Edition No. 17

Blockchain: Like a Hurricane?

bergsicht

CHAPTER 1

My antique "blockchain"

Once a year, when the candles have been lit on the Christmas tree and the family has settled down in a reflective mood after a concerted rendition of "Silent Night", the *pater familias* traditionally takes down a well-thumbed, weighty tome from the bookcase – an 18th-century edition of Luther's translation of the Bible. Having survived the Enlightenment, the French Revolution, the emigration of our liberal German forebears to Switzerland and two world wars in the 20th century unscathed, it has been handed down through more than a dozen generations. The successive stewards of this amusingly (and sometimes startlingly) illustrated volume of Holy Writ are recorded on the inside cover, initially in a barely legible Teutonic hand and then subsequently in Helvetian block capitals. The Bible was invariably passed on from one generation to the next on the occasion of a wedding, no doubt in the expectation that its bestowal would bless the new union with children – an expectation that has without exception been met to this day.

The aforementioned Luther Bible is a blockchain; or more precisely, the uninterrupted entries listing the owners *closely resemble* a blockchain, and we shall be returning to this image throughout this *bergsicht*. "Blockchain" is a term currently on everybody's lips. Indeed, the relevant magazines and newspapers – from *The Economist* through the *Wall Street Journal*, the *Neue Zürcher Zeitung* and the *Schweizer Bank* to the Tamedia Group's *Das Magazin* – are currently awash with articles on the subject. What all these column inches have in common is that the complexity of the material leaves them entirely at sea and many facets of the technology remain unexplored. The same old examples are rehashed to initiate readers into the arcana of the cryptography underpinning the blockchain concept; an abstruse blockchain vernacular has already grown up around a high priesthood of latter-day *illuminati*, excluding unsuspecting outsiders and choking off naïve enquiries. The other factor common to all these articles is a preoccupation with predicting the next structural crisis, which – in the wake of the upheavals wrought by Web 1.0 and 2.0 – is set to send many, many more jobs to the scrapheap.

In this *bergsicht*, we hope to avoid writing a single incomprehensible sentence about blockchains – quite a challenge! Moreover, we wish to get to grips with the topic – from a technological point of view initially, and then by addressing its anticipated social, political and economic consequences in particular. As these are uncharted waters, and future investment will be required to open up the *terra incognita* we encounter, we shall conclude with a few ideas for potential asset positioning vis-à-vis the blockchain phenomenon. This edition of *bergsicht* features a glossary that may be useful for readers wishing to explore the subject in greater depth.

But let's return to the handwritten entries in the Luther Bible. These document which member of the family in question was the legal owner of the volume at any given time. In blockchain jargon, the wedding date is a "timestamp" through which the transfer of title to a new name (a "public key" that is essentially accessible to all) is unambiguously confirmed. These days, if a descendant is called upon to prove lawful ownership, he/she might resort to a DNA test, the result of which will confirm legal title in a manner that is impossible to counterfeit. The line of descent would be something like a security lock that can be opened with the key of the DNA fingerprint (the "private key"). There is hardly likely to be a second key of this kind, as it is extremely improbable that two individuals would have the same DNA, and less likely still that that implausible other individual might turn up within any useful period of time to contest ownership on his/her own behalf. The timestamp is validated when the family members present on the wedding day forever hold their peace and confirm their consent to bequeathing the Luther Bible.

So what is a blockchain? A system that acquires evidential value to regulate a property regime on the strength of its seamless record-keeping. That actually says it all. Or almost all.

CHAPTER 2

Property is precarious

"Property" – that is, the proprietary relationship between a person and an object defining exclusive possession and use – requires some explanation at this juncture. Except in the rare event that a person is literally sat inside or atop his property ("possess" is etymologically derived from *potis*, "able, capable" and *sedeo*, "sit"), defending it on his own mettle if required, the proprietary relationship between person and object obtains only within the context of a *third-party authority* that is empowered to *guarantee* such ownership. In most systems of jurisprudence around the world, a distinction is made between "property" and "possession", as to "have" and to "hold" are not necessarily always coterminous. The Bible in the bookcase of the *pater familias* is undoubtedly both the latter's property and in his possession; he may, in his capacity as proprietor, exercise his rights in the matter, viz. to have direct use (*usus*) and beneficial use (*usus fructus*) of the property, or to dispose of it – by selling it, for example, or even destroying it (*abusus*). A possessor who is not a proprietor does not enjoy the last of these rights; you may not simply sell or throw away a borrowed book that happens to be in your possession. Common law uses simple principles that closely map the practicalities of everyday life to regulate the relationship between people and real goods that is fundamental to peaceful co-existence. These include, for example, the assumption that possession is nine points of the law, not to mention the principle that a guaranteed right to dispose – the legality of an object's acquisition by a previous owner – may be presumed. In the specific case of a banknote, the highways and byways through which previous proprietors or possessors came by that little slip of paper are of little or no interest to us – although many of the notes in our wallets presumably have a story or two to tell ...

