Veiligheid in blockchain gebruik

@henkvancann

Korte omschrijving van de presentatie (3-5 bullets)

- Blockchain fundamentals voor Auditors -> dit leidt tot **onwijzigbaarheid**
- Waarom vertrouwen verplaatsen? -> geeft daar als auditor zelf maar antwoord op (iets met mensen?)
- Hoe zelf zin en onzin van de technologie scheiden -> hier en nu het begin, eindeloos leerproces ter grootte van het leren over en werken met Internet.

NOOIT MEER VERGETEN: Fundamentele kennis is jouw pad naar professionalisering

Begin met leren: http://wiki.2value.nl/BCWS/meetup/study_more

[The Crypto Anarchist Manifesto]
Timothy C. May <tcmay@netcom.com>

“A specter is haunting the modern world, the specter of crypto anarchy.”

What is de echte behoefte aan deze kennis. Welke reële functie vervult het in ons dagelijks leven?

Vandaag niet…

- HOE de techniek van publieke blockchains in detail werkt
- WAAROM blockchains het werkende leven fundamenteel gaan beïnvloeden
- Op WELKE manier zijn blockchains verstorend

Verlies ik mijn baan, mijn vrijheid, centrale positie, mogelijkheid om te rommelen met data? Nee, nee, ja, ja.

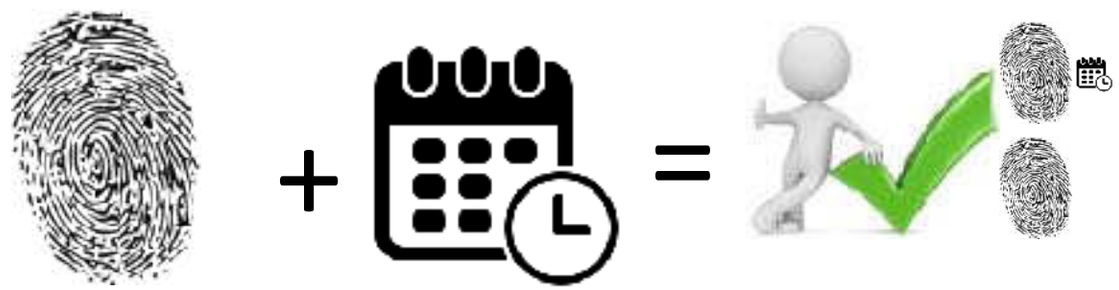
Tip: Begrijp de werking van de technologie die u gebruikt

Fundamental knowledge is your way to freedom :)

Tip: Begrijp de werking van de technologie die u gebruikt

…zodat je veilig kennis kunt maken en kennis opdoen

Stel jezelf de vraag: Zijn de digitale sleutels goed opgeslagen?



Voorbeeld SHA-256 HASH:
ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb

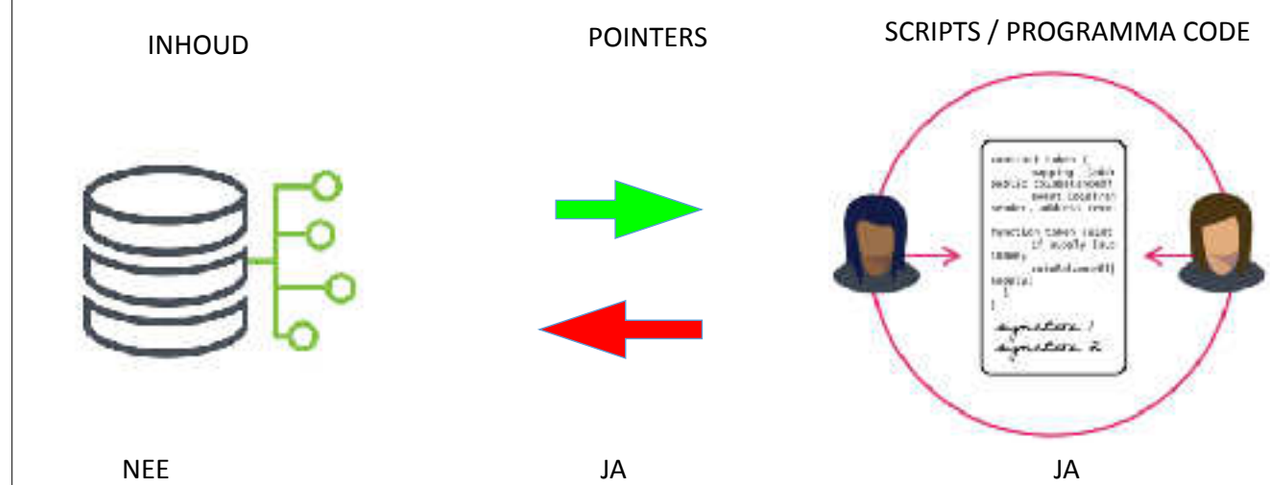
Beroemde HASH:
000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Herhaal de essentie van publieke blockchains (DATA + FUNC):
DATA
Hashing {sleutel/vingerafdruk}
Tijdstempels and consensus {stempelen}
Verificatie {check}

