CRYPTO FINANCE AG

Storing Crypto Assets at Scale

Dr. Lewin Boehnke

- Head of Research @ Crypto Finance AG (lewin.boehnke@cryptofinance.ch)
- CTO @ Crypto Storage AG (lewin.boehnke@cryptostorage.ch)


CRYPTO FINANCE AG
YOUR GATEWAY TO THE CRYPTO WORLD.
EXCELLENCE. QUALITY. INTEGRITY.
CRYPTO FINANCE
WWW.CRYPTOFINANCE.CH

CRYPTO FINANCE GROUP

Board of Directors

- Jan Brzezek
- Marc P. Bernegger
- Raymond J. Bär
- Dr. Tobias Reichmuth
- Pascal Forster
- Dr. Philipp Cottier

CRYPTO FINANCE

CRYPTO FUND

An asset manager which establishes the first swiss fund for crypto assets in Switzerland available for qualified investors

CRYPTO BROKER

Allows institutional investors to buy & sell crypto assets directly with exchanges and brokers through experienced traders

CRYPTO STORAGE

Stores crypto assets in an impenetrable, convenient and 100% Swiss technology solution

Warum ist das schwer?

- „Klassisches“ Bankensystem

- Crypto Assets

Bloomberg: Deutsche Bank makes $35bn derivatives payments mistake to Eurex Clearing

April 20, 2018

Deutsche Bank AG made an accidental $35 billion payment to Eurex Clearing when it inadvertently transferred €28 billion to one of its outside accounts, Bloomberg News has revealed. While the blunder was quickly reversed and caused no financial harm, it's a stark reminder of the vulnerability of even the most sophisticated financial firms.

The routine payment that went awry last month was one that Germany's biggest lender unintentionally sent to an exchange as part of its daily dealings in derivatives, a person familiar with the matter said. The errant transfer occurred about a week before Easter as Deutsche Bank was conducting a daily collateral adjustment, the person said. The sum, which far exceeded the amount it was due to post, landed in an account at Deutsche Boerse AG's Eurex clearinghouse, temporarily boosting the collateral held by the world's fourth-largest clearinghouse by more than half.

Es braucht nur eine einzige Zahl zum Ausgeben

- Warum ist das schwer?
  - **Privater** Schlüssel
    - z.B. KzVg7Z2mY63uMgZxrGrC4oweDZRd95KjyhFL27V7ZeEM46Ld9UrV
    - notwendig zum **ausgeben**
  - **Öffentlicher** Schlüssel[1]
    - 1KhW3jWM2NjpqKmQ9DJmeSYakivNi2cTjv
    - notwendig zum **einzahlen**
    - notwendig zum **beobachten**

[1]Ein paar Schritte wurden übersprungen

[2]Kann unterschiedlich sein je nach Asset

Es braucht nur eine einzige Zahl zum Ausgeben

- Wa

Summary	
Address	1KhW3jWM2NjpqKmQ9DJmeSYakivNi2cTjv
Hash 160	cd1b265f607e5b2f09760a745e11904463fae5ec
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	1
Total Received	0.0042 BTC
Final Balance	0.0042 BTC

Request Payment | Donation Button

  - Öffentlicher Schlüssel[1]
    - 1KhW3jWM2NjpqKmQ9DJmeSYakivNi2cTjv
    - notwendig zum **einzahlen**
    - notwendig zum **beobachten**

[1]Ein paar Schritte wurden übersprungen

[2]Kann unterschiedlich sein je nach Asset

Wie handhabt man Cryptos

Sehr einfach!

- Man nehme:
  - Einen Raum ohne Fenster
  - Einen Stift und Block
  - Einen Präzisionswürfel (Cellulosenitrat)
  - Ein gutes Buch über Kryptographie
  - Ein paar Stunden Zeit
  - Eine Schüssel und Streichhölzer
  - Ein gutes Gedächtnis

Wie handhabt man Cryptos

Sehr einfach!

