The easiest way to understand blockchain and its applications

Published on January 12, 2017

Nanning de Jong | Follow
Managing Consultant at Berenschot | 3D printing | Blockchain | …

A framework for understanding blockchain: the context and four basic principles

To me 2016 was in many ways the year of blockchain, and of developing concepts for blockchain business applications. You've probably heard a lot about blockchain in the media, and you might be aware that the technology and its applications are not (yet) easy to understand. As Arno Laeven, former head of Philips Blockchain Lab, says: "It's a subject you need to *study* and that takes time." This is something I learned while working at Tymlez, a blockchain start-up and doing workshops and pilots with law firms, notaries, banking, insurance, ICT companies and governments.

I noticed that when I introduce blockchain to people in the way which follows, they can reproduce it and use it as a framework for application brainstorms. Notice that it's a simplification of the technology and algorithms. Let me know if it helps you understand the basics!

Context: blockchain is an automation technology

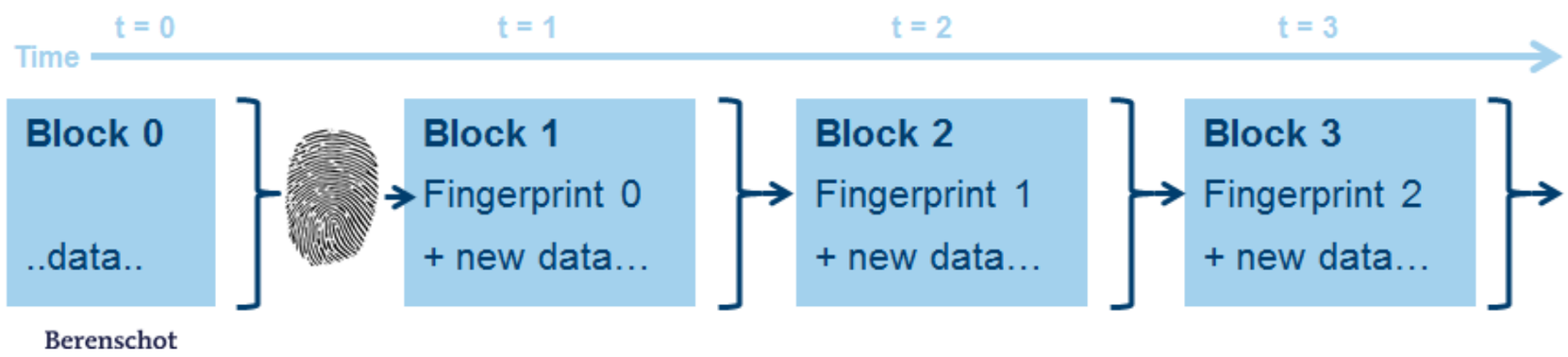
Blockchain is an automation technology, just like many previous automation technologies: from mainframes to server-clients, peer-to-peer and cloud automation. They were developed in different eras with different hardware and different applications in mind. And they still co-exist in many enterprises and governments. Mainframes and their 1970s-based programming code are still used by major banks and governments for example. Blockchain is the new 'kid on the block' in this differentiated IT landscape. So what does blockchain have that all the other automation technologies don't?

First some history. The first Blockchain application was the Bitcoin digital currency in 2009 – an invention that could impact banking significantly. With Bitcoin it's as easy and cheap to transfer money across borders as it's easy and cheap to send an e-mail across borders. Many alternative digital currencies have since been developed, such as Litecoin and Monero. But in 2015 a second generation of blockchains came to the market, with Ethereum as the major player. This added many more functionalities to the technology, impacting on many more sectors outside banking, and giving rise to a whole

new range of applications for businesses and governments. I'll explain four basic principles in the next sections.

