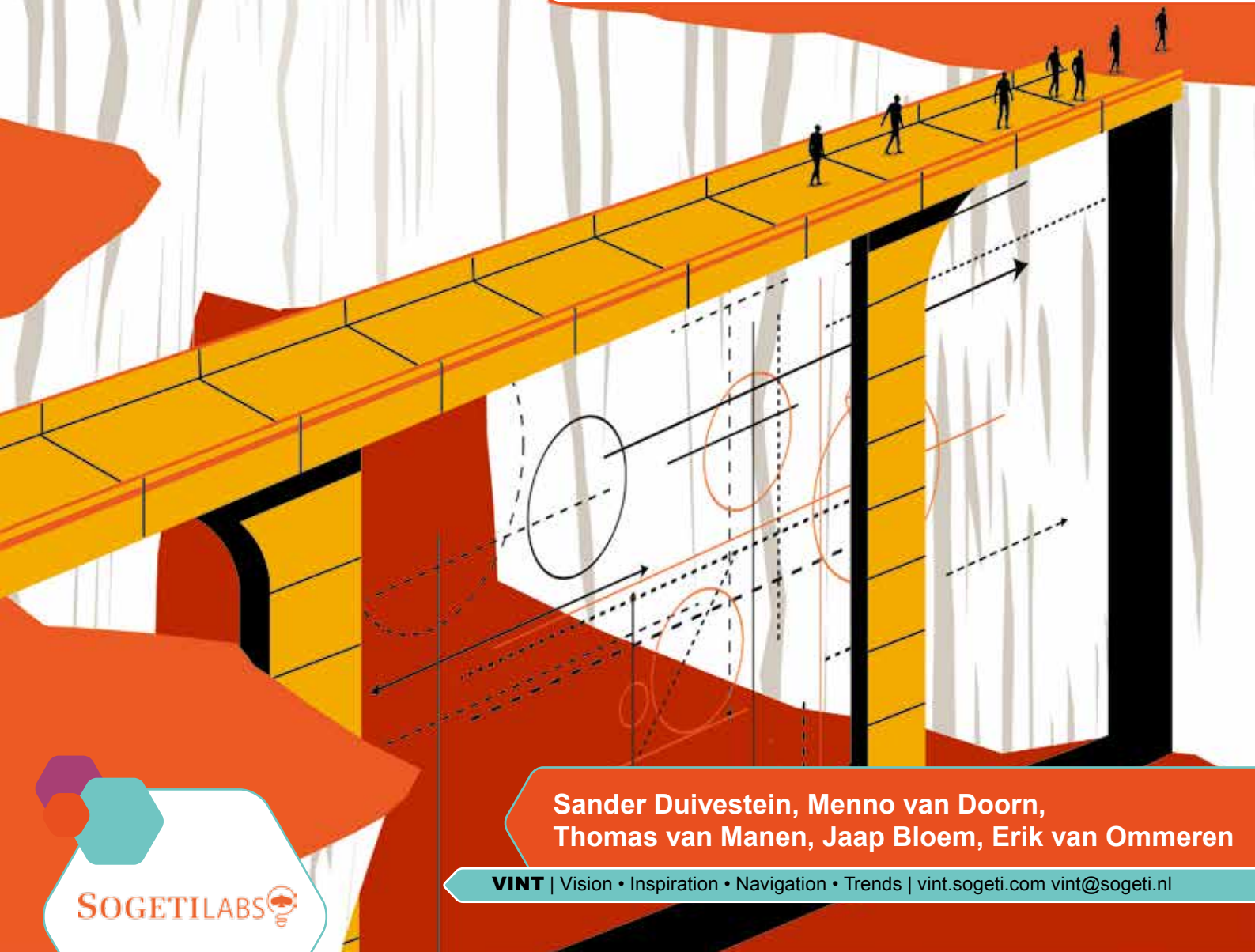
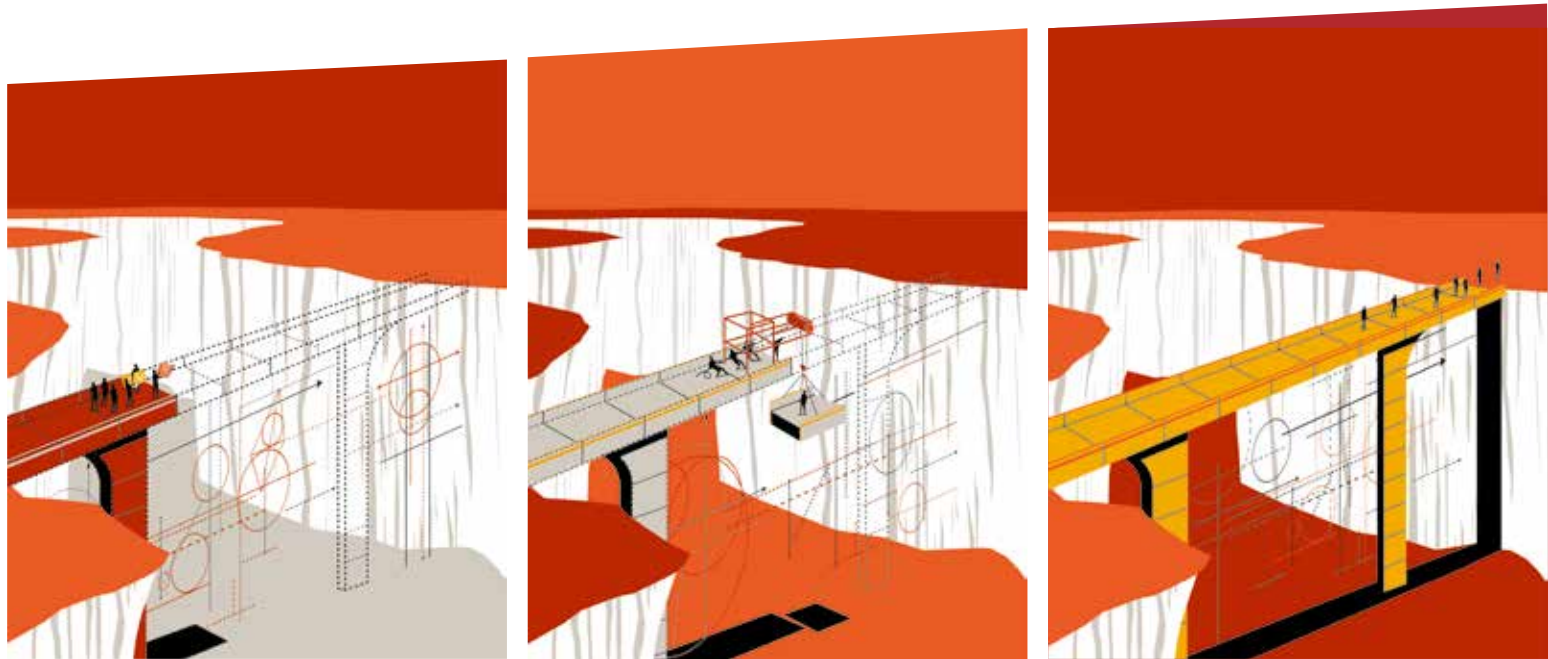


Blockchain: cryptoplatform for a frictionless economy

Design to Disrupt Report 3 of 4



Sander Duivestein, Menno van Doorn,
Thomas van Manen, Jaap Bloem, Erik van Ommeren



CONTENTS

Design to Disrupt 3

Introduction: a new basis for trust 4

Structure of this report: three versions of the
crypto-economy 6

Chapter 1 Crypto-economy 1.0 – the currency 7

Sowing in fertile soil 7

Introduction to cryptocurrency 7

What is a bitcoin and what is a blockchain? 8

Are there any other currencies than the bitcoin? 8

How does Bitcoin work? 8

How are bitcoins made? 10

Precluding fraudulent transactions with the help of a
crypto-puzzle 11

Shared single source of truth 11

The seven pros and cons of Bitcoin 12

Who will? A Bitcoin Governance Framework 16

**Chapter 2 Crypto-economy 2.0 – smart contracts
and things 17**

A new protocol 18

The Blockchain Application Stack 18

Bitcoin and the Internet of Things 22

Device Democracy 24

Smart contracts 24

Smart ownership rights 26

Chapter 3 Crypto-economy 3.0 – the Robocorps 27

Tradenet 27

Robocorps, DAOs and DACs 28

Taxis, government, employment agencies 29

Decentralized Autonomous Governments 29

Virtual reality and the blockchain 30

In conclusion: the new organization paradigm 30

The future is decentralized 30

**Wrap-up: conclusion and considerations for
business executives 31**

Glossary 34

Literature 36



DESIGN TO DISRUPT

“Disruption is the New Normal.” This is the key message from the executive introduction to this series of reports. In the first report we outlined the exponential growth of digital opportunities. Start-ups are keen to fill the gap, challenging the establishment. At the same time the speed with which innovations prove to be successful is increasing. This expansion is set off by the slow reaction of organizations that are unable to keep pace with the digital tidal wave. This phenomenon, also known as Eroom’s Law (Moore’s Law, spelled backwards), is beginning to dawn on more and more organizations.

In the second report, “Design to Disrupt: New digital competition,” the challengers were central. Few established organizations wise up to them at an early stage, as they usually come from outside these organizations’ industries and are not taken seriously at first. Their allegedly inferior propositions confuse prominent players, who should in fact be the very first to be open to disruptive innovation. This innovator’s dilemma brings us back to the major question of this Design to Disrupt project: how can you, as an organization, design your own disruptive market possibilities?

This third report is devoted to an entirely new design principle. It outlines the potential impact of blockchain, a new way of organizing trust in the presence of unreliable parties. It owes its current fame to the currency, the bitcoin, in particular, but the cryptographic capacities of the network can be deployed in a variety of other ways. It is a special kind of platform, which in its turn is a basis for numerous other platforms – in other words, a platform for platforms. We outline its relevance for organizations in three steps: the crypto-economy 1.0, 2.0 and 3.0.

“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. In fact it is even more, the blockchain concept is a new organizing paradigm.”

Melanie Swan, Institute for Blockchain Studies

INTRODUCTION: A NEW BASIS FOR TRUST

Welcome to the wondrous world of the complex and highly imaginative crypto-economy. The world of blockchain and bitcoin, of miners, sandboxes and hashes. If you are not familiar with this subject yet, you may easily fall under the spell of the fascinating and fast-growing crypto-environments. And even if you have already made a study of the subject, some elements of the crypto-economy may remain mysterious and to some extent intangible.

“The first five times you think you understand it, you don’t”

Dan Kaminsky,
American Security Researcher



This joke aims to alert you to the serious stuff we are going to dish up. Sometimes the effect of the blockchain as well as its possibilities can be a hard nut to crack. Our advice is: read, scroll back and reread, and consult sources that we refer to. Even if it fascinates you and you might consider your own form of innovation, always keep switching between effect and possibilities. As mentioned, both will be dealt with in this report.

The digital notary

Just imagine that with every transaction that you execute on the internet a notary should look over your shoulder to make sure that nothing is wrong. That would be a very costly affair indeed. But it is an entirely different matter if it could be computerized. What you have then, basically, is a possibility to do frictionless business, as the control is already embedded in the transaction. This may well be the key to lots of new possibilities. Such a system exists. It is called blockchain, a strong chain without weak links offering a solution to numerous actual problems within the digital economy. In this report we outline the new possibilities.

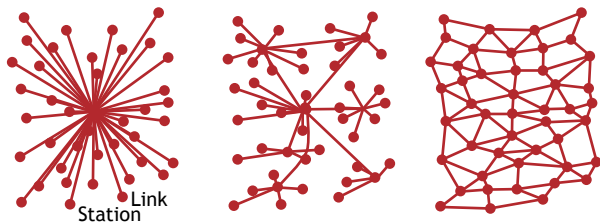
The weakest link

Until now, banks, institutions, supervisors and notaries – “trusted third parties” – have monitored the transactions. Part of their work is done by computer and part is still done by hand. The procedure is very complex and if something goes wrong, one of the parties takes action. The guarantee on the part of a bank or credit card company ensures that we trust the system. In addition, extra services such as an insurance of goods paid for with your Visa card, remove restricting factors when executing transactions.

Without these trusted parties the friction in commerce would be too strong to get things done properly. What’s more, the economy would not amount to anything much, and barter trade – one cow for three pigs – would be the norm. But still things go wrong, or we have to wait long for checks and audits to take place, or the service is not up to the usual standard for the simple reason that we are dependent on these parties. Apart from this we should realize that there is a price tag on the trusted-third-party construction: notaries, banks and brokers do not exactly do their work free of charge. However, the alternative – the blockchain – enables you to make a direct transfer of 100 million euros to America on a Sunday afternoon, safely and without transaction fees. Try accomplishing that at your own bank.

The strongest link

Originally these trusted third parties were not “designed for the internet.” Meanwhile, they can be contacted digitally, but usually this is done by building interfaces on top of the existent legacy systems. The internet itself has an entirely different design principle: decentralized, distributed, with no specific owner. We are confident that emails arrive, that we can update our Facebook page or make a Skype call, simply because the internet exists. Next to these trusted third parties there is a trusted web. Both must be able to function in order to allow the economy to run smoothly, but the design principles are different.



How to invest trust: centralized, decentralized or in a distributed network?

If the stronger link can replace the weaker links in the old system, the potential suddenly dawns on us. The fees can go down, things go faster and there is no longer a single point of failure. For if things go wrong, they go dramatically wrong. This is what we witnessed at Diginotar a few years ago, a Dutch certificate authority that had been founded by a group of trusted-third-party notaries. At the very moment when Dutch citizens were using it to make their tax declarations, Diginotar was burgled. The public keys that gave access to the tax returns had got about. The government abandoned their trust in Diginotar and the company went bankrupt.

The radical response to the fundamental lack of security of central authorities is a decentralized system, ownerless, open source, fully transparent and supported by advanced cryptography. These are some of the blockchain's attributes. In a study by MIT into a blockchain alternative for certificate authorities the blockchain turned out to be the winner (Conner, Velicanu & Yakubov, 2014).

BLOCKCHAIN

A public ledger that records all transactions and records them at the same time on computers in that network: this is the new supervisor, without the obvious weak link that is just asking to be targeted. Every transaction is checked with the help of cryptographic puzzles. The first computer that solves the puzzle – and thus verifies and approves the transaction – gets paid with newly created bitcoins. If 51 per cent of the computers in the network has verified and approved the transaction, it is entered in the ledger.