Thanks to these and other "default rules" (i.e. legal presumptions and fictions), property as it manifests itself in our everyday lives turns out to be a largely perfunctory matter. You get into your car every day without a second thought, have the enjoyment and the benefit of it, and eventually you may even run it into the ground. Not a day goes by that we don't blithely accept coins and banknotes and pass them on again; and how many women would give even a moment's consideration to whether their inherited earrings fall foul of UNESCO's convention on the Illicit Trafficking of Cultural Property? Nonetheless, property cannot survive without being anchored in a regime that, by virtue of its *superordinated* authority, is capable of asserting the *private* rights of a person to control and dispose of an object – it must be possible to secure and defend property, otherwise the concept is worthless, and defence of property using one's own devices or weapons is not a viable approach in a complex, civilised society. For practical, everyday purposes, the legality of property and the authenticity of an object – i. e. the potential problems surrounding the right of disposal mentioned above – require the existence of *regulative institutions* to ensure that society's expectations and the state of affairs as it effectively stands can largely overlap. This is how we understand the term "institution". Thanks to the good offices of the land registry and the notary public, it would never occur for one second to anyone buying a parcel of land that some unknown third party might contest ownership of the lot; expectations and the actual state of affairs are thus congruent. Even in the somewhat more cavalier automobile trade, there is generally a certain level of trust between the contracting parties, provided the dealer has earned this trust as a quasi-institution through previous good conduct. Disputes over transfer of title are relatively rare, even in the motor trade. Again, expectations and reality largely mesh and the institutions providing and regulating the property regime take care of business.

We are only dimly aware of the extent to which we make use of – and take for granted the existence of – functioning institutions. Our ownership of a monetary asset, for instance, is rendered credible by a whole concatenation of institutions – and this credibility extends not only to ourselves, but also to third parties with whom we have entered into a pecuniary relationship (e. g. through settling an invoice by means of a bank transfer). The links in this chain of institutions take the form of banks, monetary authorities and clearing houses, and these institutions are themselves guided and monitored by meta-institutions such as the Swiss Financial Market Supervisory Authority (FINMA) or the Bank for International Settlements (BIS) in order to buttress their *bona fides*. Ultimately, all we have is a figure on a bank statement but we feel like owners because we *trust* that the chain of institutions is credible enough to *guarantee ownership to us*.

We can put this credibility to the test on a daily basis – when we convert this posited property into real value (by purchasing goods, for example, or paying bills), when we use money to buy securities, or when we convert it into other currencies. This uncontested *convertibility* represents a constantly reiterated, implied *proof* of this credibility, and of the faith we place in the institution. If this convertibility should nonetheless be interrupted, as happened in the Cyprus and Greece crises, a property regime based on trust and underwritten by institutions can implode in an uncontainable manner. Only the guarantee extended by Angela Merkel was able to prevent such an implosion during the darkest days of the eurozone debt crisis. Though there were no funds to cover her cheque, on that occasion the Federal Chancellor succeeded in preventing a Europe-wide bank run on the strength of her institutionally predicated authority alone.

The less tangible an object is – let's compare the aforementioned Luther Bible with a futures contract for pork bellies, maturing at a fixed price in three months, say – the more important the role played by institutions in regulating property rights proves to be. This is especially true for that most virtual of "objects", *money*. It reflects *nothing but trust* – trust that is earned (or not) on a daily basis through the good conduct of responsible parties and reinforced (or not) through constant and uncontested convertibility into less virtual items. Trust behaves in an inconstant and discontinuous manner; breach of its principles can long go undiscovered or unremarked, but its collapse is sudden and devastating for the institutions and stakeholders relying upon it. This explains the steady stream of stability crises centred on institutions and their supposed guardians, who have silently and methodically exploited and eroded that trust. Once confidence is lost, it usually takes a very long time indeed to restore.

Institutions have their price. Recourse to a third party authority – in other words, an institution – to guarantee property is *expensive*. These costs may be direct fees (such as those levied by banks, custodians or clearing houses) or "charges" that may be exacted clandestinely, in that institutions allow a tiny, imperceptible "rip" to be torn in their credibility, ultimately causing a stability crisis that is then construed as *force majeure*; similarly, costs may arise because institutions permit or cause some kind of dilution of property – such as through inflation or financial repression (negative interest rates), which, of course, ultimately amount to the same thing. The institutions involved in guaranteeing property will, in addition, be able (or obliged) to work more or less hand in glove with the citizen's largest stakeholder, the tax authorities, to provide the latter with suitable access points for legal expropriation through taxation.

