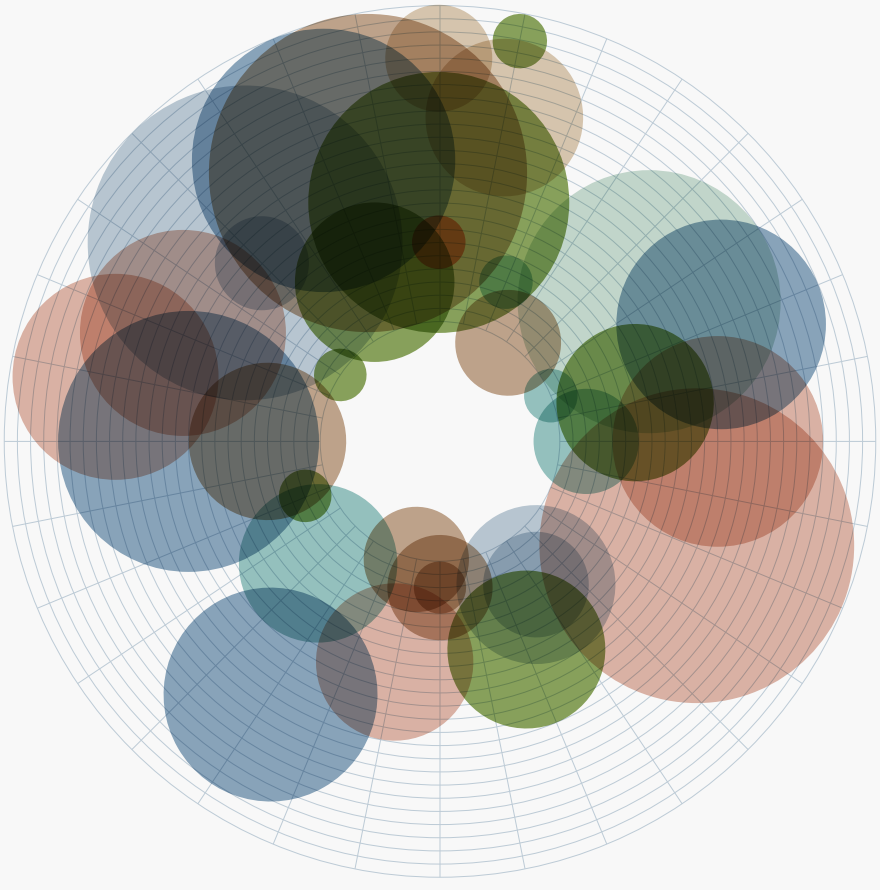
UBS

Building the trust engine

How the blockchain could transform finance (and the world)
A UBS Group Technology White Paper



Authors

Alex Batlin
Senior Innovation Manager,
UBS Group Technology

Hyder Jaffrey
Strategic Investment & Fintech Innovation,
UBS Investment Bank

Christopher Murphy
Global Co-Head of FX, Rates and Credit,
UBS Investment Bank

Andreas Przewloka
Group Managing Director,
UBS Wealth Management Europe

Shane Williams
Wealth Management Transformation and Blockchain,
UBS Wealth Management

Building the trust engine

Foreword

Anyone following recent developments in banking has almost certainly come across discussion of the blockchain. Touted as the next great thing in financial technology (and beyond), the blockchain has been the subject of countless articles in the mainstream and financial press. It has also become a focus for major players in and around the financial system – from central banks to regulators to fintech startups to global banks like UBS.

This will strike some as curious. Many (rightly) associate the blockchain with Bitcoin, and wonder why a legitimate financial institution would want anything to do with a cryptocurrency of dubious reputation. Others will note that the blockchain was designed as a way to carry out financial transactions without using the traditional financial system. Why would a bank want to be involved with a technology ostensibly created to bypass a major part of its services?

There are many reasons. While the blockchain was indeed invented to enable Bitcoin, it can do much else besides. We and our peers are not so much interested in cryptocurrencies as we are in these other possibilities. We are also fully aware of the blockchain's potential to disrupt many of our existing business models. On the other hand, it is no secret that the banking industry is facing a number of very difficult challenges. It would be irresponsible of us to ignore a technology that, on the face of it, offers the chance for such significant cost reductions and efficiency gains. That this technology is likely to enable significantly improved and potentially radically changed business models makes it all the more interesting for us.

It goes deeper than that, however. Like many of our peers, we at UBS believe the blockchain is a potentially transformative technology that will leave as deep a mark on our world over the next twenty years as the Internet has over the last twenty. For this reason we have been very active not only in understanding it, but in collaborating with the wider community in helping to shape a blockchain-enabled future financial industry.

Because of its potential impact, we consider it part of our duty to explain to our clients and the world at large as best we can what these transformations might mean. That is what we are attempting here. While there has been no shortage of blockchain white papers recently, most focus on the technology and are written for an industry audience – those likely to use blockchain to retool the financial system. Here instead we try to paint a picture of what blockchain can do in a way that is, hopefully, clear and accessible for the average user of that system. To our knowledge, this is the first attempt by a major bank to do so.

We have no crystal ball, of course, and cannot know how much if any of what we present here will ultimately come to pass. We think however we can outline with some confidence the most likely paths of transformation the blockchain could take us down. We offer this paper in the spirit of a thought experiment as a way to help readers understand where these paths might lead.

However things turn out, we think it will be a fascinating journey.

Axel Lehmann
UBS Group Chief Operating Officer

Table of contents

Foreword: Building the trust engine

Executive summary

P. 12 **The trust protocol:**
The genesis of the blockchain
– Keepers of the trust: Banking before the blockchain
– Trust in the darkness: The birth of Bitcoin
– Trust in the light: Blockchain emerges from the shadows

P. 17 **The trust elements:**
Building blocks of a blockchain-enabled financial system
– The distributed ledger: Records on the chain
– Digital value: Money on the chain
– Digital identity: People on the chain
– Digital provenance: Things on the chain
– Smart contracts: Agreements on the chain

P. 22 **The trust foundations:**
Blockchain and the financial infrastructure
– Settling down: Real-time settlement models
– Amicably parted: Split data and service level models
– Sharing the burden: Decentralized computing models
– Let the sun shine in: Regulatory inclusive models
– Look ma, no hands: Autonomous financial instruments

P. 27 **The trust app:**
Blockchain and banking for individuals
– Better than leather: Introducing your smart wallet
– The trading chain: Portfolio management on blockchain
– Chains of beings: You and your digital identity
– Chains of things: You and your "digital" possessions
– Gold chain: You and your own private currency

P. 30 **The trust platform:**
Blockchain and banking for business
– Show me the money: The real-time payment paradigm
– No issues with issuance: The direct capital paradigm
– Happy in a crowd: The direct funding paradigm
– Keeping track: The self-administration paradigm
– Keeping in touch: Managing B2B and B2C relationships on the chain

P. 34 **The trust collaboration:**
Enabling blockchain in financial services
– The long and winding road: Hurdles to a blockchain future
– A coat of many colors: The need for an open source fabric layer
– Chain gangs: Industry collaboration in the blockchain space
– Come in to the lab: Blockchain innovation at UBS

Afterword: The future of trust

Appendix: An (important) note on terminology

Appendix: For further reading

Appendix: How the Bitcoin blockchain works

Executive summary

The history of technology – like history in general – is full of ironies. When Satoshi Nakamoto introduced Bitcoin to the world in 2008, the new cryptocurrency was meant to enable electronic cash payments directly between individuals without the use of banks. Eight years later and the blockchain – the groundbreaking technology Nakamoto invented to power Bitcoin – is being championed by banks as a way to radically improve the financial system. Instead of making them superfluous, the blockchain may very well make banks better at what they do.

Like many of our peers, we at UBS have become very interested in the blockchain and its potential. Over the past year we have been studying it intensely and, in collaboration with others in the banking and fintech industries, have begun experimenting with its possibilities. Over that time we have learned a lot: enough to feel confident that the blockchain could indeed catalyze significant transformation for our industry. We have begun also to see a clear outline of what a blockchain-enabled financial system might look like. This white paper is an attempt to share that picture – in a non-technical and hopefully vivid way – with our clients and the general public.