As everyone has an exact copy of this ledger, it is pretty hard to doctor the books because you need to control at least 51 per cent of the computing power of all the computers that protect the network. Bitcoin's computer network has far, far more computing power than the 500 fastest supercomputers taken together. Everyone can join in this network and receives expenses for the arithmetical work in proportion to the added computing power. This way, what we have now is a crowdfunded and crowd-owned public, transparent and safe system of transactions.

Blockchain: everybody's collective transactions in a ledger, distributed in a peer-to-peer network.

The image shows a page from an old ledger with multiple columns. The columns are labeled: DATE, FOR, BY, DEBIT, CREDIT, and BALANCE. The page contains handwritten entries in ink, including dates like '1791', '1792', and '1793', and various numerical values. The handwriting is cursive and somewhat faded, typical of historical documents.

HISTORICAL COMPARISON

We can draw an interesting parallel with the introduction of the double-entry bookkeeping of the thirteenth century. The first form of double-entry bookkeeping was said to be responsible for a boost of the economy, which was running more smoothly (cf. *Double Entry* by Jane Gleeson-White). We expect that the crypto variant will have a similar effect. But we see another potential parallel: in those days people did not really grasp the system and it was thwarted by the rulers, e.g., the Pope; much the same as what the present-day establishment is doing.

STRUCTURE OF THIS REPORT: THREE VERSIONS OF THE CRYPTO- ECONOMY

So far we have not discussed the currency, the bitcoin, but this is in fact what the blockchain owes its fame to. For the time being, bitcoin is the killer application of the blockchain. However, the trust in the bitcoin currency and that in the Bitcoin platform (the blockchain) need to be distinguished. The one trust depends on whether the money retains its value, or whether the police will follow up the matter if your bitcoins are stolen – that sort of thing. The other trust is about an infrastructure: whether the network can go down, the system can be hacked, or the speed of transactions can be guaranteed.

At the end of the day it is about the applications of the blockchain. If both the network and the applications are trusted, there is a new basis for monetary transactions. There is no lack of ideas for these new applications. Start-ups focus on building these new killer apps, proofs-of-concept are made public. Those applications range from money to smart contracts, and from smart things to autonomous organizations.

Crypto-economy 1.0

We aim to outline the potential impact of this new application in three steps. The first we have coined the *crypto-economy 1.0*. It concerns the currency, the bitcoin,

and financial transactions. It also provides a vital explanation of how the protocol operates. We list seven pros and cons of the bitcoin, dwell upon questions regarding the supervision of the system and wrap up with the official viewpoints of the financial authorities.

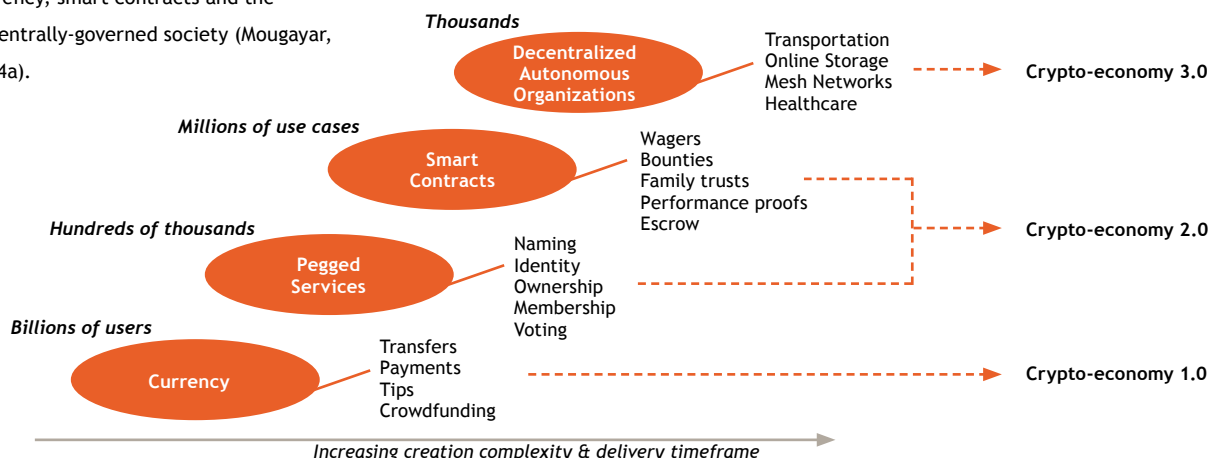
Crypto-economy 2.0

When outlining the *crypto-economy 2.0*, we go more deeply into the other possibilities of the blockchain, also called “bitcoin without bitcoin.” This concerns two kinds of applications in particular: smart contracts and smart products, and how the economy can be made to run more smoothly; or, in other words, how wasting can be stamped out.

Crypto-economy 3.0

If we let our imagination run wild, the final result is the *crypto-economy 3.0*. Here we describe the DACs (Decentralized Autonomous Corporations), also called Robo-corps. It is an Internet-of-Things scenario where objects are increasingly getting a free hand to make decisions and stimulate the economy: a potential forerunner of a zero marginal cost society. In such a case blockchain will be part of a collaborative commons, an advanced form of blockchain technology in society.

The crypto-economy in three steps: the currency, smart contracts and the decentrally-governed society (Mougayar, 2014a).



1 CRYPTO-ECONOMY 1.0 – THE CURRENCY

The Bank of England:

“It’s a significant innovation that could transform the financial system more generally.”

Goldman Sachs:

“Innovations in network technology and cryptography could change the speed and mechanics of moving money.”

Sowing in fertile soil


It is no surprise that the impact for the financial sector is always the first to come up for discussion, because there is ongoing speculation on disruption in that sector. Not in the last place, obviously, because what has been going on in the last few years. This year Joris Luyendijk, a Dutch anthropologist and journalist, published his bestseller *Dit kan niet waar zijn* (This Can’t Be True). He was asked by *The Guardian* to make an analysis of the financial sector. His conclusion, after hundreds of interviews, was that a completely different DNA is needed for a true solution to the problems. The blockchain might well be a part of that DNA: an alternative way of organizing trust, also with a view to the necessary transparency in a by now hypercomplex system. Nowhere has this been more clearly underscored, perhaps, than by a statement of Andrew Haldan, the second in command at the Bank of England, who in an interview with *Der Spiegel* said that the balance sheets of the major banks are still “the blackest of all black holes.”

Bill Gates once said “We need banking, we don’t need banks,” and this is food for thought for venture capitalists who aim to devise the “Uber for the financial sector”: a bank without branches and offices, like a taxi-control center without a control center. In 2012, investments in bitcoin technology amounted to 2.3 million dollars; in 2013 it was 95.81 million, in 2014 347.29 million and in the first two months of 2015 it was 105.84 million dollars. In 2013 another 200 bitcoin start-ups joined in, and in 2014 over 500. The currency, too, has a strong tailwind. According to figures of the US Federal Reserve Bank (Badev & Chen, 2014), the number of bitcoin users is doubled every eight months: an exponential growth curve. In October 2014, one of the best-known investors, Marc Andreessen, founder and maker of Netscape, said the following in an interview with Bloomberg:

“You don’t need 100,000 people, prime locations in Manhattan and huge data centers full of mainframe computers dating from the 70s to make an online payment. You wouldn’t structure a financial enterprise along the same lines nowadays. In my view the unbundling of banks is central.”

Introduction to cryptocurrency

Bitcoin is one of the first incarnations of a concept called “cryptocurrency,” which was described for the first time in 1998 by Wei Dai, on the Cypherpunks mailing list. Here an idea for a new currency was launched that uses cryptography instead of a central authority to administer the creation of money and transactions. In 2009 the first specification and proof-of-concept were published on a cryptography mailing list, by someone using the pseudonym Satoshi Nakamoto. Satoshi left the project by the end of 2010, without divulging many details about himself. Meanwhile, various searches have been undertaken to discover his identity, but to this day these have not resulted in the disclosure of the name of Bitcoin’s inventor. The fact that the network protocol and the accom-



panying software have been published under an open-source license makes the identity of the maker of minor importance.

By and large, this is what the picture looks like. Someone makes a request to transfer bitcoins. The miners pick up the request and start processing. Some ten minutes later the first confirmation is received and the transaction starts winning in confidence. After ten more minutes, when the second confirmation is received as well, the transaction is almost 100 per cent reliable. The approved transactions are added block-wise to the public ledger. This way a blockchain is created where all transactions can be read over.

What is a bitcoin and what is a blockchain?

Essentially, Bitcoin is a consensus network that enables a new payment system and a new form of digital money. It is the first decentralized, user-driven peer-to-peer payment network functioning without the intervention of a central authority or other intermediaries such as banks, notaries or insurers. Basically, a bitcoin is just a unique number. Bitcoins can easily be copied and printed, but once they have been spent their unique numbers are entered in the ledger and cannot be used again. The algorithms have been designed in such a way that a fixed number of new bitcoins is generated every day. Each day that number is decreasing slightly, so that by 2140 the maximum is reached. By that time the number of bitcoins is no longer growing, and there will be 21 million in circulation.

Are there any other currencies than the bitcoin?

The bitcoin is not the only cryptocurrency. Within a brief period of time it has been joined by many more alternative currencies, so-called altcoins. The website Map Of Coins keeps an eye on all these currencies. At the moment of writing there are 705 cryptocurrencies, and 45 of these were created within a month's time.

The interesting thing about these altcoins is that they facilitate a new monetary culture for a specific community. FitCoin, for example, enables its users to capitalize their health club visits. By means of all kinds of activity trackers and wearables the sports(wo)man's heart rate is measured and subsequently converted into digital currency. The founders of FitCoin hope that the currency can be used to buy exclusive articles from partners such as Adidas to reduce insurance premiums. Even banks are experimenting with their own altcoin. For example, Citibank is running a test platform for digital currencies and is pondering its own solution, CitiCoin.

How does Bitcoin work?

Before we go more deeply into how Bitcoin works, we first need to discuss the role of scarcity in an environment where plenty prevails: the internet. Here everything circulates at breakneck speed, is liked, forwarded or whatsappped. But in the case of money, contracts and currency trade, the main thing is that there are unique pieces to be identified. A summary of this process can be found on pages 20 and 21.

Imagine you are sitting on a bench and the person next to you gives you an apple. You thank him and take a bite. For you as well as the person next to you this is a simple ritual that requires no further explanation. This is rather different in the case of digital transactions, where, for example, someone sends you a picture of an apple.



It is not much of a problem for the owner to make a thousand copies and send the same picture to a thousand other people. Presumably, as long as it is just a picture of an apple, you won't care less that others also enjoy it. But of more valuable things, such as contracts, you will no doubt want to make sure that the transaction is correct. You are not in a position to check everything empirically, as you do on the bench, which is why you invite an arbitrator, a trusted third party: a bank, notary, marketplace, credit card company or PayPal. To create the same level of trust, uniqueness or "digital scarcity" will somehow have to be organized in the world of digital plenty. In other words, you will want to be sure that you are the only receiver of this unique copy. Until now this could only be effected through a central agency, such as a bank. Now an opportunity presents itself to solve this in a technically different way, and it is called the Bitcoin protocol.

To get a good grasp of Bitcoin, the best thing to do is regard it as a digital account. Imagine that you are sitting at a table with a group of friends. They all have a laptop and they can all access the same logbook simultaneously, which shows exactly how many bitcoins each of your friends possesses at any moment.

When, at one stage, one of them wants to transfer some bitcoins to another, he is to inform all the others at the

table. When that is done, the whole group adds the transaction to their logbooks, provided they have all confirmed its authenticity. Despite the fact that the money in such a system is digital and has no physical shape, it is impossible to spend the same money more than once. The thing is that double spending is immediately spotted by the network and rejected as a consequence.

Obviously, in actual reality all participants are part of a global peer-to-peer network, and the transactions do not take place between individuals but between addresses in the network. The verification process of those addresses is done by means of cryptography, without divulging the true identity of the owners.

DOUBLE SPENDING

To this date not a single case of double spending is known. However, theoretically such a fraudulent attack is possible as long as the hacker controls at least 51 per cent of the computing power of all the computers that protect the network. But deceiving the network during the time needed to carry out one double spend would not be a very sound option from an economic and organizational point of view. Bitcoin's computer network has far, far more computing power than the 100 fastest supercomputers taken together. Any attempt at double spending would require too substantial an investment and a complex organization. In addition, the source code was recently changed so as to make it easier to detect and neutralize such attacks – regardless of the hacker's motivation.

How are bitcoins made?

New bitcoins are mined virtually (this is actually called mining) by means of a competitive and decentralized process. Bitcoin miners process transactions and protect the network with specialized hardware. For their services – creating, dealing in and checking bitcoins – these persons are rewarded in the form of new bitcoins. There are big professional miners, such as ASCIMiner, as well as small players.



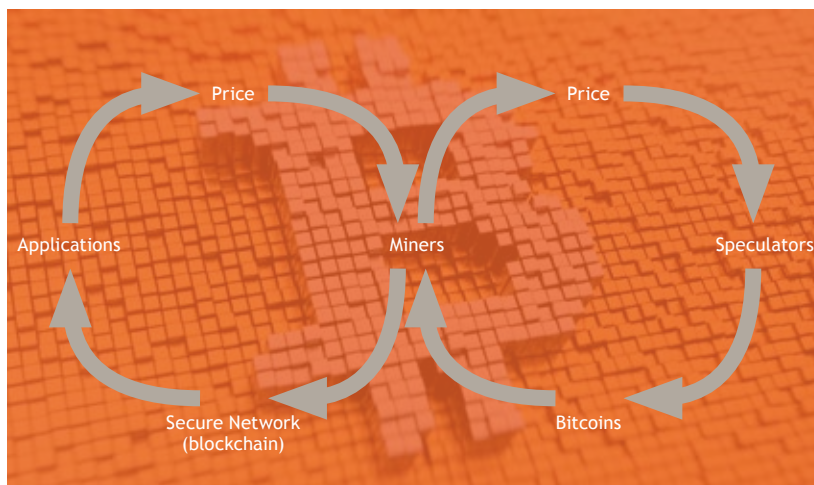
Example of a modern bitcoin mine, ASCIMiner, in Hongkong's Kwai Chung. The cooling installations are on the roof of the building.


In the second research report, “Design to Disrupt: New digital competition”, we dealt at great length with the way various technological platforms are changing our economy. Bitcoin is what we call a multi-sided platform (MSP). Within this platform miners have a crucial role in

attending to the various sides. On the one hand they are mining the new crypto-coins to be used for speculation, on the other they build and manage the infrastructure on which all kinds of applications can be built. The figure below makes clear that the digital currency cannot be unlinked from the underlying network protocol. Miners need an incentive (= the bitcoin currency) to maintain the network. Would you like to mine bitcoins yourself? In that case the “Beginner’s Guide to Mining Bitcoin” that you can read on startbitcoin.com is a useful start.