The four-fold cost burden with which the institution is freighted – fees to cover its own costs and generate a profit where appropriate, stability crises, a tendency towards dilution, and the provision of access points for the fiscus – is crying out for a system that would, ideally, allow *property to be released from its institutional anchoring*. The reason for this is simple: institutionally underwritten property is too expensive and ultimately too insecure; *game theory predicts* that a creeping *betrayal of the property owner* by the authority guaranteeing the property is *inevitable*. In edition 14 of *bergsicht* ("Cash, Credibility and Coercion"), we outlined how the central banks' highly questionable policy of financing their own country's (and/or their own currency area's) public debt might accelerate the need for such a wholesale abandonment of the "institution". With the rise of the blockchain, we now see this perspective vindicated. We may conclude that the way property is administered – institutionally, as described above, through actual physical possession, or alternatively, in future (as will be outlined), using algorithmic proof – will be decided by the price of one or other of these options.

CHAPTER 3

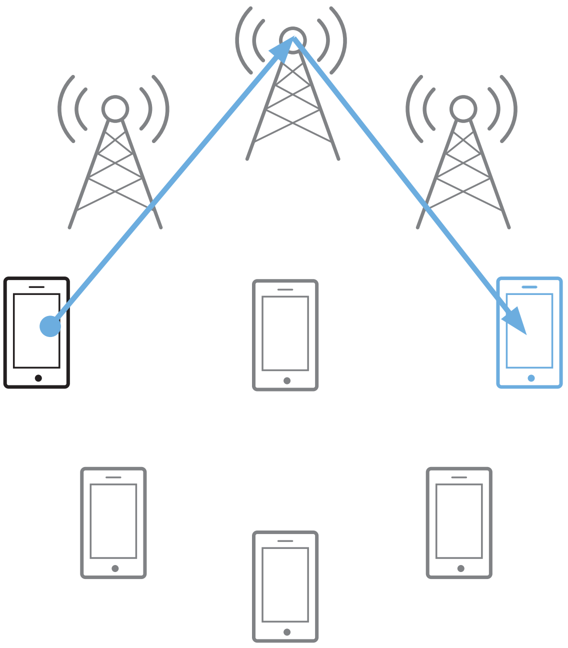
Encryption and decentralisation as stabilising factors

Thanks to technology, *institutions* – traditionally superordinated and thus, by dint of operating for a multiplicity of individuals, *centralised systems* – are being turned inside out by the most extreme form of de-centralisation (in the sense of Robert Nef's notion of "non-centralisation"). To illustrate this, let's take an example that has little or nothing to do with the blockchain technology we shall describe below. Until now, we have habitually purchased our smartphones from a large service provider such as Swisscom, Deutsche Telekom or Vodafone, subscribing to a minutes plan and making use of the masts and equipment belonging to and operated by these *carriers* to conduct our conversations. These carriers are hefty institutions that make fat profits, and for the moment at least, we are forced to work with them;

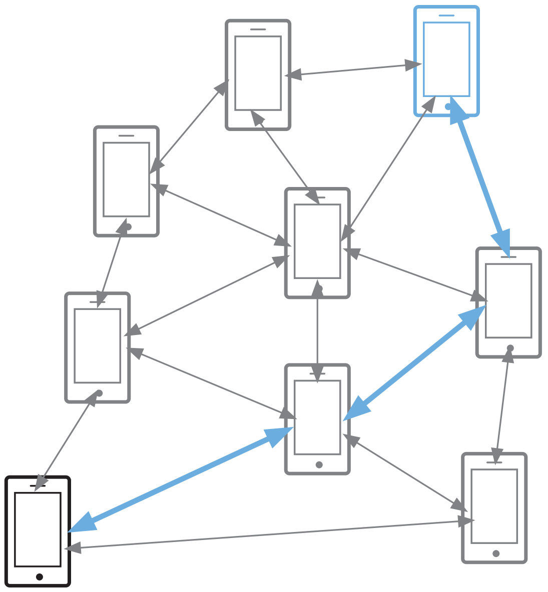
there is no way round centralised bundling and transmission of all those conversations.

One option that is conceivable, and technically quite feasible, is a telephony system that operates exclusively across the millions of individual aerials within the mobile phones themselves, i.e. that can dispense with carriers. Each of us would thus become a mini-carrier, as it were, by providing an antenna service for third parties while also making use of such a service from others. The high concentration of mobile telephones would allow the bits of the conversation to skip from mobile to mobile at lightning speed until they reach their destination. Swisscom, Sunrise and Vodafone would be forced to hang up their boots and/or at best would be reduced to selling hardware in glorified kiosks. Pure fantasy? Not really. We see this as only a matter of time; "value" that is technologically no longer required is not "added value" and can be discarded. Such was the fate that befell candle-makers and match producers at the advent of electric light, coachmen when we went over to automobiles, and typewriter manufacturers at the triumphal entry of the laptop and the PC – with one, important difference: those technological developments made *products* obsolete; the latest innovations will invalidate entire *institutions*.