000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f Genesis block #0 (Jan 3, 2009, 10 leading zeros)
Expert vraag: Wat is het toevallige gedeelte van de blockchain ontdekking? -> Antwoord: Het (later gewijzigd ‘op_return’) data field of a transaction.

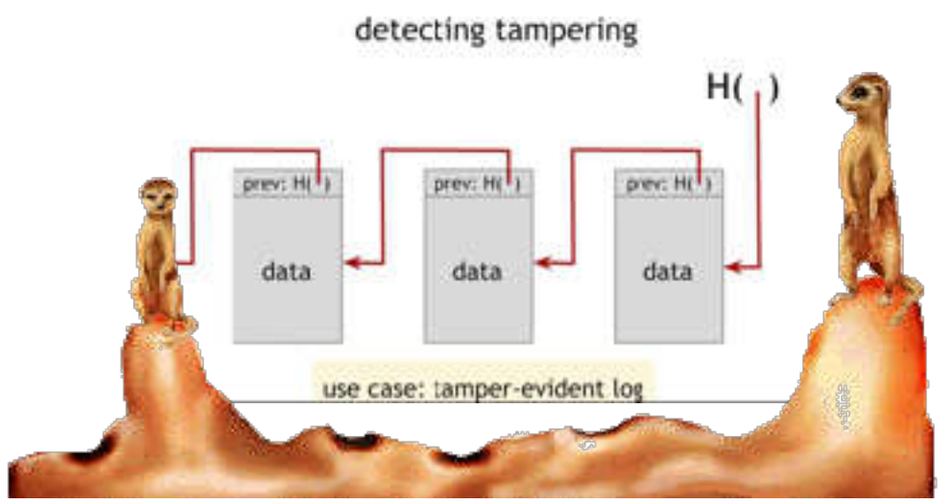
FUNC : smart contracts -> lex cryptographia
“Lex Cryptographia is a plan for addressing trust and recourse problems in online commerce in a way that does not depend on unreliable, inaccessible, non-existent, or contradictory government law systems. By combining the concepts of insurance, surety, smart contracts, and third party arbitration where necessary, it is possible to greatly reduce the risk of non-performance.”

Wat staat er OP de blockchain?!



Picture of CODE: https://www.coindesk.com/information/ethereum-smart-contracts-work/
CODE spread out over many computers, transparent, open source, immutable, etc.
SCRIPTS as (optional) parts of the protocol

Ketting van hashes: evident dat ermee is geknoeid!



Hashpointer -> hash die wijst naar data en het tegelijkertijd valideert!
Log N validatie tijden
Elke 10 minuten een block met transacties.
Geen circulaire ketens toegestaan of mogelijk -> blockchain, chain of blocks

Inbreuk op veilig gevoel of Fraude

MENSEN zijn de bepalende factor

"If you control your keys, it's your bitcoin. If you don't control the keys, it's NOT your bitcoin."

Andreas Antonopoulos, 2015

"Why you have to carefully manage your keys. And why you won’t"

Henk van Cann 2018 :)

Een leerproces, is niet iets wat je even een keer ’s avonds doet.

Hoe zien cryptografische sleutels er nu uit?

- Sterke wachtwoorden
- Seeds 12 woorden, 24 woorden, 25 woorden
- Hexadecimale strings
- QR codes

2kWqP2AKQqVaiv]Pykk;

(we focus on control and private keys)
Strong passwords first : generated from and stored in a Password Manager.

Een bitcoin, dat ben ik!

Kennis is controle, controle geeft een veiliger gevoel

Doen:
Noteer je gevoel van veiligheid
Noteer je gevoel van Onveiligheid
KENNIS opdoen. Google is your friend! + 18 oktober a.s.!

Mensen zijn het probleem (jijzelf onbewust/per ongeluk en anderen per ongeluk en bewust), niet de techniek. Blockchain zijn dus veilig in de techniek, onveilig in het gebruik.