Eric Nelson, a small player who decided to make just one bitcoin, works out how much money he makes out of the whole operation and what his economic considerations are. Nelson states a bitcoin price of 92 dollars, but meanwhile the bitcoin is quoted at 260 dollars and consequently his earnings would be just over 8 dollars a day.

“I decided to mine one bitcoin with my spare computer to see how it all works. I am part of a ‘slush’s pool’, and running GULminer on Windows. When I shut down everything but my mining computer, my UPS reports that I am using 0.261 kw, or 6.264 kwh/day. I pay 12.5 cents per kwh, so I am paying 78.3 cents per day. I have averaged about 0.03 bitcoins per day so far (approx. 330 MHash with some video card that was top of the line a year or two ago), with that number about to drop a lot since the ASIC rigs are coming online. Bitcoins are \$92, so my total revenue per day is \$2.76, with \$1.98 in profit [which is less than the depreciation on the machine]. I’m going to stop as soon as I hit one bitcoin though, as the extra heat in my office will be uncomfortable in the summer. This is more of a wintertime activity.”





The Bitcoin protocol is designed in such a way that new bitcoins are created at a fixed pace. As more miners join the network, it is getting more and more difficult to make a profit and miners will have to seek efficient approaches to reduce their operating costs. By now various groups are active on the internet where people can together look for the electronic money by using the collective computing power of the computers during mining, the mining pools. The system cannot be administered or manipulated by a central authority or developer to raise the profit. Every Bitcoin node in the world will reject any transaction that does not meet the rules of the system.

GOLD VERSUS BITCOINS

Choosing the mining metaphor was no coincidence. You have to mine bitcoins (make bitcoins), just like gold. Gold is particularly useful because it does not perish, it is small enough to keep it in your pocket, it is easy to tell imitation from the real stuff etc. All of them attributes shared by the bitcoin. The fact that the bitcoin is scarce, like gold, plays a crucial role.

Precluding fraudulent transactions with the help of a crypto-puzzle

To make sure that only genuine transactions are accepted by the blockchain, all the linked-up computers in the network need to compute a control number, a cryptographic puzzle, by way of a competition. The first to find the control number is initially trusted and allowed to enter the transaction in the blockchain. As more computers end up with the same number, the result is getting more reliable. Many computers are trying to find the same solution, and therefore the chance that a fraudu-

lent computer can enter the solution (to a fraudulent transaction) in the blockchain is minimal. The chance that such a transaction is confirmed several times is even more negligible. If over half of the computing power available in the network is at the disposal of the correct, reliable algorithms, it is statistically impossible to tamper with the blockchain. This also means, incidentally, that bitcoin transactions can only be realized after a few minutes. Meanwhile, several solutions have been devised to sidestep or shorten the transaction time.

Shared single source of truth

As mentioned, the basis of bitcoin is the blockchain. The blockchain is for bitcoin what the ledger is for a bank. A regular bank has a large pile of money in a safe and a ledger where they record what part of the money is whose. This is essential: the ledger is administered by a bank. That is why all transactions are executed by that bank.

In the case of bitcoin the ledger is decentralized. In other words, the entire network is in effect the ledger (the blockchain). No specific person administers the ledger, because everyone does. Everyone can add something to the ledger, but no one can remove something from it. The ledger contains an indelible history of all transactions. It is a kind of financial DNA that makes fraud or other incorrect transactions virtually impossible, because the procedure is checked and verified by tens of thousands of servers worldwide that use the public and permanent processing history of the code block. Which bitcoins are assigned to which wallets (addresses) is recorded by all nodes in the entire network, much the same as when a notary keeps a close watch on every transaction. Transactions simply go from wallet to wallet, peer to peer.

The decentralized nature of the blockchain offers many advantages as well as the possibility to devise other new applications that could not possibly exist in a centrally organized world. The fact that financial censorship by a single party is impossible, implies that there is no longer a single point of failure. The mere concept offers a wide range of opportunities. Unlike the bank's ledger, everyone has access to the blockchain. It is a shared single source of truth. The same shared version of the truth is available to everyone. In consequence, bitcoin transactions are fully transparent. However, the "account numbers" (bitcoin addresses) that are added to the blockchain are anonymous, in principle. This offers users of Bitcoin the choice between anonymity or, on the contrary, transparency: everyone who publishes his address, provides direct insight into its cash flows, whereas everyone who prefers to keep them out of sight, can do so.

The seven pros and cons of Bitcoin

Pro 1: Freedom of payment

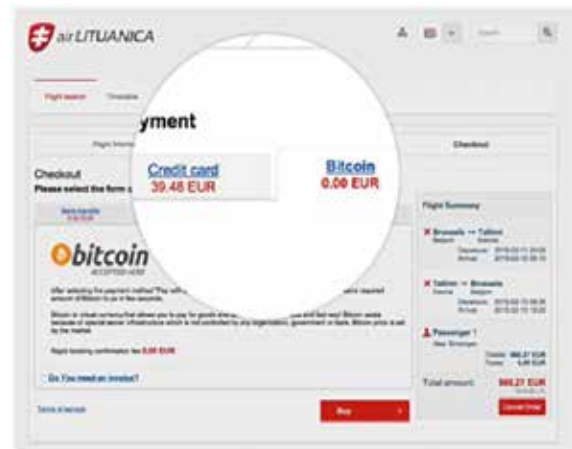
Bitcoin is like email for money. One can send and receive any amount, always, everywhere and with no delay. No public holidays. No borders. No imposed limits. With Bitcoin, you can transfer money to persons or businesses within a matter of minutes – anywhere in the world, at a fraction of the fees charged by banks.

Contra 1: There are only few places where you can use it

Many people are not aware of the existence of Bitcoin. More businesses accept bitcoins on a daily basis, because they aim to take advantage of the pros. But the list is still short and needs to grow to profit from network effects.

Pro 2: Extremely low fees

Currently, bitcoin payments are processed at no or extremely low fees. At a certain charge, users can arrange to have transactions effected with priority, so that they are confirmed by the network more rapidly.



Buying an airline ticket can turn out cheaper with Bitcoin.

In addition, there are exchanges to help sellers during the processing of transactions, the conversion of bitcoins into fiduciary currencies and the direct daily transfer of money to the seller's account. Being based on bitcoin, these services can therefore be offered at far lower fees than is the case with PayPal or other credit card networks.

Contra 2: The value may tend to fluctuate considerably

The total value of bitcoins in circulation and the number of businesses that actually use them is still quite small compared to what it could be. Therefore, relatively small changes in the market may impact the price substantially. Theoretically this volatility will decrease as bitcoin obtains a more prominent position in the market and the technology is improved.



Price trend of the bitcoin. In late March 2015 the coin was worth about 260 dollars. Eighteen months earlier the price was still over 600 dollars.

Pro 3: Micropayments are going without a hitch

Bitcoin can process payments of only a few cents. This opens the way to new models of payment that are very interesting for suppliers of content in particular. Content suppliers are limited in the way they generate income. With Bitcoin you can pay for a single block of content, for example for a single listen (listening to a single song only once) or buying bandwidth of a wifi hotspot per kilobyte. Publishers can simply place a button next to their articles to sell the relevant item oneself for a small amount, an alternative for Blendle. What also comes to mind is the irritating commercials when you are watching YouTube. What if you can skip them once and for all by paying a few cents? What is particularly wonderful is the Streamium application, a kind of Periscope or Meerkat, but on steroids. Watchers of a livestream pay real-time per minute, through micropayments.

Contra 3: It is still a bit shaky in places, it is not finished yet

The Bitcoin software is still in a beta phase with a lot of incomplete functions that need a great deal of doctoring. New tools, functions and services are being developed to make Bitcoin safer and more accessible to the public at large. A number of them are not yet ready for all. The majority of the bitcoin businesses are new to the game and do not offer insurance yet. Bitcoin is still on the way to maturity.

Pro 4: Transparent and neutral

All information with regard to the bitcoin money supply is readily available in the blockchain, so that everyone can verify and use it in real time. Persons or organizations cannot control or manipulate the Bitcoin protocol, as it is cryptographically protected.

Contra 4: It facilitates illegal trade and dubious practices

There are secret routes to facilitate online trade in anonymous, uncensored ways, e.g., via OpenBazaar and Silk Road, the Amazon of the darknet, and Dark Wallet. Dark Wallet is a plug-in for Chrome and Firefox (Mac, Windows and Linux), which functions as a bitcoin wallet and guarantees anonymous payments. The Dark Wallet software encrypts and combines the transactions of others. Combining those transactions is done in a totally indiscriminate manner: when Alice buys socks in a bitcoin-friendly clothes shop and Bob orders LSD from Silk Road (or its successors) at the very same moment, these two transactions can be combined to one, even if Bob and Alice do not know each other. This means that governments have no insight at all into the effected transactions.

Where are the unbanked?



Adults with an account at a formal financial institution (%)

0 - 20	61 - 80
21 - 40	81 - 100
41 - 60	no data

SOURCE: World Bank

Pro 5: Banking the unbanked

According to figures of the World Bank, over half of the adult working population has no access to all kinds of financial services to save or borrow money. This means that more than 2.5 billion adults worldwide cannot participate in economic activities. Thanks to Bitcoin everyone with internet access has the possibility to carry out his own banking.

Contra 5: The government can no longer listen in

Bitmessage is a P2P communication protocol to send coded messages to someone else or to many subscribers. It utilizes strong authentication, which means that the sender of a message cannot be forged, and it tries to hide “non-content”-related information (such as the sender and receiver of messages) from eavesdroppers such as the NSA.

Pro 6: Protection and control

Bitcoin users have total control over their transactions. For sellers it is impossible to demand fees as happens with other money processing intermediaries. Bitcoin payments take place without showing personal details. This ensures strong protection against identity theft. In addition, Bitcoin users can protect their money via backups and encryption.

Contra 6: Bitcoins can be stolen

The data required to exercise control of your bitcoins can be stored in various ways: in a digital wallet or via websites that offer bitcoin accounts. But the data needs not necessarily be stored digitally: you can also write it on a note (a so-called cold wallet) or simply commit it to memory. With this data, bitcoins can subsequently be transferred via the internet to anyone who has a bitcoin address – similar to sending an email. What should be borne in mind, however, is that crypto-money can be stolen, much as may happen in the physical world. People have been given a fright more than once when bitcoins disappeared from their wallets because they had not protected their data properly.

Pro 7: Lower risks for sellers

Bitcoin transactions are safe, irreversible and do not contain sensitive or personal customer-related data. This way sellers are protected against loss through fraud or fraudulent account adjustments and PCI compliance is not necessary. Sellers can simply enter new markets where credit cards are not available or the fraud percentage is unacceptably high. The net results are lower fees, larger markets and lower administrative fees.



Contra 7: Getting used to a different form of supervision

There is little regulation on the part of the government or any other supervising body. That is the main reason to be skeptical. There is no central authority that issues money or checks whether there are false coins in circulation. The reason, amongst other things, is that the bitcoin is not regarded as a currency by these authorities.

The idea that trust can be organized in a different manner – in codes and systems – requires a mind-shift. It will probably take a while before the public will accept the useful attributes of the bitcoin and blockchain. Clearly, the central issue is not that there is little regulation on the part of the government, but that we will have to get used to this new concept and come to realize that things can also be resolved differently.

The European Central Bank (ECB), incidentally, is not getting overly worried at the moment. In their view bitcoin does not amount to anything much and is leading a marginal existence. In addition, they are aware that so far no major accidents have occurred. The danger that they envisage is that if the bitcoin economy incurs heavy losses, the trust in the official currencies and e-payments can also be undermined. And this is something they will want to prevent at all cost; after all, this is why the ECB was established in the first place.

The ECB report “Virtual currency schemes – a further analysis” (2015) provides a good picture of how the various global supervising bodies currently look at the subject. To begin with, the ECB says that the bitcoin is not money: “They are something else, different from known currencies.” A logical conclusion, possibly, because the key attribute of money is that it is universally accepted where the bitcoin still has a long way to go. In an earlier definition (2012) of the ECB the word “money” was still used, but obviously the central bank has now dis-

tanced itself from this. This may well be a weight and/or responsibility off the shoulders of the financial supervisors, as it is primarily their task to watch the money. The ECB has likewise deleted the word “unregulated” from the definition, for – as the ECB puts it – “regulation has caught up with innovation.” So the ECB does not see the bitcoin as money, but yet somehow regards it as regulated, whether or not by other authorities than the traditional financial institutions. The idea that the body issuing the regulations need not do so in the case of the bitcoin, is supported by the US Federal Reserve Bank:

“The Federal Reserve simply does not have the authority to regulate the bitcoin in any way.”

The director of the American Consumers’ Guide, Richard Cordray, feels there are reasons to be worried:

“Virtual currencies are not backed by any government or central bank, and at this point consumers are stepping into the Wild West when they engage in the market.”

Warnings with respect to the bitcoin are legion – not in the last place from the supervisors: from the Bafin, the German financial authority, to the French, Dutch and Belgian central banks. In addition, the People’s Bank of China, the Reserve Bank of India, Singapore’s monetary authority and the Indonesian central bank, among others, have issued warnings. Apart from warning and emphasizing that the bitcoin is not an official (legal) currency, banks in some countries have made licenses compulsory for specific services. Sweden, for example, issues licenses for the trade in bitcoins (the bitcoin exchange). In Germany, the financial authorities allow you to use, buy, sell and mine them, but licenses may be required for supplementary services.



In China, trading and paying in bitcoins is not allowed. Likewise in Thailand, but the Thai central bank is said to have no ways to enforce that decree. The question is which country does have adequate means. Russia sees the bitcoin as substitute money and it is banned for that reason; the Russians feel that it is potential proof of being engaged in dubious transactions.

More than anything else, the main question is to what extent the algorithms behind the bitcoin currency can be trusted. The code is open-source and a network of computers ensures that fraud is impossible, but nevertheless it feels odd to have a mortgage deed executed via the blockchain. What authority guarantees that the house I have bought is actually mine? What institution makes sure that my last will, stored in the blockchain, is actually carried out?