⟶ *Continued on p.8*



Communication via carrier masts



Communication via mobile phone aerials

Glossary

The key terms

[«Blockchain»]

Algorithm

A schedule of operations to solve a particular problem, consisting of a finite sequence of defined, individual steps.

Bitcoin

Best-known decentralised payment system and the name of its cryptocurrency. The system's market capitalisation is currently more than USD 6 billion.

Bitcoin protocol

Digital documentation of transaction blocks.

Block

Each block contains the previous block, the current transactions, a timestamp and a nonce. These components are each encrypted with the hash function.

Block hash

Hash value of a complete block.

Blockchain

Chain consisting of blocks with encrypted information.

Blockchain 1.0

Development and implementation of cryptocurrency-based applications relating to money, currencies and payments.

Blockchain 2.0

Comprehensive applications with relevance for the entire economy.

Blockchain 3.0

Applications that transcend currencies, finance and markets, e. g. state organisations, healthcare systems, science, etc.

Clearing

Establishing mutual requirements or liabilities and delivery commitments.

Glossary

The key terms

Crowd-funding

Method of financing in which seed capital is provided by a large number of people, each providing a small sum. Investors are usually sourced via the internet.

Cryptocurrency

Digital currency based on an encrypted (cryptographic) code.

Cryptography

Encryption of data to secure information.

Ethereum

Decentralised (programming) platform for blockchain-based applications (company based in the Swiss canton of Zug).

Hash function

Function that maps comprehensive input data (the key) to target data (hash value) of uniform size. This is one method of encryption.

Hash value

The target data generated by a hash function.

Internet 1.0

The user features merely as a consumer of content supplied by the internet.

Internet 2.0

The interactive internet. The user not only consumes but also provides content.

Internet 3.0

The semantic web. Web content is designed to be more comprehensible for machines; the machine "thinks" independently.

Merkle tree

Data structure that forms a tree of hash values, preserving the integrity of the data. Named after the American mathematician Ralph Merkle.

Miner

Network participant engaged in mining.

Mining

Computing process in which new blocks are generated by solving a complex mathematical problem. Miners are compensated for mining; this corresponds to the money creation process of a central bank.

Node

Participant in the decentralised system.

Nonce

A key that can be used on a single occasion ("number used once"). Solving the mathematical problem (see Mining) through trial and error corresponds to finding the key.

Peer-to-peer

Communication between equals – direct interaction between persons or companies without an intermediary.

Glossary

The key terms

Private key

A secret, personalised (confirmation) code.

Proof of work

Work required by a service to prevent disproportionate use.

Public key

Public “address” of a participant.

Root hash

The root of the hash tree (Merkle tree); this allows the integrity of the individual branches of the Merkle tree to be checked.

Satoshi Nakamoto

Founder of bitcoin; his real identity is unknown.

Smart contract

Digital contact for transactions that can be processed using smart property. The contract is based not on trust in the classical sense but on cryptography and the blockchain.

Smart property

Goods that can be traded, managed and used via the blockchain.

Timestamp

A variable that ensures a block can be unambiguously assigned to a point in time.

Transaction

A signed batch of data relating to an alteration that can be transmitted in encrypted form into the network and collected in blocks.

Turing complete

A system with no limits to its programmability, i.e. even for itself. The mathematician Alan Turing formulated the parameters for this status; in principle, it amounts to a programming language.

Wallet

A digital, cryptographic purse controlled via a public key and private key.

⟶ *Continued from p.4*

Having made this brief excursion into the world of mobile communications (which is relatively easy to picture), let's now move on to the blockchain. In Chapter 1, we concluded that a blockchain was no more than a system that acquires evidential value to regulate property rights on the strength of its seamless record-keeping. This seamless record is generated in a blockchain by stringing together a series of unalterable *verification logs* (the "block"), consisting of four components: its past (i. e. the preceding block); the current "timestamp" to place it correctly on the timeline; the current transactions, which are yet to be confirmed and are broken down into a cryptographic code ("root hash"); and a "number used once" (known as a "nonce") which has to be found by trial and error ("proof of work"). This trial-and-error procedure is the so-called mining process. Network participants ("nodes") that take an active part in this process add value to the system and are compensated once the process is successfully completed. The system ensures that a new verification log can only be generated when it is docked into the *most recent block* – hence the image of a chain. A system based on a lock ("public key", coterminous with an "address") and a key ("private key", i. e. a personal secret number) permits transactions, i. e. alterations of content, to be carried out. Only the authorised user is able to deploy the private key. The blockchain system is thus extremely secure, as the verification logs are stored in a *decentralised* manner – in the most extreme case, on every participating computer in the world. A change in one location that is traceable back to one hacker, for example, would be instantaneously recognised by the millions of other participants present in the system and overwritten. For a hacker even to stand a chance, more than 50% of users must categorise the "wrong" version as correct. The probability that such a person would ever be successful is extremely low, however, as he will be vying against the brutal *asymmetry* of the past and current development of new blocks; he will always be playing catch-up. The elimination of counterfeit blocks resembles that of the tumorous cells destroyed in the healthy human body on a daily basis; in this respect, there is nothing new under the sun.

