FumbleChain

A Purposefully Vulnerable Blockchain

August 2019 Nils Amiet Blockchain Village

KUDELSKI SECURITY

Who am I?

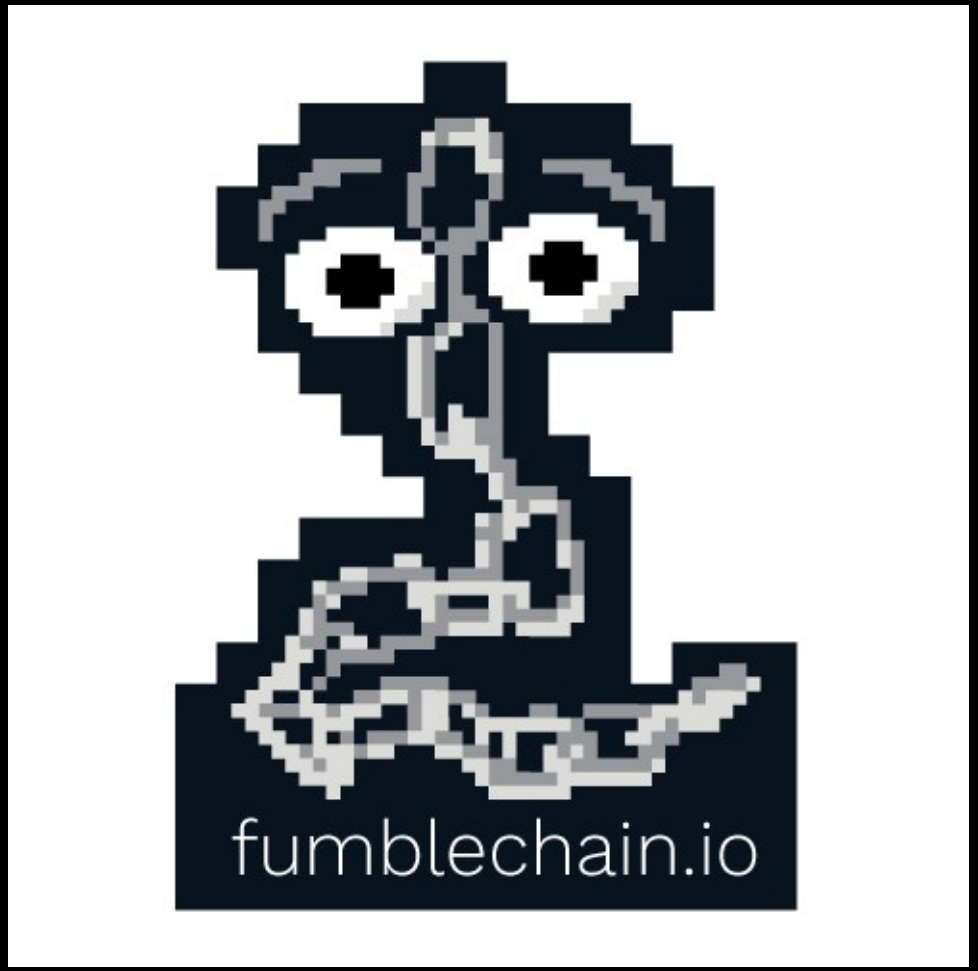
- Nils Amiet
- Research team @ KUDELSKI SECURITY
- Public speaker
- From Switzerland

Table of Contents

Introduction

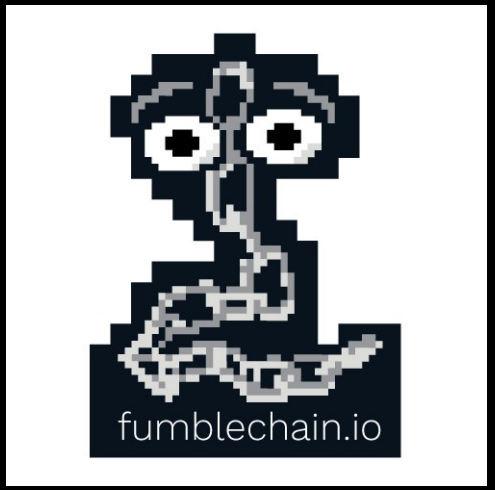
- Cryptocurrencies and blockchains are still relatively new
- Lots of news stories about people losing money due to compromises in blockchain ecosystem