Who will? A Bitcoin Governance Framework

As yet, it is like reading tealeaves. It is not entirely clear at the moment what shape the regulation of the cryptocurrency will take in the future. Expectations are that it will be a mix of governments, central institutions and the underlying algorithm. A report and inventory published by Global Solution Networks propagates a “multi-stakeholder solution to the challenges of the cryptocurrency.” It is also the subtitle of the report “A Bitcoin Governance Framework.” Many of these challenges have been formulated in the list of seven cons above. Specific

spearheads of a new governance framework are Anti-Money Laundering (AML), Know Your Client (KYC) and Combating the Finance of Terrorism (CTF). Parties that need to be involved in the governance of bitcoin/blockchain, are the Worldwide Web Consortium (W3C), the ICANN, the Internet Engineering Task Force (IETF), for example, in addition to the governments. In the meantime all parties have become fully alive to the fact that the Bitcoin protocol has a number of pros. On top of this so-called “fifth protocol,” all kinds of applications can be built enabling large-scale improvements to the existent and obsolete financial system. As the ECB has pointed out, it is not money. It is a network, a digital infrastructure, a new protocol and new opportunities. The next chapter deals with these new applications.



2 CRYPTO-ECONOMY 2.0 – SMART CONTRACTS AND THINGS

If your organization is in any way involved with one of the following matters, the crypto-economy 2.0 could be very interesting for you.

Money, shares, mortgages, passports, birth registers, poll cards, gun licenses, vehicle registrations, digital identities, hotel bookings, software licenses, track & trace of parcels, medical files, contracts, wills, diplomas, DNA, latchkeys, keys of lockers, coupons, vouchers, domain names, patents, cinema tickets, sim cards, copyrights.

And, apart from these, all physical equipment that could be connected to the internet (Internet of Things).

The whole list of intangible assets (such as contracts) and hard assets (all devices) can be given a new dimension thanks to the possibilities of the blockchain. Here it is about smart contracts and smart things. According to Melanie Swan, founder of the Institute for Blockchain Studies, these two form the basis for the new opportunities, a “Blueprint for a New Economy.” This is also the title of her most recent book. With this form of crypto-economy, we enter new territory. As has been mentioned before, it is still early days. Swann expressly refers to a blueprint, but it can serve as a basis for further building and testing, as is happening on a large scale.

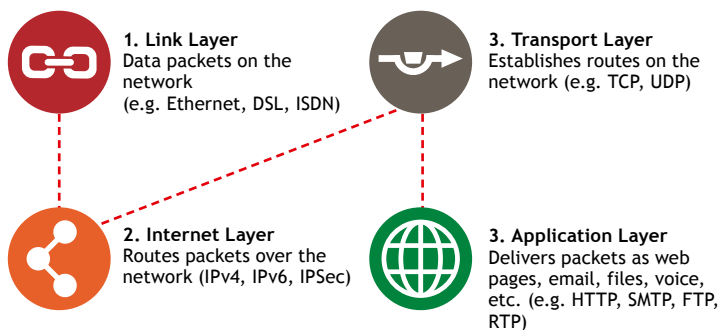
The list at the beginning of this chapter provides examples of agreements that we make to structure the physical world. According to Andreas Antonopoulos, author of the book *Mastering Bitcoin*, who was elected the most influential bitcoin expert by the bitcoin community in late 2014, we can now restructure/reorganize the physical world. In his view we can regard money as data, as a new *content type*. Digital money, obviously, consists of nothing but ones and zeroes. The blockchain converts money into programmable entities, which allows it – together with other forms of valuables and ownerships – to flow frictionless across the internet, much the same as webpages, email, video and music. The idea is that we can provide money with a particular sort of behavior based on preconceived rules. This is currently stated in rules that are being monitored via bureaucratic processes. No wonder that some banks are fearing the larger implications of the blockchain. Or as financial securities research analyst Johann Palychata of BNP Paribas says: “Its core is the first successful attempt for a secure and decentralized register. It should be considered as an invention like the steam or combustion engine. [...] In its purest form, a distributed blockchain system allows all market participants direct access to the DSD (Decentralised Securities Depositary), to the exchange and to the post-trade infrastructure (clearing and settlement). If this setup develops then existing industry players might be redundant.”

So with the help of a mechanism such as the blockchain we can program these rules into the money itself. So: prior compliance. This way health care insurers could use a so-called “CareCoin” that can only be issued if it is used for pre-programmed purposes.

In such a case it is all about the creation of a totally new network, with all the opportunities that come with it: from internet money to an internet of money.

A new protocol

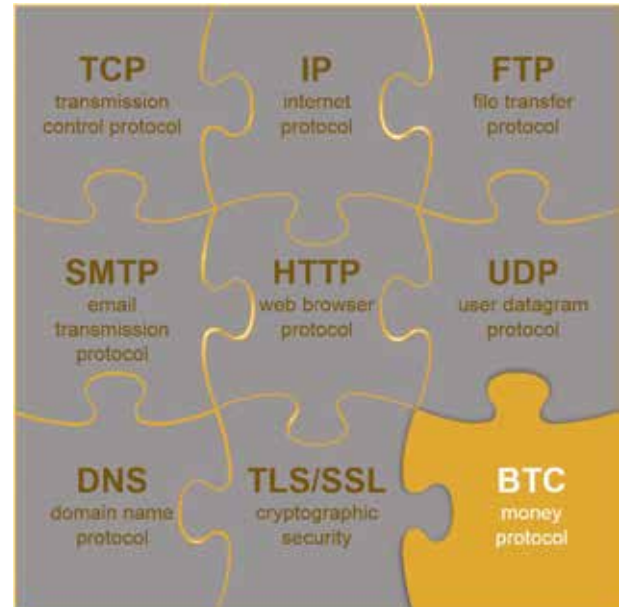
Ever since 1960, the largest data network in the world has been under construction. This network, which we call the internet, sends packets of data back and forth by utilizing various communication protocols. Together they are known as the Internet Protocol Stack, which consists of four layers: a data link layer (to transport data on the network), a network layer (to route the packets over the network), a transport layer (for the trouble-free transport of data over the network) and an application layer (containing the internet applications, such as HTTP, SMTP and FTP).



Source: Winklevoss & Winklevoss (2014)

Over the years, this network has been instrumental in exchanging data, but not in the intrinsic transfer of value. Thanks to the internet we can now trade globally; it is just the exchange of money and the transfer of value or ownership that still present problems. The Bitcoin protocol, the blockchain, solves this problem and consequently shows great promise. This is also why the provocative statement “The Fifth Protocol” is sometimes used by the bitcoin experts when they refer to the potential of the blockchain.

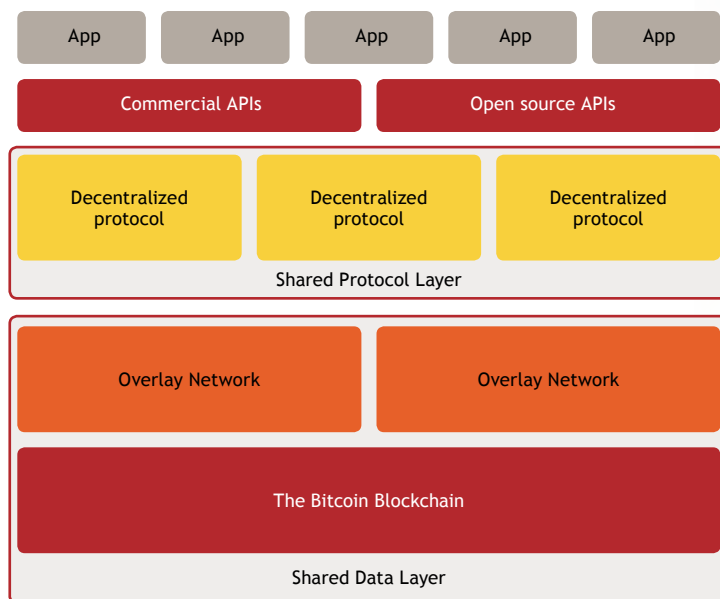
An internet that “allows real money, commodities, services or other assets to change hands across large distances at a minimum of friction”: the blockchain is the missing jigsaw piece to complete the Internet of Value.



Source: Reddit, see http://www.reddit.com/r/Bitcoin/comments/2x5de0/the_final_piece_of_the_protocol_puzzle/

The Blockchain Application Stack

One of the bitcoin experts arguing that the blockchain infrastructure is more important than the cryptocurrency is Joel Monegro. He works for the investment firm Union Square Ventures of Fred Wilson, and has developed the Blockchain Application Stack. This construction shows how it is possible to make decentralized applications with the help of Bitcoin. According to Monegro, the first phase of Bitcoin was about installing an infrastructure – gateways, consumer wallets, developer platforms, merchant services and so on. The next phase involves the building of native Bitcoin applications, which could not be built prior previously. These applications must ensure that Bitcoin will be mainstream at last.



Source: Monegro (2014)

Now the time has come for developers to build all sorts of applications with user-friendly interfaces on this platform. The fight for the killer apps can begin.

CLOUD COMPUTING IS THE KILLER-APP CANDIDATE

One candidate is the Storj application. This is a decentralized cloud solution to store files. Users can install an application on their computers, giving part of their hard disk to the cloud to enable other users to store their files in a protected and encrypted state.

In the meantime, a Mega-Master Blockchain List¹ can be found on the internet that has been created by means of a Twitter brainstorm. This can be considered an adequate inventory of killer-app possibilities. The list features 84 different applications by now, which are subdi-

vided into 6 categories in which the blockchain can be used. A fairly concrete translation of the list into potential services is provided by a study of William Mougayar. In February 2015 he performed extensive research into the crypto-technology landscape. In all, Mougayar listed some 430 businesses, which all focus on developing all sorts of applications for the blockchain. He distinguishes four categories: applications, middleware services, ancillary services, and infrastructure and platforms.

¹ <http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list>

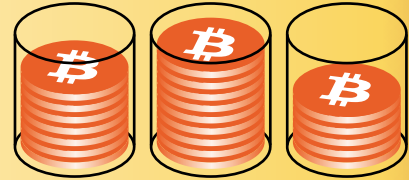
THE BITCOIN BLOCKCHAIN AT WORK IN FIVE EASY STEPS

Online retailer CashCoin accepts bitcoins and Betty wants to pay with the currency from her wallet.

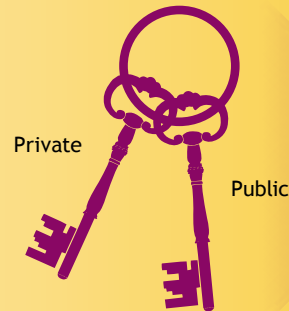
Wallets and Addresses



Both CashCoin and Betty have virtual Bitcoin wallets on their computer. These files provide access to Bitcoin addresses. Each address is a string of letters and numbers and contains a certain amount of bitcoins.



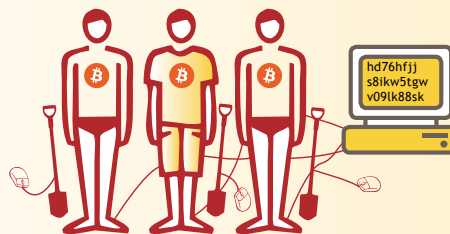
The signage of a message with your private key (which only you know) can be verified by anyone on the network using the matching public key (which everyone knows). Cashcoin's new Bitcoin address is a unique public key that is published on the network, while the corresponding private key is safely stored in the company's wallet.



Submitting a Payment

Verifying the Transaction

Jill, Jack and John are Bitcoin miners. Their computers bundle the transactions of the past ten minutes into a new transaction block to be added to the Bitcoin blockchain.



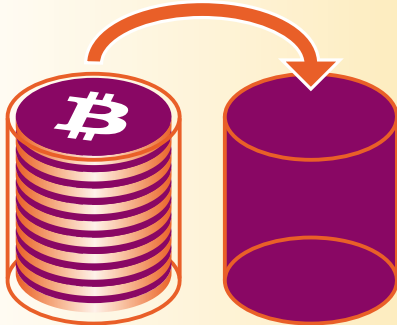
The block is identified by a new cryptographic hash value, i.e. a fixed-length string of numbers and letters, since Jill's Jack's and John's computers are set up to do so.

Every new Bitcoin hash value must have a specific form and must start with a certain number of zeroes. There is no way of predicting which nonce will generate the required number of zeroes. For Jill, Jack, John, and all other Bitcoin miners this is a trial and error process that needs enormous computing power.



When the coinbase that is part of every transaction block on the Bitcoin blockchain has been hit - let's say by John - this winning Bitcoin miner is rewarded 25 newly minted bitcoins by the Bitcoin system. John receives an address in his wallet which represents the money he earned for his successfully accomplished transaction verification effort.

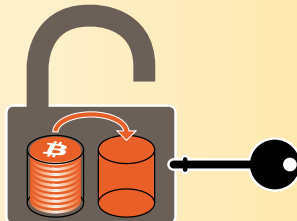
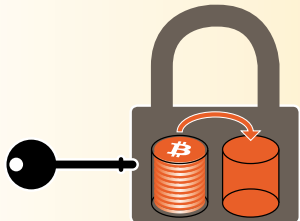
Creating a New Address



At CashCoin, the cashier replies to Betty's payment request by creating a new Bitcoin address where the money can be submitted. By creating the address a cryptographic key pair is being generated, consisting of a private key and a corresponding public key.

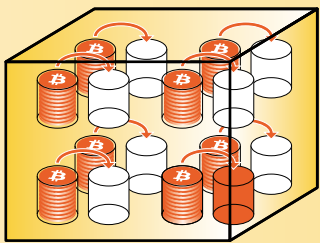
Private

Public

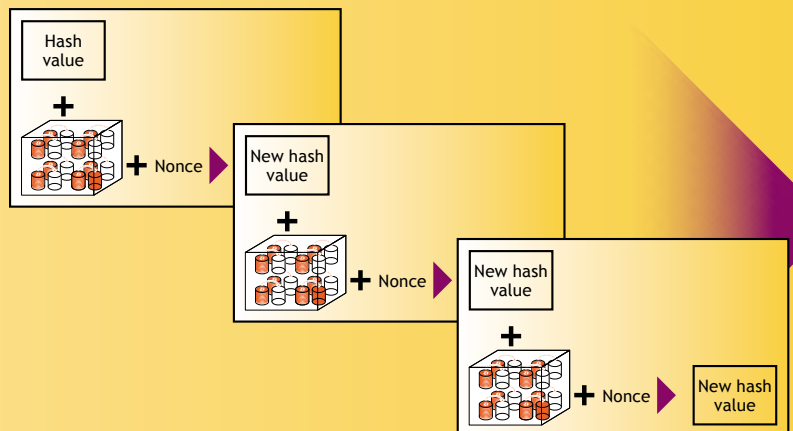


Betty's Bitcoin wallet holds the private key for each of the addresses it contains. The Bitcoin program on her computer signs Betty's transaction request with the private key of the address that she chooses to transfer bitcoins from.

Anyone on the Bitcoin network can verify with the public key whether the transaction request is actually coming from Betty.



