Center for Innovative Finance
30. April 2018

BitBox

SHIFT
CRYPTOSECURITY

BitcoinCore

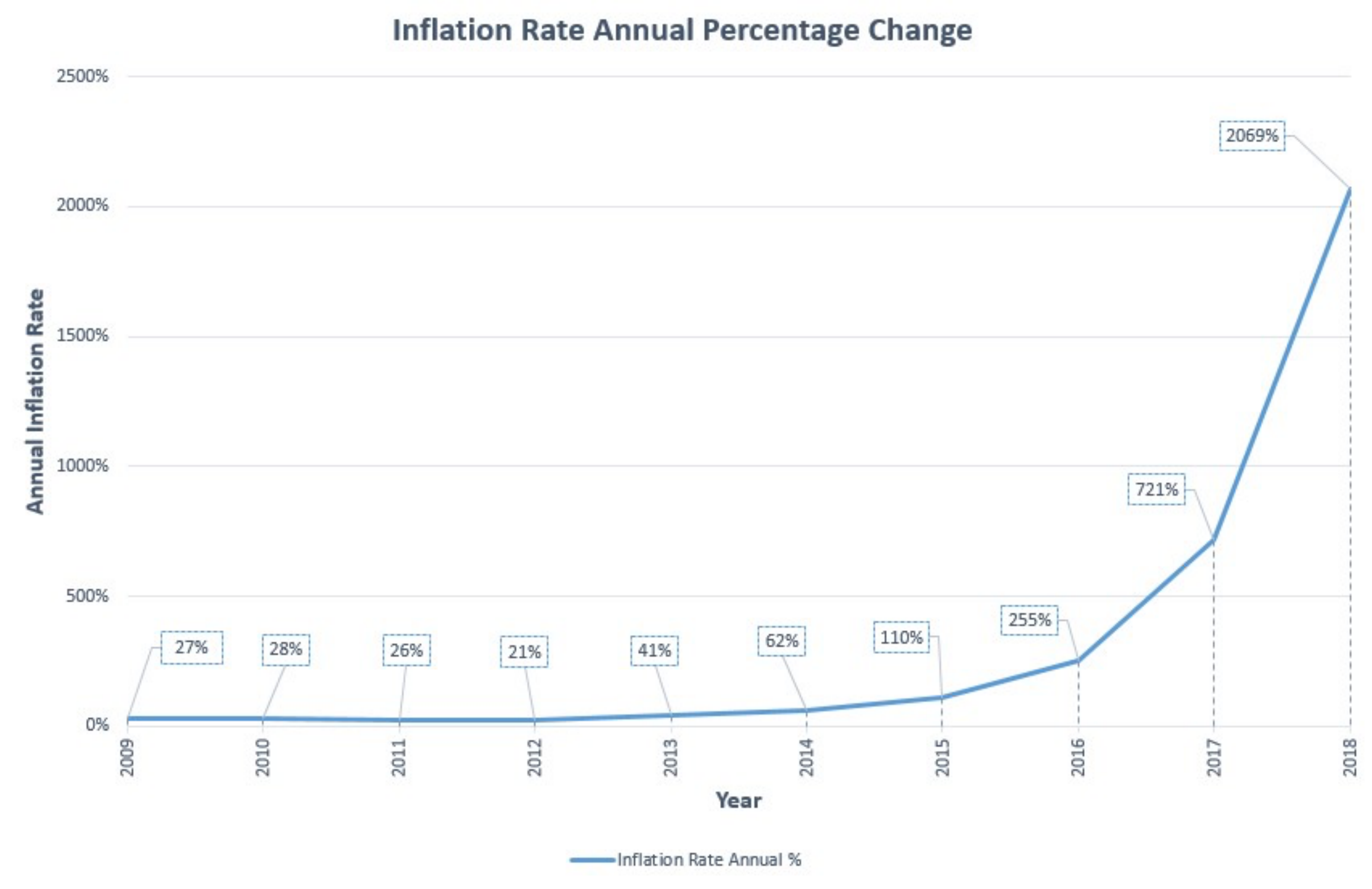
dev@jonasschnelli.ch

PGP: CA1A2908DCE2F13074C62CDE1EB776BB03C7922D

The Bitcoin Mindset

Wie viel Geld „besitzen“ wir wirklich.

ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ
NATIONAL BANK
NBG GROUP
ΙΚΗ ΤΡΑΠΕΖΑ
NATIONAL BANK


Inflation Rate Annual Percentage Change
Annual Inflation Rate
2500%
2000%
1500%
1000%
500%
0%
27%
28%
26%
21%
41%
62%
110%
255%
721%
2069%
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
Year
Inflation Rate Annual %

CREDIT
SUISSE
10 oz
FINE GOLD
999,9
CHI ESSAYEUR
FONDEUR
031851

Don't Trust, **Verify**

Trusted Third Parties

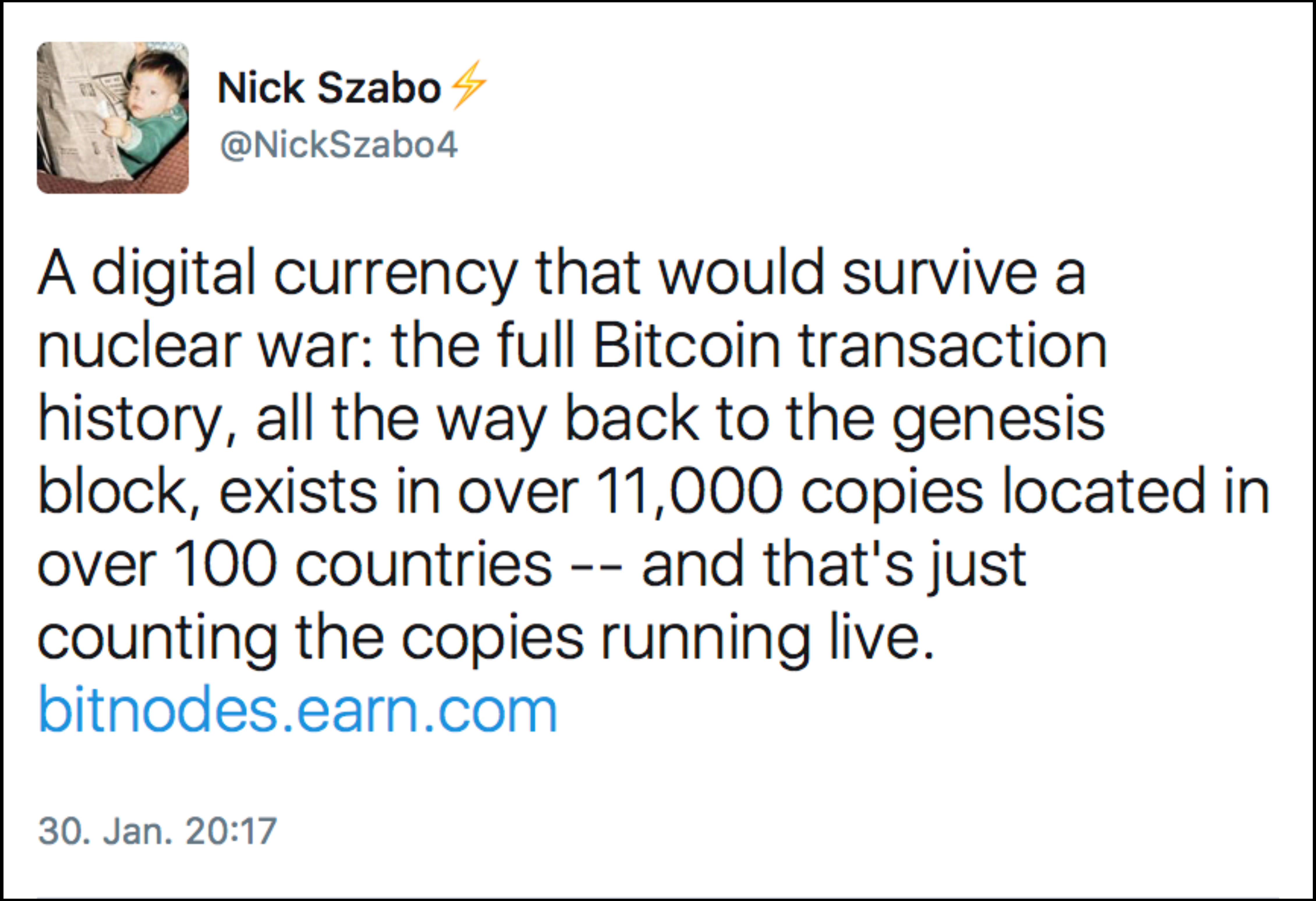
are

Security Holes

Proof of work

Peer-to-peer network

Asymmetric Cryptography
Digital Signature (ECDSA)



