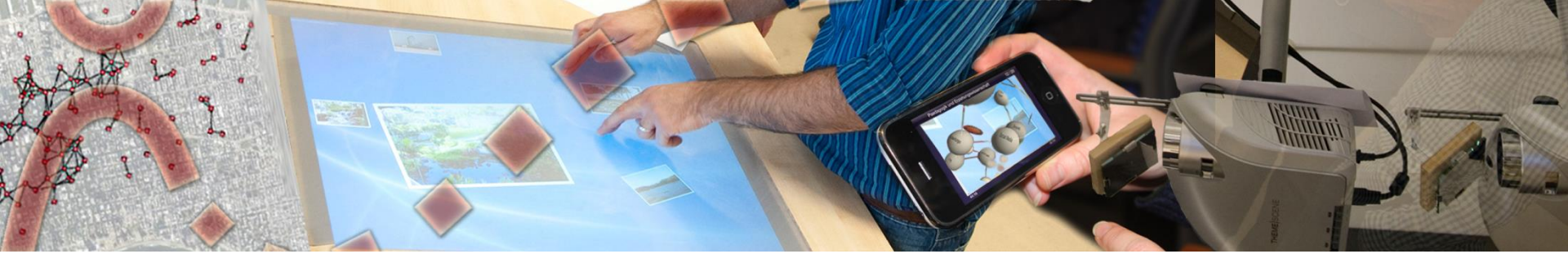


Building Decentralized Trust with Blockchains

CENTRIC 2017 Tutorial
08.10.2017
Athens, Greece

Nikolaos Alexopoulos, Telekooperation

Technische Universität Darmstadt

About me (1)

- Doctoral researcher at the Telecooperation lab of the Technische Universität Darmstadt since May 2016, working on computer and network security.


LUDEWIG

About me (2)

- Doctoral researcher at the Telecooperation lab of the Technische Universität Darmstadt since May 2016, working on computer and network security.

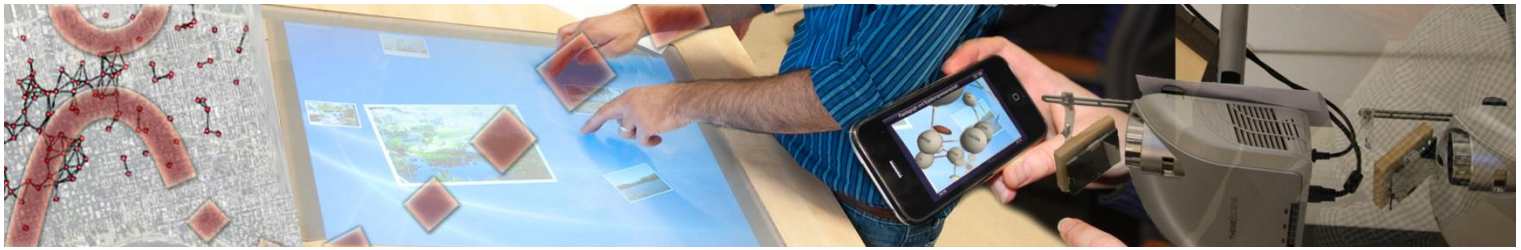
- Obtained my diploma from ECE NTUA, Athens (2016).

About TU Darmstadt and TK

TECHNISCHE UNIVERSITÄT DARMSTADT

- First university in the world to set up a chair in electrical engineering (1882).
- Around 26.000 students and 5.000 staff.
- 2 campuses.
- The Telekooperation lab is headed by Prof. Dr. Max Mühlhäuser and consists of ≈25 researchers.


MDCCCXCIII
MDCCCXCV

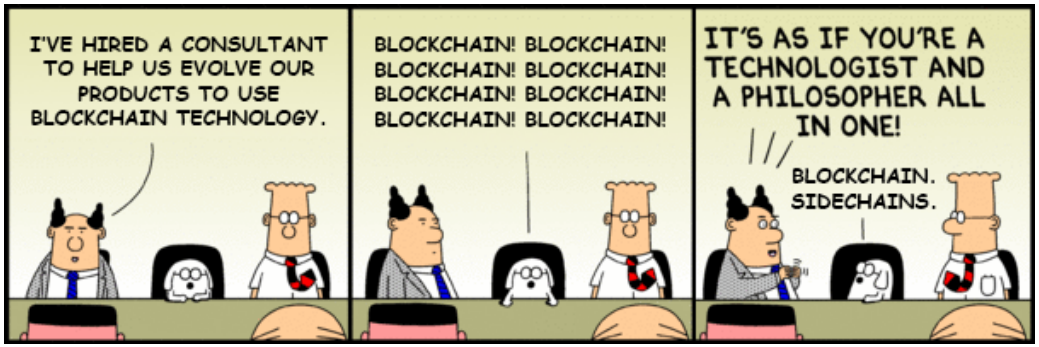


CONTENT

- Blockchains and cryptocurrencies
- Trust in the internet
- Some of our work
- Discussion

Part 1: Blockbits & Bitchains (??)

TECHNISCHE UNIVERSITÄT DARMSTADT



3 The Bitcoin Backbone Protocol

We start by introducing blockchain notation. Let $G(\cdot), H(\cdot)$ be cryptographic hash functions with output in $\{0,1\}^\kappa$. A *block* is any triple of the form $B = \langle s, x, ctr\rangle$ where $s \in \{0,1\}^\kappa, x \in \{0,1\}^*, ctr \in \mathbb{N}$ are such that satisfy predicate $\mathsf{validblock}_q^T(B)$ defined as

$$(H(ctr, G(s,x)) < T) \wedge (ctr \leq q).$$

The parameter $T \in \mathbb{N}$ is also called the block's *difficulty level*. The parameter $q \in \mathbb{N}$ is a bound that in the Bitcoin implementation determines the size of the register ctr; in our treatment we allow this to be arbitrary, and use it to denote the maximum allowed number of hash queries in a round. We do this for convenience and our analysis applies in a straightforward manner to the case that ctr is restricted to the range $0 \leq ctr < 2^{32}$ and q is independent of ctr.

A *blockchain*, or simply a *chain* is a sequence of *blocks*. The rightmost block is the *head* of the chain, denoted $\mathrm{head}(\mathcal{C})$. Note that the empty string ε is also a chain; by convention we set $\mathrm{head}(\varepsilon) = \varepsilon$. A chain $\mathcal{C}$ with $\mathrm{head}(\mathcal{C}) = \langle s', x', ctr'\rangle$ can be extended to a longer chain by appending a valid block $B = \langle s, x, ctr\rangle$ that satisfies $s = H(ctr', G(s', x'))$. In case $\mathcal{C} = \varepsilon$, by convention any valid block of the form $\langle s, x, ctr\rangle$ may extend it. In either case we have an extended chain $\mathcal{C}_{\mathsf{new}} = \mathcal{C}B$ that satisfies $\mathrm{head}(\mathcal{C}_{\mathsf{new}}) = B$.

The *length* of a chain $\mathrm{len}(\mathcal{C})$ is its number of blocks. Given a chain $\mathcal{C}$ that has length $\mathrm{len}(\mathcal{C}) = n > 0$ we can define a vector $\mathbf{x}_\mathcal{C} = \langle x_1, \ldots, x_n\rangle$ that contains all the x-values that are stored in the chain such that x_i is the value of the i-th block.

Consider a chain $\mathcal{C}$ of length m and any nonnegative integer k. We denote by $\mathcal{C}^{\lceil k}$ the chain resulting from the "pruning" the k rightmost blocks. Note that for $k \geq \mathrm{len}(\mathcal{C})$, $\mathcal{C}^{\lceil k} = \varepsilon$. If $\mathcal{C}_1$ is a prefix of $\mathcal{C}_2$ we write $\mathcal{C}_1 \preceq \mathcal{C}_2$.

Garay et al. Eurocrypt 2015

Blockchain

- Blockchain technology as introduced with Bitcoin offers a ditributed immutable ledger and a solution to the consensus problem (see Byzantine Generals), assuming an honest majority of computing power.
- Main use at the moment is monetary systems
- It is being tried out in a wide variety of different domains
- Has a relatively high communication and storage overhead
- Provides provable security under assumptions about the adversarial computational share and the network connectivity

How Blockchain works

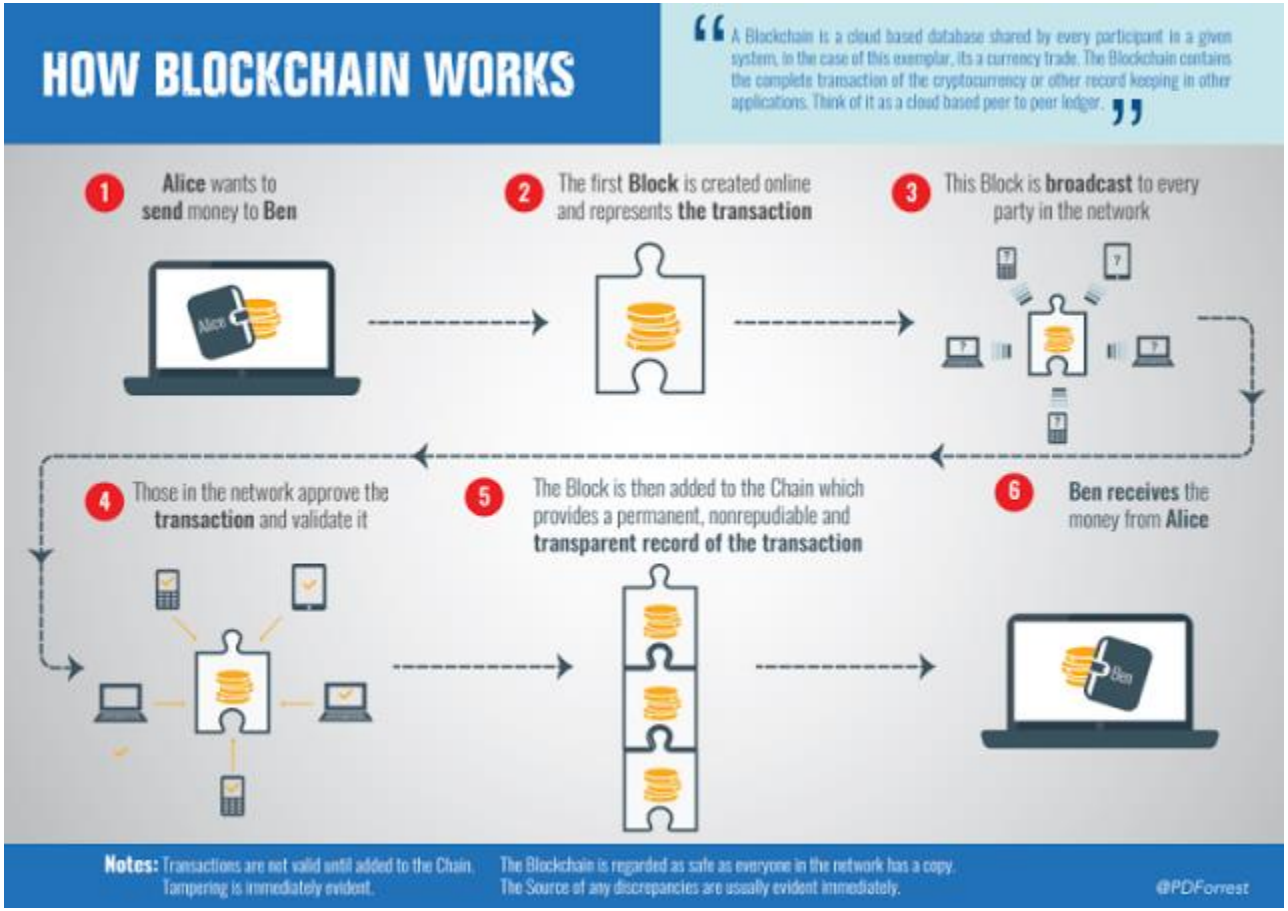
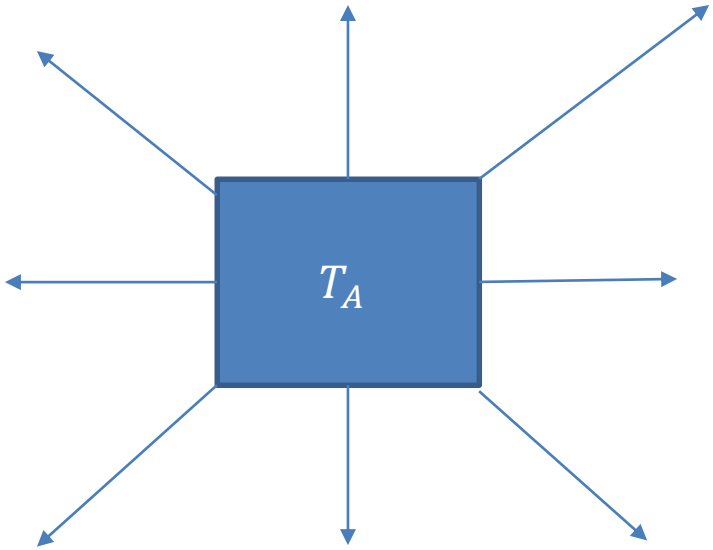