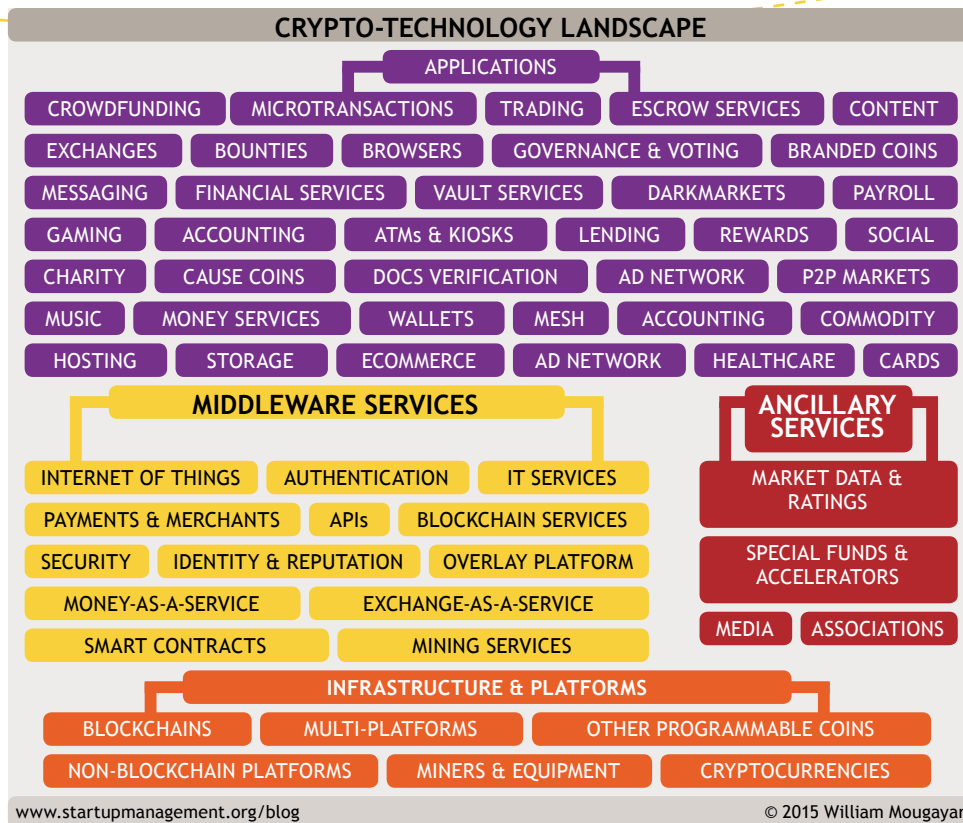
Each new hash value in the Bitcoin blockchain contains information about ALL previous Bitcoin transactions. A nonce is a random number that is added prior to hashing. The computers of Jill, Jack and John create new hash values based on a combination of the previous hash value, the new transaction data block, and a nonce.



Want to Break the Bitcoin or Any Other Blockchain System?

Anyone aspiring to takeover the Bitcoin system would have to redo what John did and all subsequent miners. That is practically impossible.





The figure above shows at a glance the diversity of the total of applications built. Bitcoin experts claim that in the years to come numerous applications will be developed, specifically in the context of the Internet of Things and the smart contracts and ownership rights.

Bitcoin and the Internet of Things

The Samsung washing machine W9000 is equipped with a new information architecture of IBM: ADEPT (Autonomous Decentralised Peer-To-Peer Telemetry) based on blockchain. The washing machine can order detergents itself, browse its “peer” network for the right supplier, communicate, negotiate, order and provide the delivery address, and pay. It can also find the best service engineer if it spots a breakdown (does not feel well), and to save energy it can independently establish a dialogue with the energy provider or the TV. To prevent a peak load, it can ask the TV to switch itself off (but the TV can decline the request).

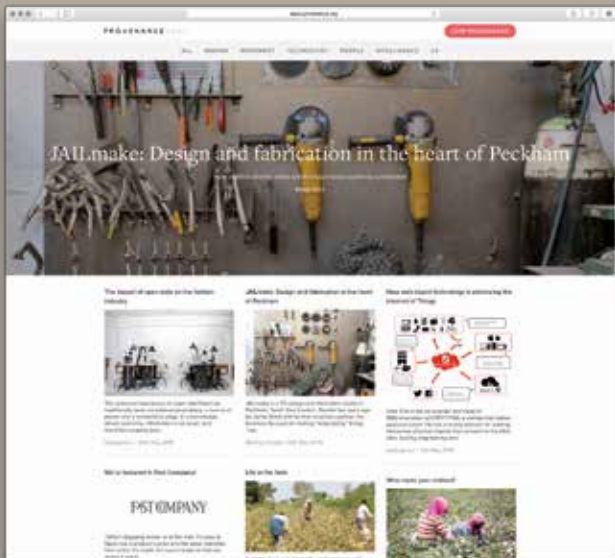


The Samsung W9000, functioning with blockchain, elaborated and described in the IBM paper “ADEPT: an IoT Practitioner Perspective.”

The Samsung W9000 blockchain washing machine is a proof-of-concept and smart contracts are as yet a “blue-print” for future practice. The blockchain is not being used on a large scale yet. All the same, it can be interesting to explore such a future. From the very moment that a product rolls off the production line, it can be recorded by the manufacturer in a universal blockchain, and this represents the beginning of the life of the prod-

uct in question. A simple washing machine can become a semi-autonomous appliance that is able to manage the delivery of its own consumables, organize maintenance and negotiate with other peer equipment so as to respond to its environment as efficiently and effectively as possible. In other words, a form of autonomous Product Lifecycle Management, where the products determine their life, termination of life and generation of new products autonomously (we will revert to this when discussing crypto-economy 3.0).

The British company Provenance has developed a software service where parts of products are recorded and shared based on the blockchain. “Made in”, “made of” and “made by” information can be added to the products. Provenance claims that the value is in the possibility to tell other stories about your product. The APIs can communicate with the larger e-commerce platforms, so that this information is made more readily available on larger platforms than Provenance.



The Provenance platform

Using Provenance it's simple for maker to add products and open up information using our online tools in three simple sections:

Made In

Locations: Making, materials and business addresses

Made Of

Materials, accreditations, certifications and processes

Made By

Maker stories, company information, employees

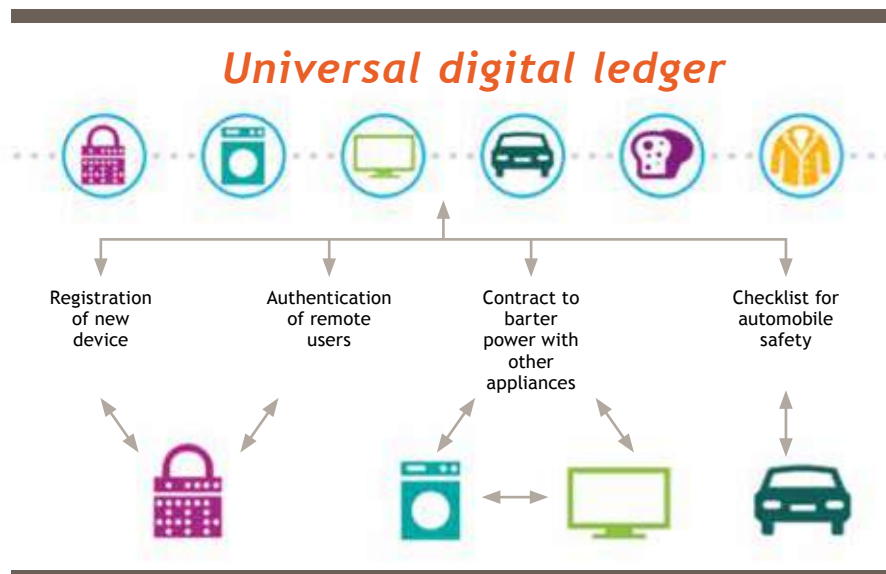
Device Democracy

One of the companies trying to capitalize on the above range of ideas is 21 Inc. In the past few years venture capitalists – such as Andreessen and Horowitz, chipmaker Qualcomm and the founders of companies such as eBay, PayPal, Dropbox, Expedia and Zynga – invested more than 161 million dollars in the company. It was not until May 2015 that the company disclosed its plans. It has developed a special mining chip called Bitshare, which fits into every mobile device: *“21 Inc. will insert ASIC chips for bitcoin mining into such daily devices as routers, gaming consoles, USB battery chargers, toasters, set-top boxes, and chipsets.”* From a conceptual point of view, the chip thus transforms Bitcoin into *“a fundamental system source that can be equated with CPU, bandwidth, harddisk space and RAM.”* With the help of this chip, each device can generate its own flow of digital currency and subsequently use it to pay others for the services rendered. According to one of the developers of 21 Inc., it will not be people who execute transactions in the future but, on the contrary, the machines: *“Everyone assumes that humans will be driving transactions, not the case.”*

Three-quarters of the proceeds of the mining activity goes to 21 Inc. Part of the plan is to offer products for free in order to bring in new customers rapidly. After all, the profit comes from another source. This model is in line with the trend outlined by IBM in their report about Device Democracy.

Smart contracts

When “blockchaining” contracts, the main idea is that all kinds of rules and agreements that are implied in contracts can now simply be programmed on the blockchain. Mediation and registration by a central authority such as a notary or a bank is no longer required for the drawing-up and observing of a contract. In this case a smart contract equals a small programmed block of code in which contractual agreements are placed that can be verified by the blockchain with automatic transactions or suspension of payments if the blockchain knows if agreements have been kept or not.



The blockchain functions as a universal digital ledger that can be used by all kinds of devices to enter into different types of mutual transactions (Brody & Pureswaran, 2014).

DIGITAL NOTARIES

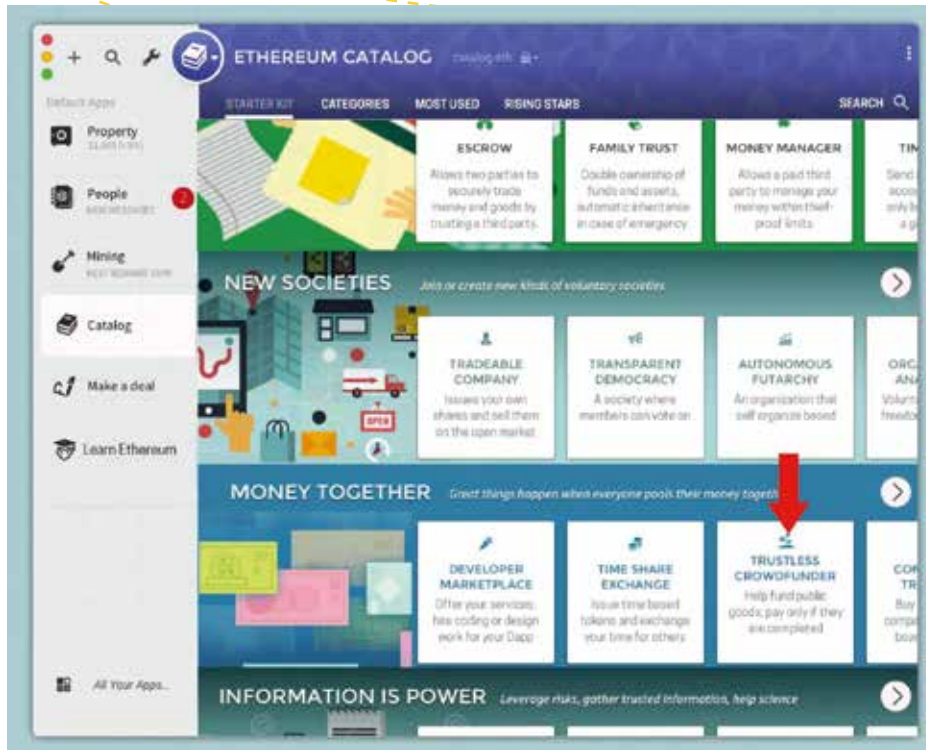
There are a few concrete implementations that use the blockchain for notarial functions. For example, the Argentinian developer Manuel Araoz created Proof of Existence. This service makes it possible to publicly record the authenticity of a document at a certain moment by equipping it with a unique code (sha256-hash) and recording it in the blockchain. This way a journalist or an attorney can prove that at a certain point in time he was in possession of a specific document without publicly sharing the contents. Virtual-Notary, Bitnotar, Chronobit, Pavilion.io and btcluck are services that offer such a functionality.

Online gambling would be perfectly suitable for these smart contracts. The code demands the result of a sports contest and pays, if necessary, in accordance with the rules. This way the organizer of a gambling game, for example, can be passed over altogether. Augur is a fully decentralized prediction market that utilizes the blockchain mechanism. With Augur it is possible, for example, to predict the result of the next presidential election or to place a bet who will be this year's national soccer champion.

The company Ethereum arranges and organizes many of these smart contracts and is market leader in this developing market. Ethereum is an open-source platform that distributes value tokens called “ethers” via the blockchain. Via a WYSIWYG interface, the Mist browser, everyone can click up smart contracts. The platform offers a number of templates to make such contracts. A piece of cake, it seems.

In addition to contracts, Ethereum also aims to realize other financial applications, such as opening a savings account, drawing up a will and issuing shares. Semi-financial applications are also deemed feasible, such as rewarding someone who executes difficult arithmetical jobs on his systems. In addition, much thought is given to other decentralized processes, such as creating a system to ensure secure voting, but also to set up a “competitor” for Dropbox.





Smart ownership rights

An essential part of a contract can be property. This ownership can be placed in the blockchain and due to the programmability the assets in question know who is their owner. What comes to mind is a stolen automobile that will not start because the blockchain knows that it is stolen. Here the blockchain functions as a control database linked to a unique “fingerprint” that precludes unlawful use. A company such as Mine employs a combination of identity, reputation history, digital documentation and the blockchain as proof of ownership. This generates interesting opportunities for new online market places that are fully decentralized and where everyone can do business based on the trust put in the network. Or for existing market places: if an automobile is sold through a market place, the ownership is not transferred until the payment is received. An example of such a P2P

market place is OpenBazaar. This is a new way of facilitating online trade in an anonymous, uncensored way. It employs technologies such as BitTorrent, Tor and Bitcoin. Founder Brian Hoffman claims that the aim is not to trade in all kinds of illegal products and services, but considering the nature of the project this can hardly be avoided. In addition to OpenBazaar there is also a similar enterprise, BitMarkets.