- Man nehme:
  - Einen Raum ohne Fenster
  - Einen Stift und Block
  - Einen Präzisionswürfel (Cellulosenitrat)
  - Ein gutes Buch über Kryptographie
  - Ein paar Stunden Zeit
  - Eine Schüssel und Streichhölzer
  - Ein gutes Gedächtnis

Wie handhabt man Cryptos

Sehr einfach!

- Man nehme:
  - Einen Raum ohne Fenster
  - Einen Stift und Block
  - Einen Präzisionswürfel (Cellulosenitrat)
  - Ein gutes Buch über Kryptographie
  - Ein paar Stunden Zeit
  - Eine Schüssel und Streichhölzer
  - Ein gutes Gedächtnis

Wie handhabt man Cryptos

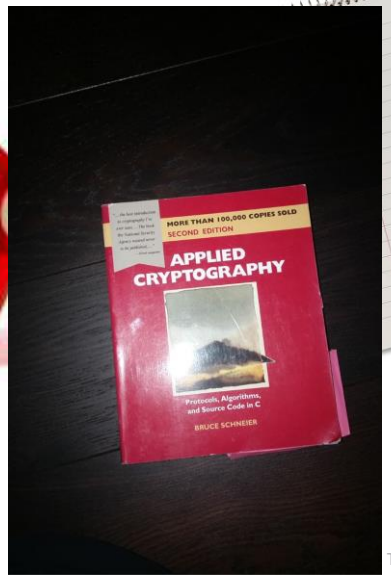
Sehr einfach!

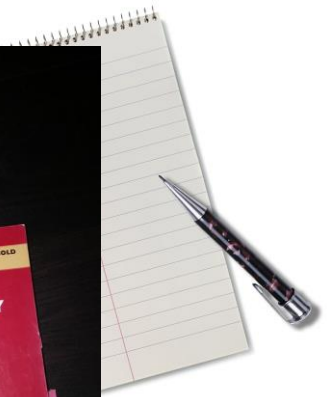
- Man nehme:
  - Einen Raum ohne Fenster
  - Einen Stift und Block
  - Einen Präzisionswürfel (Cellulosenitrat)
  - Ein gutes Buch über Kryptographie
  - Ein paar Stunden Zeit
  - Eine Schüssel und Streichhölzer
  - Ein gutes Gedächtnis

Wie handhabt man Cryptos

Sehr einfach!

- Man nehme:
  - Einen Raum ohne Fenster
  - Einen Stift und Block
  - Einen Präzisionswürfel (Cellulosenitrat)
  - Ein gutes Buch über Kryptographie
  - Ein paar Stunden Zeit
  - Eine Schüssel und Streichhölzer
  - Ein gutes Gedächtnis

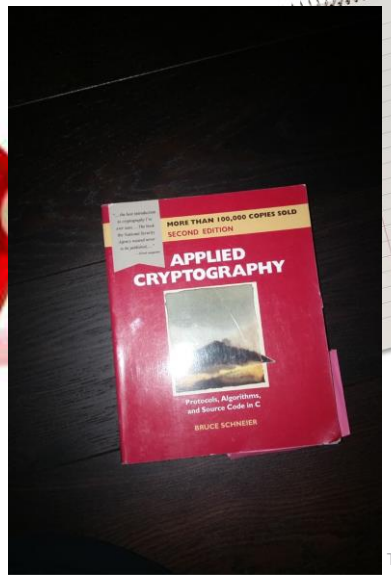




Wie handhabt man Cryptos

Sehr einfach!