Illustration: https://datafloq.com

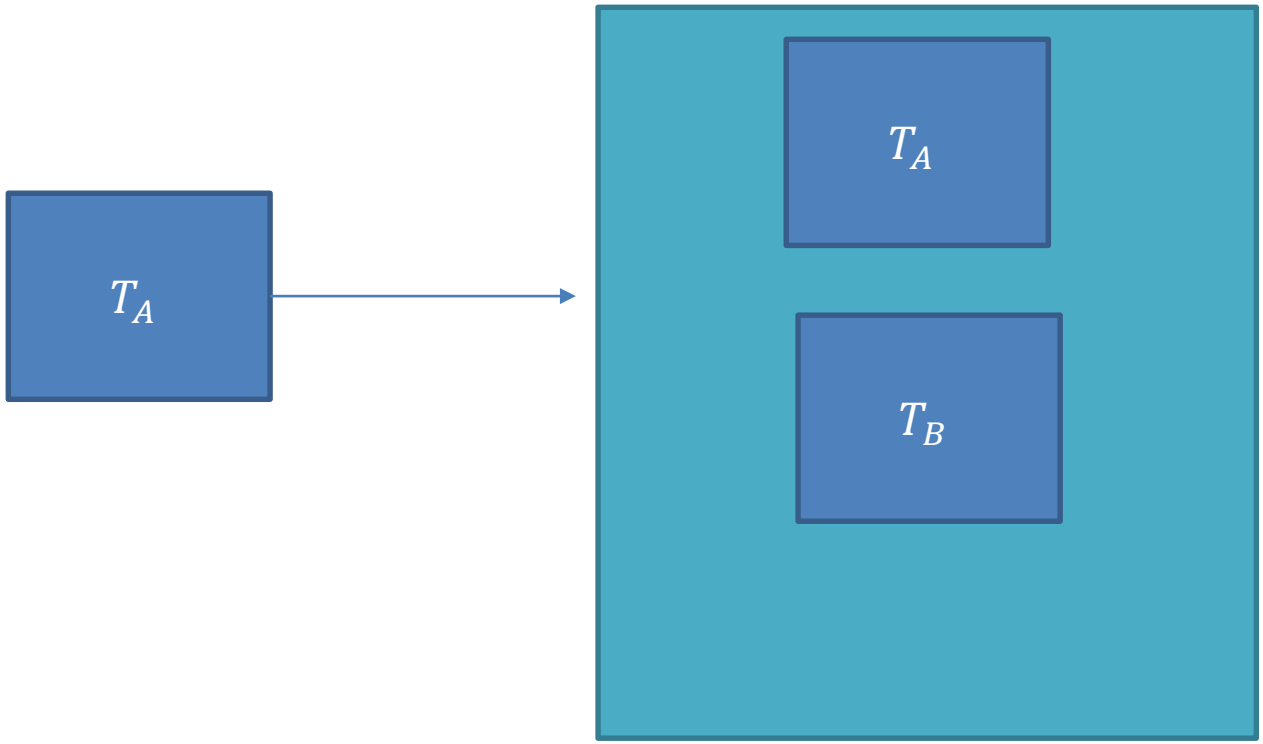
How Blockchain works (1)

- A peer A generates a transaction T_A and broadcasts it to the network (via flooding - gossiping)



How Blockchain works (2)

- Each miner checks T_A for protocol compliance and validity
- If valid, miner will add T_A to a block for mining



What's in a block

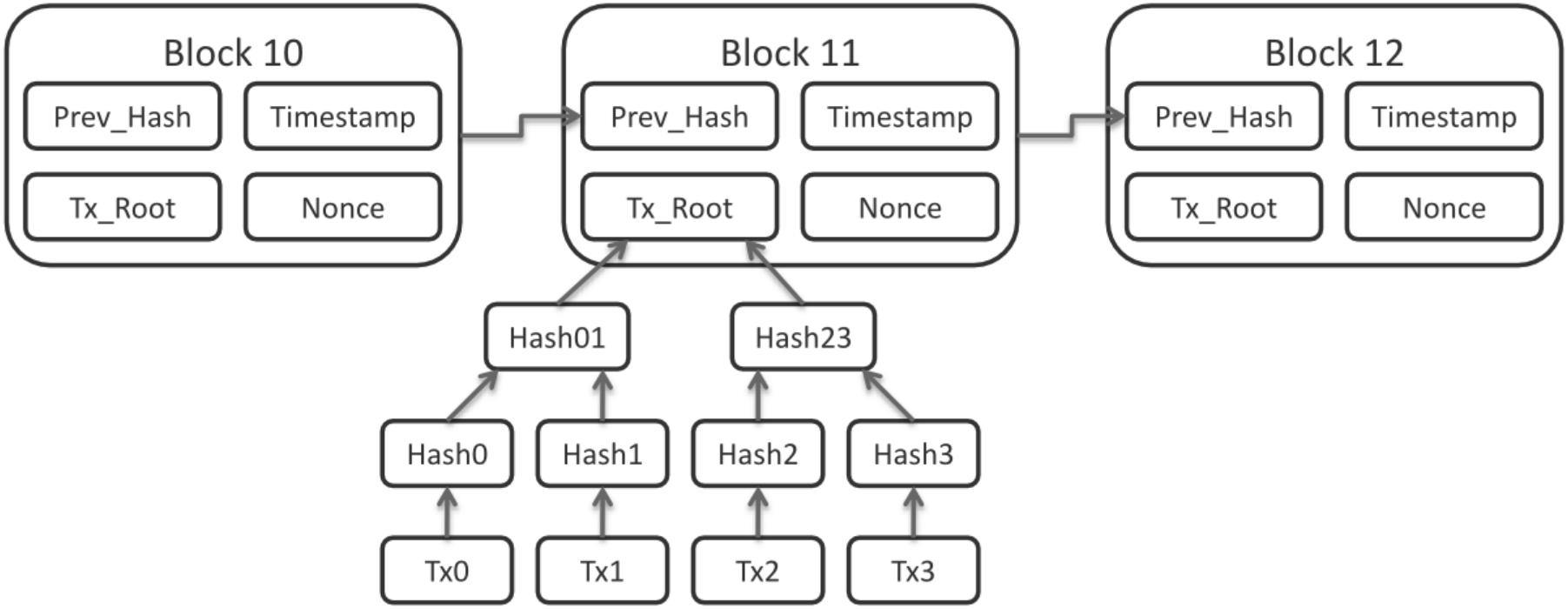


Illustration: Matthäus Wander (Wikimedia)

How Blockchain works (3)

- Each miner tries to find a solution to a (fairly difficult) computational puzzle (Proof-of-Work)
- There exist other approaches (Proof of Strake, - of Space, etc.)

Image source: dreamstime.com

How Blockchain works (4)

- The miner(s) that finds a solution broadcasts the winning block to the network
- He also collects a reward

Image source: The Sun

How Blockchain works (5)

- Each miner (peer) checks the block for validity
- If valid, he adds the block to his blockchain
- Race conditions are solved by “longest chain rule” (more difficult chain)
- The chain probabilistically converges (if adversary controls less than 50% of computational power)

How Blockchain works (6)

- Miners start working on the next block…

Why are Blockchains secure?