To make this easier to picture, let's complement the genealogy in the Luther Bible outlined in the introduction with another analogy resembling a blockchain: a share register. Anyone who as a board member has known the delights of maintaining such a document will be aware that the best protection against mistakes (we are dealing with who owns – or does not own – shares in a company, after all) consists of storing all the versions in a large folder. If alterations have to be made to the list of shareholders as a result of capital increases, inheritance, sale or purchase of shares and the like, the recommended approach is to create a new one that can be checked against the previous iteration at any time, and then to have the board of directors or an appropriate committee approve the new version of the share register – precisely in order to use the timestamp of the board's decision to lend this verification legal weight until the next alteration. This is a process requiring the utmost attention, as any mistakes that creep in will be devastating.

The blockchain system is based on *encryption technology* ("hash function") by means of which the difficulty of identifying the target value can be incrementally – but exponentially – escalated with very little effort. The system is, as it were, miles ahead of, and pulling away from, its opponents. So, thanks to its decentralised structure, it is virtually unhackable; ultimately, the PC of any participant in the system can take over the role of a network node. Unless the world literally ends, it is actually impossible to imagine the system failing, or at least it is far easier to picture the failure of institutions that establish proof of ownership in a conventional, relatively centralised, way.

CHAPTER 4

Applicability *sans frontières*?

What property rights might now be regulated using a blockchain? All and any of them, in fact. The most immediately apparent are of course those rights and services that are directly linked to the internet. You could assign to a single individual unambiguous ownership (and thus reading rights) of an online newspaper, if you so wished. But the reading matter might just as well be a secret document. Or an illegal image. Or a *billet doux*. Or an account balance. Or instructions for building an atomic bomb. Or rights to storage capacity in the cloud. Music, movies, you name it. A blockchain is constrained by neither material boundaries nor morality, and herein lie both its strengths and its weaknesses, as with a match that you can use to light a candle or start a forest fire.

Now, you might object that there is still a disjunction between the property right laid down on the screen and the person operating the screen. This is true. The *man/machine interface* is *critical*. This Achilles heel can to a certain extent be countered with identification technology – the use of fingerprints to unlock mobile phones is already widespread, for example. And there are many other methods that go to greater lengths to ensure that interlopers are kept at bay. Absolute security is unlikely, however, as the man/machine vulnerability is of a piece with the imperfection of Man himself. A person can be intermittently *non compos mentis*, or be subjected to violent coercion by third parties. To our mind, the obviation of institutions as a putative corrective for the flaws inherent in humans represents one of the limiting factors in the expansion of the blockchain. We shall return to this point.

The second logical interface, namely that between the *machine* and the *object* for which property regulation is being established, is becoming increasingly *easy to master*. While penning these lines, we had a look at a promotional video at www.slock.it. Here, the company presents a locking system for homes based on blockchain technology that would, among other things, be well suited to managing access to AirBnB apartments without having to hand over a physical key. The advantage lies in particular in the fact that payment for the apartment can be directly linked to the "Open Sesame" code, as can locking-up, of course. Such "intelligent" locks are just the first steps in the unstoppable march of the "internet of things", for which blockchain technology betokens a decisive leap forward; one aspect (among many) that the internet of things will constantly be called upon to address is the authorisation and inclusion (or exclusion) of groups and individuals. Such concerns can be managed highly efficiently and adapted to changing circumstances via a blockchain.

We are likely to see a convergence between the functionality of equipment and the regulation of specific property (and/or usage) rights – the latest jargon speaks of *smart contracts*. It is not hard to imagine a drastic reduction of risk in international trade, for example, with facilities and machinery programmed to start up only when authorisation has been explicitly confirmed in the blockchain, and operations being sustained only for as long as the *conditions* stipulated in the smart contract are fulfilled. Such mechanisms will open up unimaginable possibilities for improved enforcement of intellectual property rights; institutional protection of patent rights in particular is shockingly lax and the associated costs are exorbitant.

We are already subjects or objects of such smart contracts on a small scale – whenever we hire a car and need a code sent to our smartphone to start it, or, as a board member, gain access to the data boardroom using a "TAN" code (a single-use password), or allow our nearest and dearest access to our photo cloud, we are inhabiting the realm of (sometimes only temporarily granted) property rights without having to involve a third-party authority, i.e. an institution. Blockchain technology is likely to become a new standard for these and other routine matters in tomorrow's world.