Another example is Airlock.me, a new way of opening locks. You no longer require a physical key, but the door can be unlocked by means of cryptocurrencies. This way an apartment can be rented via Airbnb, for example. As soon as the tenant has transferred the amount in bitcoins, the Bitcoin blockchain – after verification – grants access to the apartment for the agreed period. It is a combination of smart contracts and smart things.



Lockmasters

A Lockmaster connects their smart lock to Airlock. A lock can be public or private and is always communicating with the Airlock network.

Keyholders

A keyholder is granted access to a Lock by its owner. Access can be open-ended, limited by date and time, or one-time only, as determined by the Lockmaster.



3 CRYPTO-ECONOMY 3.0 – THE ROBOCORPS

For the very reason that we position the blockchain so emphatically as a platform technology with various potential outcomes and applications, it is worth thinking in the realm of thought of the imaginative thinkers who have entered the world of the blockchain. The one person capable of doing so par excellence, is Mike Hearn. He is a former engineer of Google, one of the developers behind bitcoin, and also a worldwide authority in the field of blockchain. His vision of the future is called Tradenet.

Tradenet

There is a brilliant future in store for emancipated automobiles that do business all by themselves – and not particularly for the electric automobiles of Tesla or for the controversial Uber taxi company. In his theoretical experiment, Hearn assumes that in the future autonomous automobiles will be perfectly common and that for the same reason only few people will still have their own car. If, in addition, those autonomous taxis are no longer owned by a large company but function fully autonomously, taxi rides will become cheaper in the bargain.

It becomes truly interesting if those autonomous automobiles can be programmed in accordance with our wishes. Hearn: “We can program them in such a way that they make small, but not excessive profits. This way we can make the most moral and socially conscious capitalists ever.”

The automobiles communicate with customers and infrastructure via a new online trade system: Tradenet. You could use an app that logs in to Tradenet and says: “I am here and this is where I want to go. What’s your best price?”

The autonomous taxis will then let you know their best rates, based on where they are, how much fuel they have, the quality of their programming... Next, you or your phone selects the best offer, not just based on the best price but also based on driving data and how attractive the automobile is.

Hearn stresses that although the automobiles function autonomously, they have no consciousness. They can, however, be programmed in such a way that they update themselves. For example, the money they earn can be used to hire human software developers to adjust their codes, but also to pay for maintenance or refueling. Also, they can be offered the opportunity to put their “savings” together to have new automobiles made: to have “children.” When a new automobile rolls off the production line, it would join the competition with existing cars. The new automobile would then have to give up part of its earnings to its “parents,” by way of a kind of “birth loan” that it would have to pay off to its parents before it becomes fully autonomous. According to the same principle, life termination is also programmed into the system, to get antiquated models off the road or to





respond to a changing market. If at some stage there are too many automobiles in proportion to the number of people, some automobiles might go to a long-term parking facility and simply switch off. According to the same principle, automobiles might also move to other cities to find work there, says Hearn.

As banks would probably refuse to give money to machines – certainly at first – the automobiles could work with virtual money such as bitcoins. According to Hearn, doing business with machines would be far more transparent for customers than doing business with people.

“You do not run the risk of being overcharged and there is no chance of misunderstandings.”

Robocorps, DAOs and DACs

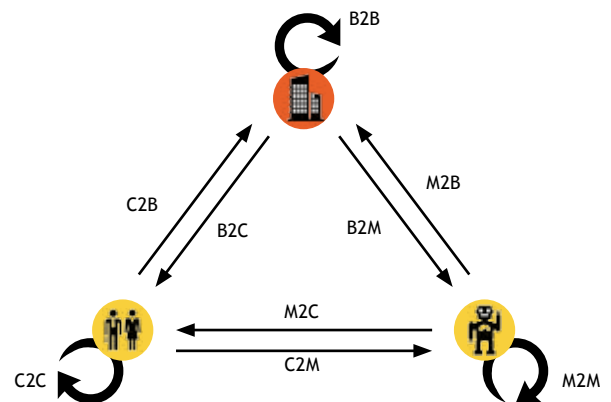
Hearn’s vision is a further interpretation of a broadly-based way of thinking in the world of blockchain and bitcoin: Decentralized Autonomous Organizations (DAOs) are going to play a more important role in society. Central authorities and hierarchies will be less and less essential. The machines will organize things far more efficiently among themselves. Such efficiency – where a robot company is no more than a commodity – approaches the new paradigm that is presented by Jeremy Rifkin

in his book *The Zero Marginal Cost Society*. The shared use of automobiles will reduce costs to an extremely high extent and transaction fees will decrease due to decentralized autonomous machine-made decisions. This is what Rifkin calls a collaborative commons.

A Decentralized Autonomous Organization (DAO), also called Fully Automated Business Entity (FAB) or Distributed Autonomous Corporation / Distributed Autonomous Company (DAC), is a decentralized network of autonomous agents that have a productive function, based on output maximization. These DAOs, FABs and DACs function without human intervention and are based on business rules that are said to be incorruptible.

“You become a stakeholder by buying ‘stock’ in the (DAO) company or being paid in that stock to provide services for the company. This stock may entitle you to a share of its ‘profits’, participation in its growth, and/or a say in how it is run.”

Stan Larimer,
president of Invictus Innovations



In addition to a business-to-business and business-to-consumer economy, the blockchain ensures an autonomous machine-to-machine future.

Thus every person or object is able to have a bank account and perform financial transactions. A world where a soft drink vending machine is an autonomous economic entity, with its own bitcoin bank account, responsible for the management and sale of its own stock, will be within the bounds of the possible. A machine that apart from autonomously selling soft drinks to consumers (M2C) can also place an order with suppliers (B2M). It can even place orders with consumers (C2M) to replenish the stock. IBM architect and blockchain expert Richard Gendal Brown formulates it as follows:

“On the Blockchain no one knows you are a refrigerator.”

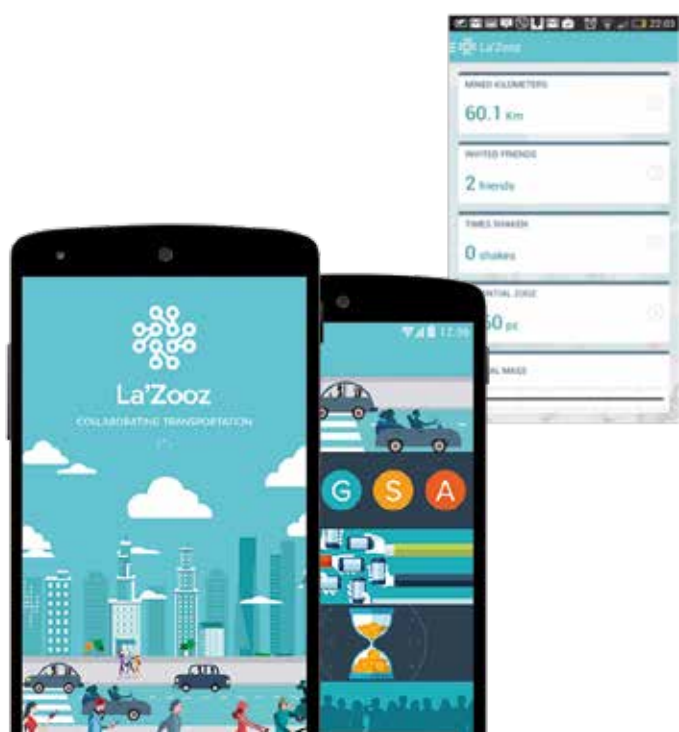
Taxis, government, employment agencies

The company La’Zooz is an example of a Decentralized Autonomous Organization. You can earn money (a “Zooz”) if you give someone a ride. A central register of the number of kilometers covered with the passenger is the basis of the system. It is a kind of Uber or Lyft, but without a central organ. La’Zooz works according to proof-of-movement. The smartphone with the La’Zooz app records the number of kilometers (the proof of movement). Each time more than some 20 kilometers have been covered, the driver earns a Zooz, which he can use if he needs a ride himself.

This need not necessarily stop at a soft drink machine, a fridge or an autonomous automobile. Corporate strategies can be wrapped in a block of code that can act autonomously in the economy after execution. But what also comes to mind here is employment agencies. When you need someone to do a job for you, you call the employment agency, explain what the temporary worker is expected to do and the agency will make sure that the ideal candidate turns up at the correct time. But how difficult is it to program these assignments in the form of an algorithm? The blockchain can also be the basis for a completely new model for self-employed professionals. The entrepreneurs who also launched Layar are working on it. Their new company is called Clock and aims to create a global Networked Autonomy, including a ledger where all value exchanges take place through the blockchain, such as micropayments for inspiration from one participant in the network to the other.

Decentralized Autonomous Governments

The above view may also apply to the government. The Bitcoin software can take over large parts of government duties such as issuing a birth certificate or passport, purchasing land and the voting process in elections. Melanie Swan terms this idea a DAS (Decentralized Autonomous Society). In conceptualizing the blockchain idea for the government, Bitnation has made more progress than others. Their slogan is “Blockchains, not borders.” According to founder Susanne Tarkowski Tempelhof, Bitnation can best be described as a Do It Yourself government. One of the pilot projects is the issuing of a blockchain ID. Attempts are underway in Australia to found the political party of the future with the help of the blockchain. Founder May Kay calls the party the Neutral Voting Bloc (NVB). In his view it is a “political app,” where the electorate learns from the digital rank and file how to vote. No hidden agendas anymore: in this way all political decisions are open and transparent via the blockchain. It is what Kay calls “true democracy.”



From non-Bitcoin quarters, incidentally, similar steps are being taken to change the government into a decentralized body. A fine example is the e-citizenship in Estonia. As from late 2014, foreigners have been able to apply for e-citizenship, which grants them access to all “digital services” in Estonia.

Virtual reality and the blockchain

Simon de la Rouviere, author of the book *The Blockchain: Mapping the Decentralized Future*, goes one step further. He envisages a future where people spend an increasing amount of time (and also earn their money) in a virtual world – such as Second Life, Eve: Online, and World of Warcraft – and argues that the blockchain can support all these alternative realities: “alternative realities as legitimate means to ‘live’ in different ways. By utilizing a combination of decentralized finances, real estate, trade, organizations, artificial intelligence and the law, it not only creates a decentralized basis for our current reality, but also for any other one.” Decentraland is such an example. It is an open-source initiative to build a decentralized virtual reality. Blockchain technology is used to claim and transfer land and keep a permanent record of ownership.

In conclusion: the new organization paradigm

The blockchain is a new organization paradigm. But the centralized autonomous organizations described above can hardly be called organizations. It is software with a high degree of autonomy. This looks like a revolutionary development: you no longer need businesses; algorithms do all the work. It is a “vanishing point” for organizations. It is perfectly consonant with Marc Andreessen’s statement: “Software is eating the world.” Everything that can be digitalized, will be digitalized, including organizations in all their aspects.

Seen through the lens of history, it is less revolutionary. The blockchain modus operandi is just a logical follow-up of computerization. After all, this means having machines do the work wherever possible. Since the internet we know that decentralization and peer-to-peer networks are strong links in this context. An important question that remains as yet unanswered is which organ-

izations are going to fill this gap and how strong they will be. “Who will own the future?” is the critical question we will have to ask ourselves. Will it be a democratic game or are we entering the Uber and Google era of the blockchain? The latter scenario is an extra consideration to be informed in good time about the possibilities and to start experimenting ourselves.

The future is decentralized

However, thinking in blockchain terms requires an entirely different mindset. Our traditional way of organizing our economy and society, “the old way of thinking,” is completely turned upside down thanks to the blockchain. The oft-heard statement “the future is decentralized” demands people and organizations to let go of the past, to think outside the box or, what’s more, to throw the box away and start anew, from scratch. Back to the drawing-board. And this is no easy matter. The thing is that companies are trying to preserve the problem to which they themselves were once the solution.

In 2004 the economists Frank Levy and Richard Murnane, in their book *The New Division of Labor*, wrote that autonomous cars could never become reality: “But executing a left turn against oncoming traffic involves so many factors that it is hard to imagine discovering the set of rules that can replicate a driver’s behavior [...]” Six years later, in October 2010, Google announced that they had been driving Toyota Priuses for quite a while that were fully autonomous. As we demonstrated in our first report, “Design to Disrupt: An executive introduction,” the pace of technological innovations is increasing. Companies would do well to embrace this acceleration with a view to enabling internal changes. Blockchain may still be in its infancy, but now is the time to get to work with it.

WRAP-UP: CONCLUSION AND CONSIDERATIONS FOR BUSINESS EXECUTIVES

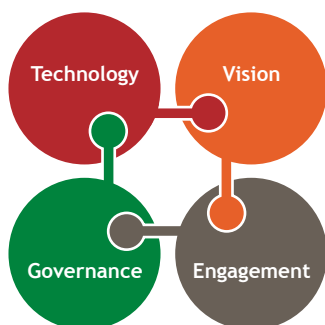
In our previous reports we presented the four-phase model from “Leading Digital,” as a line of action for digital disruption. We made an appeal to the CIOs and the business executives to steer the course of the digital change.

Leading Digital in Four Steps

Fuse IT and business to build digital skills and transform technology platforms

Create a shared transformative vision of the digital future

Establish strong digital governance to steer the course



Engage employees at scale to make vision a reality

With the blockchain, with all its technical details and imponderables, you may well ask yourself who will take charge of the Leading Digital campaign, and where that will be. “Nowhere, until we come to truly understand the technology” is the most likely answer. But how long are you prepared to wait before a transformative vision of your own digital future based on the blockchain is formulated?



Internet Yellow Pages: all addresses of the internet in one book.

Early days

The blockchain is a fascinating phenomenon. It calls to mind the internet before browsers came into being. In those days the whole internet fitted in a book (Internet Yellow Pages) listing all addresses you could go to. It was not until much later that we saw the arrival of the killer apps, Google and Facebook, and a long time after that of mobile banking and WhatsApp.

We are on the threshold of the blockchain's Netscape moment. The development of applications is in full swing, and what we are waiting for is the new Google or Spotify of this new network. If the basis really turns out to be so strong, we will forget the “strongest link” and all eyes will be on the applications themselves. It will then join the other building blocks of the modern IT landscape: SMOCT (Social, Mobile, Analytics, Cloud and Things), and in due course possibly B-SMOCT (“be smacked”). That's not saying which course you should take to reap the benefits and when the moment has arrived for you to jump onto the bandwagon.

Who is taking charge?

Expectations are that the new applications in your market will come from organizations that you have never heard of, such as Coinometrics, Helloblock, Kraken, BTC-Jam, BlockCypher, DigitalTangibleTrust, Bifubao and Bitpagos, to mention a few.