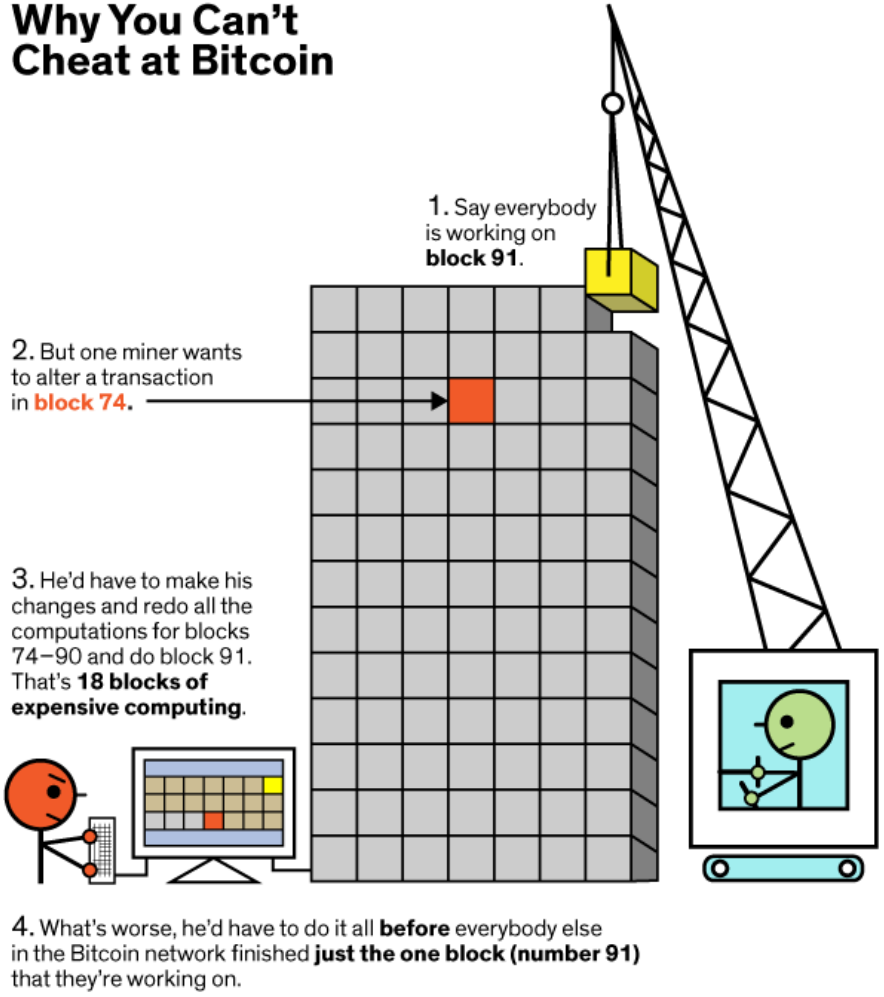
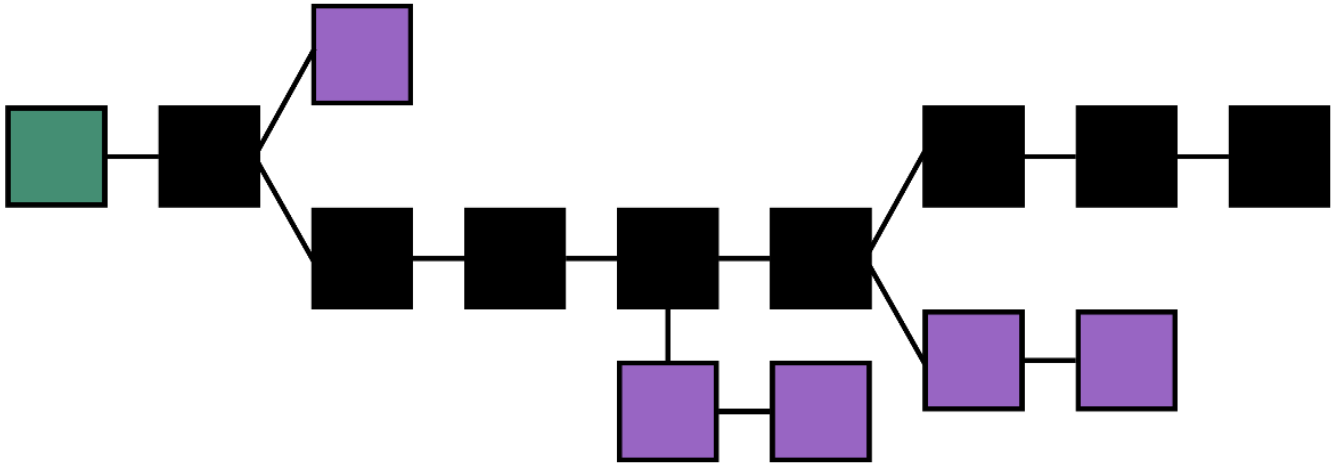


Illustration: Mark Montgomery

A small demo

- https://anders.com/blockchain/hash.html

The Blockchain as a distributed state machine



How decentralized is Bitcoin_

Geographical distribution of full nodes:

- https://bitnodes.21.co/

Hashrate Distribution:

- https://blockchain.info/pools

Blockchain frenzy

TECHNISCHE UNIVERSITÄT DARMSTADT

FUTURE OF FINTECH

Home > News > Future Of FinTech >

Future Of FinTech: Blockchain Frenzy Forges MBA Careers Across Sectors

Future Of FinTech: Blockchain Frenzy Forges MBA Careers Across Sectors

Technology's pioneers scrambling to hire 'blockchain tsars'

Written by Seb Murray | Future Of FinTech | Sunday 21st February 2016 23:46:00 GMT

© AFP

There are few more sexy tech topics setting the business world abuzz than blockchain — the virtual record of asset ownership underpinning the digital currency bitcoin.

FINANCIAL TIMES

HOME WORLD US COMPANIES MARKETS OPINION WORK & CAREERS LIFE & ARTS

Blockchain + Add to myFT

Has the blockchain hype finally peaked?

Sober reality bites on automating networks of trust on which modern finance rests

The bitcoin currency is supported by blockchain © AFP

16 Save


I prefer a
hands-on
experience

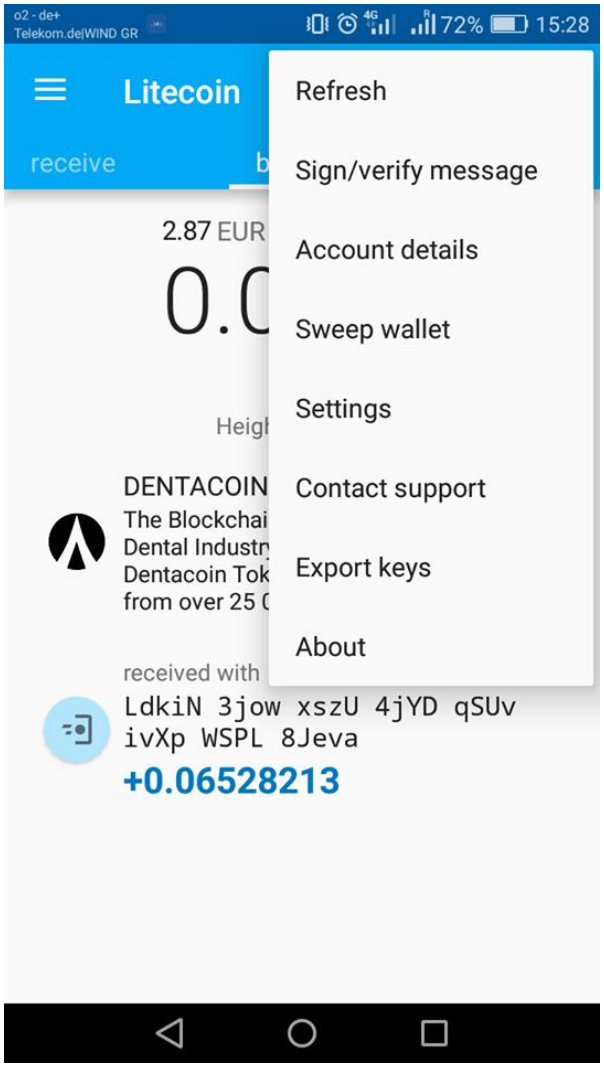
Set up a litecoin wallet

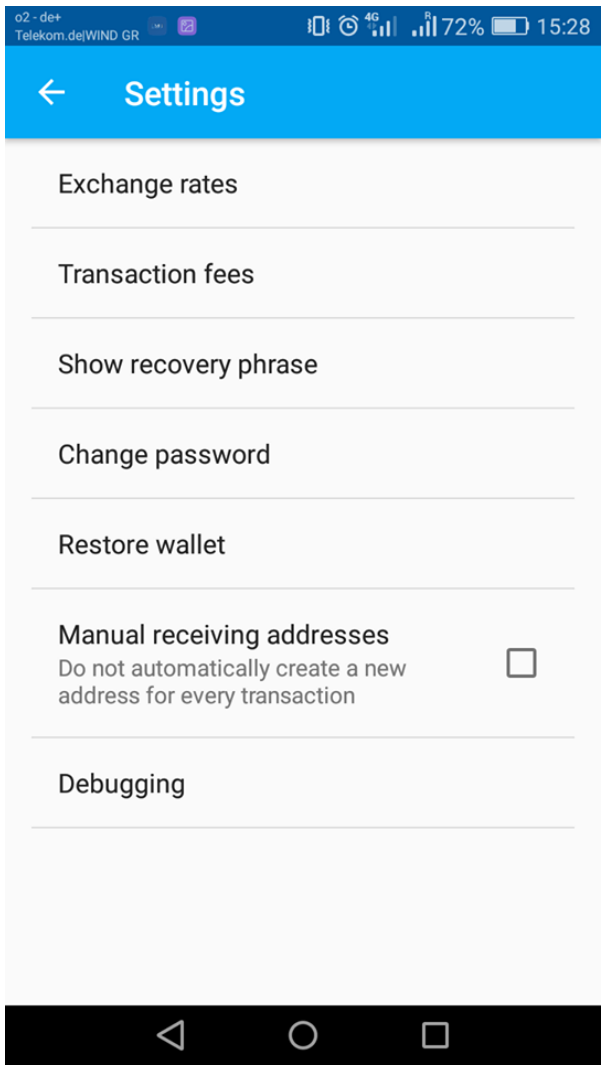
TECHNISCHE UNIVERSITÄT DARMSTADT

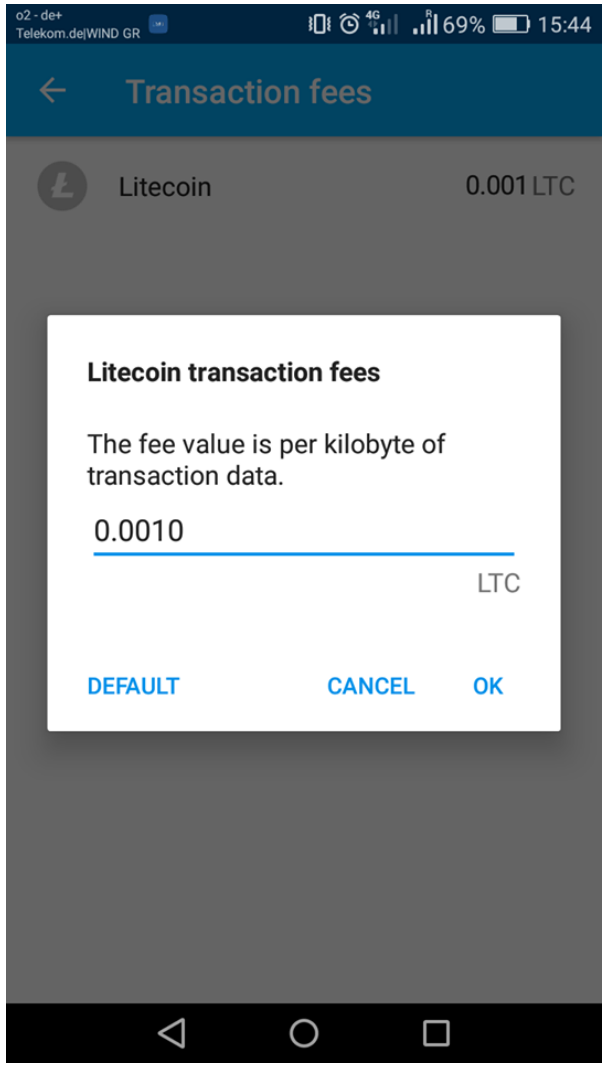
- Any wallet that can handle Litecoin transactions will do, but I propose:
  - **Coinomi (Android)** multiwallet- choose Litecoin (https://play.google.com/store/apps/details?id=com.coinomi.wallet)
  - **Loafwallet (ios)** (https://itunes.apple.com/us/app/loafwallet-litecoin-wallet/id1119332592?mt=8)
  - **Electrum-LTC or other (Desktop)**