Introducing FumbleChain



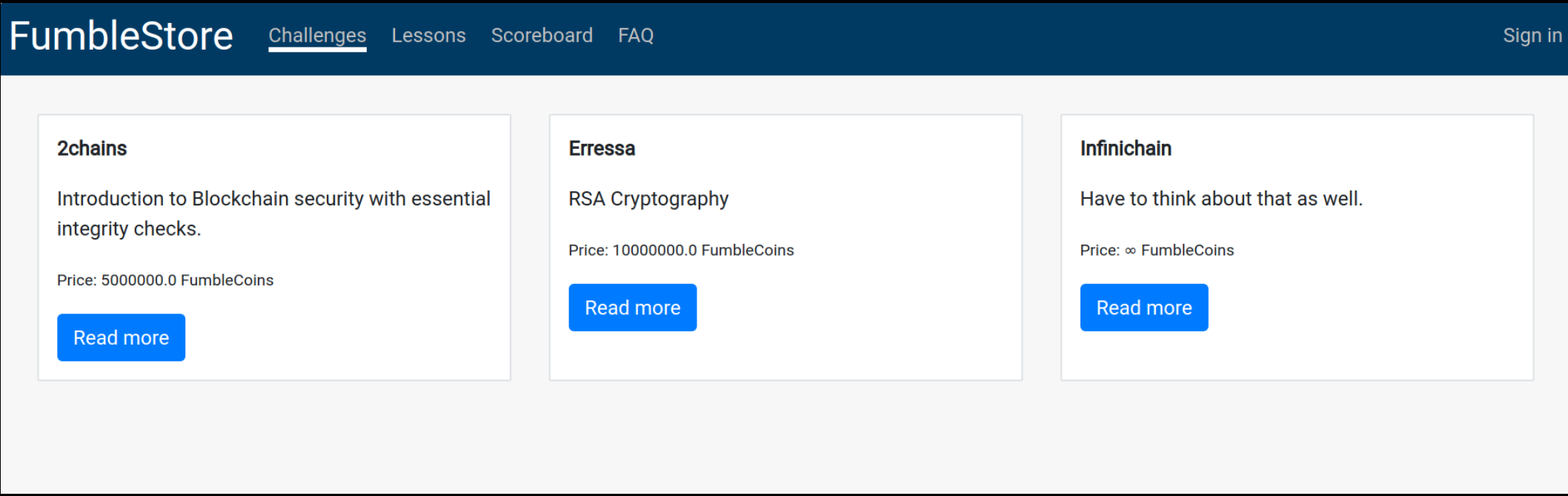
What is FumbleChain?

- FumbleChain hopes to bridge the awareness gap in a fun way
- Allows you to play with blockchain technology in a way that is easy to setup
- The “WebGoat” of blockchain
- Education tool
- Purposefully vulnerable Python3 blockchain



What’s included (1/4)

- FumbleStore: CTF in the form of a fake e-commerce website
  - Buy products with FumbleCoins
  - Exploit flaws and steal coins from crypto-wallets
  - Buy flags with coins to solve challenges


FumbleStore
Challenges
Lessons
Scoreboard
FAQ
Sign in
2chains
Introduction to Blockchain security with essential integrity checks.
Price: 5000000.0 FumbleCoins
Read more
Erressa
RSA Cryptography
Price: 10000000.0 FumbleCoins
Read more
Infinichain
Have to think about that as well.
Price: ∞ FumbleCoins
Read more

Description

FumbleCorp inc. introduced its latest innovative blockchain-based product named FumbleChain. It is an infrastructure allowing anyone to securely transfer FumbleCoins, a digital currency.

The FumbleChain network (mainnet) is the production network and the one people use to exchange real funds. Developers can use the FumbleChainDev network as a test network (testnet) for building the future of FumbleChain.

Client download

Download the client here: fumblechain.tar.gz

Then extract the archive and change to the `fumblechain` directory:

```
tar xf fumblechain.tar.gz
cd fumblechain
```

Challenge details

- Price: 5000000.0 FumbleCoins
- Solved 0 times

Are you stuck?

Show hint

Purchase

Please Sign in to purchase this product.

