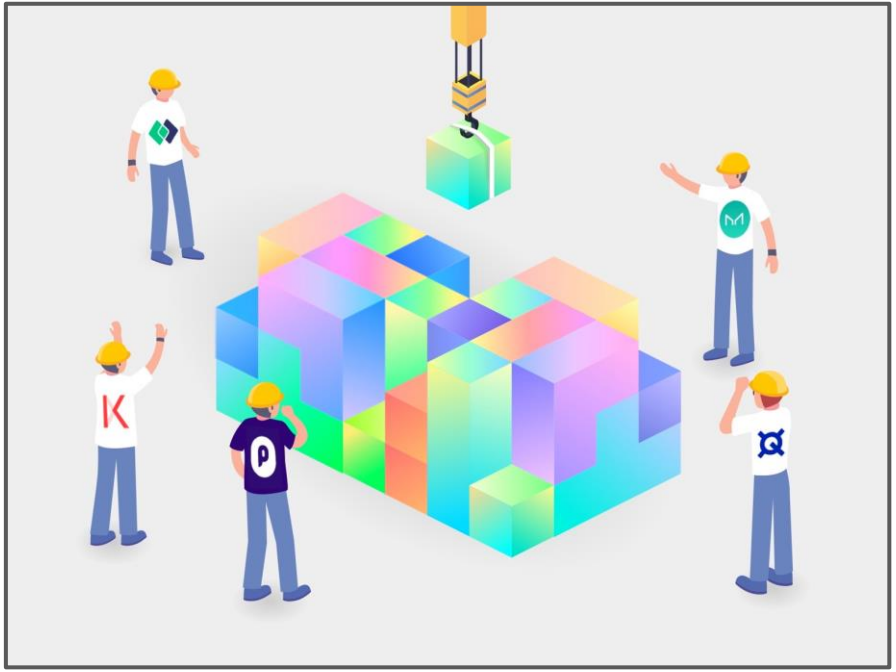


New Design Choices

- Gas efficiency
- Privacy level
- Privileged access vs. decentralization
- Mechanism design
- Oracles

Implementation and Testing

- Value simplicity
- Use tested patterns
- Write clear documentation
- 100% test coverage
- Use static analysis tools
- Get an external audit



Getting an External Audit with Quantstamp

The process:

- Code freeze
- Send clear documentation
- Receive initial report
- Respond with fixes
- Receive an audit certificate.

Paying Attention to Future Developments

- ETH 2.0
- Layer 2 developments
- eWasm
- Privacy solutions
- Generating randomness

Acknowledgements

Jan Gorzny
Blockchain Researcher

Martinet Lee
Research Engineer

Thank you!

Questions?

Quantstamp™

julian@quantstamp.com