Welke aspecten bij gevoel van “veiligheid”

- Complexiteit, moeilijk binnen te komen
- Geld, het kost meer dan het oplevert
- Tijd, je bent te lang bezig
- Zichtbaarheid, de actie loopt in het oog
- Volwassenheid, hoe “oud” is de technologie

Waarom is dit wezenlijk? ->
Het gaat altijd over ‘mij’ omdat:
Technisch netwerk is heel solide, fouten en fraude/stelen door mensen + Onbewust fouten door jezelf. -> Kennis opdoen: hoe kun je op alle fronten voorsprong krijgen?

Informatie nu opgeslagen voor later

Het is verkeerd om te denken dat er nog geen probleem is, omdat het nog lang duurt voor wetenschappers 'klaar' zijn met de kwantumcomputer, zegt Tanja Lange, hoogleraar cryptologie aan de TU Eindhoven. Ze verwees naar de affaire rond Edward Snowden, de klokkenluider die grootschalige afluisterpraktijken van de Amerikaanse geheime dienst NSA naar buiten bracht. 'We weten dankzij Snowden dat geheime diensten alle communicatie opnemen en bewaren. Wat nu nog niet kan worden ontsleuteld, wordt alvast opgeslagen voor over twintig jaar, als de kwantumcomputer er is.'

Bron citaat: FD artikel

Speech op SURFnet - slides, CC by SA Tanja Lange.

Photo: Henk van Cann, SURFnet security & privacy 2018

Eight conditions to avoid pointless blockchain applications - [Nov 2015 article](#) :

1. **shared db,**
2. **multiple writers,**
3. **mistrust,**
4. **disintermediation,**
5. **interdependent transactions,**
6. **set rules,**
7. **validators,**
8. **asset backing**

1st out of 8 conditions to avoid pointless blockchain projects: Blockchains are a technology for shared databases, do you need one?!

2nd out of 8 conditions to avoid pointless blockchain projects: there needs to be more than one entity which is generating the transactions that modify the database. Do you know who these writers are?

3rd out of 8 conditions to avoid pointless blockchain projects: there also needs to be some degree of mistrust between those entities; it can also exist within a single large organization, for example between departments or the operations in different countries.

4th out of 8 conditions to avoid pointless blockchain projects: disintermediation, is there any good reason to take away (the service of) a middleman?!

5th out of 8 conditions to avoid pointless blockchain projects: Blockchains truly shine where there is some interaction between the transactions created by these writers. Interdependencies wanted!

6th out of 8 conditions to avoid pointless blockchain projects: This isn't really a condition, but rather an inevitable consequence of the first 5 points: the database must contain embedded rules restricting the transactions performed.

7th out of 8 conditions to avoid pointless blockchain projects: a blockchain's job is to be the authoritative final transaction log, on whose contents all validators provably agree, do you know them and trust them?

8th out of 8 conditions to avoid pointless blockchain projects: Is there anyone standing behind the assets represented on the blockchain? If the database says that I own 10 units of something, who will allow me to claim those 10 units in the real world?

Pamela Morgan quotes

- ‘my failure to implement good security wasn’t totally my fault; it was a **combination of misunderstanding the risks, overestimating the effort it takes to implement’**
- ‘I had heard about people **getting hacked**. But it was **always other people’**
- **‘the risk wasn’t real enough for me to do anything about it’**
- **‘**the real danger is that when your credentials are stolen **your life can be disrupted in a major way’**
- **‘**Maybe you’re like I used to be: **simply unsure of what to do — so you do nothing’**

- LINK TO ARTICLE

Pamela Morgan quotes

- **‘Basic good security practices** are now part of my **routine** without even noticing. **Like putting on a seatbelt** after getting into a vehicle, it’s just something I do**.’**

- LINK TO ARTICLE

Famous bugs in contracts for Ethereum

- DAO, June 17 2016
- KING OF THE ETHER THRONE, RUBIXI, GOVERNMENTAL SMART CONTRACTS
- HACKERGOLD BUG, Jan 4 2017
- BITHUMB, June 29 2017
- CLASSIC ETHER WALLET, June 30 2017
- AUGUR REP TOKEN, July 13 2017 - whole REP economy at risk
- COINDASH, July 17 2017 - 34,5K ETH stolen
- PARITY, July 19 2017 - over 150,000 ETH stolen
- SATHOSHI PIE - July 23 2017, $ 7M stolen
- VERITASEUM - July 23 2017 $8.5M stolen

From: https://applicature.com/blog/history-of-ethereum-security-vulnerabilities-hacks-and-their-fixes#comment-719

https://applicature.com/blog/history-of-ethereum-security-vulnerabilities-hacks-and-their-fixes#comment-719

Dank je wel!

@henkvancann

License

This work is licensed under a Creative Commons Attribution-Share Alike 4.0 license

https://creativecommons.org/licenses/by-sa/4.0/

Fundamentele kennis is jouw pad naar professionalisering