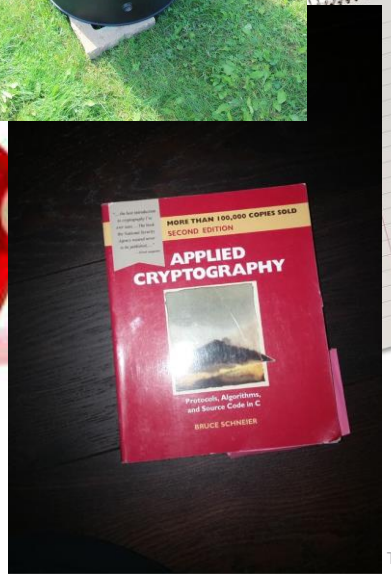
- Man nehme:
  - Einen Raum ohne Fenster
  - Einen Stift und Block
  - Einen Präzisionswürfel (Cellulosenitrat)
  - Ein gutes Buch über Kryptographie
  - Ein paar Stunden Zeit
  - Eine Schüssel und Streichhölzer
  - Ein gutes Gedächtnis



Wie handhabt man Cryptos

Sehr einfach!

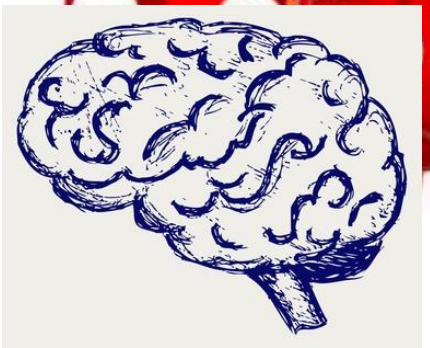
- Man nehme:
  - Einen Raum ohne Fenster
  - Einen Stift und Block
  - Einen Präzisionswürfel (Cellulosenitrat)
  - Ein gutes Buch über Kryptographie
  - Ein paar Stunden Zeit
  - Eine Schüssel und Streichhölzer
  - Ein gutes Gedächtnis

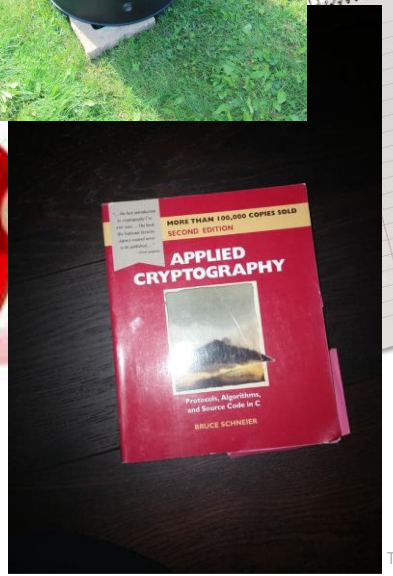


Wie handhabt man Cryptos

Sehr einfach!

- Man nehme:
  - Einen Raum ohne Fenster
  - Einen Stift und Block
  - Einen Präzisionswürfel (Cellulosenitrat)
  - Ein gutes Buch über Kryptographie
  - Ein paar Stunden Zeit
  - Eine Schüssel und Streichhölzer
  - Ein gutes Gedächtnis

