VITAS

DATA, het nieuwe ~~goud~~, *GIF*

Erich Schnoeckel

7 mei 2018

Welkom bij de bron.

Even voorstellen

- Erich Schnoeckel - VITAS Blockchain
  - 3Thin.gs Blockchain Consultancy

- > 25 jaar ervaring op het raakvlak van IT en Finance
- Start-ups, EY, Exact
- Laatste 4 jaar betrokken bij Blockchain projecten

- Amsterdam, 4 kids, hockey

Agenda

- Blockchain in het kort
- Terminologie
- Historie en ontwikkeling
- AVG
- Q&A

I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
E-mail: SCOTTADAMS@AOL.COM
S. Adams
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
© 1995 United Feature Syndicate, Inc.(NYC)
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.

TERMINOLOGIE

#FOMO

#FUD

#HODL

#DAICO

#FORK

TERMINOLOGIE

#CRUD

#CRAB

#KYC

#IPFS

#Zero Knowledge Proof

VITAS

BLOCKCHAIN

May 2009	Publication of “Bitcoin – a peer to peer electronic cash system” by Satoshi Nakamoto
1982	Publication of “Secure Digital Cash” by David Chaum
1990	Foundation of “DigiCash” First digital money company
December 2005	Publication of “Triple Entry Accounting “ by Ian Grigg

VITAS

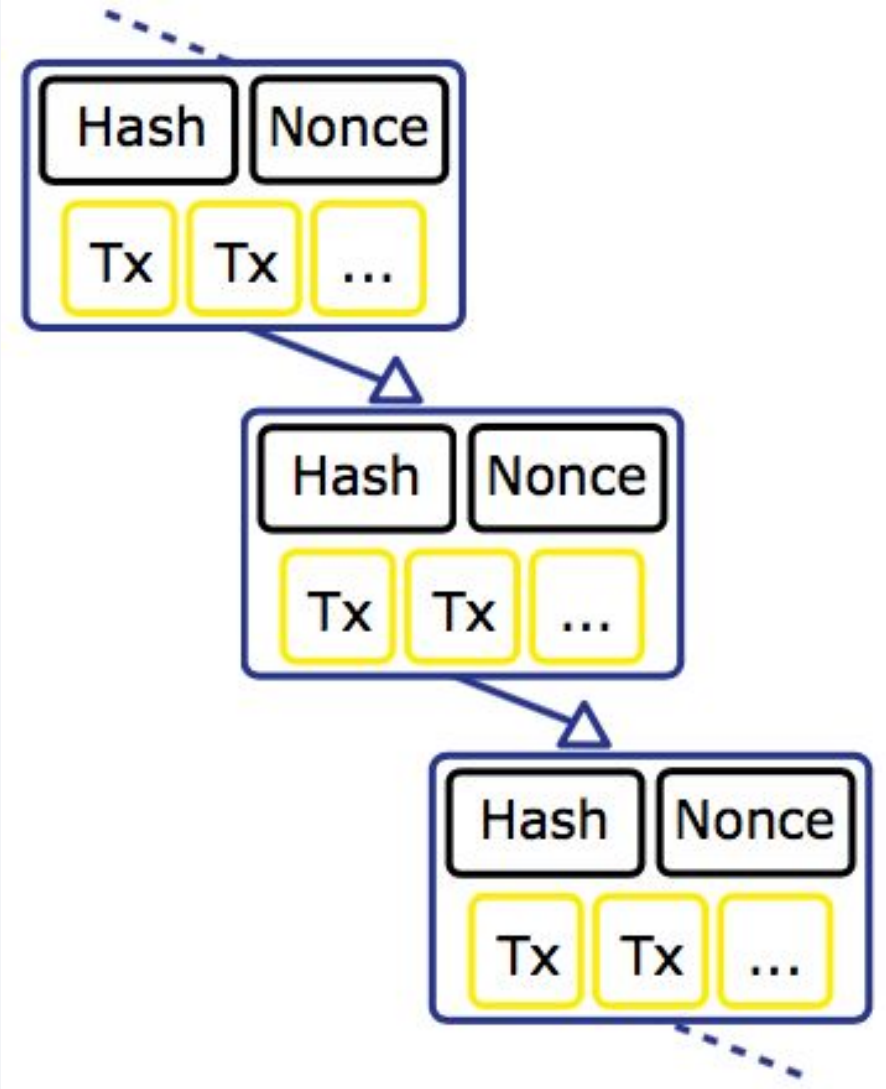
WHAT IS BLOCKCHAIN TECHNOLOGY?