Your address

Transaction fees



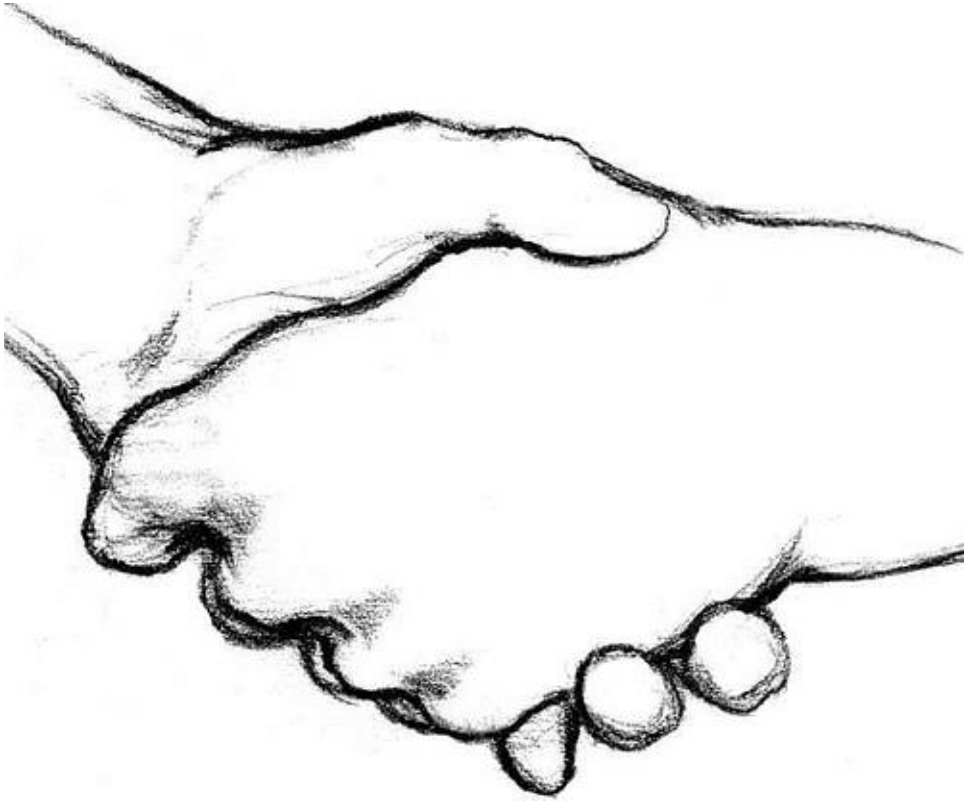




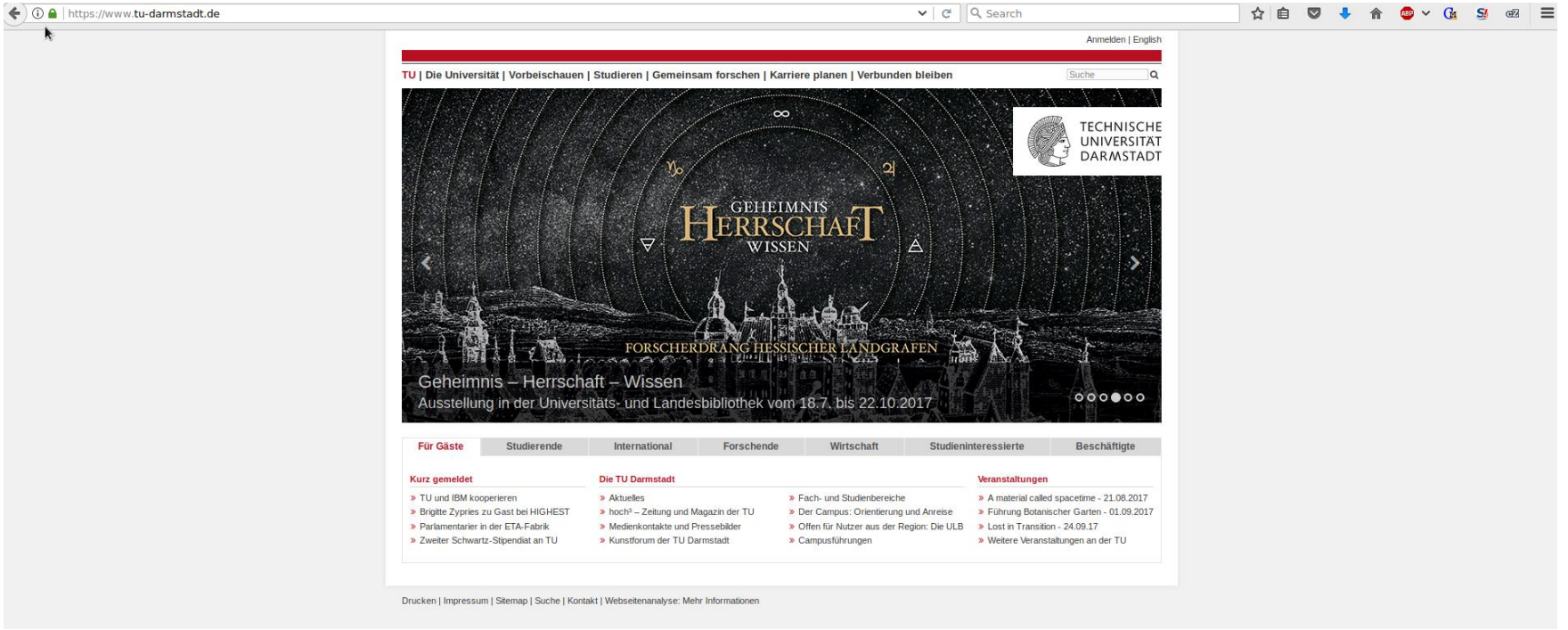
LET'S TRY IT OUT!

Credits to Crystal Brown Knox Middle School Salisbury, NC

Part 2: Trust in the Web



Remote Authentication



Q1: What does the green lock mean?

Authentication online is mainly performed through 2 means

- X.509 certificates
  - Signed by a certification authority (CA)
  - Chain of trust until a root CA is found

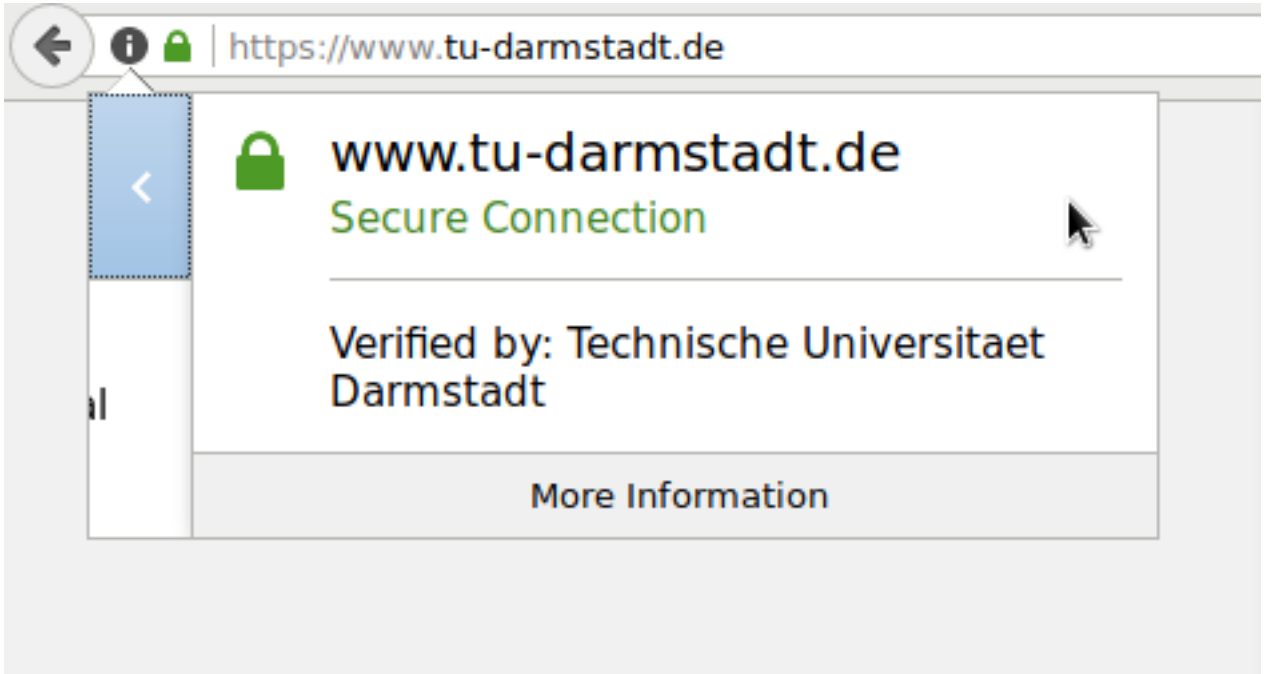
- PGP's Web of trust
  - Decentralized system
  - Chain of trust among peers
  - Mostly used (by geeks) for email communication and code signing

Q2: How are root CA's known to the browser?

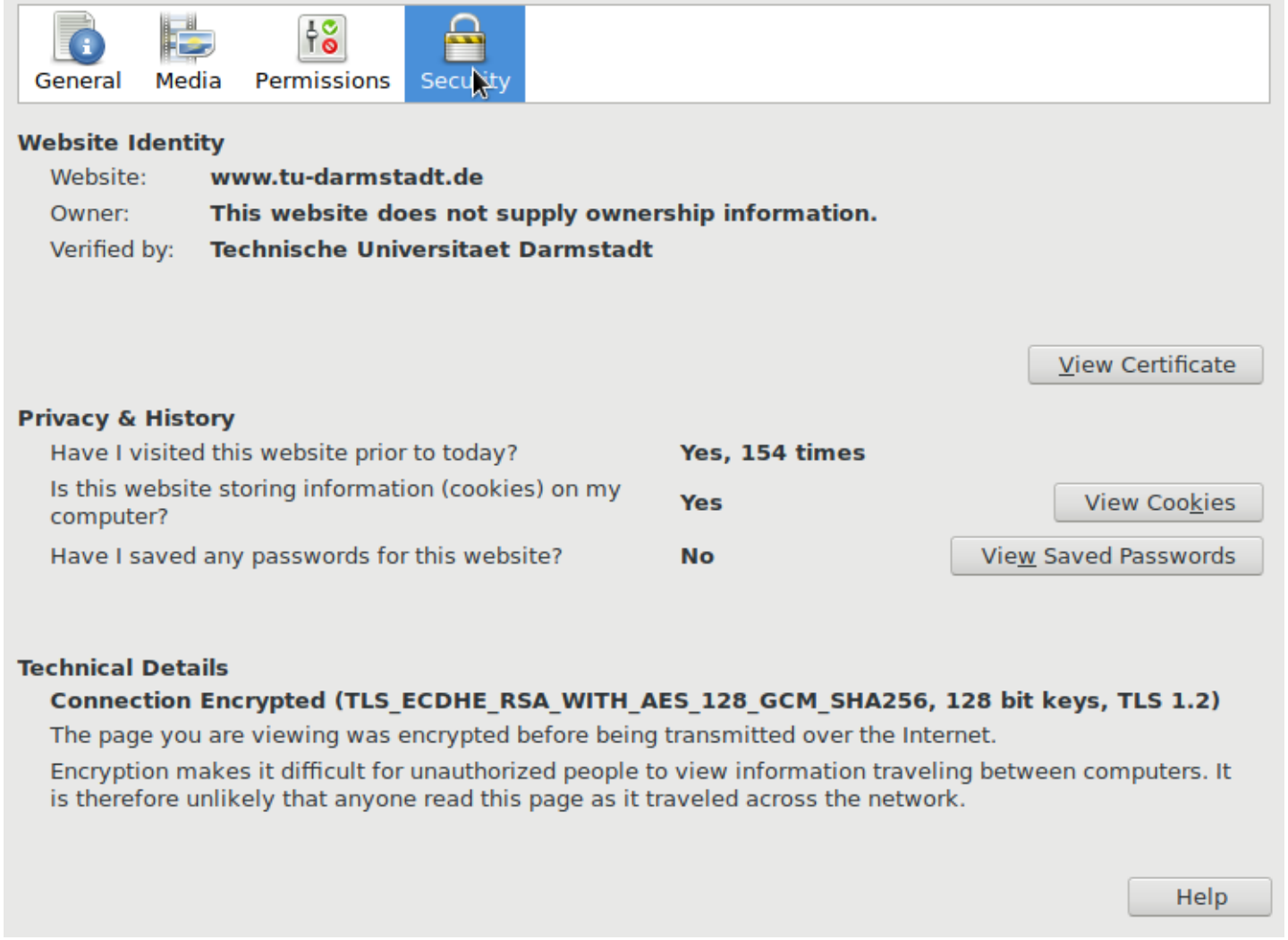
A (large) set of root CAs is trusted by the browser's vendor (and operating system)