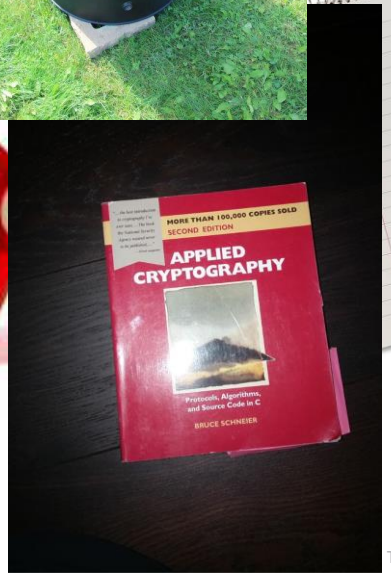




Wie handhabt man Cryptos

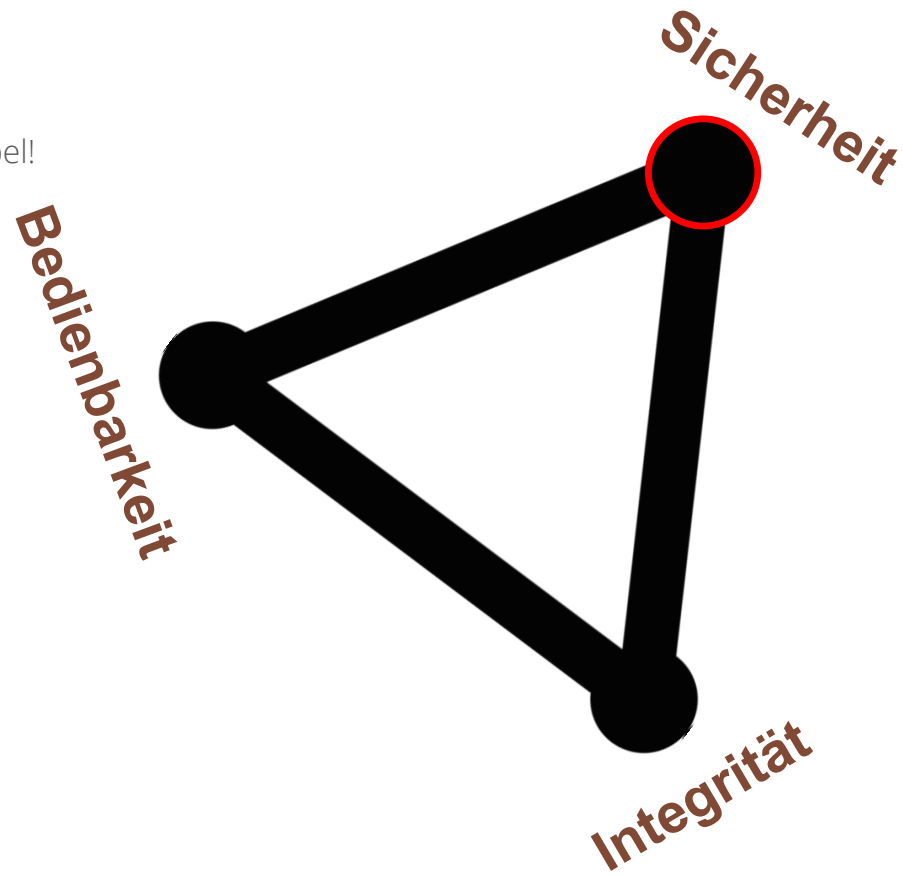
Sehr sicher!

- Perfekte Entropie
- Keine Side-Channel Attacken
- Keine externen Abhängigkeiten
  z.B. (Zufallszahlengenerator)



Sehr sicher!

Aber nicht Praktikabel!



Andere Lösungen

Web Wallets?

- Einfach zu benutzen
- Volle Abhängigkeit von Drittparteien

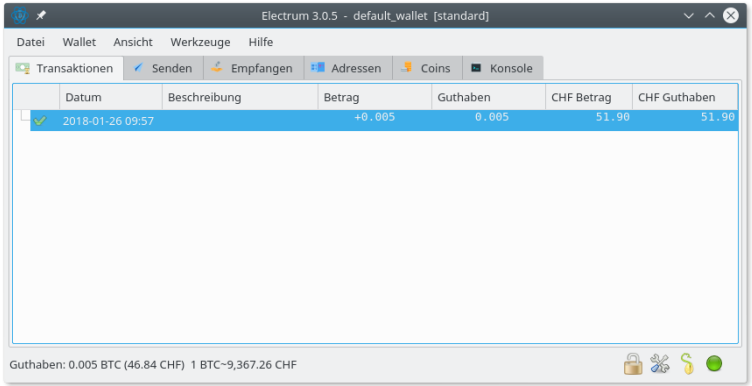
NEIN!