Blockchain principle 1: creating an unchangeable chain of data blocks over time

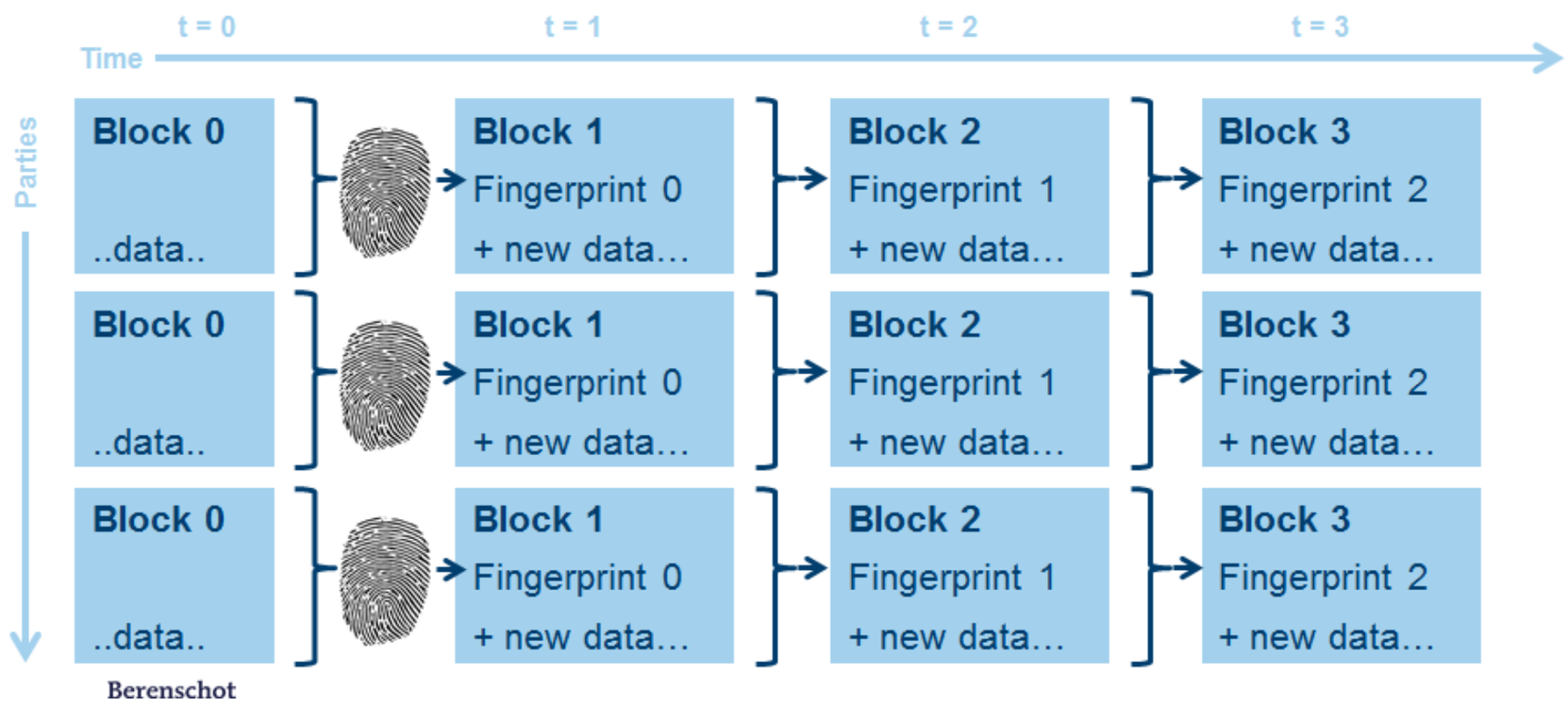
First, a blockchain stores data in a new way by interconnecting every written data block with cryptographic methods. In theory the data can contain anything, from transaction data to documents and even video. However in most blockchain designs, the smaller the package, the better. A 'hash' is a 25-year-old cryptographic algorithm to make a 'fingerprint' of a digital file (or a block), so that the file can be identified uniquely. If a single digit is changed in the file, the new hash will not match that of the original file. Hashes create the interconnecting proof in a blockchain, that all the data in the blocks is authentic and has not been tampered with. The hash of a data block is stored in the following block, which interconnects all blocks and forms the chain over time, as shown in the diagram below.



Why does this matter? This functionality creates an **audit trail** of the stored data for instance. Who stored what data is transparent and proves that it's authentic and was not manipulated. This is important for applications in organisations **where data trustworthiness is valuable**, such as accountancy, pharmaceutical compliance, (financial) regulatory compliance, notaries and law.