1. The trust protocol: The genesis of the blockchain

Imagine a world where everyone was perfectly honest and trustworthy when it came to money…

Banks arose from the need for trusted intermediaries to help people protect and transact with their money. From the early Renaissance bankers with their paper ledgers to today's highly complex financial system with its millions upon millions of databases, banks have fulfilled this role among other things by being reliable and discreet keepers of lists. Considering the complexity of our modern society, we think it fair to say that the financial system we have built handles this task remarkably well. But no one would deny that the current system is also frighteningly complex, highly redundant, and very expensive.

Bitcoin was developed as an electronic cash system that would allow people to make direct payments between themselves without the need for a third-party intermediary to keep things honest. The protocol relies heavily on existing technologies and methods – in particular peer-to-peer networking and digital cryptography. But it also adds one key new element to the mix: the blockchain. This is an ingenious technology that uses sophisticated cryptographic techniques and clever incentives to ensure an autonomous but absolutely reliable accounting of Bitcoin transactions. With it, everyone using Bitcoin can be sure of one tamper-proof version of the truth, and so can trust the currency. No one had figured out how to do this before in an open source, intermediary free system. As a result, Bitcoin succeeded where other attempts had failed. While its spectacular rises and falls garnered Bitcoin a high degree of notoriety among the public, the underlying technology quietly began to capture the attention of the financial industry (and others). The object of interest wasn't cryptocurrencies, it was shared list-making. The blockchain revolution had begun.

2. The trust elements: Building blocks of a blockchain-enabled financial system

Imagine a world with a single, universal, absolutely trustworthy and completely indestructible financial ledger…

The blockchain can be used to provide the basic services that are essential to any financial system, and can do so in ways that are often better and more efficient than the tools we use now. For one, blockchain technology creates a viable, decentralized record of transactions – the distributed ledger – which allows the substitution of a single, inviolable master database for large numbers of proprietary ones. That could lead to radical simplification and cost reduction for large parts of our financial system, while making it more secure and reliable. Blockchain technology also allows for the creation of digital currency with the attributes of non-counterfeitable cash, providing a mechanism for direct and unambiguous transfer of value while keeping the advantages of digital networks.

The blockchain also offers a far better means of establishing and using identity than the one we have now. By providing unique, non-forgeable, cryptographically sealed pseudonyms, which could then be associated with any number of verified credentials, individuals in a blockchain network can simultaneously authenticate their identities while protecting their privacy. By providing unique, non-forgeable identities for things as well, along with an inviolable record of their ownership, the blockchain can greatly simplify the direct transfer of physical assets and increase confidence in their provenance. Finally, by adding full programming capability to blockchains, we can create "smart contracts." These will allow us to not only better record our financial agreements, but to make these agreements autonomous and self-enforcing.

3. The trust foundations:
Blockchain and the financial infrastructure

Imagine a global financial infrastructure that is slim, trim, safe and secure…

Using the elements described above, we can potentially retool the existing financial infrastructure and employ new business models to radically improve some of its core functions. The blockchain for example could enable near real-time settlement models for most types of financial transactions, which could eliminate counterparty risk, free up capital and radically reduce transaction cost. It also allows for split data and service level models in which individuals in effect become the keepers of their own accounts. This could give them not only more security, but much more freedom in choosing financial service providers. The blockchain relies on decentralized computing models, which by their nature are more robust and secure than the proprietary, centralized models we now use. This could help create a safer, more reliable system at a far cheaper cost.

By giving regulators a real-time view of what is happening in the system, the blockchain can allow for regulatory-inclusive models too. That means regulators could act to stop crises before they happen instead of regulating after the fact in an attempt to avoid the next crisis. It could also allow for regulatory rules to be "baked in" to financial products and services, making the system more compliant and harder to abuse for criminal ends. Finally, smart contract technology could allow us to create new, autonomous financial instruments. Smart securities for example could issue and administer themselves, vastly reducing the cost of accessing capital markets as well as of asset custody, servicing, and reporting.

4. The trust app:
Blockchain and banking for individuals

Imagine a world where you can download your own personal bank onto your phone…

A blockchain-enabled financial system would likely look very different for individuals than the system we use now. Tomorrow's "smart wallets" – the apps people will use to connect to the blockchain-enabled financial system – could for example be configured as personal, freely programmable portfolio managers. These apps would be able to trade on their users' behalf, and even read the news and make their own trading decisions based on market developments.

A blockchain-enabled financial system could also give people far more control over their identities. With credentialed pseudonyms based on public-key cryptography, verified identities could easily be used to open accounts at multiple institutions or prove suitability for certain financial products. They could also allow people to share different parts of their identities in different contexts. Similar approaches could allow for far more secure and reliable means of identifying assets, giving people more confidence in the provenance and authenticity of the items they purchase and opening up possibilities for direct markets in high-value assets. The blockchain also allows for the easy creation of private currencies, something which was common in the past and may now see a renaissance – with interesting implications both for high-net worth individuals and retail clients.

5. The trust platform:
Banking and blockchain for businesses

Imagine a future where all sales involve immediate transfer of funds and businesses have instant access to cash…

The blockchain could also bring great benefits to businesses. By enabling direct transactions the blockchain could make most business payments cash-like, reducing or eliminating late payments and so freeing up capital. By reducing transaction costs to near zero, it could allow for extremely small micropayments and with them new business models. Smart securities could make it easier for corporations to access capital markets, and cheaper for them to service and report on the securities they issue. The blockchain could potentially provide new impetus to crowdfunding by increasing trust in those seeking financing, no matter where they might be. It also has the potential to radically reduce business administration costs by automating such things as payroll, accounting, VAT payments and regulatory compliance.

The new identity paradigm associated with the use of credentialed pseudonyms may also change the way businesses gather and use customer data. Instead of relying on the flood of unstructured and unreliable information available to businesses today, they may instead increasingly use the data their customers choose to share. This would be far more reliable and easier for businesses to process. As it is freely given, it should help strengthen customer loyalty. In a blockchain-enabled world, businesses may develop new and improved ways to interact with their customers and, through the Internet of Things, to keep track of and service the items their customers have purchased.

6. The trust collaboration:
Enabling blockchain in financial services

Imagine a technological revolution that was the result not of competition but of collaboration…

While most of this paper is dedicated to optimistic future scenarios for blockchain, we are well aware of the many hurdles the technology must overcome if it is to achieve its potential. There are technical issues, issues involved with whether the technology is developed in a coordinated or fragmented way, and issues of governance of the new platform. At UBS, we believe strongly that the industry must develop a common underlying blockchain-based market fabric upon which all parties can build their value-added services. This will mean solving a number of particular challenges outside blockchain proper, including how the industry will handle the identity of people and entities, how it will bring legal tender onto the chain, and how it will handle the many governance and legal issues associated with the various parts of the new platform.

The good news is that much of this work has already begun in earnest. Over the past year, the blockchain has garnered an intense amount of interest and investment, and this trend is set to explode. Nor is this interest to be seen only among banks and fintech companies. Central banks and regulators around the world, as well as organizations involved in providing shared financial services infrastructure, have also begun working on possible blockchain applications. With industry-wide collaboration platforms like the R3 consortium, which brings together more than 40 global banks in an effort to set common standards, the stage has been set for the cooperation necessary to bring out blockchain's full potential as quickly as possible. At the same time, experiments by individual institutions, including by us at UBS in our innovation lab, are adding to the growing corpus of knowledge about this exciting new technology.

Afterword: The future of trust

While we are very optimistic about the blockchain, we are not naïve about its potential to disrupt our business. Quite the contrary, the more we learn about this technology, the clearer its transformative nature becomes. With the disintermediation of trust may come new paradigms which could put large, centralized organizations at a disadvantage. We are sanguine about this change, and indeed are embracing it. There is more to banking than just transactions. Since its early days it has also been about personal relationships, expertise and advice. These functions will not disappear. Current industry players servicing different parts of the system will have to adapt, but their know-how will also still be needed to build the new trust engine. If this engine is as powerful as we think it might be, it could take us very far.

The trust protocol: The genesis of the blockchain

Imagine a world where everyone was perfectly honest and trustworthy when it came to money. Where no one could cheat. Where financial transactions were always immediate and final. Where ownership of assets was always crystal clear. Where money could be neither laundered nor embezzled. Where agreements to pay, once entered into, were always kept.