Andere Lösungen

Wallet auf PC/Natel

Z.B. Electrum (Bitcoin, PC), Parity (Ethereum, PC), Mycelium (Bitcoin, Android)

- Einfach zu benutzen
- Backups gegen Verlust
- So sicher wie der PC

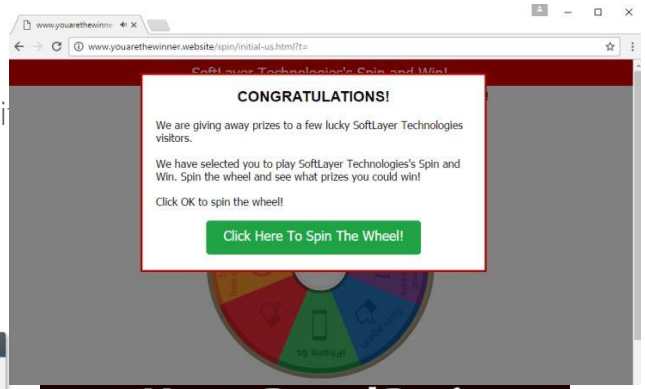


Andere Lösungen

Wallet auf PC/Natel

Z.B. Electrum (Bitcoin, PC), Parity (Ethereum, PC), Mycelium (Bi

- Einfach zu benutzen
- Backups gegen Verlust
- So sicher wie der PC



Andere Lösungen

Wallet auf PC/Natel mit Hardwarewallet

Z.B. Electrum (Bitcoin, PC), Parity (Ethereum, PC), Mycelium (Bitcoin, Android) mit BitBox, Trezor, Ledger

- Einfach zu benutzen
- Backups gegen Verlust
- ~~So sicher wie der PC~~
- Schlüssel sind auf der Hardwarewallet

Warum ist das schwer?

- „Klassisches“ Bankensystem

- Crypto Assets


Support The Guardian

The Guardian

News | Opinion | Sport | Culture | Lifestyle

Business ▸ Economics | Banking | Money | Markets | Project Syndicate | B2B

Spelling mistake prevented hackers taking $1bn in bank heist

New York Fed reveals spelling of ‘foundation’ as ‘fandation’ prompted bank to seek clarification and stop transfer, but hackers still got away with about $80m

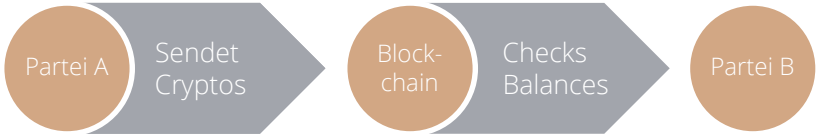
Reuters

Thu 10 Mar 2016 18.31 GMT

Warum ist das schwer?

- „Klassisches“ Bankensystem

- Crypto Assets




Support The Guardian

The Guardian

News | Opinion | Sport | Culture | Lifestyle

Business ▸ Economics | Banking | Money | Markets | Project Syndicate | B2B

Spelling mistake prevented hackers taking $1bn in bank heist

New York Fed reveals spelling of ‘foundation’ as ‘fandation’ prompted bank to seek clarification and stop transfer, but hackers still got away with about $80m

Reuters

Thu 10 Mar 2016 18.31 GMT

Checks and Balances - Multisig

Nativ möglich:

- Bitcoin
- Litecoin
- Ripple

Über Umwege möglich:

