Introduction to the secure storage of digital assets

Conférence-débat "Blockchain et trésorerie"
Présentation à l'ACTSR, 2 Novembre 2018

HYPOTHESIS

THE WORLDS OF DIGITAL ASSETS AND TRADITIONAL FINANCIAL ASSETS WILL CONVERGE (ARE CONVERGING)
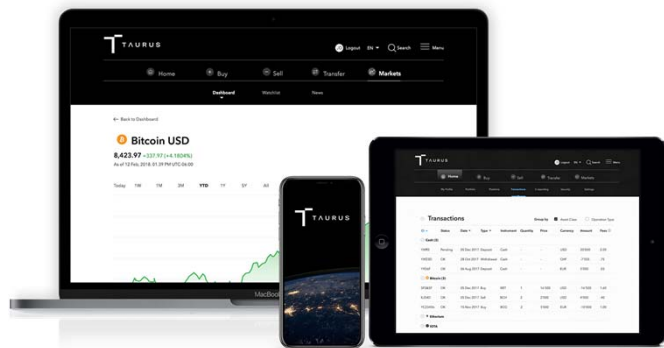
APPLYING THE HIGHEST INSTITUTIONAL STANDARDS IS REQUIRED TO FOSTER TRUST AND ACCELERATE ADOPTION

CONFIDENTIAL

BUILDING AN INSTITUTIONAL-GRADE PLATFORM

TRADE

Digital asset trading platform and services

INVEST

Advisory in digital assets & blockchain investing

Digital asset research incl. technology assessment

Structured products / collective investment schemes

Securitization / tokenization of assets

PROTECT

High-security cold storage vault for digital assets

CONFIDENTIAL

AGENDA

1. Basic Concepts

2. Digital Assets Market

3. Digital Assets Custody

4. Outlook

CONFIDENTIAL

1. DIGITAL ASSETS

Digital Assets **are** currencies, assets, tokens, securities, contracts or rights, booked on a **decentralized ledger** such as **blockchain**

=

Blockchain-based assets

1. DIGITAL ASSETS ARE STORED IN THE BLOCKCHAIN. PRIVATE KEYS ARE STORED OUTSIDE

Public Key

Private Key
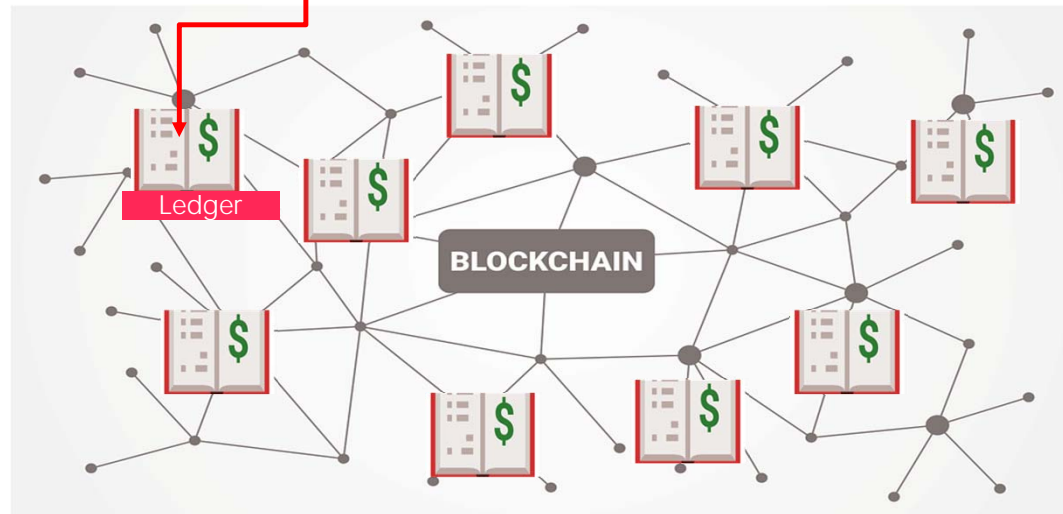

- <u>PUBLIC</u>

- DERIVED FROM PRIVATE KEY

- USED TO GENERATE ADDRESSES

- <u>SECRET</u>

- STORED WITH USERS. OUTSIDE THE BLOCKCHAIN

- SIGN TRANSACTIONS

- LOSING THEM = LOSING ACCESS TO YOUR FUNDS

2. DIGITAL ASSET MARKET OVERVIEW: SOME FIGURES

>2085

digital assets

USD 203b

market capitalization

54%

Bitcoin dominance

USD 12b

average daily trading volume

731

ICOs ytd

USD 18+b

raised via ICOs ytd

1 situation as of 31.10.2018
Source: coinmarketcap, team analysis
TAURUS GROUP © 2018