This is a utopia most would welcome – and one we may never see. But the advent of the blockchain has spurred a movement which may take us a long way down such a road by revolutionizing how we handle financial transactions. Like our society, our financial system has grown extremely complex. The blockchain is a technology that could make money simple again. That's big news.

Keepers of the trust:
Banking before the blockchain

Trust is one of the main prerequisites for a functioning society. We routinely put our lives in the hands of total strangers because we trust them to do the right thing: the doctors who keep us healthy, the pilots who land us safely, the other drivers on the road who stop at the red light. In these and other areas of our lives, trust works remarkably well. But there are limits, and so we have also had to develop trust-enforcing institutions. The police, for instance, exist because people cannot always be trusted not to harm each other.

In a similar way, banks exist because people cannot always be trusted to deal honestly with money. As large and complex as our modern financial system is, its primary function is to cope with this simple fact. (If we humans were all absolutely honest souls and perfectly scrupulous record keepers, then bankers would be largely superfluous.) Among other things, banks keep our money safe, provide us with confidential and accurate records of how much money we have, make available secure and reliable means for us to send and receive money, and ensure that people don't cheat us or the system.

They do this, in essence, by keeping lots and lots of lists.

The immense size, complexity and expense of our current financial system can be seen as a simple function of the unfathomable number of money-related lists required in our modern world, as well as the incomprehensible complexity of ensuring that these lists are accurate, secure and in agreement with each other.

Despite its complexity, the financial system we have built serves us rather well. Today we have truly global financial markets, routinely process billions of transactions a day, and keep track of trillions of dollars' worth of value. Without such mechanisms, our society would not be able to function. Yet our current regime is by no means perfect. It relies on large numbers of private and public entities each with their own organizations and proprietary IT systems. That makes it expensive and, as information is replicated through the system, often needlessly redundant. Many of the key parts of the system are centralized, creating potential single points of failure. By their nature opaque (they were built to ensure privacy), financial infrastructure systems are also hard to monitor.

With the blockchain, we have perhaps found an alternative method of keeping extremely large and dynamic lists that may very well address many if not all of these issues. Hence the excitement.

Trust in the darkness:
The birth of Bitcoin

On Halloween of 2008, as the financial crisis raged, a person or group using the name Satoshi Nakamoto, and whose true identity as of this writing remains unknown, published a short white paper on a cryptography mailing list. The paper proposed the creation of a peer-to-peer electronic cash system based on a currency it dubbed Bitcoin.

At the heart of the project was the desire to "allow online payments to be sent directly from one party to another without going through a financial institution."[1] Bitcoin was therefore clearly designed to bypass key elements of the traditional financial services infrastructure. While it was not the first digital currency to be proposed for this purpose, it was the first to succeed on a large scale. That's because the solution Nakamoto devised solved the key problem that had bedeviled all previous digital currencies: the problem of trust.

The solution is rather simple in theory, if harder to understand in practice. The Bitcoin protocol uses a combination of extremely sophisticated cryptographic techniques (hence it is also known as a cryptocurrency), and subtle social engineering to create an autonomous,

trustworthy decentralized network for the exchange of bitcoin between anyone who cares to join. The protocol allows for the creation of new bitcoins in the network at regular intervals, and it provides financial incentives for special users – known as miners – to take on the work of carrying out and validating transactions.

Much of the Bitcoin protocol, as Nakamoto readily admits in his, her or their paper, is built on already existing technologies and methods. It relies on peer-to-peer networking to create the Bitcoin network. It uses public-key cryptography[2] to uniquely and definitively identify all members of the network while hiding their true identities; as well as to – in effect – uniquely identify each unit of bitcoin. All of this was possible before. But Nakamoto added one key new element to the mix which made Bitcoin different and more powerful than any previous attempt at creating an autonomous digital currency. This was the blockchain.

The blockchain is a record of all the transactions ever made with all the bitcoin in existence, back to the first-ever transaction. What makes the blockchain special is that this record is not kept by any central authority. Instead it is maintained by the collective efforts of anyone who cares to join the network and become a miner.

Miners are incentivized by earning bitcoin as well as transaction fees in exchange for their work. They are prevented from cheating by the ingenious process they are obliged to use to carry that work out. This process – the details of which are not in the scope of this paper, but which are a fascinating study in themselves[3] – makes it impossible for anyone to introduce bogus transactions, for example to double spend coin. Only valid transactions can make it through the process, and each valid transaction is cryptographically linked to the previous one, forming a chain of transactions. The chain is then updated in blocks of 500 valid transactions each (hence the name).

The most current version of the chain, which by its very nature cannot be altered or counterfeited[4], is constantly updated on all the computers on the network, creating a viable "distributed ledger." This ledger can be inspected and verified at any time by anyone. The system, which is fully autonomous, therefore provides its own trust.

Bitcoin's real innovation has not been in building a robust, open and secure platform for transferring value directly between individuals. Rather it has been in building a functioning *trustless* system for that purpose: one that works even though the people who use and run the system do not know and therefore, by definition, *cannot* trust each other.

A work of genius, we may also note that at heart Bitcoin is nothing more than a very clever means of automatically creating, updating and storing absolutely trustworthy and indestructible lists.

1 See: bitcoin.org/bitcoin.pdf

2 Also known as asymmetric cryptography.

3 See the appendix for a short explanation of how the Bitcoin blockchain works as well as a blockchain reading list.

4 The ledger is sealed with a cryptographic hash, a unique, practically unguessable number (even with the most powerful computers available today, you have a better chance of being hit by an asteroid than guessing this number). If even one bit of information in the ledger is altered, the hash changes, revealing the misdeed.

Trust in the light:
Blockchain emerges from the shadows

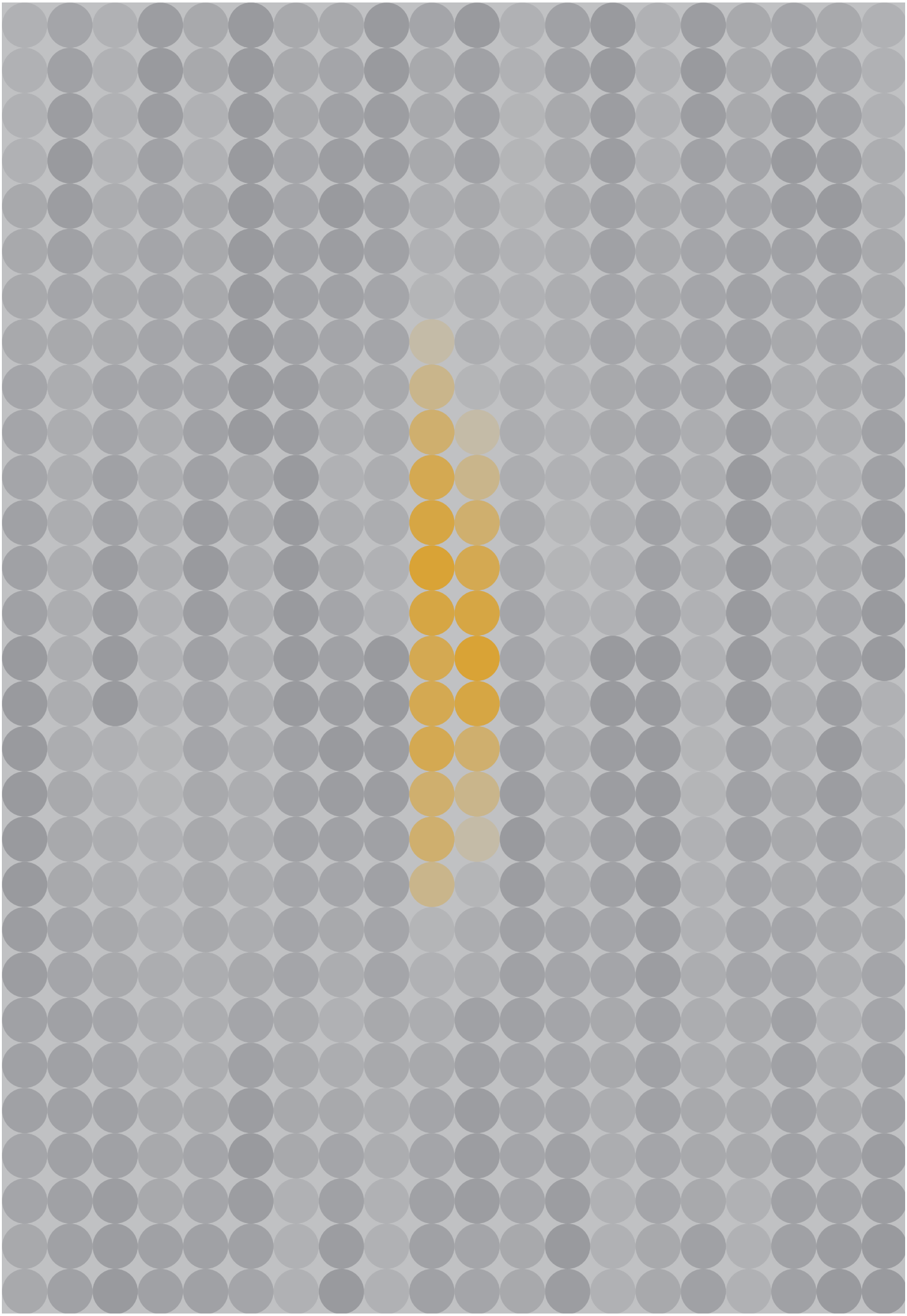
Although not without its teething pains, Nakamoto's system worked, and Bitcoin soon became the world's most popular and valuable digital currency. For a variety of reasons, including early adoption by criminal elements (drawn by Bitcoin's ability to transfer funds anonymously out of the reach of governments) and some well publicized thefts, it was also soon its most notorious.