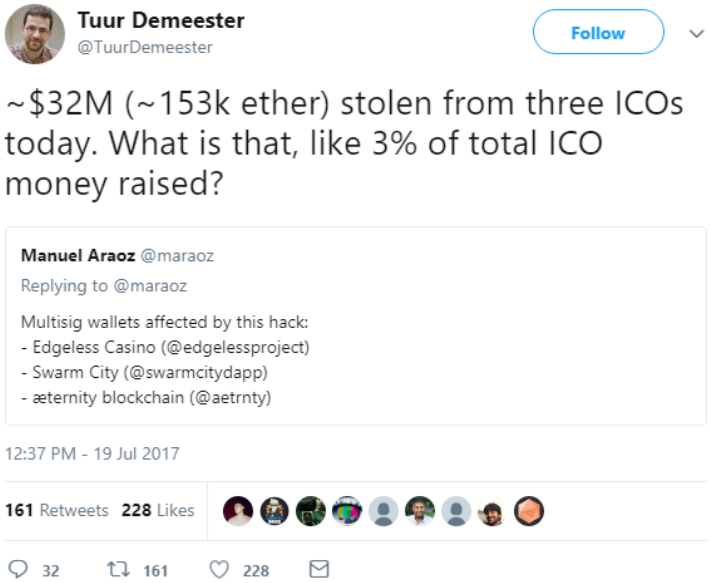
- Ethereum
- Monero

Unmöglich:

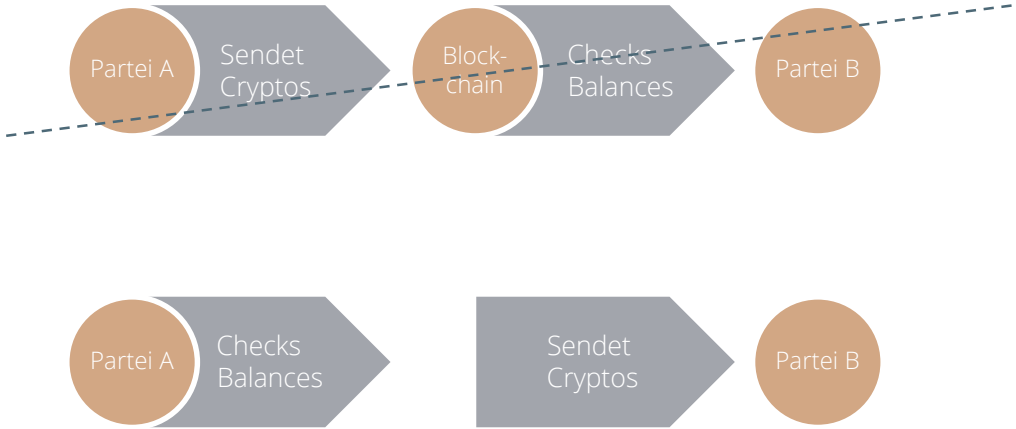
- IOTA

Umwege?

Für Ethereum nur via Smart Contracts



Oder andersherum?



YOUR **GATEWAY** TO THE **CRYPTO WORLD**.

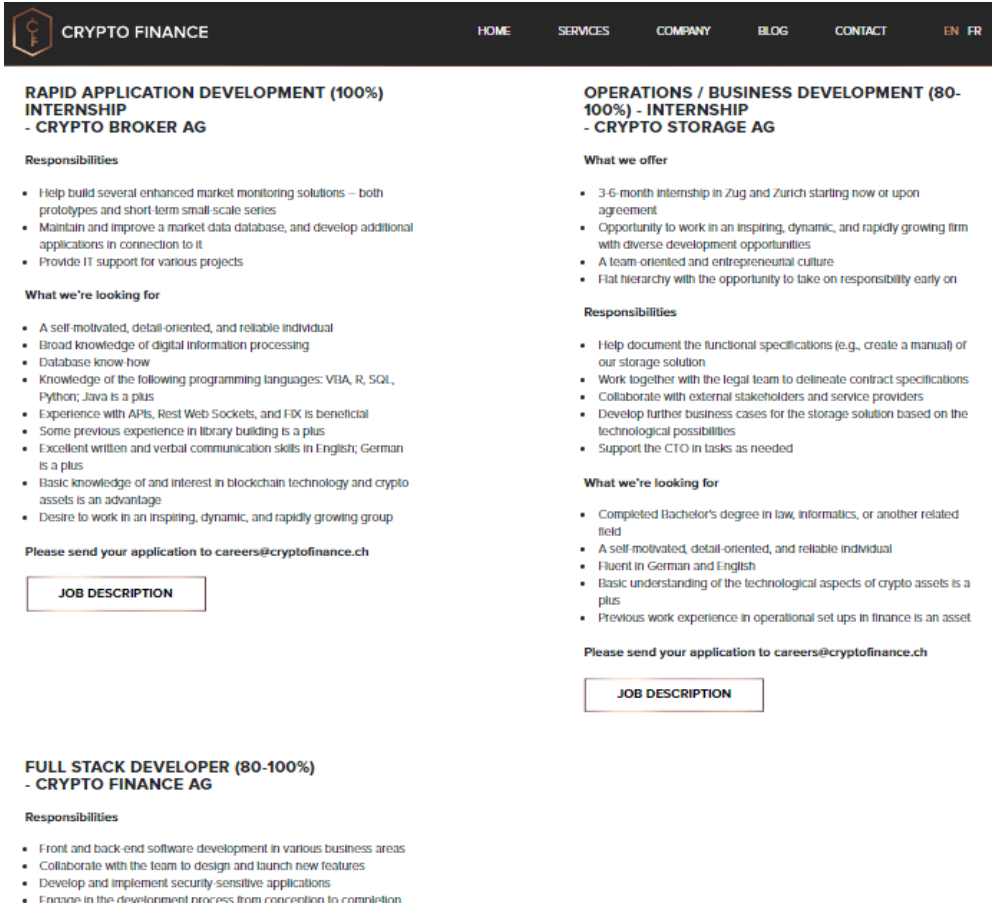
CRYPTO FINANCE AG
Gotthardstrasse 28
CH-6300 Zug