CONFIDENTIAL

2. INSTITUTIONALS ENTERING THE MARKET

20 percent of financial firms such as banks and hedge funds are looking to trade cryptocurrencies soon, survey finds

- One in five financial firms, ranging from hedge funds to considering trading digital currency in the next three to to a new Thomson Reuters survey published this week.
- Of those that showed interest, about 70 percent said th trade in the next three to six months.
- The news is a sign of improving sentiment and should b bitcoin prices, Brian Kelly, founder and CEO of BKCM, s

Kate Rooney | @Kr00ney
Published 11:19 AM ET Tue, 24 April 2018 | Updated 7:04 PM ET Tue, 24 Ap

CNBC

Goldman Sachs launching trading desk for bitcoin, report says

Evelyn Cheng | @chengevelyn
Published 3:58 PM ET Thu, 21 Dec 2017 | Updated 4:05 PM ET Thu, 21 Dec 2017

CNBC

Bitcoin + Add to myFT

Goldman backs fundraising by payments company Circle

Cash infusion will help fund start-up's expansion beyond

SIX to launch full end-to-end and fully integrated digital asset trading, settlement and custody service

Switzerland's stock exchange – owned and managed by SIX – today announced that it is building a fully integrated trading, settlement and custody infrastructure for digital assets. SIX is regulated as an operator of Financial Market Infrastructure (FMI) by Swiss Authorities, FINMA and the Swiss National Bank, and intends that the planned 'digital asset ecosystem' – SIX Digital Exchange ("SDX") – will enjoy the same standard of oversight and regulation.

Stephen Foley in New York APRIL 30, 2015   💬 2 🖶

Goldman Sachs is backing the latest fundraising by Circle Internet Financial, a mobile payments start-up built on the bitcoin network.

2. SWISS BANKS HAVE BEEN VERY ACTIVE THIS SUMMER

Zurich Bank Open for Cryptocurrency Assets

Thursday, 2 August 2018 16:32 | Written by Claude Baumann
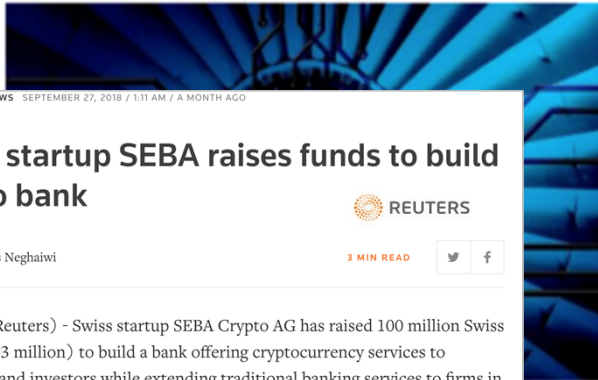
TECHNOLOGY NEWS SEPTEMBER 27, 2018 / 1:11 AM / A MONTH AGO

Swiss startup SEBA raises funds to build crypto bank

REUTERS

Brenna Hughes Neghaiwi   3 MIN READ
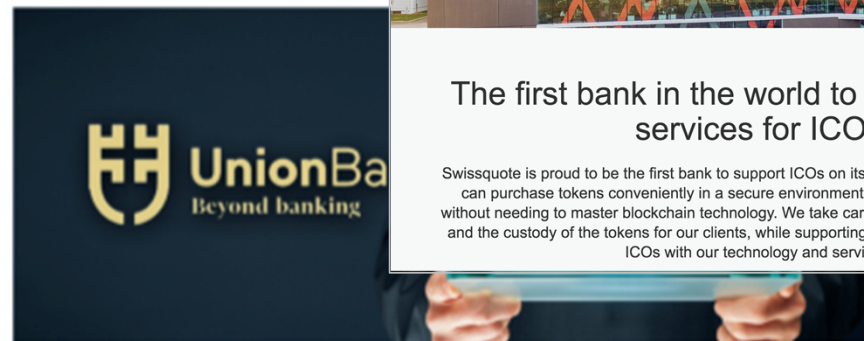
ZURICH (Reuters) - Swiss startup SEBA Crypto AG has raised 100 million Swiss francs ($103 million) to build a bank offering cryptocurrency services to companies and investors while extending traditional banking services to firms in the new industry.