X.509: SSL/TLS green lock means authentication successful

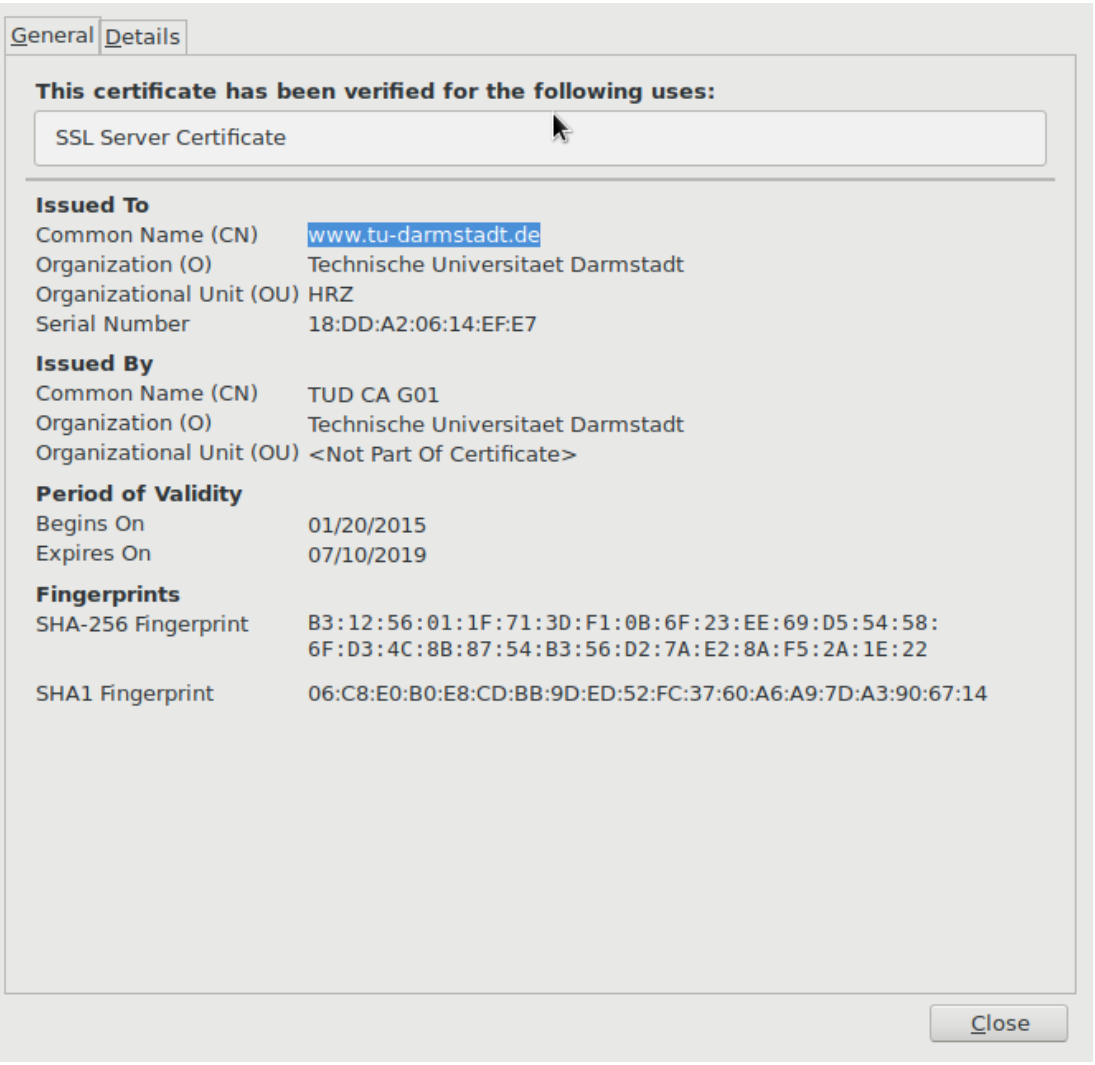
Upon closer inspection



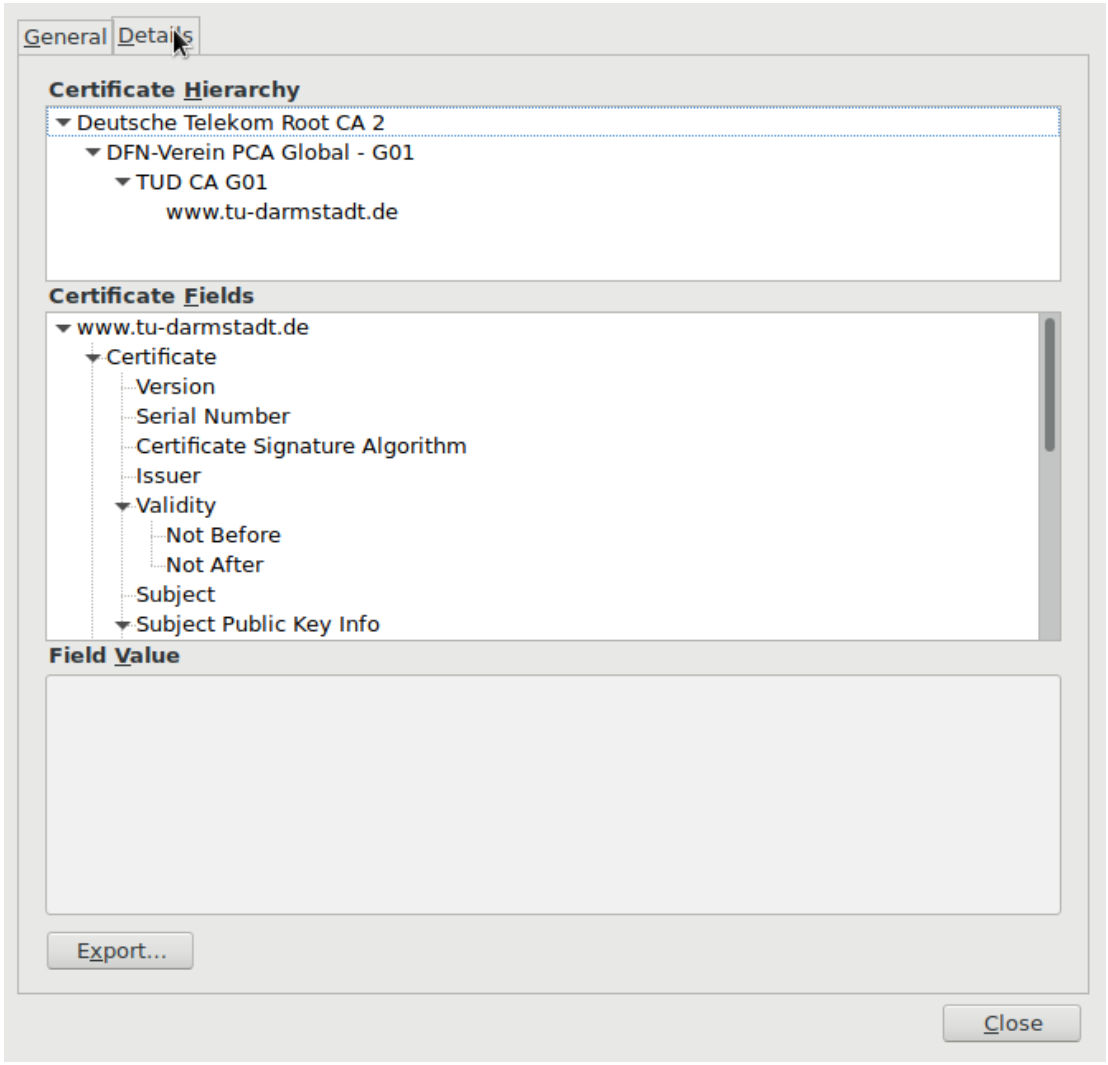
Connections security details show encryption algorithms etc.