Blockchain principle 2: the chain is distributed to all participating parties

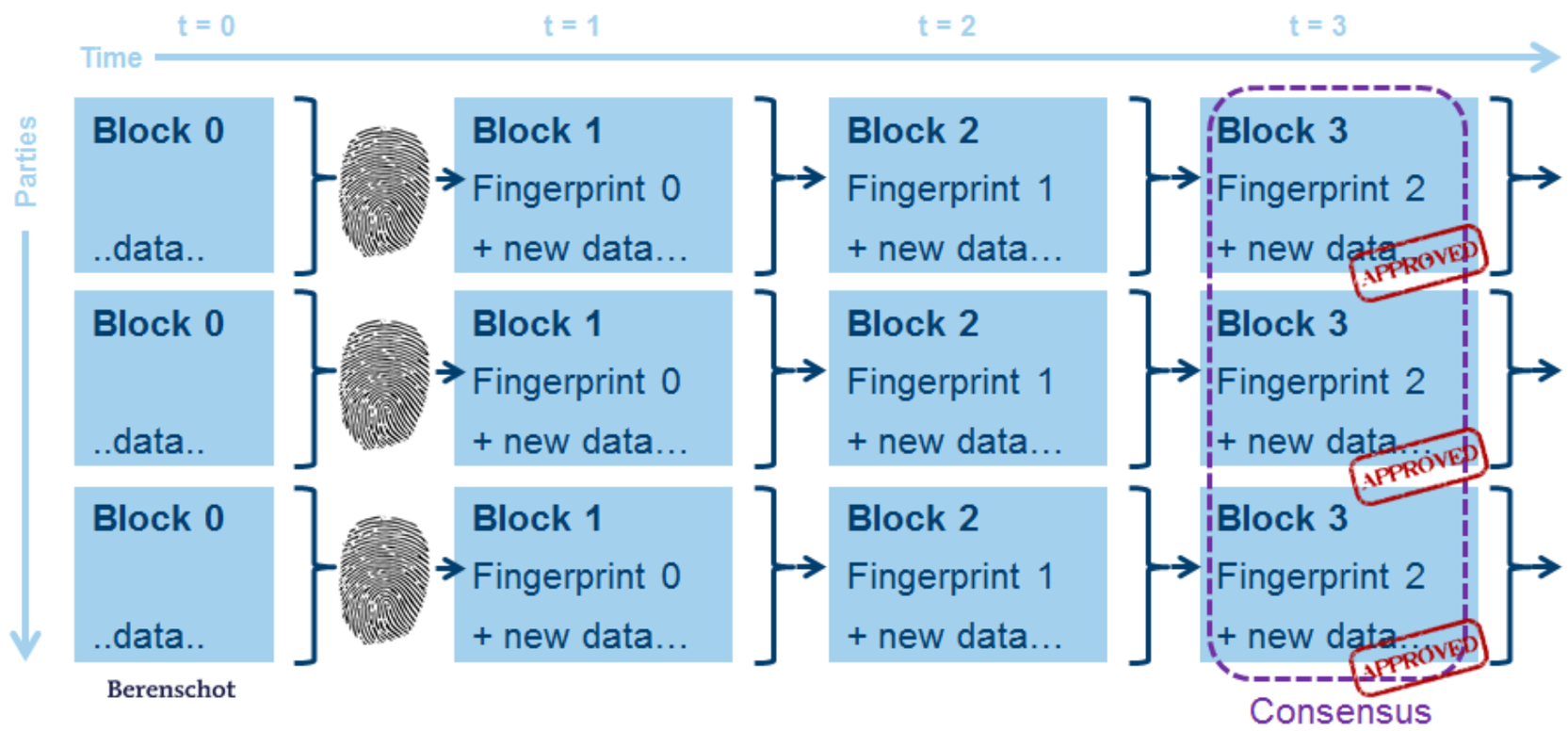
Second, the growing chain from the first principle can still be stored and used by one party. What makes blockchain extra-reliable is that this complete chain is shared with and **distributed** to other parties (e.g. computer nodes). All parties can get an exact copy of all data and its interconnecting proof, and can check that these copies remain identical (synchronised). Now it becomes even harder to tamper with data.



The interesting part is the absence of a powerful central party – there is no trusted third party, like a bank, which controls everything. Based on the design and set-up of a blockchain, it can be *public* to anyone who wants to join (like the internet), or *private* to a certain group of parties (like an *intra*net) or a *hybrid* with more differentiated read/write access rights. These functionalities create new opportunities for people and organisations working together. Consider for instance developing applications for co-creation platforms, facilitating cooperating in consortia, and automating processes with many different stakeholders, like government institutions or supply chains. With proper access rights and data encryption, blockchains could also become a system for Electronic Patient Records and legal records.

Blockchain principle 3: the parties must reach consensus on what data is stored in the latest block

Third, the hard part of this distributed network is to reach **consensus** on what data the latest block should contain. There are several automated approaches for this decision: the Bitcoin network uses cryptographic algorithms to decide with ‘proof of work’ (e.g. mining), but other systems use voting mechanisms and ‘proof of stake’. These approaches differ in security levels and speed, and can be designed and set-up for different blockchains for specific use-cases and applications. In all cases consensus is prevented if the group of parties (nodes) do not reach agreement on the data (and hashes) that the latest block should contain.