UnionBa
Beyond banking

Swissquote

The first bank in the world to provide global services for ICOs

Swissquote is proud to be the first bank to support ICOs on its trading platform, where clients can purchase tokens conveniently in a secure environment against fiat currency (CHF), without needing to master blockchain technology. We take care of the execution of the orders and the custody of the tokens for our clients, while supporting companies seeking to launch ICOs with our technology and services.

BLOCKCHAIN/BITCOIN LIECHTENSTEIN

Liechtenstein's Union Bank AG Becomes First Licensed Bank to Issue Its Own Stable Coin

Crypto und Blockchain

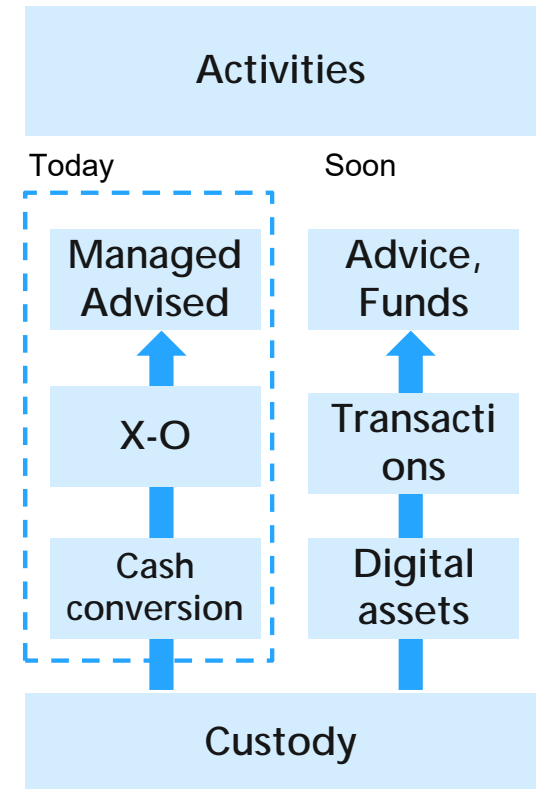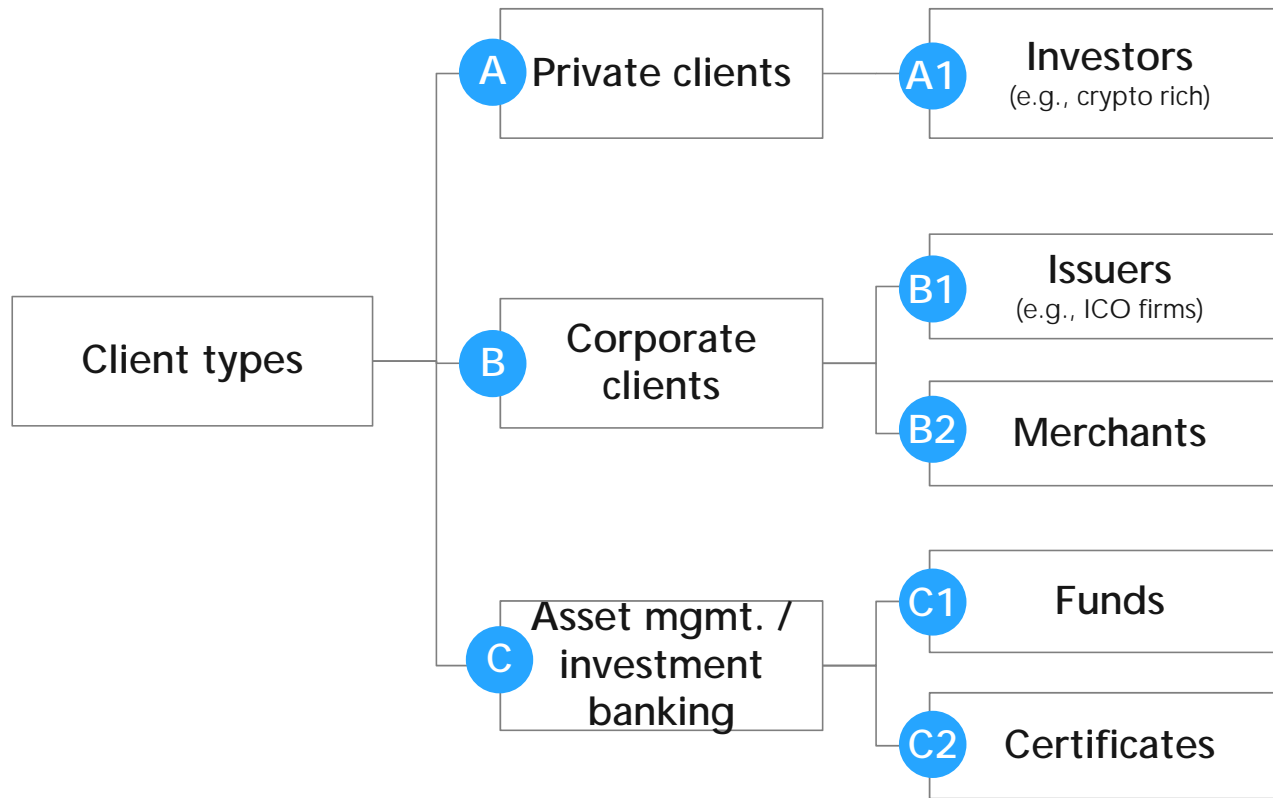Die Hypothekarbank Lenzburg AG treibt ihre Digitalstrategie aktiv voran. In diesem Zusammenhang werden Geschäftsbeziehungen im Blockchain-Umfeld geprüft.