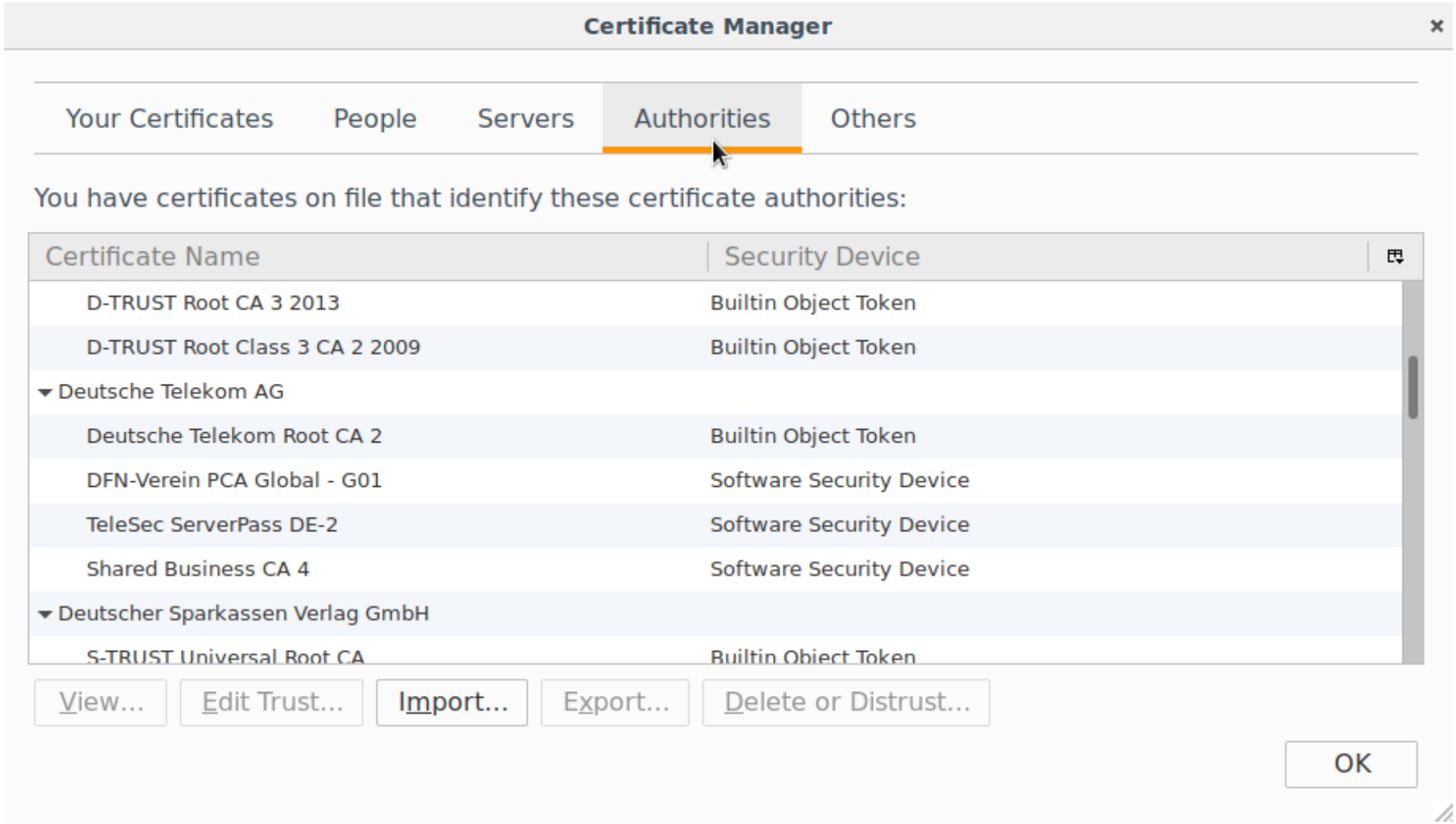
Certificate inspection: organizations involved and fingerprints



Trust chain: DT is root of trust



We can find DT in the list of Root CAs



Real-world issues

TECHNISCHE UNIVERSITÄT DARMSTADT

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

RISK ASSESSMENT —

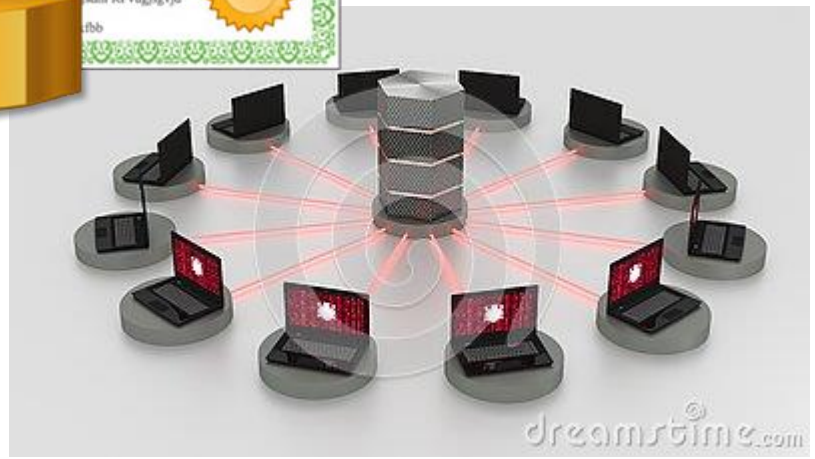
Another fraudulent certificate raises the same old questions about certificate authorities

For the second time this year, Iranian hackers have created a fraudulent ...

PETER BRIGHT - 8/30/2011, 5:12 AM

Earlier this year, an Iranian hacker broke into servers belonging to a reseller for certificate authority Comodo and issued himself a range of certificates for sites including Gmail, Hotmail, and Yahoo! Mail. With these certificates, he could eavesdrop on users of those mail providers, even if they use SSL to protect their mail sessions.

COMODO
Creating Trust Online®



Ethereum Bug Sends Smart Contracts Back to the Drawing Board

Alyssa Hertig (@AlyssaHertig) | Published on November 2, 2016 at 21:51 GMT

FEATURE

399 259

The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

What about PGP?

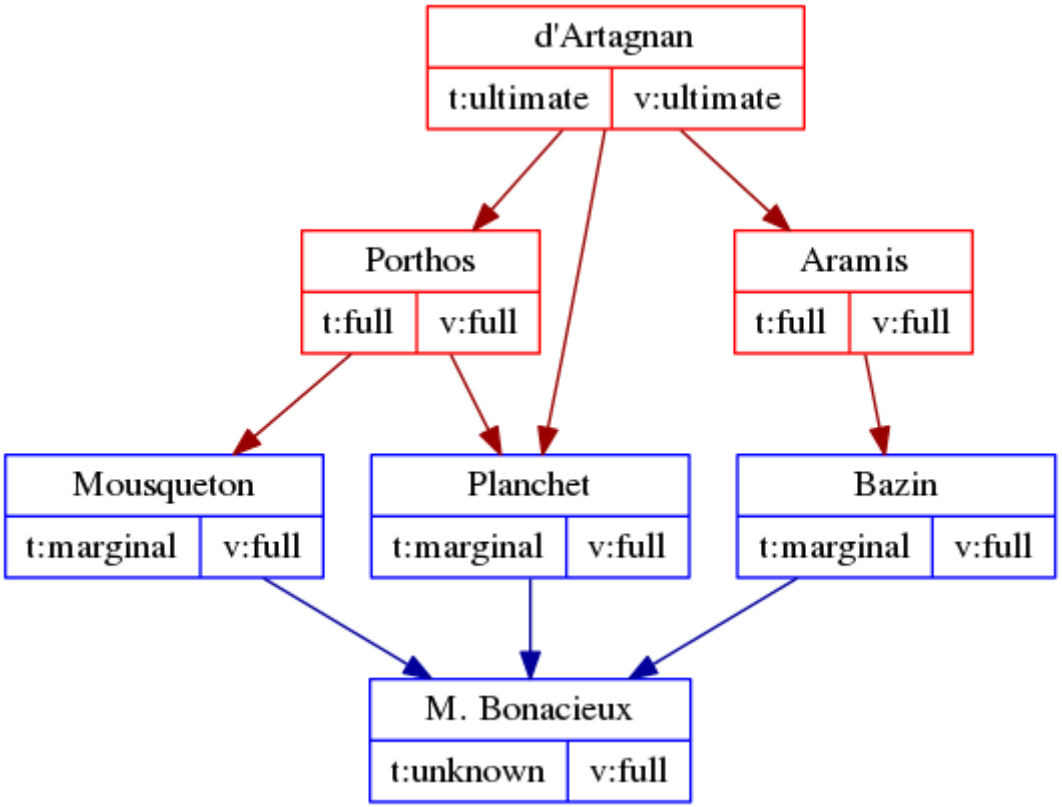


Illustration: Konstantin Ryabitsev

PGP is good but…

TECHNISCHE UNIVERSITÄT DARMSTADT

- Lacks usability (and user-base)
- Nightmare key management
- Has many distributed single points of failure
- Key distribution is handled by authorities known as key servers
- Key revocation is also handled by these servers
- No forward secrecy
- No privacy
- …

Q3: What is forward secrecy/security?

Secure authentication is an open problem with its main issues:

- Binary notion of security is unrealistic
- Centralized solutions are dangerous
- Difficult to use solutions are also dangerous

Secure authentication is an open problem with its main issues:

TECHNISCHE UNIVERSITÄT DARMSTADT

- Binary notion of security is unrealistic
- Centralized solutions are dangerous
- Difficult to use solutions are also dangerous

✓**Proposed approach: Combine *computational trust* models with *Blockchain technology* to build decentralized and secure systems**

Part 3: Some of our work

(Computational) Trust: a definition

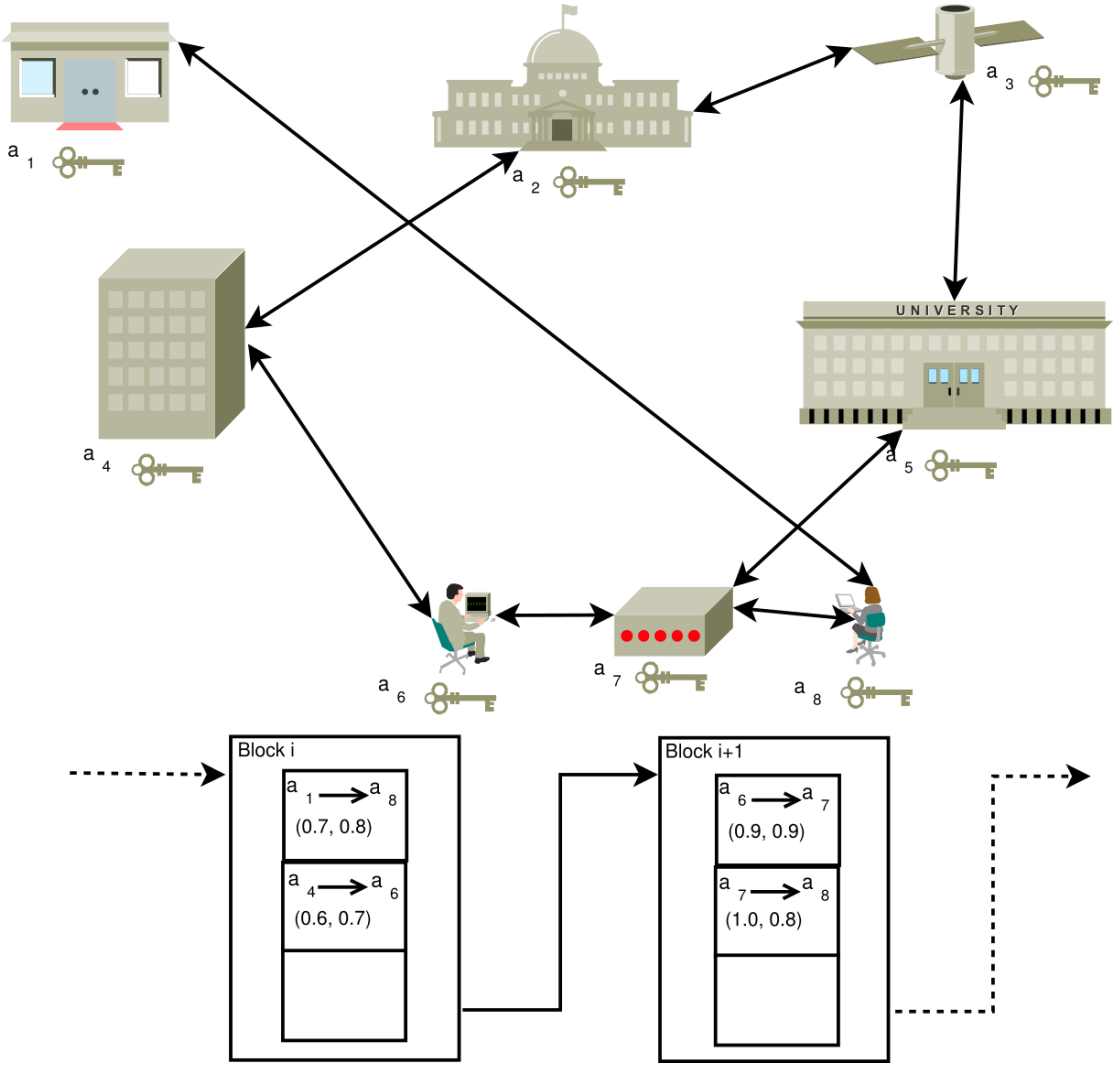
- *"a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action… in a context in which it affects his own action" [Gambetta, 1990]*