This also reflects the essence of the disruption as described in the executive introduction: the challengers are coming from outside your own sector and are not taken seriously at first. It is primarily the competitors offering seemingly crappy products and services that need to be guarded against. This is the lesson taught by innovation guru Clayton Christensen.

The telcos, the banks, the IT sector

That telcos want to be there as early as possible is probably because they are quicker to understand IT infrastructure innovations, it being their business. Telecom giant Orange is having talks with bitcoin/blockchain start-ups and supplies money for investments. George Nahon, CEO of Orange Silicon Valley (OSV):

“There’s something intriguing in this technology, so we want to be there as early as possible.”

But it is common knowledge that DoCoMo, T-Mobile and Perseus Telecom are also investing in this new technology. DoCoMo, from Japan, was a co-investor in January 2015, in the 75 million dollar injection in “coinbase.”

For the financial sector, and for the banks in particular, the inference is that they will follow the lead of UBS: open a Bitcoin Innovation Lab and invest seriously in it. The CIO of UBS, Oliver Bussmann, has already termed the blockchain the major potential disruptor for his market.

“The blockchain is the technology with the biggest potential to disrupt financial services and trigger massive simplification of banking processes and cost structure, changing not only the way we do payments but also the whole trading and settlement topic.”

Infosys goes one step further and in April 2015 it announced the integration of blockchain into its “core banking software” Finacle, especially with a view to making mobile money processing safer (Sood, 2015).

Acquiring more knowledge

For the majority of organizations that choose not to set up an innovation lab, but do intend to incorporate the blockchain into their core software or venture to invest money in start-ups, there is plenty to do: getting a better understanding of the blockchain and the bitcoin. This could be an individual action, or an assignment, if you like, for the reader of this report. We are pleased to provide the following list of ten suggestions in conclusion.



1. **Follow an online course.**

For example at Khan University: <https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it>

Or enroll for the MOOC of Nicosia University: <http://digitalcurrency.unic.ac.cy/free-introductory-mooc>

2. **Watch one of these six bitcoin documentaries:**

<http://www.coindesk.com/six-bitcoin-documentaries-watch>

3. **Open a bitcoin wallet** at www.coinbase.com and buy a bitcoin.

4. **Add bitcoin to your Microsoft account** and buy a game.

To add money to your Microsoft account with Bitcoin:

1. Sign up your Microsoft account for **Microsoft account – Payment and invoicing**.
2. Select **Payment options > Microsoft account > Exchange Bitcoins**.
3. Select the amount you wish to add and click **Next**.
4. Check the Bitcoin amount needed and complete the transaction within 15 minutes with your digital wallet.
 - On your computer: select **Paying with Bitcoin** and pay with your Bitcoin wallet on the same device.
 - On your smartphone: scan the QR code that is shown on the page to pay via your mobile Wallet app.
 - If your wallet is on another device, you can copy the receiver's address and the BTC amount to the wallet on your device or the web, and continue to make the purchase.

5. **Make a micropayment** via ChangeTip.com, the “love button” for the internet.

6. **Install a mining program** and read the “Beginner’s Guide to Mining Bitcoins”: <http://startbitcoin.com>

7. **Follow a transaction** on the blockchain: www.blockchain.info

8. **Build your own smart contract** on Ethereum within an hour: <http://forum.ethereum.org/discussion/1402/how-to-get-started-your-first-dapp-under-one-hour>

9. Map out the existent bitcoin/blockchain knowledge among your staff and **organize a blockchain night**.

10. Examine your own organization from a decentralized point of view. Which centralized parts can be replaced with decentralized blockchain solutions?



GLOSSARY

Altcoin – Bitcoin is the best-known cryptocurrency. There are, however, hundreds of other alternative digital currencies on the market, generally with slightly different properties. An overview of all altcoins can be found on the website Map of Coins.

Bitcoin – Bitcoin is a form of electronic money and also the name of the open-source software designed to use it. It is one of the first implementations of a concept called cryptocurrency or cryptographic money, which was first outlined in 1998 by Wei Dai on the Cypherpunks mailing list, and was implemented in 2009 by Satoshi Nakamoto (pseudonym of an unknown person or group).

Blockchain – A public decentralized ledger that records all bitcoin transactions while simultaneously recording them on all computers in that network.


Cryptomoney – Cryptomoney (or cryptocurrency) is a kind of digital currency that is often used as an alternative money system for the regular currencies. Cryptomoney is based on cryptography (encryption systems) and goes hand in hand with a proof-of-work scheme, which is used to create the money, to authenticate it and deal in it. In effect, cryptomoney is a block of encrypted code in which the transactions are stored. Every time a transaction takes place, the code is supplemented or changed with a new encrypted block of code.

DACs (Decentralized Autonomous Organizations) or Robocorps – This is a new type of companies. It concerns software that is run on top of the Bitcoin blockchain and operates autonomously.

Ethereum – Ethereum is a combination of a decentralized mining network and the development of a software platform that will enable people to create their own altcoins with countless properties. But in addition to a mining network it is also a kind of operating system to run your cryptocurrency “apps.” People write those applications with the help of a programming language designed by the Ethereum team. As soon as the application is completed, they broadcast it on the system in the form of a “contract.” A contract is a computerized agent on the Ethereum network together with an Ethereum address. It can receive and send transactions and stores the balances of these transactions.

Hash – A hash function turns an arbitrary long row of ciphers into a unique “signature” of 128 or 256 bits (~ 40 or 80 decimal ciphers). A good hash makes it impossible to reconstruct the original row or even part of it. A hash looks as follows: 1NkbuV2VLU2u8s1Y2kSA3YqXBb1ty6x-6Up

Public key / Private key – The protection of Bitcoin transactions is based on a cryptographic principle of public keys and private keys. The private key is linked to the public key, but cannot be accessed by someone having the public key. With the private key you can prove that the public key is yours. To transfer bitcoins, you need a unique key (private key) to make a digital signature that demonstrates you are the owner. Bitcoin addresses are derived from the public key. They consist of a combination of usually 34 ciphers and letters, beginning with a 1, with which one particular private key is associated. It can be used to sign transactions to prove that you own the bitcoins to be forwarded. A bitcoin address is generated arbitrarily. This can be done because there are so many possible bitcoin addresses that the chance of generating a double bitcoin is considered negligible. To give you an idea: the number of bitcoin addresses is roughly comparable to the number of atoms on earth (one grain of sand contains many more atoms than one million billion!).



Mining – The bitcoin needs to be “mined” virtually. Every day a certain amount is released to people mining the bitcoin. This is done by using the computing power of computers. Meanwhile, various groups of people are active on the internet who are pooling the computing power while mining – in so-called mining pools – with a view to scanning for the electronic money.

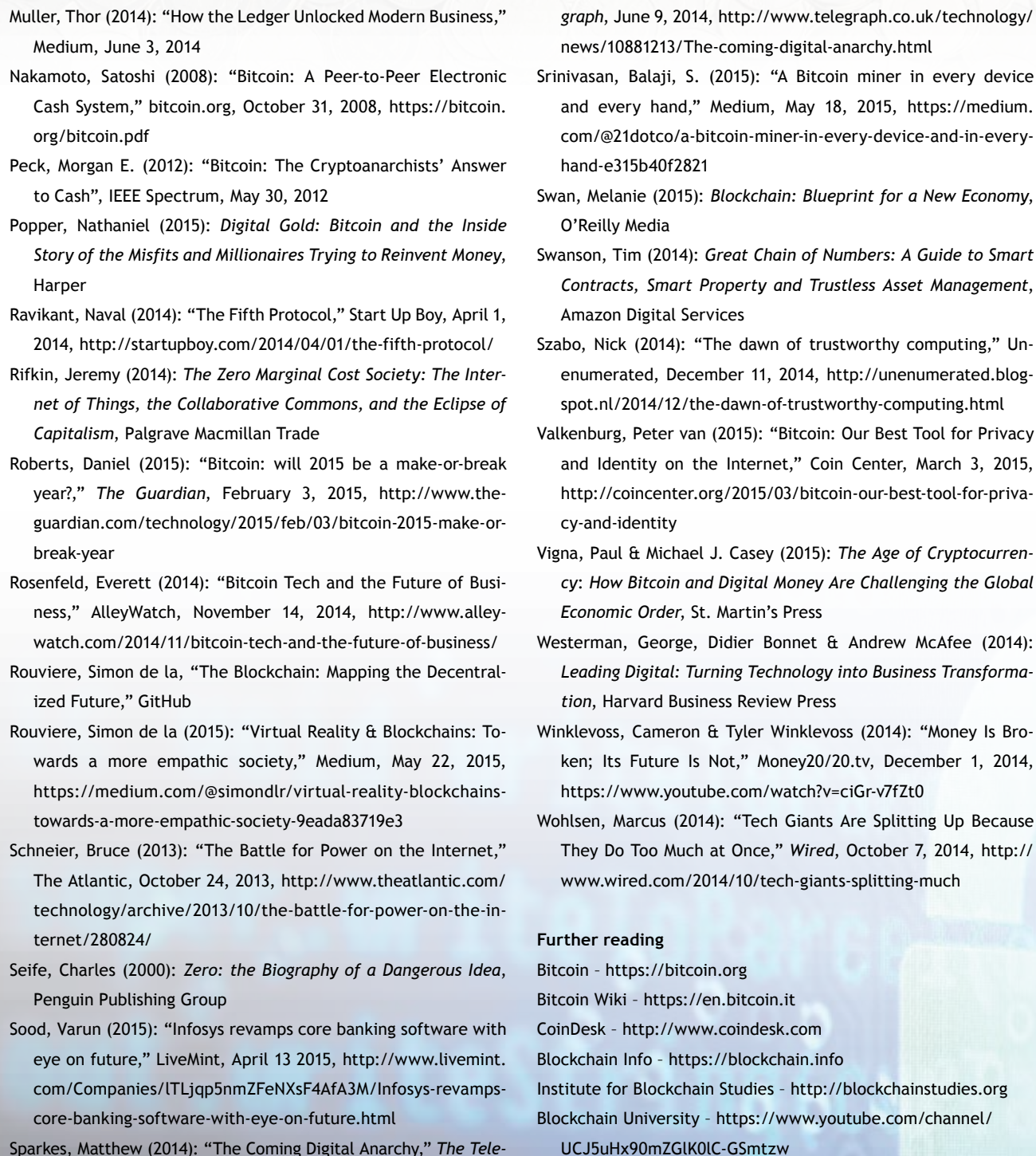
Sidechains – New chains that zero in on the core structure of the blockchain, and enable developers to add features and functionality to the system without modifying the core. The sidechain is nothing but a sandbox environment on the blockchain. This way people are able to experiment more quickly and the system is more flexible.

Wallet – A wallet can be compared to a digital purse that you can put money in and take out of to make payments. With a wallet you can see how many bitcoins you own, you can transfer them or pay with them. Contrary to popular belief, a wallet does not contain bitcoins. What a wallet does contain are the private keys. These grant access to your bitcoins. Without these keys there is no way of getting at anything. It is therefore essential to store your wallet and the private keys in it in a safe place.

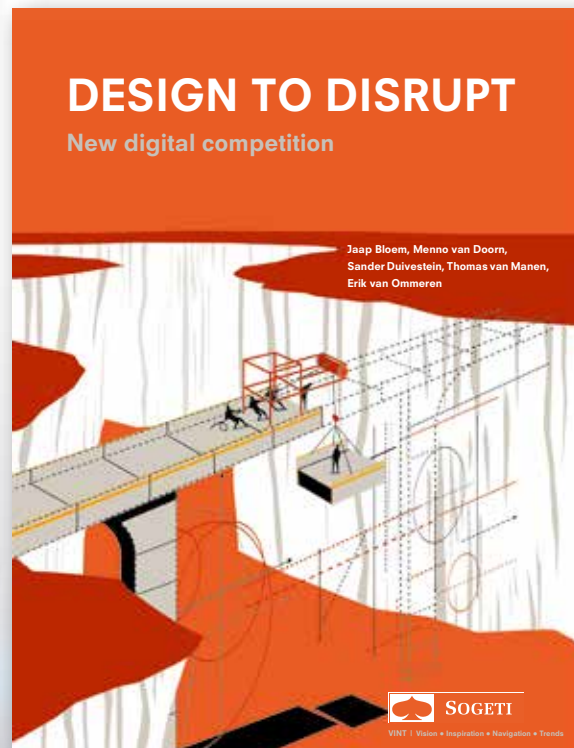
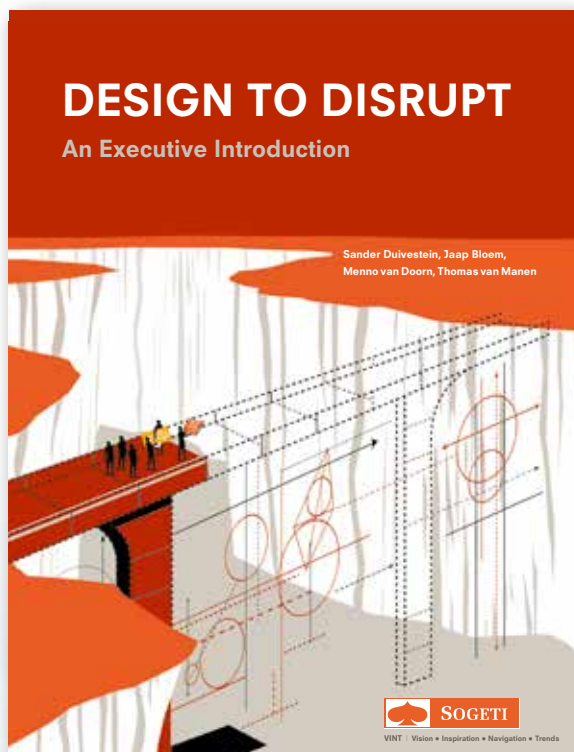
LITERATURE