Morgan Stanley has poached a Credit Suisse crypto banker to head 'digital asset markets'

3. WHAT TYPES OF CLIENTS DO (SWISS) BANKS FACE? WHAT TYPES OF ACTIVITIES DO THEY OFFER?

Client types

A Private clients
- **A1** Investors (e.g., crypto rich)

B Corporate clients
- **B1** Issuers (e.g., ICO firms)
- **B2** Merchants

C Asset mgmt. / investment banking
- **C1** Funds
- **C2** Certificates

Activities

Today	Soon
Managed Advised	Advice, Funds
X-O	Transactions
Cash conversion	Digital assets

Custody

Source: team analysis

3. SECURITY STILL A MAJOR ISSUE

MT.GOX
-$460m
Feb. 2014

BITSTAMP
-$22m
Jan. 2015 + Jan. 2016

OK
-$3m
Aug, 2017

BITGRAIL
-$187m
Feb, 2018

2014   2015   2016   2017   2018

BITFINEX
-$77m
Aug. 2016

Coincheck
-$500m
Jan. 2018

bithumb
-$72m
Jun. 2018

Coinrail
-$40m
Jun, 2018
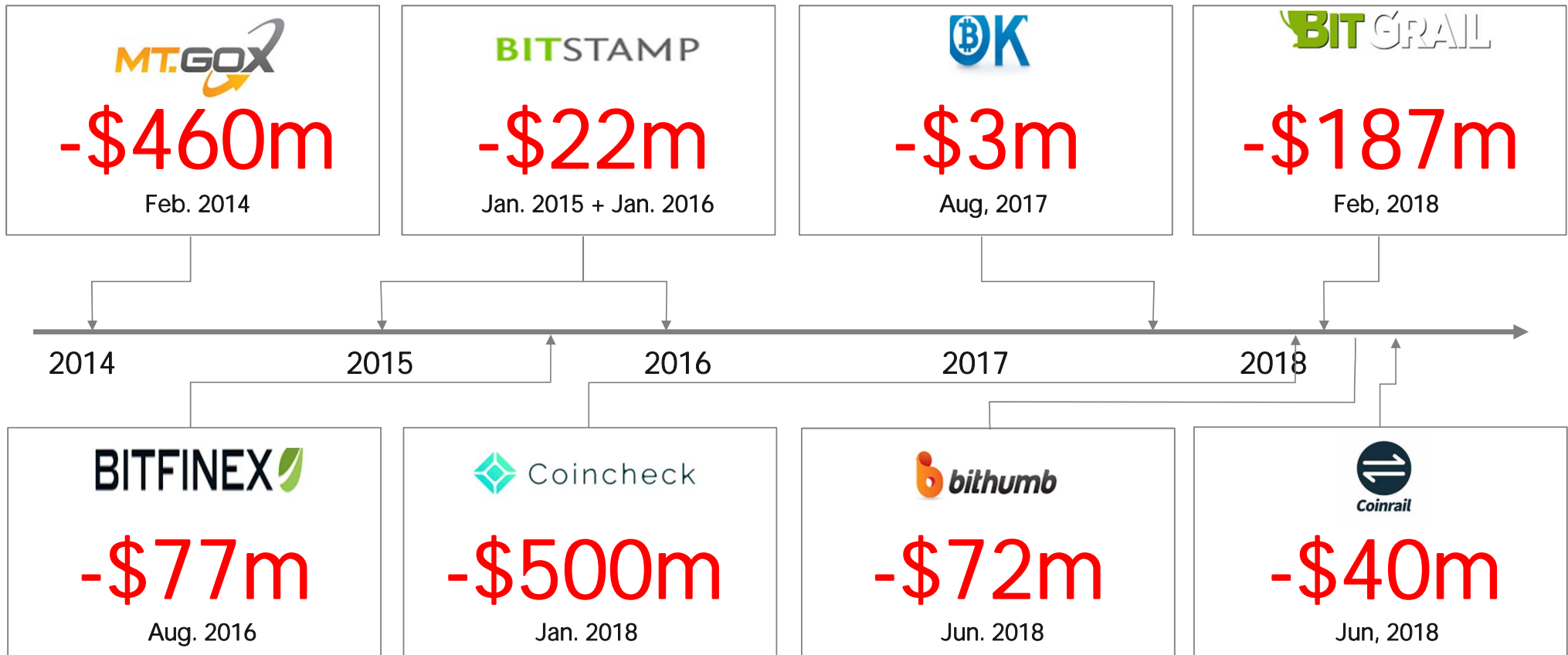
Note: non-exhaustive list used for illustration purpose
Source: Internet, https://coiniq.com/cryptocurrency-exchange-hacks/, team analysis