While the rise of Bitcoin brought public and media attention to the sometimes shady world of cryptocurrencies, it also sparked interest in understanding how its underlying technology worked. It wasn't long before people realized just how ingenious and powerful this new technology was – not for its cryptocurrency aspects, but for its list-making ones.

This was particularly interesting for the financial industry. If the blockchain made it possible to build a bullet-proof and fully-automated system for maintaining a ledger of bitcoin transactions, what other kinds of financial transactions could it potentially keep track of? And if the blockchain enabled automatic bitcoin transactions that were immediate and final, what other kinds of transactions could it theoretically automate? The potential was intriguing, and seemingly limitless.

What followed is the blockchain revolution we are living through today. Like all technological revolutions it is characterized by a certain degree of hype, but also by a lot of hard work and creative thinking. A large and growing number of people both within and outside the industry – including ourselves at UBS – have been looking at ways of improving or expanding on the blockchain idea, for example by adding new functionality to the Bitcoin blockchain, or applying it to novel use cases, or even, inspired by the Bitcoin blockchain, designing alternate blockchain-like systems that do the same thing in different ways.

In this sense, the blockchain is as much a mindset as it is a technology. Once it was possible to see a workable decentralized list-keeping platform in action – a tool and a methodology for building digital trust engines that could be used for a wide range of purposes – the cat was out of the bag. People began to see things in new ways, and to get excited by what they saw. Out of such moments are true technological transformations born.



The trust elements: Building blocks of a blockchain-enabled financial system

Imagine a financial system with a single, universal, absolutely trustworthy and completely indestructible ledger. One master list to record everything having to do with money, all over the world. A ledger freely accessible to all yet completely secure, reliable and tamper proof. One in which our privacy is securely protected while our identities are definitively authenticated. Where transactions involving money and things can immediately be recorded with absolute confidence and no ambiguity. A ledger which can automatically carry out our transactions, and on which we can sign contracts that autonomously execute and enforce themselves. A ledger at the heart of an "Internet of Value", as some have called it[5], as powerful and easy-to-use as the Internet of communications we know today.

While a single, universal ledger of everything is more of a rhetorical device than an actual future scenario, blockchain technology can move us in that direction – along the way radically improving the means we have to handle money. In this chapter we take a look at some of the basic building blocks of the financial system and the new paradigms the blockchain represents for each of them.

5 See https://www.bitconnect.co/bitcoin_news/bitcoinfront/details/78 for a discussion on who coined the term.

The distributed ledger: Records on the chain

As mentioned, one key function of banks is to provide a reliable and secure accounting of assets and transactions. In the current paradigm, each bank keeps its own records. The result is an impenetrable jungle of lists: all the bank accounts in the world, all the credit card, mortgage and securities accounts, all the names of people, organizations, and other assets associated with these accounts, the records of the trillions of transactions that are made between the accounts, and the copies of all of these records that are created as transactions wind their way through the system.

In the blockchain world, this paradigm is turned upside down. Instead of each member of the network having its own list in its own proprietary system, there is one list – the distributed ledger – which everyone shares. Since the list runs on an open platform that contains verifiable consensus mechanisms, all parties can be sure of its validity. As it is open to all to inspect, it can also constantly be monitored and checked for accuracy. Before blockchain, none of this was technically viable.

Shared list-keeping is highly desirable for a number of reasons. For one, blockchain-based systems are radically simple – it is much easier to deal with one list than one thousand. They are also, at least in theory, radically less expensive to build and maintain. Sharing one list also means that everyone must agree up front on how data should be structured and stored (hardly the case in today's proprietary model), so these systems have the advantage of built-in standardization and interoperability too.

Because it is distributed over a vast number of computers, a blockchain-based system is for all intents and purposes indestructible. Unless every single computer in the network is destroyed, there will always be a valid version of the ledger available somewhere to keep the system going. Because blockchain ledgers are cryptographically sealed, they are extremely secure as well.