“ We should think about the blockchain as another class of thing like the Internet – a comprehensive information technology with tiered technical levels and multiple classes of applications for any form of asset registry, inventory, and exchange, including every area of **finance, economics**, and **money**; **hard assets** (physical property); and **intangible assets** (votes, ideas, reputation, intention, health data, information, etc.). In fact the blockchain concept is even more, it is a new organizing paradigm. ”

– Melanie Swan, Founder, Institute for Blockchain Studies

DATA STRUCTURE

- Een keten van blokken
- Elk blok bevat:
  Een of meer transacties
  Een hash van het voorgaande blok
  (optioneel) een nonce
- Een niet te manipuleren of te wijzigen data structuur



TYPES OF BLOCKCHAIN

- Proof of Work
- Proof of Stake
- Proof of Authority

- Public Blockchains
- Permissioned Blockchains / Consortium Chains

CRYPTO CURRENCIES

- Wat is een crypto currency?
- Waarvoor wordt het gebruikt?
- Welke voorbeelden zijn er?

DIGITAL ASSETS

- Wat is een ICO / ITO
- Wat koop ik dan?
- Hoe gebruik ik het?
- Wat is het waard?

SMART CONTRACTS

- Stukjes code die automatisch in gang gezet worden
- Worden gepubliceerd in de Blockchain
- Zijn moeilijk aan te passen en te verwijderen

```
pragma solidity ^0.4.8;
contract financingApplication{

    enum states { open, goods_sent, goods_received,
                    audit_request_sent, audit_request_received,
                    ...
                    finance_request_received, financing_approved}
    address public seller, LSP, Auditor, FSP, buyer;
    contractState public zorgState;

    //modifiers to control invokation rights
    modifier restrictedToLSP() { if (msg.sender == seller) _; }
    modifier restrictedToLSP() { if (msg.sender == LSP) _; }
    modifier restrictedToAuditor() { if (msg.sender == Auditor) _; }

    //constructor
    function financingApplication() { seller = msg.sender; }

    //functions to change state of contract
    function sendGoods restrictedToSeller(address _LSP){
        LSP = _LSP;
        contractState = states.goods_sent;
    }

    function receiveGoods restrictedToLSP (){ contractState = states.goods_received; }

    function sendAuditRequest restrictedToSeller(address _Auditor){
        Auditor = _Auditor;
        contractState = states.audit_request_sent;
    }

    function receiveAuditRequest restrictedToAuditor(){ contractState = states.audit_request_received; }

}
```

VITAS

The DAO Attacked: Code Issu
$60 Million Ether Theft

Jun 17, 2016 at 14:00 UTC by Michael del Castillo

Ethereum • News • Ethereum

in 466

The DAO, the distributed autonomous organization that had collected over
ether, has reportedly been hacked, sparking a broad market sell-off.

A leaderless organization comprised of a series of smart contracts written
DAO has lost 3.6m ether, which is currently sitting in a separate wallet afte
grou

The DAO Falls Victim to Cyber Attack Leading Ethereum to Crash Over 20%

The event is still ongoing as hackers have already stolen over 3.5 million ETH from the DAO's coffers.

Avi Mizrahi | Trading (CryptoCurrency) | Friday, 17/06/2016|12:45 GMT

CNBC

Search Quotes, N

CYBERSECURITY

Security

Parity: The bug that put $169m of Ethereum on ice? Yeah, it was on the todo list for months

Just didn't get round to fixing it – our bad

version 1.5 or later of its wallet software.

So far, 150,000 ethers, worth $30 million (£23 million), have been reported by the company as stolen, data confirmed by Etherscan.io.

www.jamesedition.com

Smart contract coding company Parity yesten
issued a security alert, warning of a vulnerabi
in version 1.5 or later of its wallet software.