✓*Therefore we model trust as a probability under uncertainty, e.g.:*

$$o = (t, c, f) \in \{[0,1] \times [0,1] \times [0,1]\}$$

$$E = t \cdot c + (1 - c) \cdot f$$

Idea: Store trust assessments/ certificates in the blockchain



Blockchains and trust: (Some) Related work

- **"Perspectives: Improving SSH-style Host Authentication with Multi-Path Probing" (Usenix ATC '08)**
- **"Towards robust and effective trust management for security: A survey" (TrustCom'14)**
- **"From Pretty Good to Great: Enhancing PGP Using Bitcoin and the Blockchain" (NSS'15)**
- **"Blockstack: A global naming and storage system secured by blockchains" *(USENIX ATC 16)"***
- **"TrustIsRisk: A Decentralized Financial Trust Platform" (FC'17)**
- **"IKP: Turning a PKI Around with Decentralized Incentives" (Oakland'17)**

Our research question

- Can Blockchain technology offer more secure systems for cryptographic authentication?

Important questions

TECHNISCHE UNIVERSITÄT DARMSTADT

- How can we model Blockchain-based trust management systems (TMSs)?
- What advantages do these systems have compared to existing approaches?

✓ We present a model for TMSs built upon a blockchain

✓ We present 5 prevalent attacks on TMSs and how they can be mitigated by our design

Our model: Trust relation

- Definition1 (Trust relation): A Trust relation (TR) is a tuple

$\prec A, B, c, v, \alpha, t \succ$, where:

  - A is the trustor
  - B is the trustee
  - c is the context*
  - $v \in [0,1]$ is the computational trust value
  - α is a set of cryptographic artifacts, i.e. digital signatures
  - t is a logical time component (partial time ordering)

Our model: TM network and trust assessment

- Definition 2 (TM network): A TM network or trust graph is a directed multigraph $G = (V, E)$, where:
  - Each $v \in V$ is an entity, e.g. CA, physical person etc.
  - Each $e \in E$ is labeled with a trust relation

- Definition 3 (Trust assessment): A trust assessment $T^c_{A \to B}$ is defined as:

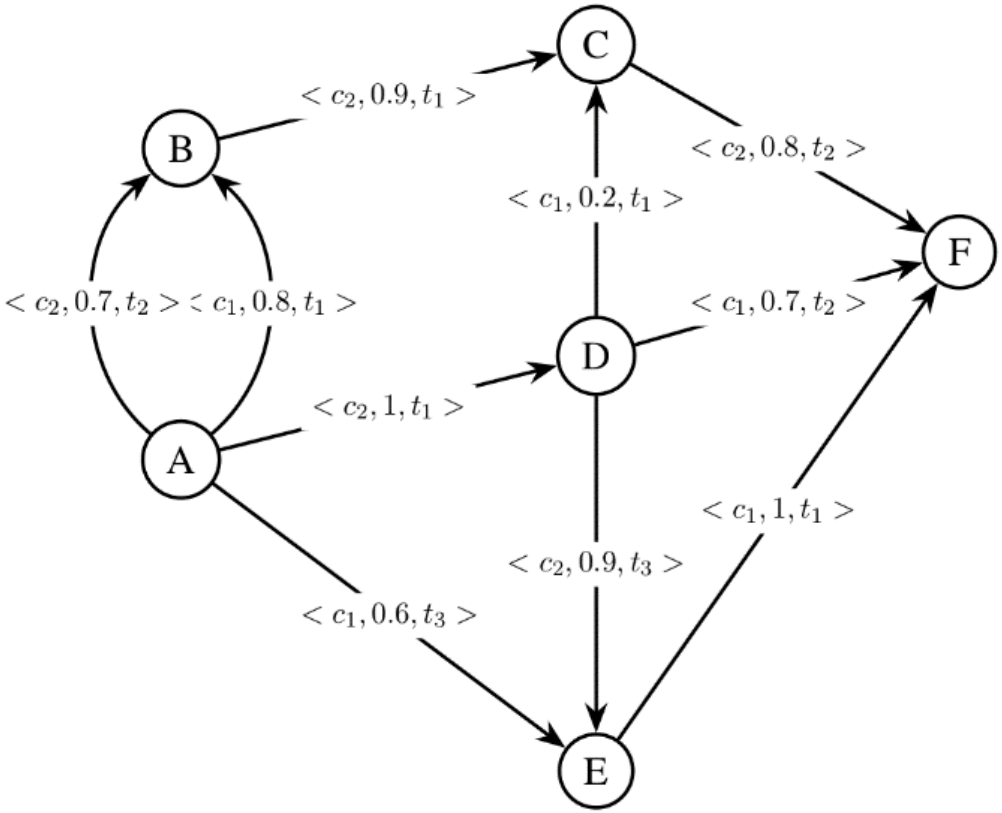
$$T^c_{A \to B} \stackrel{\text{def}}{=} P(c, H)$$

where:

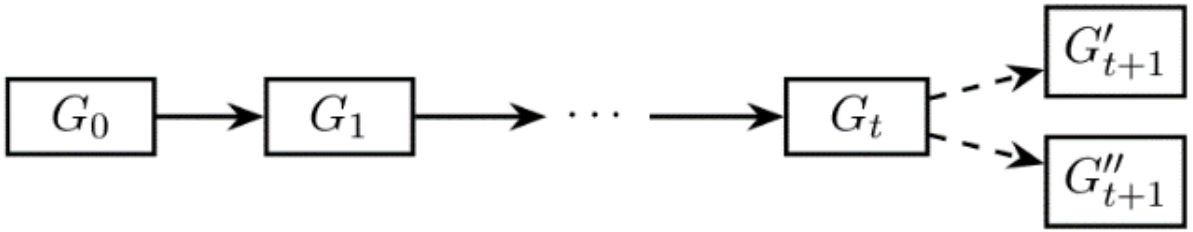
$$P : c \times H \subseteq G \rightarrow [0, 1]$$

P is a program that takes as input a trust network H and outputs a trust value in a given context.

Our model: a trust graph



The blockchain as a state machine for trust

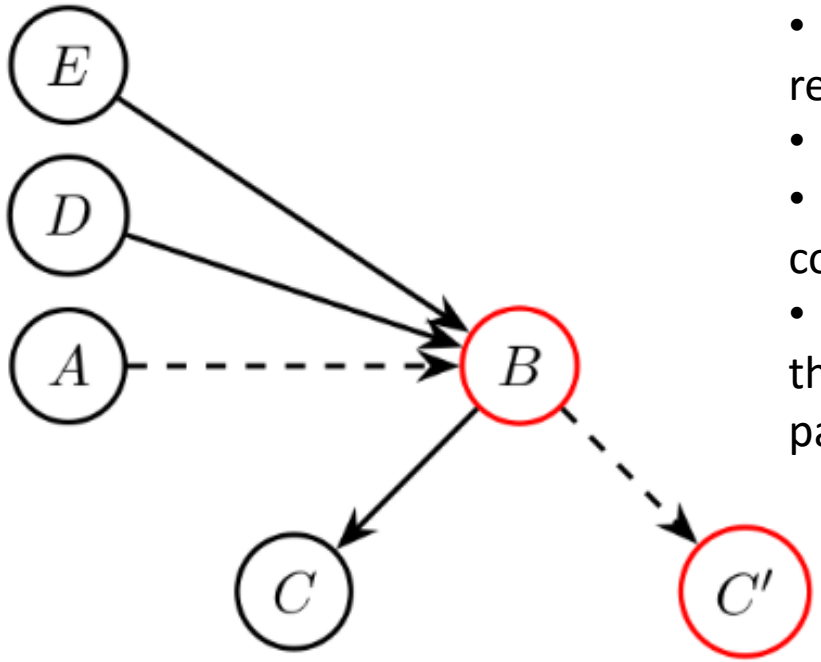


- Blocks are states of the trust graph
- A fork can happen for a short period of time but will be resolved

Attacks against TMS

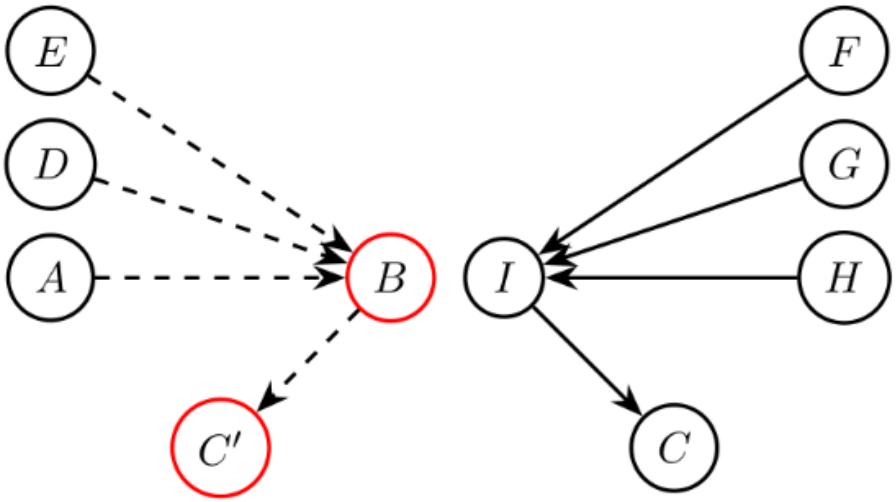
- Adversary: arbitrary, can control a subset of the entities in the system, along with a subset of the communication channels BUT he cannot break crypto
- Objective: Man in the middle (MITM) – fake identity – impersonation + remain undetected (optionally)
- Resources: The number of entities and communication channels the adversary controls

A1: Stealthy targeted attack



- MITM against specific user, without the rest of the network realizing.
- E.g. malicious CA
- Similar in nature to discrimination or conflicting behavior attack in TMS
- Consensus property of Blockchain makes this attack improbable (proof sketch in the paper)