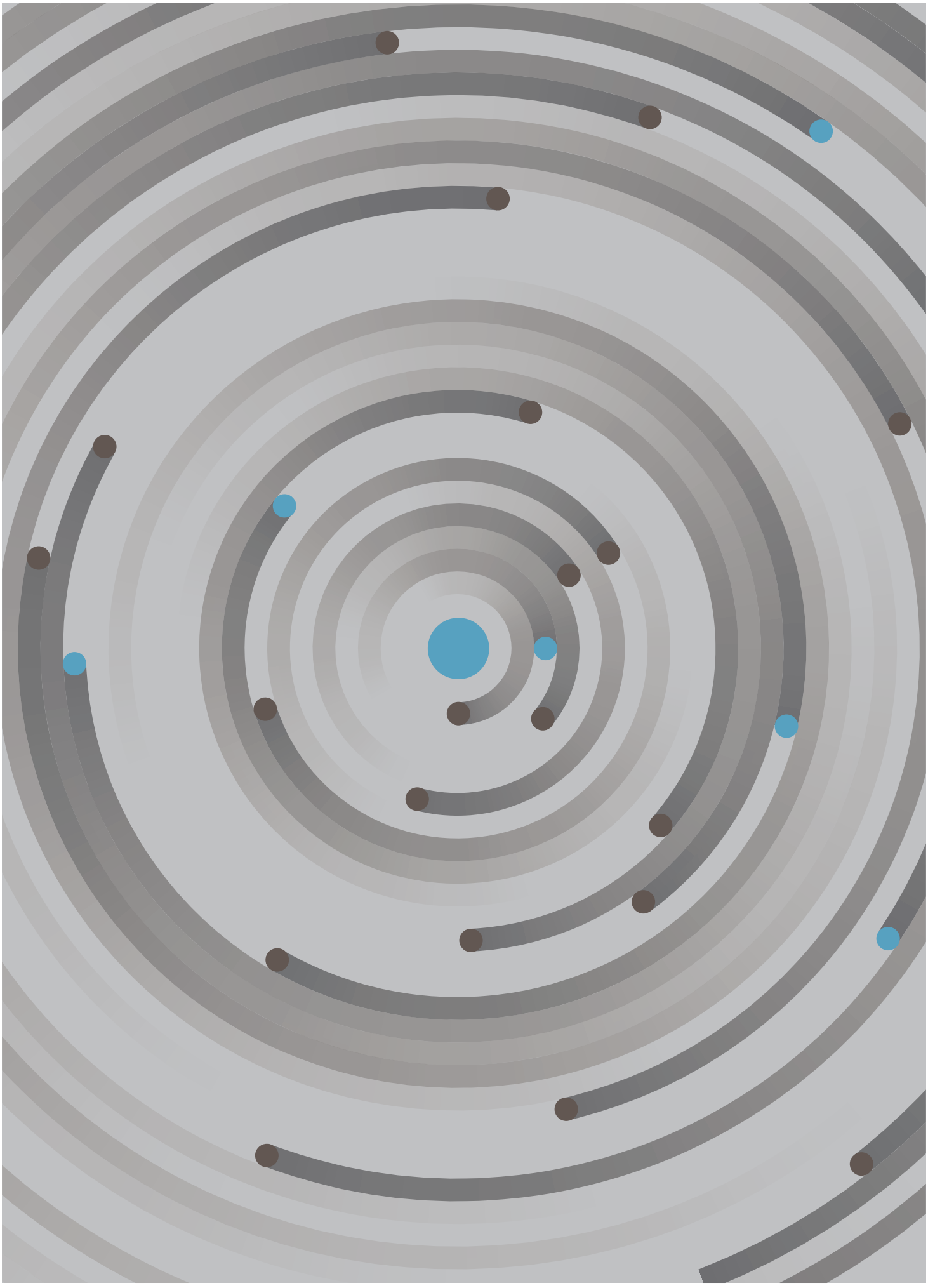
Digital value: Money on the chain

Since the move to fiat-based currency 40 years ago[6], the vast majority of money in the world has become nothing more than an entry on a ledger. It is made by central banks when they create reserves or, far more frequently, by commercial banks when they extend credit, and it lives in electronic databases spread out through our financial system. Fiat money is therefore not really a thing – it is a promise to pay. Making financial transactions today simply means adjusting our many ledgers to reflect changes in these promises.

Money in blockchain is also just an entry on a ledger. Unlike fiat money, however, the "coins" in a cryptocurrency are uniquely identifiable – represented by cryptographically generated keys so complex they are impossible to guess or forge, even for the most powerful computers[7]. As with today's money, transferring a cryptocoin from one person to another involves assigning it to a different account on the ledger. Because the reference is to a uniquely identifiable "piece" of money, as long as the ledger is correct, this transfer is as definite and irrevocable as a physical exchange of notes or coins.

Money in the blockchain world is therefore like cash, but with significant improvements. Thanks to cryptography, blockchain-based currencies cannot be counterfeited. Being digital, they can't be picked out of your pocket. Like banknotes with serial numbers, blockchain coins can also be easily traced. Blockchains function in fact by being records of the movements of each coin from the moment it is created. Since the record is public, it is easy to ensure that each coin is only assigned to one account.

No double spending, no counterfeiting, "tangible" currency which can be directly exchanged instantly via digital networks. Here too, the blockchain offers means for handling money that could greatly improve upon those we have now.



Digital identity:
People on the chain

A financial system can only function if someone, somewhere, knows who the parties to a transaction really are. Without this, there can be no correct accounting. On the other hand, we do not want our financial transactions to be public, nor the records of what we are worth. Here too we rely on banks as intermediaries. They verify our identities when we open our accounts, keep our records safe from scrutiny, and transact on our behalf in non-public, secure ways.

The system is far from perfect. Banks rely on various forms of documentation to verify our identities, and these can be forged. Modern technology has unfortunately made identity theft much easier, making it easier in turn for criminals to impersonate us to banks and steal our money. Because banks on purpose do not share identities, we need to prove who we are each time we open an account at a new one. Multiple copies of our identity are therefore spread all over the system, inviting error and making it hard to update should something about us change.

Blockchain has a better way. It uses public-key cryptography to in effect assign a unique ID, in the form of a cryptographic key, to each user on the network[8]. This key has two parts: a public key, which is the network identifier, and a private key, which is like a password that gives the holder control of what goes on in the name of the public key. The combination of private and public key is unique, and cannot be guessed at or forged. As long as no one else has your private key, you in effect have a secure pseudonym that allows you to carry out completely anonymous transactions.

Such anonymity, of course, can be abused. That is why in mainstream blockchain applications we will still have need for outside authorities to vouch for our identities. This could take the form of a central registry, perhaps held by the government, or – more interestingly – be the result of a system of attested identities. Your consulate for instance could attest that the person associated with your key is the holder of a valid passport. The motor vehicles department that that person holds a valid driver's license. The birth registry that that person is of a certain age and gender. A bank that that person is the holder of an account. And so on.

You could then use these attestations – which are *bona fide* yet not publically traceable to your real name – as needed. By attaching such credentials to their anonymous public keys, honest people can build trust in their identities while maintaining privacy. Criminals would have a much harder time. Later in this paper we will explore some interesting ramifications of this approach.

Digital provenance:
Things on the chain

As with people, so with objects. Today, ownership of assets is recorded by a network of intermediaries. Your bank has the record of your financial assets, the county clerk the record of title to your house. For the vast majority of things in your possession, proof of ownership is contained in your receipt, and disappears if you lose it.

In the blockchain world physical assets – a house, a car, a TV or a diamond ring – can have unique identifiers the same way people do. That means they can be accounted for, and transacted with, on the ledger. In current parlance this is done using so-called colored coins: blockchain coins which, instead of representing money, are tokens of things.

Just as with currency, the ownership of things on the blockchain is clear and irrevocable – a token of an asset can

not be counterfeited and can only be associated with one account. Also as with the currency, transfer of assets is easy, immediate and final, with a traceable, auditable record of ownership going back to when the asset was first added to the chain. Digital tokens can also accumulate attestations, and so gain *bona fide* credentials. If experts can verify the authenticity of a painting, for instance, and that attribute is attached to the painting's token, all interested parties can be confident that it is not a forgery.

Smart contracts:
Agreements on the chain

Finally, a very important function of the financial system is to keep records of our agreements with regard to money. While payments are a simple form of this – an agreement to move funds from A to B – most financial agreements are more complex. Escrow arrangements, for example, where funds are only transferred when goods are delivered. Or derivative financial instruments that only pay out if certain things happen in a market. Whatever the conditions are, it is the job of banks and other intermediaries to record these agreements and execute their stipulations.

In the blockchain world these tasks can be handled by adding programming capabilities to the ledger. This was already possible in the original Bitcoin blockchain, which features a simple programming language allowing users to attach basic conditions to transactions. Today a lot of work is being done to add more powerful programming capabilities to blockchains that would allow them to understand and execute any kind of business logic. This enables the creation of what have come to be called "smart contracts."

Smart contracts have some interesting attributes. Since like everything else on the blockchain ledger they have unique identifiers, they can send and receive information. Among other things, that means they can hold money and so be programmed to make autonomous decisions about buying and selling things.

Smart contracts are probably the most exciting and powerful extension to the original blockchain idea yet developed. As we will see in later sections, they open up a number of very intriguing possibilities, from automated escrow agents to self-servicing digital securities. Like any powerful new technology, they will also likely open the door to new ideas and possibilities beyond our current imagining.

6 See "Identity is the New Money", Birch, Loc. 156 in the Kindle edition. (Full citation in appendix.)

7 This is admittedly simplifying for the sake of clarity. In Bitcoin, only transactions have IDs, not currency. But since the transactions are the currency, the end effect is the same. Some have worried that the advent of quantum computing-based decipherment could end cryptocurrencies. While this is possible, it is equally likely that quantum computing will result in quantum cryptographic techniques capable of creating quantum cryptocurrencies strong enough to baffle future quantum code-breakers.

8 Here too we are simplifying somewhat. In Bitcoin, for instance, the ID is not assigned to a person but to a wallet. People can have as many IDs as wallets. As long as they have the corresponding private key to the wallet, the wallet's ID is in effect their ID.

The trust foundations: Blockchain and the financial infrastructure

Imagine a global financial infrastructure that is slim, trim, safe and secure. A system that combines the ease and finality of cash payments with the speed and reach of global communications. Where transaction fees are reduced to the minimum, because the effort to carry out transactions is minimal as well. A system so robust that it could easily survive the collapse of even the largest institution, making too-big-to-fail a thing of the past. A world where stocks and bonds administer themselves: automatically paying dividends and coupons, registering their new owners, and reporting on their prices.

Imagine a financial system where money laundering and terrorist financing are impossible, while at the same time personal privacy is strengthened. A financial system that could be far more effectively regulated, because regulators can view developments in real time – giving them the tools to prevent financial crises before they happen. In this chapter we look at how the blockchain might transform some core financial services business models and so help us turn such imaginings into reality.