Why does this matter? The consensus mechanism keeps the blockchain instances synchronised and trustworthy so that all parties can work with a ‘single source of truth’. This was originally designed for Bitcoin to prevent the ‘double-spending’ problem. For the first time it could be proved (without a trusted third party) that the same digital coin could not be spent fraudulently multiple times. This is important for proving the ownership and transactions of all digital goods, like digital currencies, digital pictures etc. Another benefit of a ‘single source of truth’ is that it increases the quality of data for organisations. Large organisations like governments, banks and supply chains often handover data between departments or organisations in batches and enrich the data along the way. In the end all departments and organisations have slightly different data to work with, which can be troublesome and costly to repair.

Blockchain principle 4: programming code can be stored and executed in blockchains (smart contracts / decentralised apps)

Fourth, the data in a blockchain can contain logic, business rules and **programming code**, which is synchronised and secured between all parties and can be **executed** in a decentralised way. This is the most innovative and least understood feature of blockchains. It was first applied as ‘smart contracts’ in the Bitcoin network, where transactions of coins could be made conditional with ‘if-this-then-that’ statements. For instance, an insurance service could be set up where the transfer of digital coins is conditional on specific weather (like hail) at a location or conditional on the delay of an airline flight (InsurETH), and which could have this ‘smart contract’ executed automatically without a central ‘insurance company’. This matters as the execution does not depend on a central server and is therefore more robust. Second-generation blockchains, like Ethereum, expanded the functionality of ‘smart contracts’ and now almost any programmable code can be stored and be executed in a decentralised way. I prefer to call this ‘decentralised apps’ (dapps), because this feature could be far-reaching and the word ‘contract’ could limit our creative thinking on new applications. In 2016 we saw the first rise and fall of the first Decentralized Autonomous Organisation, or DAO in short, built on this second-generation technology. It’s a crowdfunding and investment organisation run without employees or a central authority. I’m looking

forward immensely to seeing the dapp functionality explored and implemented more in the years ahead.

Looking forward to blockchain implementations in existing organisations and consortia

So to conclude, a blockchain is a new automation technology, which adds four new principles:

1. **storing** data in a growing and interconnecting chain of blocks;
2. **distributing** this chain of data blocks to many parties in a network;
3. **consensus** on which data the last block should contain;
4. **executing** programming code in a distributed network.

This matters for all applications where the quality and trustworthiness of data is essential and/or where it is desired that the automation does not rely on one trusted third party. The applications started with ownership transactions, like payments, real estate, art and other valuables, but we are going to see many other (decentralised) applications in the years ahead, from government processes, audit-trails and electronic patient records to new supply chains and manufacturing.

After years of pilot projects and experiments, I hope we are going to see and work on many real implementations of blockchains in existing organisations and consortia this year. At Berenschot we will also be developing and implementing a blockchain application for our management consulting services. An exciting start to 2017!

Puck Bulthuis ··· 13h
eigenaar Puck Bulthuis Consultancy

Dag Nanning, helder geschreven zelf voor een leek, zoals ik! Ken jij toepassing in de zorg voor kwetsbare mensen! Zo niet , welke mogelijkheden zie je om de toepassing te organiseren op indivudueel en ziektebeeld niveau?

Like Reply

Owe Dantuma ··· 1d
Business Owner at Kea Proserv BV

Best explanation I ever read. To-the-point, comprehensive, good graphics. Top!

Like Reply | 1

Cindy Taphoorn ··· 1d
Senior Relationship Manager Sales Solutions Benelux at LinkedIn

Thanks Nanning I believe for the first time I really get the principle

Like Reply | 1

Klaartje Vreeken ··· 1d
Helpt organisaties te innoveren met ondernemers

Bedankt Nanning! Yvonne Haneman!

Like Reply | 1

Eva Carlsson ··· 2d
Project and Quality Manager, FiloProcess

Thanks for the clear explanation!

Like Reply | 1

Tineke Muller ··· 2d
Coordination business relations RDM Rotterdam-Centre of Expertise

Thxs for sharing.

Like Reply | 1

Arthur Nodelijk ··· 2d
Consultant | Coach | (Interim)manager | Eigenaar bij Arthur Nodelijk Volmachtsupport

Nanning thank you for this nice overview!

Like Reply | 1

Patrick van Oirschot ··· 2d
Partner at GPP Support & Co-founder at Cure-Box

This makes many things clear!

Like Reply | 5

Top stories from Editors Picks

There are better governments than America's — it's time to learn from them

Parag Khanna on LinkedIn

Brett King on how China, Kenya and technology are disrupting financial services

Walden Siew on LinkedIn

Understanding the new phase of globalisation

Robert E. Moritz on LinkedIn

Looking for more of the latest headlines on LinkedIn?

Discover more stories