CONFIDENTIAL

3. MAIN SECURITY RISK: LOSS OF FUNDS

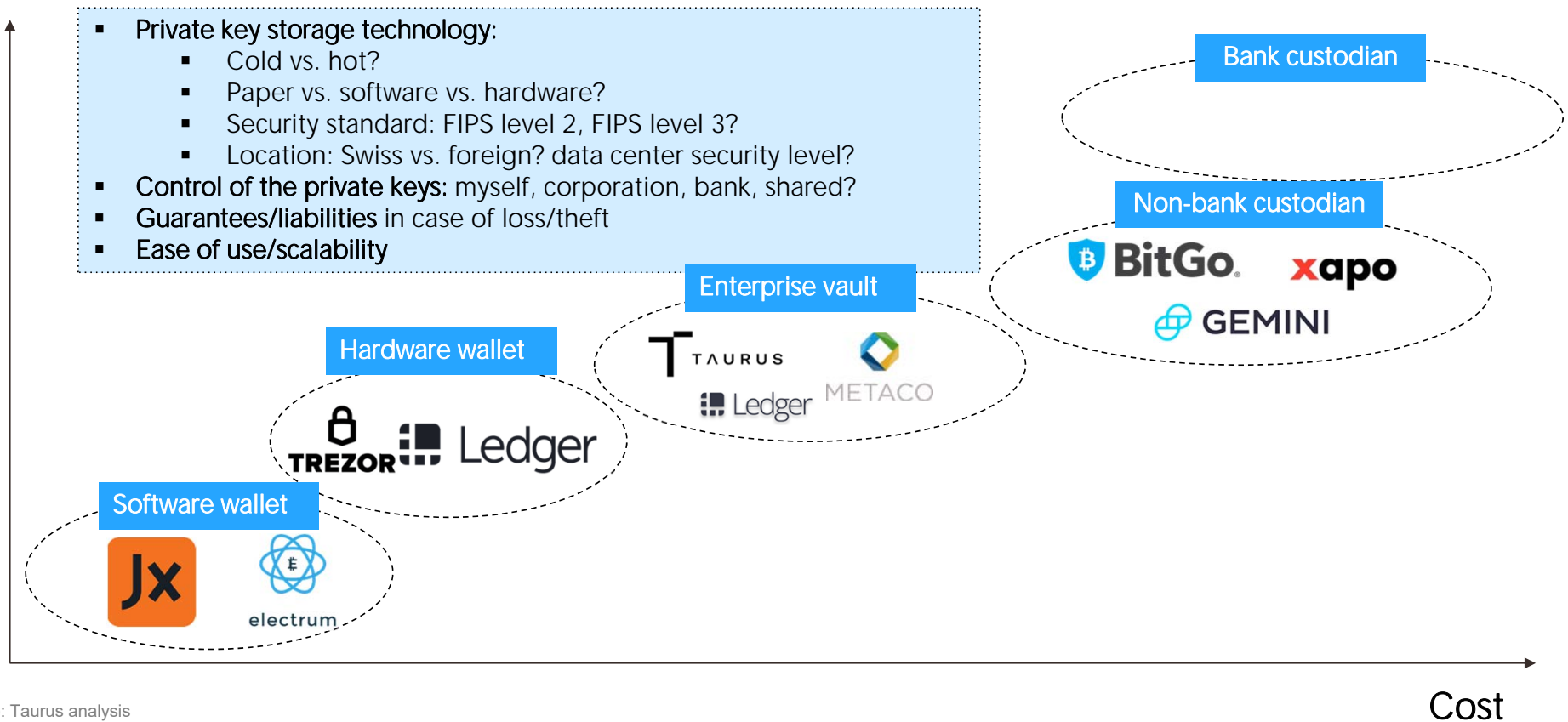| Exchange	USD m Loss (time of incident)	Year	Main cause
coincheck	500	2018	• Lack of multisignatures • Hot vs. cold storage mismanagement
MT.GOX x	460	2014	• Information security and management loopholes
BIT GRAIL	170	2018	• Defects in cryptocurrencies software
YouBit	100 +	2017	• TBD (north-korea rumoured attack)
BITFINEX	72	2016	• Multisignature abuse
bithumb	31	2018	• Phishing & social engineering
Bitstamp p	22	2015/16	• Phishing & social engineering

Lessons: cryptocurrency custodians need:
- Technology components with solid security features
- Real-time monitoring features (intrusion detection, anomaly detection)
- Access control, processes, employees training, legal framework

CONFIDENTIAL

TAURUS

Digital Assets Custody

=

Protection and Custody of your "private keys"

3. MANAGING DIGITAL ASSETS' CUSTODY: THE SECURITY / COST TRADE-OFF

Security / investor protection

- ▪ Private key storage technology:
  - ▪ Cold vs. hot?
  - ▪ Paper vs. software vs. hardware?
  - ▪ Security standard: FIPS level 2, FIPS level 3?
  - ▪ Location: Swiss vs. foreign? data center security level?
- ▪ **Control of the private keys:** myself, corporation, bank, shared?
- ▪ **Guarantees/liabilities** in case of loss/theft
- ▪ Ease of use/scalability

Bank custodian

Non-bank custodian

BitGo   xapo   GEMINI

Enterprise vault

TAURUS   METACO   Ledger

Hardware wallet

TREZOR   Ledger

Software wallet

Jx   electrum

Cost

14

3. HOW TO STORE DIGITAL ASSETS: EXAMPLE TAURUS PROTECT

Functionalities

- Secure connexions with the external world
- Wallets fully segregated

Integration in banking systems

- Governance processes and business rules enforced in the HSM (FINMA 3-lines of defense)
- Full reconciliation and integration with core banking systems

Security

- Defense in-depth mechanism
- Isolation between core service and internet-connected node
- Strong emphasis on defense in depth
- FIPS level 3 certified HSM
- On-premise infrastructure