Settling down:
Real-time settlement models

It has never been easier for consumers to make payments. Whether by credit card, computer or phone, it can seem like we are able to use our money instantly whenever we want anywhere in the world. This impression is misleading. When you buy a coffee on vacation with your card the record of your purchase is immediate. The actual transfer of money from your account to that of the merchant takes days. In the meantime information about your latte has travelled through a dizzying maze of systems. The same can be said for the settlement of almost any type of financial transaction today, from simple payments to complex trades.

The truth is, our current settlement regime, while admirable in many ways, is far from ideal. It is full of redundancies. It requires information to be passed along a chain of proprietary systems where glitches can result in discrepancies. When discrepancies occur they must be manually reconciled, which costs money. The lag between when a transaction is agreed and when it is settled invites risk – one of the parties could conceivably go broke during the settlement period. Insuring against such counterparty risk costs money too. It also ties up capital, as the funds earmarked for a transaction are not available until that transaction settles.

There's little or no waiting in the blockchain world. That's because blockchain enables direct and irrevocable transactions between counterparties, with almost immediate transfer of funds. This could theoretically enable near real-time settlement for almost any financial transaction, a long-time industry dream.

Near real-time settlement has many advantages. For banks it means a simpler, cheaper and more robust settlement

infrastructure that could drastically reduce transaction costs and hence fees. It could also mean drastic reductions in counterparty risk and the need to post expensive collateral at central banks to insure against it. That capital would then be free to use for other ends. Trades that settle immediately and irrevocably can also by definition contain no errors, eliminating the need for expensive manual follow-up.

Near real-time settlement would free up capital for corporations and investors too. Today when a trade is made, money is tied up until it settles. In the blockchain world, funds are ready to be put to use again almost immediately. In this world there can also be little or no disagreement as to what was actually transacted. The blockchain by its nature provides an unambiguous and incontestable version of the truth available for all to consult.

Amicably parted:
Split data and service level models

Most of us, if asked where our money was, would probably say "in the bank." And it would be a fair representation of the truth. Today our money, or at least the records of it, resides in the databases run by our financial institutions. If we want to do something with that money, we first have to send instructions to the institution.

In the blockchain world our money is an entry in a single ledger, copies of which exist on countless computers connected in a vast network. In other words it is everywhere and nowhere at the same time. That may sound eerie. But since our records are secured by a cryptographic key only we know, we could just as easily say that our money resides with us – a much more comforting thought. Taken to its logical conclusion, this means we

wouldn't really need banks to keep our accounts for us anymore. We could keep them ourselves.

This of course would hold true for any kind of information stored on the blockchain. In this new world, we will therefore likely see a split between data and service – that is, between our information and the systems and organizations we choose to process it. This will give us all much more freedom. If you no longer have an account at a specific bank, then you are no longer obliged to use that bank for your transactions. You can pick and choose. As we examine in more detail in the next section, this is also a safer approach. If a bank's systems go down or become corrupted you have nothing to worry about. Your data is always safe in your own hands.

Sharing the burden:
Decentralized computing models

At some point in your life you have probably experienced the nuisance of data loss. A corrupted hard disk, a bad USB stick, losing the password to a backup. When our personal systems fail, it can be irritating and painful. Sometimes it can be costly. If a bank's systems fail, it is nothing short of a disaster. That's because each bank is individually responsible for caring for its customer's data.

There is another way – decentralized, peer-to-peer networking of the kind employed in blockchain. In this model, instead of one central server holding and processing the data, all computers on the network share the information and the workload. This model offers several key advantages over the centralized one we use now.

For one, it is cheaper to build and maintain. In place of a host of proprietary systems that have to learn to talk to each other, there is one network and one protocol. In the blockchain world there is also one data set, the distributed ledger. This could drastically reduce development and maintenance costs. This model is also more robust. In the event of a catastrophe, unless every single computer on the network is destroyed, there will always be at least one node with the latest copy of the data that will be able to carry on the processing. That means reduced costs for business continuity management. Since the blockchain uses sophisticated cryptographic methods to ensure the viability of the ledger, it is also highly resilient to cyber attack. That reduces the cost for cyber security.

Decentralized computing does not just reduce operational costs. The blockchain could also potentially reduce the requirements for resolution planning, for example to meet too-big-to-fail regulations. When Lehman Brothers collapsed, it took years to untangle all the open trades and figure out where the assets were – a costly and nerve-wracking process for all involved. On a blockchain-enabled system such a failure would not lead to catastrophic uncertainty because there would be no open trades. With a distributed ledger, everyone knows the exact location of all assets at all times.

Let the sun shine in:
Regulatory inclusive models

Banking is one of the most highly regulated industries in the world. The rules governing banks are meant to protect consumers, ensure fair competition, and avoid banking crises. As we saw in the crisis of 2008, this is not always easy to do. One big problem regulators face is that they can often only act after the fact. They can look at what happened in a crisis and write rules to ensure the same mistakes are not repeated; yet the causes of future crises are rarely the same as those of previous ones.

In a blockchain-based system, where transactions are immediate and the ledger public, regulators could have a real-time view of what is transpiring in the system at all times. This would give them a host of powerful new tools. They would be able to spot anomalies as they arise, and calculate systemic risk on-the-fly. This would allow them to install "circuit breakers" to "cool off" the system before catastrophe hits. They would be able to do the same with individual institutions in danger of failing, quickly cordoning them off from the rest of the system to avoid contagion. Such capabilities would allow regulators to move from a cure-based approach to one of prevention, making for a much safer financial system.

Regulators could also theoretically code compliance rules directly into the blockchain. The system could automatically check transactions against sanctions lists, for instance, and block infringing ones before they happen. This would make terrorist and criminal financing much more difficult. With people's (anonymized) identities and attested characteristics on the chain, regulators could add suitability checks directly to financial instruments, reducing the risk of mis-selling. They could also in theory inspect and sign off on smart-contract based financial instruments before they are released for sale, so that consumers could trust that the financial products they are purchasing do what they say.

Such regulatory inclusive models would be a boon to banks as well. Right now, it is the banks' responsibility to comply with the rules, and a great deal of time and money is expended doing so. With compliance "baked in" to the system, compliance efforts could be greatly simplified and streamlined. The savings on compliance costs could be tremendous.

Look ma, no hands:
Autonomous financial instruments

The above examples illustrate the ways the blockchain could improve the financial system we already have. But the blockchain really is a technology of the future. The combination of the distributed ledger, smart contracts, near real-time settlement, decentralized processes, regulatory inclusiveness and other capabilities will allow us to move to fully digital financial markets, and so do completely new things.

One early area of experimentation along these lines is with digital securities: "smart" bonds, equities and other instruments that live entirely on the chain, and so exhibit some interesting properties.

For one, they are self-administering. A smart equity, for instance, can automatically register ownership when it is purchased, pay its own dividend, carry out its own stock splits, and perform any other task associated with its lifecycle. This means no asset servicing fees for the issuer. Residing on the ledger, smart securities also require no custodian.

This of course is only the beginning. Fully digital financial markets would represent a completely new environment. It is possible – indeed highly likely – that as we get used to this environment we will come up with completely new types of financial instruments, perhaps even completely new ways of thinking about financial markets. If the past is any guide, this should result in completely new products and services the like of which we cannot even conceive of at the moment.

The trust app: Blockchain and banking for individuals

Imagine a world where you can download your own bank onto your phone – not an app that connects you to your bank, but one that connects you directly to the global financial system. An app that not only holds your money, but manages it for you – more quickly, and likely more effectively, than you could do yourself.

Imagine an online world where you had complete control over your own identity, sharing only as much as you want or is necessary with different people and organizations. An online world where you could anonymously meet and directly transact with like-minded individuals whose true identities you don't know, but in whom you can still place your complete trust. Or a world where you could share private currencies with others, or even issue your own, to meet a variety of special needs. In this chapter we sketch out some of the new possibilities for individuals that could result from the blockchain-enabled financial system.

Better than leather:
Introducing your smart wallet

Today when we say we are "banking" we mean we are using the services of a bank or other financial intermediary: We are opening an account, visiting our financial advisor to help us decide how to manage our portfolios, making investments via our broker, or carrying out transactions via our bank's systems.

In the blockchain-enabled financial system, individuals may be able to perform a large number of these tasks on their own. They would do so with their "smart wallets" – the apps that they will download to connect them directly to the blockchain infrastructure.