The technology is trammelled by limitations in respect of the machine/object relationship where property rights (use, enjoyment and disposal) can be exercised independently of any technology – in the case of the Luther Bible mentioned in the introduction, for example. Theoretically, a blockchain would be an ideal way to bring order to the art business; museums across the globe are currently reviewing the legality of their ownership rights to pictures and other artworks. Identification conflicts between the object *per se* and its machine-readable history will nonetheless arise. Will an unambiguously identifiable RFID chip have to be built into the pictures? Could it be implanted in a way that is unforgeable?

Vulnerabilities at both the man/machine and the machine/object interface demonstrate that despite everything, superordinated institutions will probably continue to play a role in the regulation of property regimes and, as such, will survive. There is no alternative to institutions where people and property can be protected only through manifest power and, ultimately, brute force – which is not to say that these institutions will not diminish massively in importance.

CHAPTER 5

Blockchain currency as the lowest common denominator

You may have noticed that in our disquisition on the new blockchain phenomenon we have so far not mentioned the bitcoin cryptocurrency that has become so fashionable of late. There is a good reason for this – bitcoins are just one of a potentially unlimited array of applications for blockchain technology. There are already dozens of other cryptocurrencies besides bitcoin, although their market share is estimated at no more than some 10%, with bitcoin taking the rest. The increase in bitcoin transactions has been remarkable, from fewer than 10,000 per day (in the tiniest amounts) in 2012 to far in excess of 150,000 today. The first capital market transactions have already been attempted, such as the recent recapitalisation of Ethereum (a blockchain company based in the Swiss canton of Zug) for the equivalent of no less that USD 18 million. Despite all the smear campaigns and Cassandra-like prophecies, it is highly unlikely that bitcoins and other cryptocurrencies are going away any time soon.

Notwithstanding the forthright opinions of the renowned economists Eugene Fama and Richard Thaler (whom we greatly respect), who hold that bitcoins are of value only to "crooks and tax cheats", your writer has offered himself as a test subject for a self-imposed experiment over the last few weeks and obtained bitcoins for a modest sum. The transaction was something of an adventure as it involved opening a bitcoin wallet through a London company (headquartered in California) and then paying this firm in EUR via an Estonian bank. The bid and ask price for bitcoins fluctuates wildly; there can be no question of trouble-free convertibility. Once you have got your feet wet in the world of bitcoins, however, an entirely new universe opens up with an astonishing number of companies that apparently never stray outside this continuum. The *Tages-Anzeiger* informs us that there is a pub in Sydney, Australia, where bitcoins can be exchanged for beer. This would certainly be one potential end use for the cryptocurrency we have acquired, but for the moment, we wish to have a further look around this very peculiar world, leaving indelible – but anonymous – blockchain tracks here and there as we go.

What makes cryptocurrencies like bitcoin so exciting? Clearly, the fact that it is possible to effect transactions *without recourse to banks*, i.e. peer-to-peer. Anyone belonging to the bitcoin world can directly credit – or be credited by – any other participant; the bitcoins flow from one wallet straight into the other. Transaction costs are negligible, although you pay a little more for quick settlement (within a few minutes) than for low-priority transactions, which similarly take very little time; transactions involving several recipients are also more expensive. In any case, we are talking about micro-payments. Are bitcoins a good or a bad investment? To the extent that they clearly diversify classic currencies, they are indubitably a good one, but whether the exchange rate will continue to head north in the way it did in the years 2013 and 2015 remains to be seen. Since joining, we have achieved a return of three percent, which is at least better than the zero percent earned on our bank account, once all the fees are deducted … Overall, bitcoin has performed in a highly volatile manner, like everything that's new. Our conclusion? Risk-averse investors should look elsewhere.

To us, there is no question that the *combination* of a blockchain system with a *blockchain-based transaction currency* is ideal for settling smart contracts, trading securities and providing goods and services of all kinds. The transaction currency options include, but are not limited to, bitcoin. The advantage of such a combination resides in the almost breathtaking simplicity of settlement. While two or more parties conducting a traditional securities transaction, for example, will each require a bank, a custodian and a clearing facility, not to mention a crediting system based on trust and mutually exchanged collateral, in the blockchain world, the same transaction can be settled *pari passu* using a blockchain transaction currency as the lowest common denominator. For such combinations to actually gain a foothold, new internet standards will have to be defined upon which this world – with its institutions scaled back or abolished entirely – can be built.