Unprivileged write to storage

Any user may change the wallet's owner

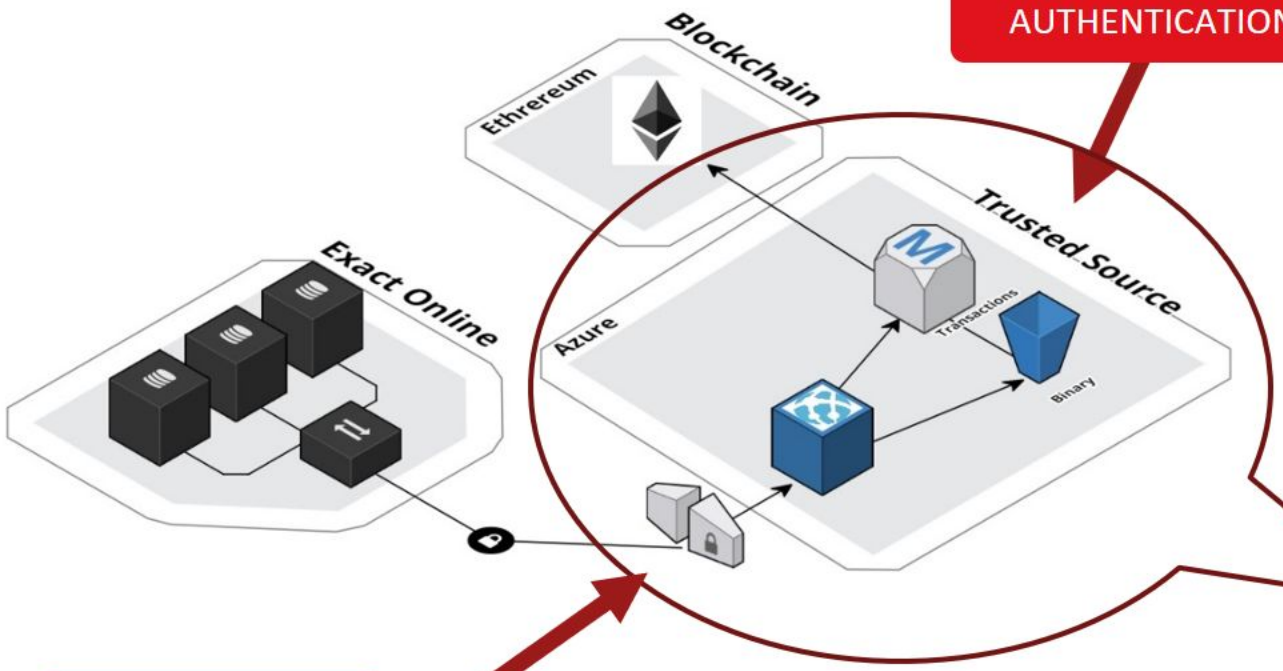
Wallet Contract

```
address owner = ...;

function initWallet(address _owner) {
  owner = _owner;
}

function withdraw(uint amount) {
  if (msg.sender == owner) {
    owner.transfer(amount);
  }
}
```

Only owner can send ether

+ (☞)

AUTHENTICATION



ERP AGNOSTIC
API LAYER

FOUNDATION

© 2017 EXACT

= exact

RESULTS

- Proof of ownership
- Payment reputation
- Quality of goods
- Location of goods
- Quality of delivery, terms
- Etc.

- Minder risico
- Sneller en makkelijker lenen
- Tegen lagere rente?

IMPACT

- De veranderende rol van de “middle man”
  - Notaris, Accountant, Bankier
  - Douane, Controleurs
- Zelfbeschikking over uw eigen data
  - LinkedIn, Facebook, Uber, Google
  - GDPR
- Transparantie, Betrouwbaarheid
  - Consensus mechanisme

BLOCKCHAIN en de AVG

- Persoonlijke data
  - Toestemming en het intrekken van deze toestemming
  - Inzicht in gebruik, doel moet vastgesteld worden
  - De mogelijkheid om vergeten te worden
  - De mogelijkheid om de data in een transporteerbaar formaat mee te nemen