Nick Szabo⚡

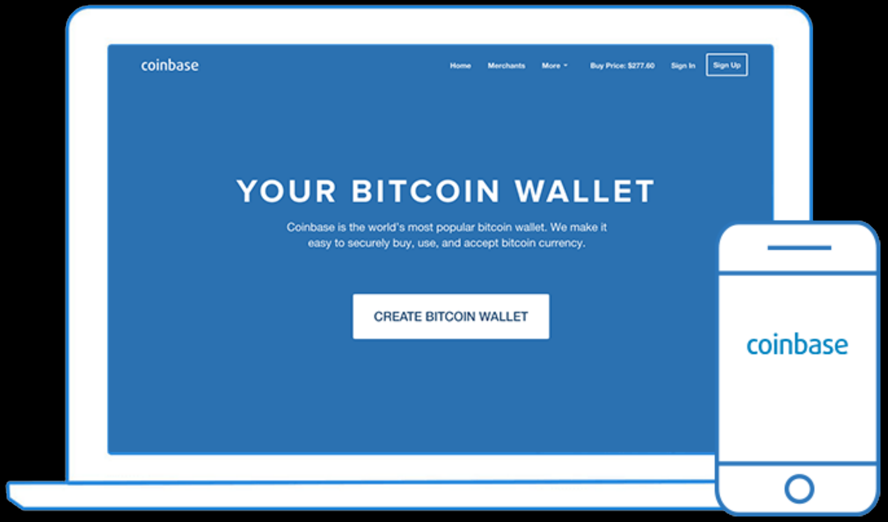
@NickSzabo4

A digital currency that would survive a nuclear war: the full Bitcoin transaction history, all the way back to the genesis block, exists in over 11,000 copies located in over 100 countries -- and that's just counting the copies running live. bitnodes.earn.com