All the big commercial banks are keen to find and establish a connection to this new world – with good reason – and 42 global institutions (including Credit Suisse and UBS) have now joined a consortium called R3 to examine how blockchain can be applied to the financial system. R3 describes itself as uniting veterans from the fields of finance, technology and cryptography with digital currency specialists in order to define standards that are decoupled from institutions. There are also some intriguing and beguiling initiatives originating from the London Stock Exchange Group (LSEG), no doubt galvanised by the efforts of Chi-X founder Peter Randall, who has come up with a new, blockchain-based settlement platform called SETL even as *Goldman Sachs* announces that it has obtained a patent for an internally developed *digital currency* christened SETLcoin. Borrowing from the bitcoin model, SETLcoin is intended to become a transaction currency for securities trading in the fullness of time. The leading Swiss bank UBS is taking a leaf out of the Zug start-up Ethereum's book (see above) with Level39, its in-house fintech incubator. Ethereum is said to have made great strides in standardising a widely applicable programming language for blockchains. The "brains" behind Ethereum is a 21-year-old Russian named Vitalik Buterin who was recently described in a portrait in the *Tages-Anzeiger* magazine supplement as a "boyish enigma".

All this reflects the mixture of fear-fuelled panic and expectant euphoria that currently holds sway in the financial sector, as one thing is for certain: whatever form the various structures may ultimately take, blockchain technology is going to consign a very great number of things to the dustbin for ever. Margins are going to shrink and new providers are going to pop out of the woodwork. In short, it is more than likely that the winds of change will turn the system as we know it on its head. The banks will be faced with a similar dilemma to that once confronting the big media concerns, when distribution of digital content was just beginning on the internet: do you join in, taking a saw to the branch you're sitting on? Or wait, and watch helplessly as the train pulls out of the station? A further, plausible option would be to skilfully establish links with a regulator to make the transition to the "New Normal" bearable.

CHAPTER 6

Dinosaurs die out slowly – and later than you might think

The dilemma is deep-rooted, as institutions (a term that undoubtedly subsumes banks, trading floors and clearing houses) wishing to be involved in developing a system that is mostly or entirely cleansed of institutions constitutes a *contradictio in adjecto*. They may suffer the same fate as will one day overtake the carriers in the telephony business when large masts are replaced by nothing more than the diminutive transmitters and receivers of millions of scattered smartphones. They will have done their duty; they can go. The carriers will be reduced to hardware-peddlers and the proud pavilions of their high street shops refitted as feudal kiosks. Systemic relevance? A phenomenon of the past, axiomatically inconceivable in the world of blockchains, as only institutions can be systemically relevant, and this brave new world is doing very nicely without them, thank you very much. It was from systemic relevance that the great institutions drew their monopoly rents and hiked the prices of capitalism; now they're old hat. But need we be concerned? No, because banks are organised as private enterprises and know how to re-orientate themselves. At worst, they fail. Alternatively, they are taken over by others, they adapt, they seize new opportunities and they relish a new and far more efficient kind of capitalism. And new companies with undreamt-of business opportunities and operations will spring up at the foot of these old Ozymandiases. We are far more worried about the evolution of that institution *par excellence*, the state. It has hitherto derived its *raison d'être* from the stabilising role it plays in the co-existence of the civil populace and in respect of the private property regime it imposes on objects, on possessions. Blockchain technology will render a part of this function redundant. Much was made of land registries in a recent *Economist* feature, and we would endorse its conclusions – particularly in places where there has hitherto been no properly functioning land registry, in other words in all the developing nations and in many emerging markets. There is a good chance that this will – finally! – allow the weakest in society to know the joy of acquiring property and, by virtue of it, to become creditworthy economic subjects to boot. This dream has been anticipated in literary form by the South American writer Hernando de Soto Polar and might now become a reality, thanks to blockchain technology. Provided the introduction of a land registry blockchain were accompanied by land reform cementing the new property regime, growth would inevitably follow in such areas of the world.

Despite all these obvious advantages, we remain concerned. *Power structures and oppressive conditions* are an inevitable function of imperfect and slapdash state institutions, and these will not disappear overnight. The Moloch will not stand by and witness its own (partial) annihilation without a fight. This may crop up in harmless and even amusing forms in the widespread use of "stoker" strategies: famously, for decades after the introduction of electric locomotives in the UK, every footplate featured a fireman, whose job during the age of steam had been to furiously shovel coal, but who had since become expendable. It took Margaret Thatcher to stand up to the overweening power of the unions and put an end to such nonsense.

The death throes of institutions that have been consigned to the trash may prove less harmless and amusing when power and the use of force, on which the state has a monopoly, are on the line. Will decentralised cryptocurrencies one day replace the national currencies established and controlled by the institution of the central banks? Or at least compete with them? Will that be permitted? Under whose aegis, and with what argumentation, will attempts be made to prevent it? Much is at stake, it should be noted – not least the predominance of the USD in world trade. This said, in free social orders, the more efficient solution (in the sense of Pareto optimality, where improvements are made to the positions of all without anyone else being disadvantaged) will always win out in the end.