BLOCKCHAIN en de AVG

- Systemen moeten ontwikkeld worden op basis van
  - Privacy by design
  - Best effort you can do
- De combinatie van geslacht, leeftijd en postcode is voldoende om 87% van de bevolking persoonlijk te identificeren (Carnegy Mellon, 2000)

VITAS

ALGEMENE
VERORDENING
GEGEVENSBESCHERMING

BLOCKCHAIN en de AVG

- Dataverwerker (Data processor)
- Data controller
- Verwerkers overeenkomst
- Data lekken

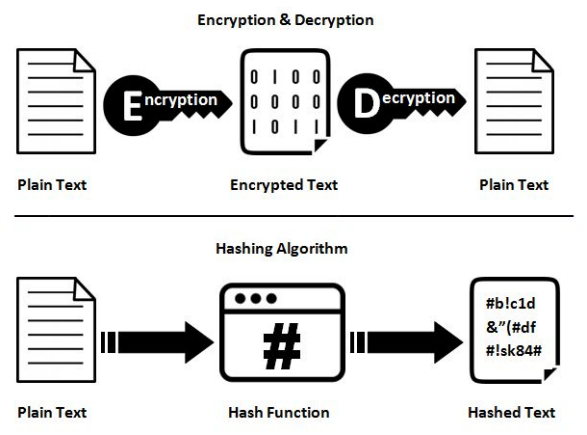
BLOCKCHAIN en de AVG

- Data Controller
- natuurlijk persoon, bedrijf of andere organisatie die alleen of met anderen het doel en nut van het verwerken van persoonlijke data bepaald

VITAS

BLOCKCHAIN en de AVG

- Dataverwerker (Data processor)
- Beheert en verwerkt de data in opdracht van de data controller
  - Iedereen die over de data beschikt
  - Elke miner (PoW), block producer (PoA)
  -



BLOCKCHAIN en de AVG

- Data op een Blockchain
  - Zijn hashes terug te herleiden naar persoonlijke data?
  - Is encrypted data terug te herleiden naar persoonlijke data?
  - Is pseudonieme data terug te herleiden naar persoonlijke data?
  - Van wie is de data eigenlijk?

BLOCKCHAIN en de AVG

- Datastores
  - Azure data stores
  - Hyperledger
  - BigChainDB en de CRAB methodiek
  - IPFS
  - …
- Forked Blockchains

BLOCKCHAIN en de AVG

- Datalekken
  - Data lekken kunnen dus op veel plaatsen ontstaan
  - Wie is er verantwoordelijk?
- Wie te benaderen als je vergeten wil worden?
- Hoe wordt er met data omgegaan als deze het doel niet meer dient?
- Waar ga ik heen voor mijn inzage recht?

VITAS

BLOCKCHAIN en de AVG - Use Case

BCDiploma
Degrees certified on the blockchain

- BCDiploma
  - een Ethereum gebaseerd systeem voor het opslaan van diploma’s
- 3 weg beveiliging
  - Graduate key - onderdeel van het diploma en eigendom van de geslaagde
  - Persistent key - eigendom van de onderwijsinstelling en als de geslaagde vergeten wil worden hoeft alleen deze key vernietigd te worden
  - Permanent key - beheerd door de onderwijsinstelling en kan alleen gebruikt worden na toestemming van de geslaagde

BLOCKCHAIN en de AVG

- Handhavingswet aangenomen op 13 maart
- Voorlopig geen harde handhaving
- Hulp in plaats van boete
- Aantoonbare progressie en medewerking
- Argos uitzending “Badmeester wat weet u van mij?”