- Andreessen, Marc (2011): "Why Software Is Eating the World," *The Wall Street Journal*, August 20, 2011, <http://www.wsj.com/articles/SB10001424053111903480904576512250915629460>
- Antonopoulos, Andreas (2014a): "Bitcoin and the Evolution of Money As a Content Type," BitcoinSouth, December 8, 2014, <http://vimeo.com/113833922>
- Antonopoulos, Andreas (2014b): *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*
- Arnold, Martin (2014): "Barclays' Antony Jenkins Calls End of Universal Banking," *Financial Times*, December 17, 2014, <http://www.ft.com/intl/cms/s/0/ef588b42-860a-11e4-b248-00144feabdc0.html>
- Assange, Julian (2014): "Bitcoin is Much More Than Just a Currency," The Nantucket Project, October 3, 2014, https://www.youtube.com/watch?v=MaB3Zw5_p9c
- Back, Adam, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón & Pieter Wuille (2010): "Enabling Blockchain Innovations with Pegged Sidechains," October 22, 2010, <http://www.blockstream.com/sidechains.pdf>
- Badev, Anton & Mathew Chen (2014): "Bitcoin: Technical Background and Data Analysis," FED, October 7, 2014, http://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf?p=cite_@inthepixels
- Bartlet, Jimmy (2014): "Soon the Internet Will Be Impossible to Control," *The Telegraph*, December 10, 2014, <http://www.telegraph.co.uk/technology/internet/11284538/Soon-the-internet-will-be-impossible-to-control.html>
- Beikverdi, Alireza (2015): "Blockchain Technology Could Have Prevented Louisiana's Deadly Bacteria Leak," *Coin Telegraph*, March 3, 2015, <http://cointelegraph.com/news/113595/blockchain-technology-could-have-prevented-louisianas-deadly-bacteria-leak>
- Bloem, Jaap, Menno van Doorn, Sander Duivesteyn & Thomas van Manen (2015): "Design to Disrupt: New digital competition"
- Brody, Paul & Veena Pureswaran (2014): "Device Democracy – Saving the Future of the Internet of Things," IBM, September, 2014, <http://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF>
- Cohen, David & William Mougayar (2015): "After the Social Web, Here Comes the Trust Web," TechCrunch, January 18, 2015, <http://techcrunch.com/2015/01/18/after-the-social-web-here-comes-the-trust-web>
- Conner, F., D. Velicanu & S. Yakubov (2014): 'A Decentralized Public Key Infrastructure with Identity Retention', <https://eprint.iacr.org/2014/803.pdf>
- Custodio, Nik (2013): "Explain Bitcoin Like I'm Five," Medium, December 12, 2013, <https://medium.com/@nik5ter/explain-bitcoin-like-im-five-73b4257ac833>
- Duivesteyn, Sander (2015a): "Bitcoin Is the World's Most Dangerous Idea," The Next Web, April 16, 2015, <http://thenextweb.com/insider/2015/04/16/bitcoin-is-the-worlds-most-dangerous-idea/>
- Duivesteyn, Sander (2015b): "Why Bitcoin Is Changing How Banks Do Business," The Next Web, March 3, 2015, <http://thenextweb.com/insider/2015/03/03/why-bitcoin-is-changing-how-banks-do-business/>
- Duivesteyn, Sander & Patrick Savalle (2014): "Bitcoin: It's the Platform, Not the Currency, Stupid!," The Next Web, February 15, 2014, <http://thenextweb.com/insider/2014/02/15/bitcoin-platform-currency/>
- Effinger, Anthony (2014): "Marc Andreessen on Finance: 'We Can Reinvent the Entire Thing'," Bloomberg, October 7, 2014, <http://www.businessweek.com/news/2014-10-07/andreessen-on-finance-we-can-reinvent-the-entire-thing>
- Gleeson-White, Jane (2012): *Double Entry: How the Merchants of Venice Shaped the Modern World – and how Their Invention Could Make or Break the Planet*, Allen & Unwin
- Hayase, Nozomi (2014): "The Blockchain and the Rise of Networked Trust," CoinDesk, November 22, 2014, <http://www.coindesk.com/blockchain-rise-networked-trust>
- Hearn, Mike (2013): "Future of Money," Turing Festival, September 28, 2013, <https://www.youtube.com/watch?v=Pu4PAMFPo5Y>
- Higgins, Stan (2015): "IBM Reveals Proof of Concept for Block-

- 
- chain-Powered Internet of Things,” CoinDesk, January 17, 2015, <http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/>
- Irrera, Anna (2014): “UBS CIO: Blockchain Technology Can Massively Simplify Banking,” *Wall Street Journal*, October 27, 2014, <http://blogs.wsj.com/digits/2014/10/27/ubs-cio-block-chain-technology-can-massively-simplify-banking/>
- Isaacson, Walter (2014): “Big Idea 2015: The Coming Micropayment Disruption,” *TIME*, December 22, 2014, <http://time.com/3636720/2015-micropayment-disruption/>
- Ismail, Salim, Mike Malone & Yuri van Geest (2014): “Exponential Organizations (ExO),” Singularity University
- Kaplan, Robert. S. (2000): *The Nothing that Is: A Natural History of Zero*, Oxford University Press
- Kearns, Jeff (2013): “Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value,” Bloomberg, December 4, 2013, <http://www.bloomberg.com/news/2013-12-04/greenspan-says-bitcoin-a-bubble-without-intrinsic-currency-value.html>
- Kelion, Leo (2015): “Could Driverless Cars Own Themselves?,” BBC, February 16, 2015, <http://www.bbc.com/news/technology-30998361>
- King, Brett (2014): “Why the Facebook of Banking Won’t Have a Charter,” LinkedIn, December 28, 2014, <https://www.linkedin.com/pulse/why-facebook-banking-wont-have-charter-brett-king>
- Koenraadt, Mathijs (2014a): “The Protocol Wars: Bitcoin and the Internet of Value,” Medium, October 10, 2014, <https://medium.com/bitcoin-and-society/the-protocol-wars-bitcoin-and-the-internet-of-value-badc174bae4d>
- Koenraadt, Mathijs (2014b): “The Decentralize Everything Manifesto,” LinkedIn, November 25, 2014, <https://www.linkedin.com/pulse/20141125151550-259980788-the-decentralize-everything-manifesto>
- Kopstein, Joshua (2013): “The Mission to Decentralize the Internet,” *The New Yorker*, December 13, 2013, <http://www.newyorker.com/online/blogs/elements/2013/12/the-mission-to-decentralize-the-internet.html>
- Krugman, Paul (2013): “Bitcoin Is Evil,” *New York Times*, December 28, 2013, <http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/>
- Lanier, Jaron (2014): “The Myth of AI,” Edge, November 14, 2014, <http://edge.org/conversation/the-myth-of-ai>
- Lent, Adam (2014): “Farewell Corporate Power: How the Rise of the Blockchain Could Change Everything,” City A.M., December 16, 2014, <http://www.cityam.com/205708/farewell-corporate-power-how-rise-blockchain-could-change-everything>
- Levy, Frank & Richard J. Murnane (2005): *The New Division of Labor: How Computers Are Creating the Next Job Market*, Princeton University Press
- Ludwin, Adam (2014): “Why Bitcoin Apps and Bitcoin Speculators Need Each Other,” Chain, December 2014, <http://blog.chain.com/post/105287860141/why-bitcoin-apps-and-bitcoin-speculators-need-each>
- Monegro, Joel (2014): “The Bitcoin Application Stack”, November 25, 2014, <http://joel.mn/post/103546215249/the-blockchain-application-stack>
- Morozov, Evgeny (2013): *To Save Everything, Click Here: The Folly of Technological Solutionism*, Penguin
- Morris, David (2015): “Are We Ready for Companies That Run Themselves?,” Aeon, January 26, 2015, <http://aeon.co/magazine/technology/are-we-ready-for-companies-that-run-themselves/>
- Mougayar, William (2014a): “Blockchain Apps: Moving from the Jungle to the Zoo,” Startup Management, December 30, 2014, <http://startupmanagement.org/2014/12/30/blockchain-apps-moving-from-the-jungle-to-the-zoo>
- Mougayar, William (2014b): “The Blockchain Is the New Database, Get Ready to Rewrite Everything,” Startup Management, December 27, 2014, <http://startupmanagement.org/2014/12/27/the-blockchain-is-the-new-database-get-ready-to-rewrite-everything/>
- Mougayar, William (2015): “The Crypto-Technology and Bitcoin Landscape,” Startup Management, March 3, 2015, <http://startupmanagement.org/2015/03/03/the-crypto-technology-and-bitcoin-landscape/>

- 
- Muller, Thor (2014): "How the Ledger Unlocked Modern Business," Medium, June 3, 2014
- Nakamoto, Satoshi (2008): "Bitcoin: A Peer-to-Peer Electronic Cash System," bitcoin.org, October 31, 2008, <https://bitcoin.org/bitcoin.pdf>
- Peck, Morgan E. (2012): "Bitcoin: The Cryptoanarchists' Answer to Cash", IEEE Spectrum, May 30, 2012
- Popper, Nathaniel (2015): *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*, Harper
- Ravikant, Naval (2014): "The Fifth Protocol," Start Up Boy, April 1, 2014, <http://startupboy.com/2014/04/01/the-fifth-protocol/>
- Rifkin, Jeremy (2014): *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism*, Palgrave Macmillan Trade
- Roberts, Daniel (2015): "Bitcoin: will 2015 be a make-or-break year?," *The Guardian*, February 3, 2015, <http://www.theguardian.com/technology/2015/feb/03/bitcoin-2015-make-or-break-year>
- Rosenfeld, Everett (2014): "Bitcoin Tech and the Future of Business," AlleyWatch, November 14, 2014, <http://www.alleywatch.com/2014/11/bitcoin-tech-and-the-future-of-business/>
- Rouviere, Simon de la, "The Blockchain: Mapping the Decentralized Future," GitHub
- Rouviere, Simon de la (2015): "Virtual Reality & Blockchains: Towards a more empathic society," Medium, May 22, 2015, <https://medium.com/@simondlr/virtual-reality-blockchains-towards-a-more-empathic-society-9eada83719e3>
- Schneier, Bruce (2013): "The Battle for Power on the Internet," The Atlantic, October 24, 2013, <http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/>
- Seife, Charles (2000): *Zero: the Biography of a Dangerous Idea*, Penguin Publishing Group
- Sood, Varun (2015): "Infosys revamps core banking software with eye on future," LiveMint, April 13 2015, <http://www.livemint.com/Companies/ITLjqp5nmZFENXsF4AfA3M/Infosys-revamps-core-banking-software-with-eye-on-future.html>
- Sparkes, Matthew (2014): "The Coming Digital Anarchy," *The Telegraph*, June 9, 2014, <http://www.telegraph.co.uk/technology/news/10881213/The-coming-digital-anarchy.html>
- Srinivasan, Balaji, S. (2015): "A Bitcoin miner in every device and every hand," Medium, May 18, 2015, <https://medium.com/@21dotco/a-bitcoin-miner-in-every-device-and-in-every-hand-e315b40f2821>
- Swan, Melanie (2015): *Blockchain: Blueprint for a New Economy*, O'Reilly Media
- Swanson, Tim (2014): *Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management*, Amazon Digital Services
- Szabo, Nick (2014): "The dawn of trustworthy computing," Unenumerated, December 11, 2014, <http://unenumerated.blogspot.nl/2014/12/the-dawn-of-trustworthy-computing.html>
- Valkenburg, Peter van (2015): "Bitcoin: Our Best Tool for Privacy and Identity on the Internet," Coin Center, March 3, 2015, <http://coincenter.org/2015/03/bitcoin-our-best-tool-for-privacy-and-identity>
- Vigna, Paul & Michael J. Casey (2015): *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*, St. Martin's Press
- Westerman, George, Didier Bonnet & Andrew McAfee (2014): *Leading Digital: Turning Technology into Business Transformation*, Harvard Business Review Press
- Winklevoss, Cameron & Tyler Winklevoss (2014): "Money Is Broken; Its Future Is Not," Money20/20.tv, December 1, 2014, <https://www.youtube.com/watch?v=ciGr-v7fZt0>
- Wohlsen, Marcus (2014): "Tech Giants Are Splitting Up Because They Do Too Much at Once," *Wired*, October 7, 2014, <http://www.wired.com/2014/10/tech-giants-splitting-much>
- Further reading**
- Bitcoin - <https://bitcoin.org>
- Bitcoin Wiki - <https://en.bitcoin.it>
- CoinDesk - <http://www.coindesk.com>
- Blockchain Info - <https://blockchain.info>
- Institute for Blockchain Studies - <http://blockchainstudies.org>
- Blockchain University - <https://www.youtube.com/channel/UCJ5uHx90mZGk0lC-GSmtzw>

This is the third report in a series of four publications on the subject of Design to Disrupt. The first two reports can be downloaded at <http://labs.sogeti.com/downloads>. Here, among other things, you can also find the VINT reports on the Internet of Things and Big Data, and our book on cyber security.





Design to Disrupt

About VINT labs.sogeti.com

VINT, the Sogeti trend lab and part of SogetiLabs, provides a meaningful interpretation of the connection between business processes and new developments. In every VINT publication, a balance is struck between factual description and the intended utilization. VINT uses this approach to inspire organizations to consider and use new technology.

VINT research is done under the auspices of the Commission of Recommendation, consisting of • H. Wesseling (chairman), Management Advisor ICT • H.W. Broeders, Chairman of the Board Jaarbeurs Holding N.V. • P. Dirix, Managing Director Operations NS Reizigers • F.M.R. van der Horst, Head of CIO Office ABN AMRO Bank N.V. • D. Kamst, Chief Executive Officer Klooker • Prof. dr. ir. R. Maes, Professor of Information & Communication Management Academy for I & M • P. Morley, Member Supervisory Board TLS • T. van der Linden, Group Information Officer Achmea • E. Schuchmann, Chief Information Officer Academisch Medisch Centrum • K. Smaling, Chief Information Officer Aegon Nederland N.V. • W.H.G. Sijstermans, CIO a.i. Nederlandse Zorgautoriteit (NZa) • J. Tas, Chief Executive Officer Philips Healthcare Informatics Services Solutions • M. Boreel, Chief Technology Officer Sogeti Group • J.P.E. van Waayenburg, Chief Executive Officer Sogeti Group • P.W. Wagter, Chief Executive Officer Sogeti Nederland B.V.

About SogetiLabs labs.sogeti.com

SogetiLabs is a network of over 120 technology leaders from Sogeti worldwide. SogetiLabs covers a wide range of digital technology expertise: from embedded software, cyber security, simulation, and cloud to business information management, mobile apps, analytics, testing, and the Internet of Things. The focus is always on leveraging technologies, systems and applications in actual business situations to maximize results. Together with the Sogeti trend lab VINT, SogetiLabs provides insight, research, and inspiration through articles, presentations, and videos that can be downloaded via the extensive SogetiLabs presence on its website, online portals, and social media.

About Sogeti www.sogeti.com

Sogeti is a leading provider of technology and software testing, specializing in Application, Infrastructure and Engineering Services. Sogeti offers cutting-edge solutions around Testing, Business Intelligence & Analytics, Mobile, Cloud and Cyber Security, combining world class methodologies and its global delivery model, Rights-hore®. Sogeti brings together more than 20,000 professionals in 15 countries and has a strong local presence in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Cap Gemini S.A., listed on the Paris Stock Exchange.