The *Achilles heel* of blockchain technology in this context is the possibility of total *anonymity* provided by encryption, as anonymity renders it impossible to attribute liability for actions. In an age of terrorism that can strike at any point around the globe and criminality whose effects are also being felt worldwide, anonymity is a killer criterion, however profitable and rational a technology may seem. The global community and the national and supranational authorities that represent it have no choice but to assert the right to monitor and control to the best of their abilities the malfunctioning, the misled and the mad, capable as they are of unthinkable atrocities. Things will otherwise get too hot on Planet Earth. The hardcore anarchist/libertarian pioneers of blockchain technology – and there is no shortage of these – should be under no illusions about this. If the blockchain is to set sail on its beneficial, wealth-creating voyage, it can only do so if total anonymity is elided from the internet in favour of controllability. This is a harsh tribute to render unto the institutions of power, to be sure, but there is no alternative. The institutions want control mechanisms to maintain security, and they need access to people's affairs to raise taxes. It's as simple as that.

CHAPTER 7

Outlook

We have no wish to end this *bergsicht* as naysayers or doom-mongers, however. We would rather conclude our piece with a recapitulation of the new technology's great advantages and an attempt to discern what the future may hold. Let's first reconsider our definition of the blockchain as a system that is able to regulate property rights on the strength of its seamless record-keeping – quite independently, and without reference to any institution invested with power. It is completely decentralised, and thus secure. Again, we should pause here for a moment. In the irresistible rise of the internet and what seems set to be that of the blockchain, we are witnessing the gargantuan *clash of two principles*, namely: that of gaining stability by establishing hierarchies with the greatest possible degree of centralisation, and that of attaining reliability through the most atomised decentralisation imaginable.

Or, to extend the religious metaphor used at the outset, we are facing a schism between the Catholic Church, with supposedly God's vicar on Earth, dogmatically infallible, at its head, and the multitude of independent, reformed "wee free" communities and communions who proclaim of themselves that a church is constituted "where two or three are gathered together in My name". It is certainly not our business here to judge the rights and wrongs of the matter; we can instead only conclude that since – and despite – the Reformation, both doctrines have survived and even learnt to co-exist, even if the path to this point has been a painful and bloody one. The origins of the internet (the ARPANET) were famously dreamt up by the American military to guarantee stability for computational functionality and communications in the event that large portions of their centralised infrastructure should be disrupted in a nuclear conflict with the former USSR. Second-strike capability would have been barely conceivable without the ARPANET, and it was only thanks to its second-strike capability that the civilised West, scarcely capable of a first strike, was able to prevent the East (which presumably harboured fewer scruples) from launching a pre-emptive strike. The stability-producing deterrent worked, thanks to the ARPANET. The point here is that, within – of all places – the US military complex, the epitome of a *centralised, hierarchical concentration of power*, an entirely decentralised system was chosen to elicit ultimate stability; in this respect, the "reformed" creed won out over the "Catholic". The subsequent expansion of this inspired network, and/or its potentially less welcome consequences that have penetrated into every last capillary of day-to-day life, are testament to the might of a structure that is almost entirely shorn of institutions.

Blockchain technology is yet another link in the long chain that began with the spread of the PC and mobile telephony; a concatenation of couplings that allowed us to access globally distributed content via Web 1.0, broke open economic and social processes while forcing intermediaries to their knees with version 2.0, and now, with version 3.0, is striking at the very heart of institutions. We are in absolutely no doubt that this technology will determine the ongoing evolution of both the internet in general and all economic, social and political processes in particular. In our introduction, we raised the possibility of making a few suggestions (to those with capital burning a hole in their pockets) for targeted investments in what is likely to be a highly attractive new sector of the economy. We can't do that, of course. Or rather, what we cannot – and do not wish to – do, is dish out a list of investment targets that current knowledge and reasonable judgement suggest will profit from a still-embryonic technology. So what is our strategy? In a tip of the hat to the principle at hand, we are going for the most dispersed decentralisation imaginable, by compiling, almost sight unseen, a highly diversified basket of companies operating in the blockchain arena. The majority of these firms will go under, of that we are sure, but we would be kicking ourselves had we not at least dipped a toe and taken a tiny stake in one or two of the later companies – think of those who "passed" on Google or Facebook, back in the day.

Otherwise, the golden rules for annexing new territory apply: keep your eyes peeled, try to read the geography, and make sure you know which way the wind is blowing. Define your orientation points, watch out for hazards, and seize opportunities. This new continent is vast indeed.

KH, 25 JANUARY 2016

Translated by: Richard Hall (www.motif.ch)

M1 AG
P.O. Box 344, Museumstr.1
9004 St.Gallen – Switzerland
Phone +41 (0) 71 242 16 16
Telefax +41 (0) 71 242 16 17
info@m1ag.ch

Subscribe: www.bergsicht.ch