Source: team analysis

TAURUS

1. Custody: critical piece to increase TRUST

2. Mastering custody: open doors to ALL activities
    a. Deposit protection
    b. Transactions
    c. Product structuring

3. Natural home: BANKS

LEADERSHIP TEAM: COVERING THE FULL VALUE CHAIN (DETAILS IN APPENDIX)

Financial services regulation

Banking, Asset Management, Trading

Blockchain

Platform and product development

Information security

Oren-Olivier Puder

- 17 years of work experience at Law Firm (Partner of Junod, Muhlstein, Lévy & Puder), FINMA (Head Suisse Romande Asset Management Division), Lombard Odier
- Lic. iur. UniGe ; LL.M. in Securities and Financial Regulation, Georgetown University (Washington DC)
- Chairman of the Board of a Hedge Fund; Board Member Private Equity firm
- Strong expertise in Banking/Financial law and prudential regulation

Sébastien Dessimoz

- 18 years of work experience at Brevan Howard, Syz Group, Lombard Odier, McKinsey and 3Com in the Silicon Valley
- MSc. Communication Systems Engineering EPFL, MBA INSEAD, CFA
- C-level experience (ExCo member, COO) and Board Member of several regulated entities in Switzerland, Europe and Asia
- Strong expertise in asset management, IT, business building and transformation

Lamine Brahimi

- 15 years of work experience at Lombard Odier, McKinsey, IBM Research
- MSc Communication Systems Engineering EPFL, MBA INSEAD, CFA
- Deputy COO and Chief Digital Officer of Lombard Odier
- Board Member of Swiss Fintech Innovations, Member of the Swiss Bankers Association Fintech Experts Commission
- Strong expertise in Fintech, digitization, transformation, and product development

Dr. Jean-Philippe Aumasson

- 8 years of work experience in Security departments
- PhD Cryptography EPFL
- World renowned Cybersecurity & Cryptography expert
- Strong expertise in cryptography and cybersecurity; working with governments, defense, blockchain protocols
- Author of cryptography book
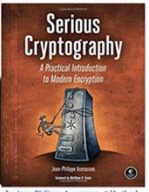
TOP QUALITY SECURITY AND TECHNOLOGY ADVISORS

Prof. Bryan Ford

- Head of the Swiss Federal Institute of Technology in Lausanne (EPFL) Decentralized/Distributed Systems (DEDIS) research group
- Expertise in building secure decentralized systems, touching on topics including private and anonymous communication, scalable decentralized systems, blockchain technology, Internet architecture, and operating systems
- Ph.D. at MIT, ex-faculty member of Yale University
- Grants from NSF, DARPA, and ONR, including the NSF CAREER award
- Has served as a member of the DARPA Information Science and Technology (ISAT) study group, and is an advisory board member of the Swiss FinTech Innovations association

Dr. Dimitri Nedospasov

- Hardware hacker, hardware design engineer, security researcher, trainer, speaker and reverse-engineerer
- Member of the world's oldest hacker club, the German Chaos Computer Club or CCC
- Renowned for his hardware reverse-engineering techniques and his unique hybrid hardware/software analysis workflow
- Experienced in analyzing anything ranging from electronics and embedded protocols to integrated circuits at a gate and transistor level
- PhD (Dr-Ing.) in IC Security at TU Berlin

Stéphane Rey

- Chief Technology Officer of Lombard Odier Investment Managers (LOIM) and co-Chief Digital Officer of the Lombard Odier Group
- Driver of technology innovation at Lombard Odier and pushed the first blockchain-based transaction of the Group
- Chairman of the cybersecurity committee of LOIM
- Recognized as Top CIO 2017 in Switzerland during the 6th Confare Swiss CIO & IT Manager Summit in Zurich
- Board member of the Swiss Fintech Innovations association
- Previously Partner at McKinsey & Company Business Technology Office, where he focused on serving financial institutions and telecommunication companies
- Bachelor degree in Business Administration and a Master in Information Technology

Thomas Roth

- Security researcher from Germany
- Has published consistently since the age of 19 independent security research on topics like embedded hardware, secure communication, payment systems and the (industrial) internet of things.
- Has gained global recognition in the security industry and regularly speaks at some of the biggest security conferences in the world
- Made it twice on the Forbes 30 under 30 list for his contributions in technology and, in 2018
- Awarded the Young Engineer of the Year award by the Critical Communications Association

CONFIDENTIAL

1. Oren-Olivier Puder

Oren-Olivier Puder is a co-founder of TAURUS Group SA and chairman of the Board.