What’s included (2/4)

- Lessons/tutorials
  - 20+ lessons

- Using the FumbleChain CLI
- Using the Blockchain explorer
- Using the WebWallet
- Scripting with scli
- Network messages

Blockchain theory

- What is a blockchain?
- Consensus mechanisms
- Wallet balance models: Account vs UTXO
- What's in a block?
- Blockchain state synchronization
- Smart contracts and DApps

Blockchain vulnerabilities and exploitation

- Transaction input validation
- Other-chain replay attacks
- Same-chain replay attacks

What’s included (3/4)

- Blockchain explorer
  - Runs in your web browser

FumbleChain Explorer Peers Transaction pool WebWallet

Wallet dOeEdhZnZFQjRNSmxaTThBODI4WmgzWg

Balance: 1 FumbleCoins

Wallet address

LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlHZE1BMEdDU3FHU0liM0RRRUJBUVVBQTRHTEFEQ0Jod0tCZ1FERFdOeEdhZnZFQjRNSmxa
TThBODI4WmgzWgpsSytEaXBwb1I6L1p2NUE3SnliUEx1azE0Uk81ZkJ4ODBaSXJZUGgxNzNIZVFWQk9NRVN5elc0c2xEY3NxRGh4ClFqYVhaSGI
KSFRFUnp1M2FzMFM1SitHV2tqT0Y3VXFCU1RJWW1mNkNNYWNLbW10Y3pMZVJxVloxV3N6dzNxREIKTWFGNW4rbjZXOE1Id285RWx3SUJB
dz09Ci0tLS0tRU5EIFBVQkxJQyBLRVktLS0tLQo=

This is the wallet's public address.

Incoming transactions

Timestamp	Index	Source	Destination	Quantity	Block	Balance before	Balance after
2019-07-31T09:26:32.811917	f235e6c4-dad3-46e4-960c-f95d35d9b16e	0	dOeEdhZnZFQjRNSmxaTThBODI4WmgzWg	1	Block 2	0	1

Outgoing transactions

Timestamp	Index	Source	Destination	Quantity	Block	Balance before	Balance after

What’s included (4/4)

- Wallet
  - Command line
  - Web Wallet (runs in your web browser)

```
└─>$ ./cli.py
Using API: http://localhost:1337/
===============================
FumbleChain v1.0
Type help or ? to list commands.
===============================
fumblechain > help

Documented commands (type help <topic>):
========================================
EOF         debug  mine  show         transaction_raw
block_raw   help   quit  transaction  wallet

fumblechain >
```

Active wallet webwallet_1.wallet Balance: 2

Wallet webwallet_1.wallet

Change

Create transaction

Destination someone

Please insert the destination wallet address.

Quantity 0.23

Please insert how many FumbleCoins to send.

Send

Requirements

- Linux, macOS
- git
- docker
- docker-compose
- About 3 minutes of your time :)

How to use it?

- git clone https://github.com/kudelskisecurity/fumblechain.git
- cd fumblechain
- git checkout fumblestore
- cd src/fumblechain
- ./init_ctf.sh
- Wait about 3 minutes
- Browse http://localhost:20801
- Start playing!

```
Successfully built 0b62ef037ad7
Successfully tagged fumblechain_echoservice:latest
Creating fumblechain_mainnet2-node_1 ... done
Creating fumblechain_mainnet-node_1  ... done
Creating fumblechain_echoservice_1   ... done
Creating fumblechain_moneymaker_1    ... done
Creating fumblechain_testnet-node_1  ... done
Creating fumblechain_fumblestore_1   ... done
Creating fumblechain_mainnet3-node_1 ... done
```

```
==========================================
=                DISCLAIMER                =
==========================================
When running this software on your own machine, you may expose yourself to attacks.
We cannot guarantee that the software is bug-free.
Upon starting the FumbleStore, various background services are started.
These services will listen for incoming connections on multiple TCP ports.
Proceed with caution and make sure your firewall rules are properly set.

******************************************
*         Accessing the FumbleStore      *
******************************************

The FumbleStore should now be up and running at http://localhost:20801

To shutdown all FumbleChain services, type:
docker-compose down
```

Tool demo

- Demo

Live demo available!

- Test it live at https://demo.fumblechain.io
- See fumblechain.io for more information

Run it on your own machine

- Open source project
  - kudelskisecurity/fumblechain @ Github
  - Community effort
- Contributions are welcome
  - New challenge ideas
  - New lessons
- Start hacking today!

Thank you

- Questions?

- fumblechain.io