TIMELINES

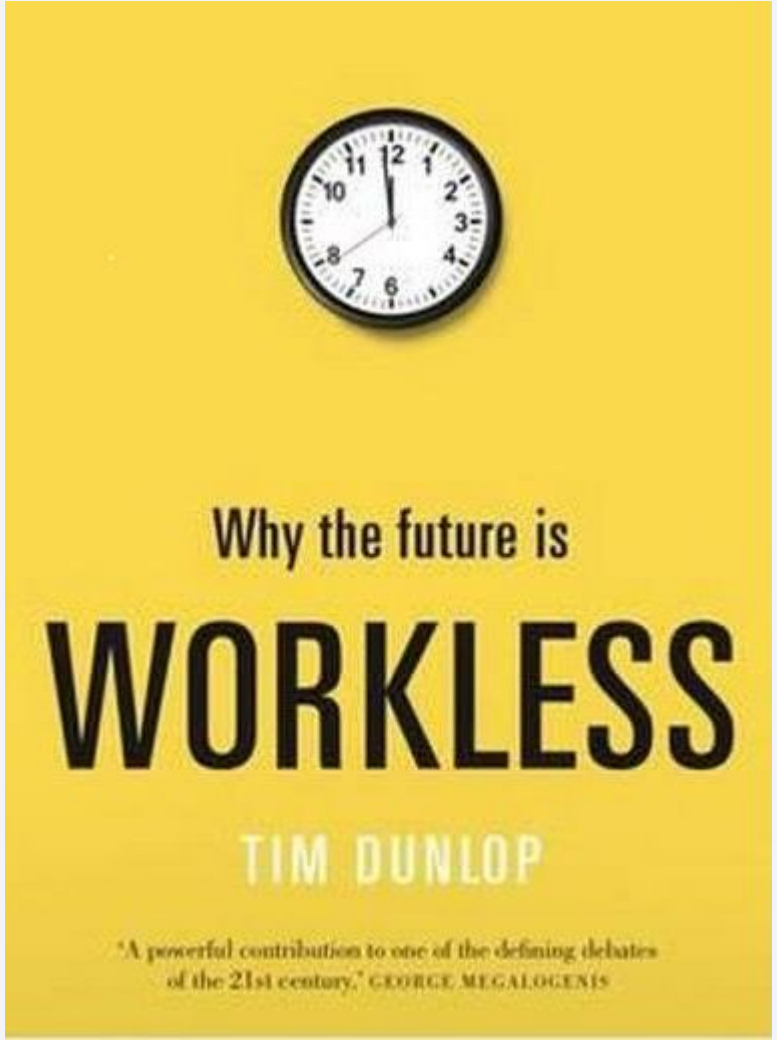
2016 was het jaar van de “ontdekking” door veel organisaties

2017 het jaar van de Proof of Concepts

2018 het jaar van de eerste succesvolle Use Cases

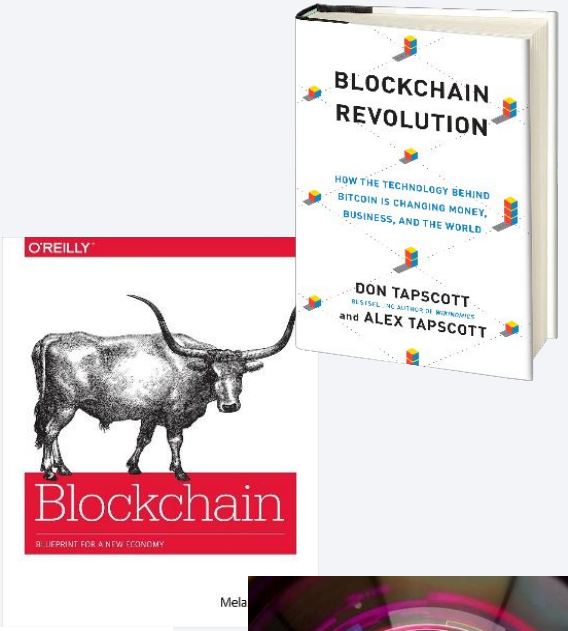
2019 Productierijpe Blockchain applicaties

VITAS


Why the future is
WORKLESS
TIM DUNLOP
'A powerful contribution to one of the defining debates of the 21st century.' GEORGE MEGALOGENIS

Knowledge & Resources

- Must read
  - Melanie Swan
  - Don Tapscott
- Websites
  - www.coinmarketcap.com
  - www.cointelegraph.com
- Exchanges
  - www.poloniex.com
  - www.cex.io
  - www.btc.com



Q&A

Erich Schnoeckel
ESchnoeckel@VITAS.nl

+31 634 227.307

Welkom bij de bron.