Oren is a lawyer by training and a Partner at Junod, Muhlstein, Levy & Puder law firm. He worked for a number of years in Bern with the Swiss Financial Market Supervisory Authority (FINMA), including particularly as head of the investment funds department for French-speaking Switzerland. He also acted as legal adviser to the president of the Swiss Bankers Association.

Oren advises Swiss and international clients particularly on banking and financial law, corporate law and contract law. More particularly, he assists financial institutions (banks, securities dealers, fund management companies, asset managers of investment funds and pension funds, independent asset managers) and represents them before the regulatory authorities and the courts. He is a financial services expert and specialises in the establishment of collective investment vehicles (transferable securities funds, alternative funds, real estate funds). He is a regular speaker at seminars on banking and financial law.
Oren is also the chairman of one of the largest hedge fund in Europe and member of the board of an independent Private Equity firm.
Oren is a graduate of the University of Geneva (law degree) and of Georgetown University, Washington D.C. (Master of Laws/LL.M). He was admitted to the Geneva Bar in 2003.

2. Sébastien Dessimoz

Sébastien Dessimoz, CFA is a co-founder and Managing Partner of TAURUS Group SA.

He previously held several C-level executive and board level positions for leading asset management firms, with strong expertise in product development, trading, IT, business development and transformation. He worked 5 years at Syz Asset Management as Chief Operating Officer, Member of the Executive Committee and Board Member of several regulated entities. Previously, Sébastien spent 3 years at Brevan Howard, the biggest European hedge fund, as Managing Director and head of the Swiss office. Sébastien Dessimoz also worked at Lombard Odier, notably as Head of Hedge Fund business development and investment manager. Sébastien spent 5 years as a senior management consultant at McKinsey & Company. Sébastien started his career as an engineer in the Silicon Valley for 3Com Corporation.

Sébastien holds a MSc in Communication Systems Engineering from EPFL and MBA from INSEAD. Sébastien is also CFA charter holder.

3. Lamine Brahimi

Lamine Brahimi, CFA is a co-founder and Managing Partner of TAURUS Group SA. Prior to co-founding TAURUS Group SA, Lamine was previously Deputy-COO, Chief Digital Officer of Lombard Odier's wealth management unit as well as General Secretary of the Group.

In his capacity as Chief Digital Officer, he spearheaded the design and development of Lombard Odier's wealth management digital strategy leading to several critically acclaimed platforms in particular in relation to investment advisory. He also pushed the first real blockchain prototype to be tested in a private bank (clearing and settlements of structured products with the Swiss Stock Exchange and Swiss Fintech Innovations). Between 2016 and 2018, he represented the Swiss Private Banks at the Fintech Commission of the Swiss Bankers Association and was a founding member and Board member of Swiss Fintech Innovations. He is a regular speaker at swiss and international seminars on innovation, fintech, and digitalisation. He started his career as a management consultant at McKinsey & Company where he advised financial services companies, industrial companies and governments on strategic, financial, and operational issues.

Lamine holds an MSc in Communication Systems Engineering from EPFL, an MBA with distinction from INSEAD, and is also CFA charterholder.

CONFIDENTIAL

4. Dr. Jean-Philippe Aumasson

Jean-Philippe (JP) Aumasson is an expert in cryptography and member of Taurus Executive Committee.

JP wrote the books Serious Cryptography (No Starch Press, 2017) and The Hash Function BLAKE (Springer, 2015), and designed the widely used algorithms BLAKE2 and SipHash.
He has performed numerous security assessments for blockchain and cryptocurrency technologies, and has worked for leading organizations such as IOHK, Waves, or ZCash.

He has spoken at leading information security conferences such Black Hat, DEFCON, RSA, CCC, Infiltrate, and Troopers about applied cryptography, quantum computing, and platform security.
He holds a PhD in Cryptography from EPFL (2009) and has previously worked for 8 years in applied cryptography, security architecture, and cybersecurity within the Kudelski Group