30. Jan. 20:17

Centralized vs. **Decentralized**

Centralized validation & **centralized** keystorage

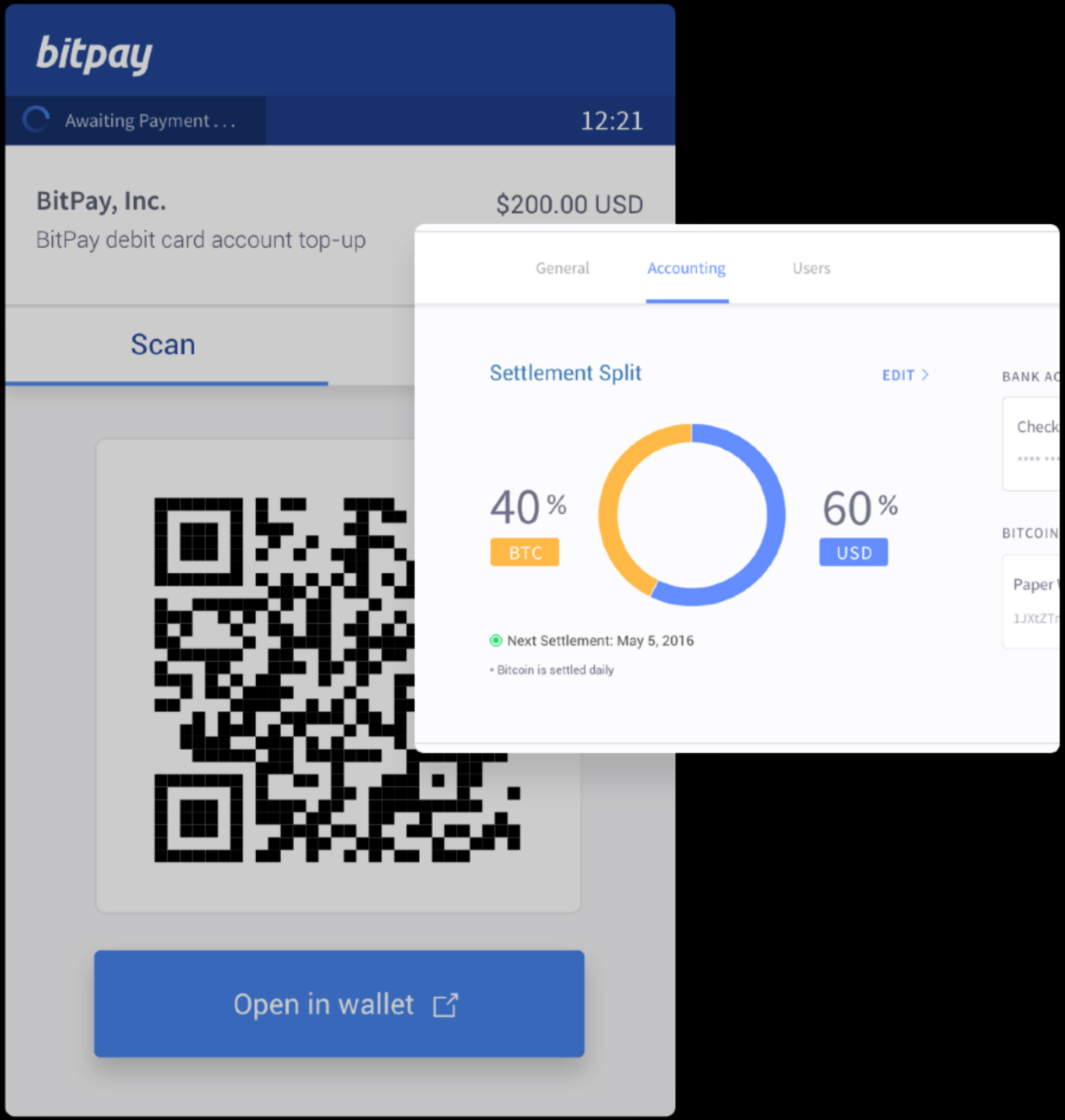


YOUR BITCOIN WALLET

Coinbase is the world's most popular bitcoin wallet. We make it easy to securely buy, use, and accept bitcoin currency.

BLOCKCHAIN

Centralized validation & **centralized** keystorage



bitpay

Awaiting Payment . . . 12:21

BitPay, Inc. $200.00 USD

BitPay debit card account top-up

Settlement Split EDIT >

40 % BTC

60 % USD

Next Settlement: May 5, 2016

• Bitcoin is settled daily

BITFINEX

kraken bitcoin exchange

Bitcoin.com

. . .

🔐

Key-management

🔐

App Store Security

Annahme: **100’000** wallets mit einem durchschnittlichen Wert von **1’000** $

================

hack bounty ist somit **100M $**

☠️ **auto-**update? ☠️

Trust **Layers**

The **Intel Management Engine (ME)**, also known as the Manageability Engine, is an autonomous subsystem that has been incorporated in virtually all of Intel's processor chipsets since 2008. The subsystem primarily consists of proprietary firmware **running on a separate microprocessor that performs tasks during boot-up, while the computer is running, and while it is asleep**. As long as the chipset or SoC is connected to current (via battery or power supply), it continues to run even when the system is turned off. Intel claims the ME is required to provide full performance. Its exact workings are largely undocumented and **its code is obfuscated using confidential huffman tables stored directly in hardware**, so the firmware does not contain the information necessary to decode its contents. Intel's main competitor AMD has incorporated the equivalent AMD Secure Technology (formally called Platform Security Processor) in virtually all of its post-2013 CPUs.

The Management Engine is often confused with Intel AMT. AMT is based on the ME, but only available on processors with vPro. AMT enables owners remote administration of their computer, like turning it on or off and reinstalling the operating system. However, the ME itself is built into all Intel chipsets since 2008, not only those with AMT. While AMT can be unprovisioned by the owner, there is no official, documented way to disable the ME.

Trezor

Ledger

BitBox

Private keys are **never exposed** to host

No „operating sytem“

Offline **backups**

Seed is generated on device

BitBox

Hardware Wallet

Blockchain?

Private **Blockchain**?

The Bitcoin blockchain is probably the **most inefficient database**

>**1$** for **80bytes**

Write operation takes **~10** mins

BitBox

SHIFT CRYPTOSECURITY

Thanks, Q&A?

dev@**jonasschnelli**.ch

PGP: CA1A2908DCE2F13074C62CDE1EB776BB03C7922D

jonasschnelli

github.com/jonasschnelli