Having a smart wallet will be a lot like having your own bank in your pocket. It will be the tool you use to manage your accounts, to configure and carry out your transactions, to manage your preferences and identity, to communicate with the institutions and individuals you choose to work with, and to purchase any new tools, information or other capabilities that might become available. This may seem like current e-banking, but in reality it will be much more. E-banking connects you with your bank. Your smart wallet will connect you directly with the financial system.

Not all smart wallets will be of the same quality. We therefore expect banks and other providers to compete in this space in the future, vying to develop better wallets and more useful value-added services on top of the blockchain-enabled infrastructure. Banks with the most skill and expertise in research, advice, customer relationships, and of course app development will be at an advantage.

The fact that smart wallets are direct connections to the financial system is a double-edged sword: it puts vast new capability in your hands, but also added responsibility. In a network with no central authority, for example, no one can restore your private key; if you lose it, you've lost all your money. In a world where transactions are immediate and final, they cannot be reversed; if you send 1,000 dollars when you meant to send 100, there is little anyone can do.

We may therefore find that in the blockchain world people will prefer to keep the services of an intermediary as a kind of buffer. This too may be an area where banks compete, providing open platforms for their clients to interact with the financial system, while also providing a level of security (key protection and recovery, plausibility monitoring for transactions) and with it peace of mind.

The trading chain:
Portfolio management on blockchain

Because of its ability to hold money, directly interact with markets and, via a set of rules baked into a smart contract, make its own decisions about buying and selling, a blockchain-enabled smart wallet is a natural portfolio manager.

We already see blockchain applications in the market that behave very much like Exchange Traded Funds, executing simple and easy to understand investment strategies using money sent to them by investors. These are generally available for a limited number of strategies and asset classes, and for predefined risk profiles.

The next step in smart portfolio management will be the ability to trade in multi-asset portfolios, basically handling all the asset classes a client deals with, whether currencies, securities or funds or even physical assets like real estate or art (provided, of course, that ways are found to put such objects onto the chain).

As the systems get more sophisticated, and as artificial intelligence and related technologies become more readily available, smart wallets will get smarter. Not only will you be able to tailor them to your exact needs; once configured, they will be able to automatically digest and implement investment advice and other information sent to them in your portfolio in ways that conform to your particular investment preferences. In the future, then, you may shop around for asset allocation or investment suggestions from various providers, which will then be delivered directly to your wallet, perhaps through a subscription service, for the wallet to use.

It is conceivable that your wallet could become smarter still, not just responding autonomously to trading suggestions, but actively scanning markets and other sources of information – in effect doing its own research – and then making its own investment decisions. Such artificial intelligence-enabled wallets could also, in theory, react quickly on their own to market-relevant events like catastrophes.

These are capabilities that are already being developed for institutions and sophisticated investors like hedge funds. In the future, thanks to blockchain, individual investors may reap the same benefits. This is part of blockchain's potential to democratize finance, providing ever more sophisticated solutions at affordable prices to all.

Chains of beings:
You and your digital identity

We saw above that in the blockchain world people are identified through their pseudonymous public key, and that in theory this key can be associated with any number of verified attributes – allowing you to both authenticate your identity and maintain your privacy.

Such capability could make using identity in the financial system (and elsewhere) much easier. Once you have gained the right credentials, you will not need to prove your identity every time you open an account, and banks won't need to carry out the expensive business of checking up on you. It will also be much easier for you to demonstrate that you are suitable for certain financial products or are domiciled in an area where a product is allowed to be sold.

Because you are free to only reveal the credentialled attributes necessary for a given transaction, you will be able to split your identity into a multitude of different profiles. You may for example want to share a great deal of your personal information with your financial advisor, and less with your broker.

You may also choose to use your public identity to broadcast certain things about yourself, like "I am a verified collector and in the market for an antique car," without revealing who you are. With credentialed pseudonyms you can conversely "meet" people online and, without knowing their names, still learn something reliable about them. This can be useful for instance when searching for potential partners in an enterprise. It should also help enable the growth of direct markets, for example for art, antiquities, houses, or boats (see next section).

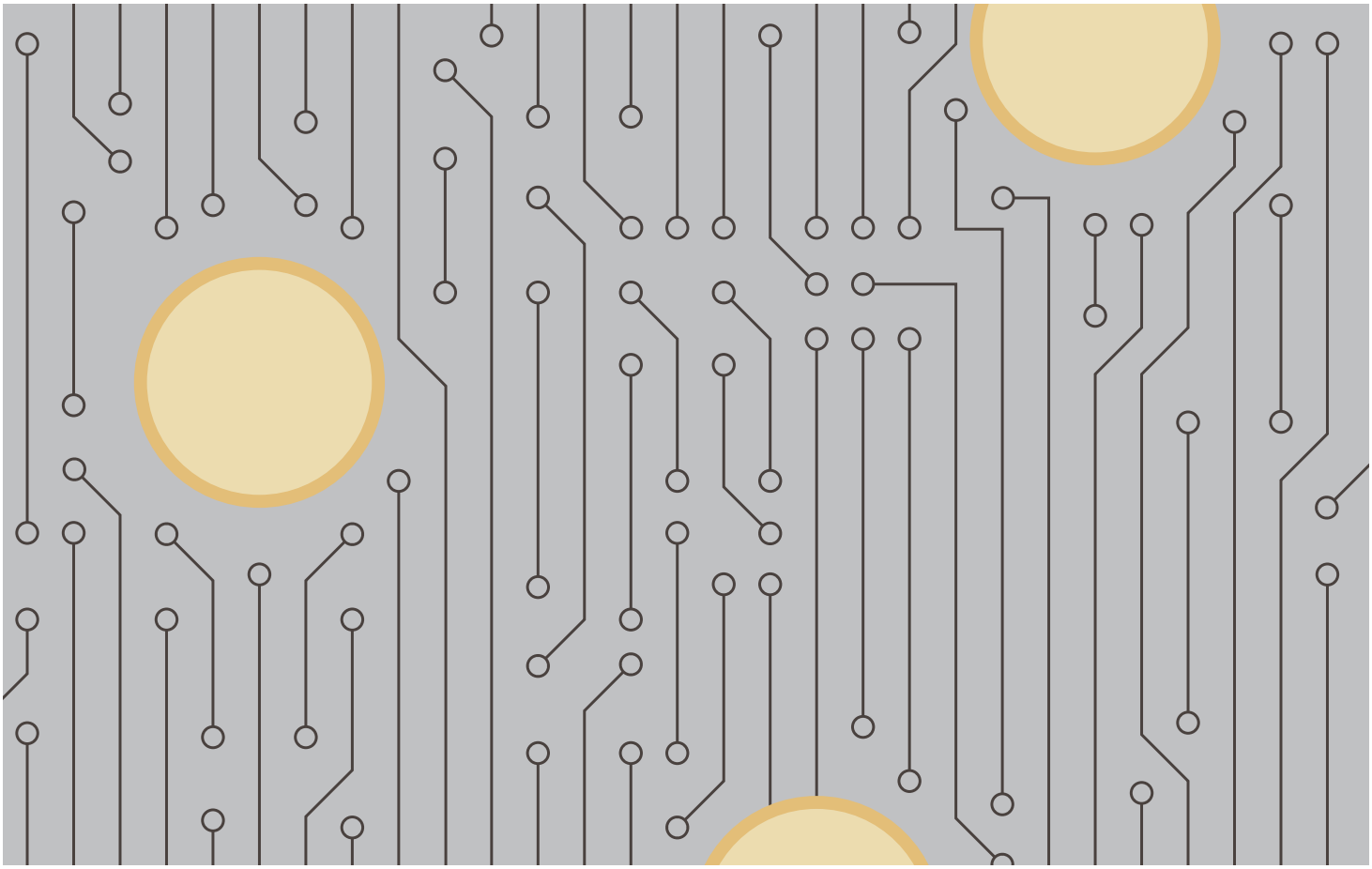
Here too, banks could serve a role as providers of credentials. As we saw above, in the blockchain world your private key becomes extremely valuable. If it is stolen, a malicious person could do you great damage. Banks could thus also provide an important function as safe guarders of private keys, and hence identities.