+41 (0)41 545 88 22

info@cryptofinance.ch

www.cryptofinance.ch

@cryptofinanceag



CRYPTO FINANCE

HOME SERVICES COMPANY BLOG CONTACT EN FR

RAPID APPLICATION DEVELOPMENT (100%) INTERNSHIP - CRYPTO BROKER AG

Responsibilities

- Help build several enhanced market monitoring solutions – both prototypes and short-term small-scale series
- Maintain and improve a market data database, and develop additional applications in connection to it
- Provide IT support for various projects

What we're looking for

- A self-motivated, detail-oriented, and reliable individual
- Broad knowledge of digital information processing
- Database know-how
- Knowledge of the following programming languages: VBA, R, SQL, Python; Java is a plus
- Experience with APIs, Rest Web Sockets, and FIX is beneficial
- Some previous experience in library building is a plus
- Excellent written and verbal communication skills in English; German is a plus
- Basic knowledge of and interest in blockchain technology and crypto assets is an advantage
- Desire to work in an inspiring, dynamic, and rapidly growing group

Please send your application to careers@cryptofinance.ch

JOB DESCRIPTION

OPERATIONS / BUSINESS DEVELOPMENT (80-100%) - INTERNSHIP - CRYPTO STORAGE AG

What we offer

- 3-6-month internship in Zug and Zurich starting now or upon agreement
- Opportunity to work in an inspiring, dynamic, and rapidly growing firm with diverse development opportunities
- A team-oriented and entrepreneurial culture
- Flat hierarchy with the opportunity to take on responsibility early on

Responsibilities

- Help document the functional specifications (e.g., create a manual) of our storage solution
- Work together with the legal team to delineate contract specifications
- Collaborate with external stakeholders and service providers
- Develop further business cases for the storage solution based on the technological possibilities
- Support the CTO in tasks as needed

What we're looking for

- Completed Bachelor's degree in law, informatics, or another related field
- A self-motivated, detail-oriented, and reliable individual
- Fluent in German and English
- Basic understanding of the technological aspects of crypto assets is a plus
- Previous work experience in operational set ups in finance is an asset

Please send your application to careers@cryptofinance.ch

JOB DESCRIPTION

FULL STACK DEVELOPER (80-100%) - CRYPTO FINANCE AG

Responsibilities

- Front and back-end software development in various business areas
- Collaborate with the team to design and launch new features
- Develop and implement security-sensitive applications
- Engage in the development process from conception to completion