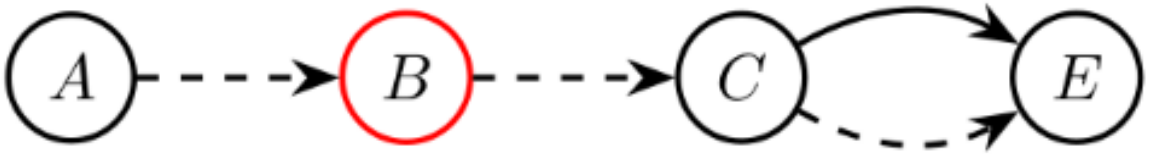
A2: Double registration attack



- Similar to identity theft and domain highjacking
- Global view of the chain by all participants

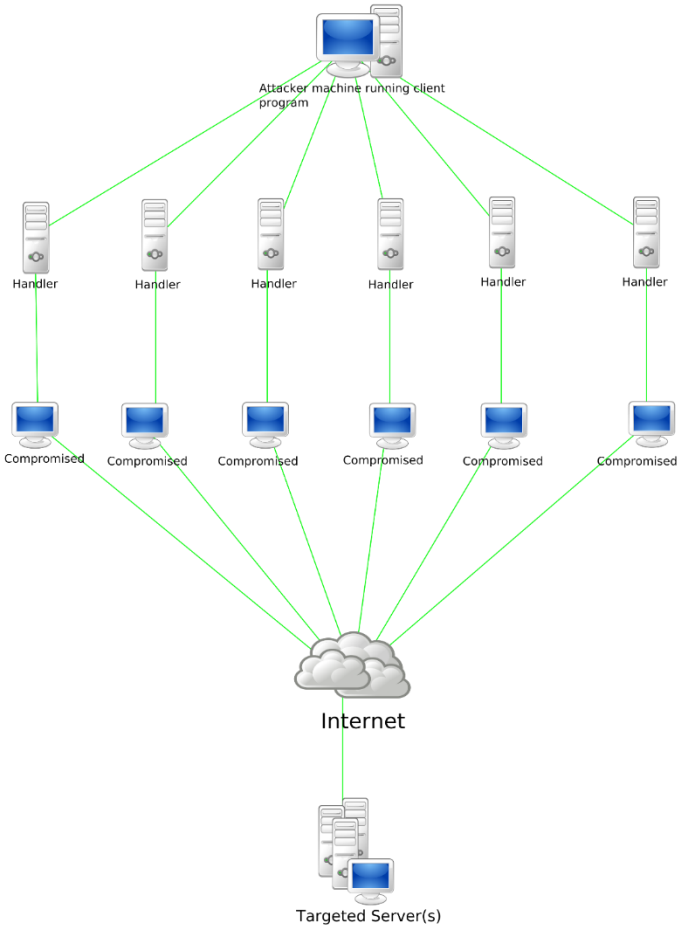
averts this attack

Stale information attack



- Old (stale) information (e.g. revoked certificates) is forwarded to a user in order to trick him into a bad decision
- Strict partial ordering of events on the chain exposes this attack (proof sketch in the paper)

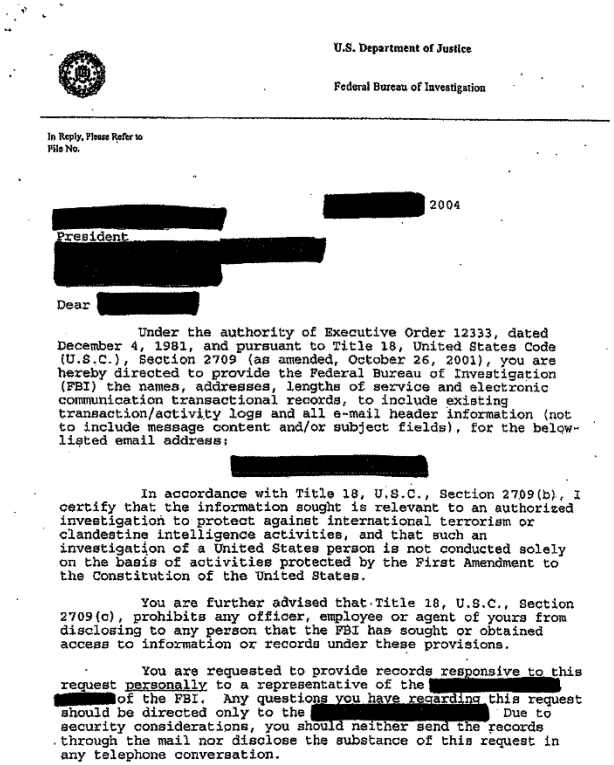
Denial of Service attack*



- Distributed Blockchain constructs are in Principle more resistant to DoS attacks than centralized solutions, although research in this field is ongoing

By Everaldo Coelho and YellowIcon - All Crystal icons were posted by the author as LGPL on kde-look, LGPL, https://commons.wikimedia.org/w/index.php?curid=3980651

Censorship (and legal)



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

[redacted] 2004

President
[redacted]

Dear [redacted]

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (as amended, October 26, 2001), you are hereby directed to provide the Federal Bureau of Investigation (FBI) the names, addresses, lengths of service and electronic communication transactional records, to include existing transaction/activity logs and all e-mail header information (not to include message content and/or subject fields), for the below-listed email address:

[redacted]

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

You are further advised that Title 18, U.S.C., Section 2709(c), prohibits any officer, employee or agent of yours from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions.

You are requested to provide records responsive to this request personally to a representative of the [redacted] of the FBI. Any questions you have regarding this request should be directed only to the [redacted]. Due to security considerations, you should neither send the records through the mail nor disclose the substance of this request in any telephone conversation.

- Increased transparency and consensus avert one-sided decisions
- Distribution of control makes consensus necessary for decisions

Conclusions and future work

TECHNISCHE UNIVERSITÄT DARMSTADT

- We showed that building TMS on top of blockchain consensus protocols can provide more secure solutions
- A number of attacks are mitigated with the assumption of a distributed ledger

- Challenges:
  - Size of the Blockchain – counter bloat
  - Privacy of trust relations
  - Choice of Blockchain (public, consortium etc.)
  - Thin clients for IoT devices

More thoughts

TECHNISCHE UNIVERSITÄT DARMSTADT

- Who owns your data?
  - ➢Google, Facebook, Amazon etc. ?
- Who owns your identity?
  - ➢Government, Google, Facebook?
- How can you own your own identity?
  - ➢Self-sovereign identity and trust

Security only with:

TECHNISCHE UNIVERSITÄT DARMSTADT

- Open hardware
- Open software
- Self-sovereign data and identity


THANK YOU

Discussion Time

Credits to Rita Platt

Some of our papers…

- “Student Research Abstract: On Enhancing Trust in Cryptographic Solutions” (ACM SAC ‘17)
- “Beyond the Hype: On using Blockchain in Trust Management for Authentication” (TrustCom’17)

Bibliography

[1] Yamaguchi, F., Lindner, F. and Rieck, K., 2011, August. Vulnerability extrapolation: assisted discovery of vulnerabilities using machine learning. In *Proceedings of the 5th USENIX conference on Offensive technologies* (pp. 13-13). USENIX Association.

[2] Perl, H., Dechand, S., Smith, M., Arp, D., Yamaguchi, F., Rieck, K., Fahl, S. and Acar, Y., 2015, October. Vccfinder: Finding potential vulnerabilities in open-source projects to assist code audits. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 426-437). ACM.

[3] Stephens, N., Grosen, J., Salls, C., Dutcher, A., Wang, R., Corbetta, J., Shoshitaishvili, Y., Kruegel, C. and Vigna, G., 2016. Driller: Augmenting fuzzing through selective symbolic execution. In *Proceedings of the Network and Distributed System Security Symposium*.

[4] Bugiel, S., Davi, L.V. and Schulz, S., 2011, October. Scalable trust establishment with software reputation. In *Proceedings of the sixth ACM workshop on Scalable trusted computing* (pp. 15-24). ACM.

[5] Johnson, P., Gorton, D., Lagerström, R. and Ekstedt, M., 2016. Time between vulnerability disclosures: A measure of software product vulnerability. *Computers & Security*, *62*, pp.278-295.

[6] Jimenez, M., Papadakis, M. and Le Traon, Y., 2016, October. Vulnerability Prediction Models: A case study on the Linux Kernel. In *Source Code Analysis and Manipulation (SCAM), 2016 IEEE 16th International Working Conference on* (pp. 1-10). IEEE.

[7] Hovsepyan, A., Scandariato, R. and Joosen, W., 2016, September. Is Newer Always Better?: The Case of Vulnerability Prediction Models. In *Proceedings of the 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement* (p. 26). ACM.

[8] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R. and Polk, W., RFC 5280: Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Internet Engineering Task Force (IETF), 2008.

[9] Zimmermann, P.R., 1995. *The official PGP user's guide*. MIT press.

[10] Zhou, L., Varadharajan, V. and Hitchens, M., 2015. Trust enhanced cryptographic role-based access control for secure cloud data storage. *IEEE Transactions on Information Forensics and Security*, *10*(11), pp.2381-2395.

[11] Chen, Z., Zhang, R., Ju, L. and Wang, W., 2013, July. Multivalued trust routing based on topology level for wireless sensor networks. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on* (pp. 1516-1521). IEEE.

[12] Kamvar, S.D., Schlosser, M.T. and Garcia-Molina, H., 2003, May. The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th international conference on World Wide Web* (pp. 640-651). ACM.

Bibliography

[13] Wendlandt, D., Andersen, D.G. and Perrig, A., 2008, June. Perspectives: Improving SSH-style Host Authentication with Multi-Path Probing. In *USENIX Annual Technical Conference* (Vol. 8, pp. 321-334).

[14] Wang, D., Muller, T., Liu, Y. and Zhang, J., 2014, September. Towards robust and effective trust management for security: A survey. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on* (pp. 511-518). IEEE.

[15] Wilson, D. and Ateniese, G., 2015, November. From pretty good to great: enhancing PGP using Bitcoin and the blockchain. In *International Conference on Network and System Security* (pp. 368-375). Springer International Publishing.

[16] Orfeas Stefanos Thyfronitis Litos and Dionysis Zindros. *TrustIsRisk: A Decentralized Financial Trust Platform (To appear in FC'17)*

[17] Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system.

[18] Garay, J., Kiayias, A. and Leonardos, N., 2015, April. The bitcoin backbone protocol: Analysis and applications. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 281-310). Springer Berlin Heidelberg.

[19] Ali, M., Nelson, J., Shea, R. and Freedman, M.J., 2016, June. Blockstack: A global naming and storage system secured by blockchains. In *2016 USENIX Annual Technical Conference (USENIX ATC 16)* (pp. 181-194). USENIX Association.

Image sources (partial list)

TECHNISCHE UNIVERSITÄT DARMSTADT

- http://www.softwaretestingtricks.com/2007/05/my-top-5-ways-to-reproduce-hard-to.html
- https://en.wikipedia.org/wiki/Computation_tree_logic
- https://www.win.tue.nl/hashclash/rogue-ca/
- https://www.certificate-transparency.org/