Chains of things:
You and your "digital" possessions

As we also saw above, the blockchain can be used to transact physical assets by using tokens that uniquely identify them on the chain. This would allow you to trade real world objects with the same levels of trust and finality that the blockchain offers for financial transactions.

In such a world, the certification of assets – providing *bona fide* credentials that can be attached to the object's token – would become increasingly important. We already see businesses arising to provide authentication of things like diamonds, art, or luxury watches, and this trend will continue. As the system matures, trustworthy records of the provenance of assets should become increasingly available on various distributed ledgers, which would go a long way to reducing fraud and counterfeiting. It would also help ethically minded buyers avoid the purchase of such things as blood diamonds or stolen antiquities.

The use of credentialed pseudonyms for people and things should also facilitate the development of direct markets for transactions in large value assets like real estate, art, yachts or planes. As a result, specialist businesses may arise – perhaps through banks – to provide credentialing services specific to these markets, as with the antique car collector mentioned above. Banks may also continue to have a role in bringing buyers and sellers together by developing such



direct market platforms themselves and vetting participants.

This phenomenon need not be exclusive to the wealthy. With the rise of eBay and similar services, we already have online markets for all sorts of goods. The blockchain could give these new impetus by providing both a means of verifying creditworthiness and making direct payments – all without a middleman.

Gold chain:
You and your own private currency

Ever fancy issuing your own money? Minting your own coin, printing your own banknotes, and seeing them circulated in the wide world as an accepted medium of exchange? While this may seem like a fantasy today, in the past private currencies were rather common. Thanks to the blockchain, they may soon experience a renaissance.

One reason is that the blockchain is, by design, well suited to the task of making currencies. It provides a simple technical platform for issuing them, bringing them into circulation, and using them for transactions. And it provides a strong decentralized trust mechanism to help back them up. No wonder that there are already over 600 blockchain-based currencies in circulation, the so-called altcoins[9].

Does this mean we will eventually see – as some have speculated – seven or eight billion currencies, one for each of us? Probably not. But an increase in the use of private money to meet specific needs is likely.

We may for example see specialized currencies offered by recognized institutions like banks, for example to mitigate currency risk when transacting high value assets. With the current volatility in currency markets, buyers and sellers of big-ticket items like planes, yachts or houses – where it can take a long time between when a sale is arranged and title transferred – are highly exposed to negative currency movements. A private currency, provided by a bank and kept stable, perhaps by linking it to gold, would solve this problem.

Specialty currencies need not be only for the rich, however. Most of us already use them in our daily lives without realizing it, in the form of loyalty points. Frequent flyer miles, for instance, are in essence an agreed medium of exchange, the same as money. So too are online gift certificates. In the blockchain world it will become easier for vendors to create such loyalty programs, and to make them more interchangeable. You can already use your air miles to buy non-travel related items provided by your airline. In the future, you may be able to trade them for anything you like.

In theory we could also use the blockchain to make our own loyalty programs, which would be like having a private currency. We could use these with our friends and acquaintances in exchange for services in informal local economies, for instance. Or as enticements for our children to behave.

9 See http://coinmarketcap.com/currencies/views/all/ for a list of cryptocurrencies with market capitalizations.

The trust platform: Blockchain and banking for business

Imagine a future where all sales involve immediate transfer of funds and businesses have instant access to cash. Where late or non-payment is a thing of the past and collections unnecessary. A future where capital markets are much more direct than they are today, and in which corporate financial instruments do their own asset servicing and accounting. A future where direct lending and crowdfunding become viable for far greater numbers of people around the world thanks to blockchain-enabled trust mechanisms.

Imagine a world where you could always be sure of the creditworthiness of your customers, without violating their privacy. Where, reassured by blockchain's privacy mechanisms, your customers more willingly share their relevant personal information with you, information you can rely on. Imagine a world where cash registers automatically send sales tax to the state, products act as their own accountants, and timesheets autonomously pay contractors. In this chapter we look at some exciting new prospects that the blockchain-enabled world holds for business.

Show me the money:
The real-time payment paradigm

If you own your own business, then you know the routine. You provide your product or service. You send your bill. You typically wait 30 days for it to be paid. A certain percentage of your invoices will be paid late, requiring you to send reminders. Some won't be paid at all, requiring legal action of some sort. Even under ideal circumstances, a great deal of your time and effort is expended dealing with accounts receivable. From a business's perspective, this is hardly an ideal state of affairs.

The blockchain may offer some relief. If a company's customers are on the chain, then the company woud easily be able to check their creditworthiness (without compromising their privacy). That should cut down on deadbeats. It would also be easier to arrange for direct payments via the chain, which would mean immediate use of funds and less costs for intermediaries like credit card companies.

But the blockchain can do more. As natural escrow agents, smart contracts could greatly simplify delivery versus payment, particularly when connected to the Internet of Things. We can imagine for example a shipping container fitted out with a radio sender and a smart contract. When it arrives at port, the recipient opens the container and verifies the contents. If satisfied, he or she could use the sender to verify receipt – and automatically unlock funds which had previously been sent to the contract and held pending delivery.

By radically reducing the cost of transactions, the blockchain will also make micropayments more feasible. Today we can subscribe to a newspaper on a day-to-day basis. In future it will be much easier for media outlets to arrange for pay-per-article or even pay-per-paragraph

schemes (in case you get bored in the middle of the piece). This capability will no doubt suggest whole new business models.

No issues with issuance:
The direct capital paradigm

One of the great successes of the capitalist system has been securitization. By allowing corporations to raise funds through the issuance of stocks, bonds and similar instruments, we have found a powerful means of allocating capital from savers to useful areas of investment, benefitting all involved.

While it works well, the business of issuing and servicing securities is not without its complexity or cost. Issuers need the services of specialists to structure, price and bring the securities to market. That involves various fees, for example accounting and legal fees, registration costs and underwriting fees. Once issued, securities need to be serviced, which involves fees as well – for custody, for example, or reporting. Companies must also have systems in place, or pay a third party, to ensure that dividends and coupons are paid on time and to the right people. There is also a great deal of reporting that needs to be done for tax and accounting purposes. The owners of a company's equity or debt must also be informed of important corporate actions, like stock splits or changes to company statutes. This too costs time and money.

We saw in a previous chapter that smart contract technology is enabling the development of smart securities.

With them, companies would be able to benefit from a much more streamlined, efficient and cost-effective securities issuing and servicing process. These programmable stocks, bonds and other instruments live on the chain. As autonomous agents, they can pay their own coupons and dividends, self-register their owners, carry out their own reporting, and so on. This would bring down the cost of securities issuance and servicing.

It would also offer new possibilities. Since they are easily programmable, it should be possible to create far more customized securities, perhaps tailored to individual investors. It would also make it easier for smaller entities to issue their own equity and debt. Issuers will still likely need the services of experts to help with pricing and market placement. But the automated nature of smart contracts should facilitate the creation of platforms to disseminate this expertise more cost-effectively, for example by providing template smart contracts which can be downloaded and customized.

Happy in a crowd:
The direct funding paradigm

One of the most interesting developments in markets over the past few years has been the advent of crowdfunding platforms that allow people to directly lend money to enterprises or individuals with ideas they believe in. This has opened up new avenues for raising capital, particularly for smaller businesses and startups.

Crowdfunding arose before the blockchain, and is not dependent on it. The blockchain, however, may provide a means to greatly expand the model. By providing verified identities and other trusted information, the blockchain could simplify due diligence on public platforms, which would be a great benefit. If two women in a garage in Nairobi or Kabul have an excellent idea for a product, they may still struggle to convince people in London, New York or San Francisco that they are legitimate. If they can attach credentials to their identities, perhaps through a non-governmental organization or some other entity specializing in such a service, they could provide more reassurance. That would help level the playing field, and could help increase investment in parts of the world that sorely need it.

The blockchain may also be a catalyst for banks to move to public crowdlending platforms, as many hedge funds have already done. After underwriting corporate issues they could use such public platforms to syndicate the loans. Because public platforms are less expensive than proprietary ones, this would reduce costs, and these reductions would likely be passed on to the issuers. These and other developments could drive significant efficiencies in the cost and complexity of financing.

Keeping track:
The self-administration paradigm

No business owner has ever complained of having too little administrative work. Between accounting, reporting, accounts receivable, accounts payable, taxes, payroll and compliance, just handling a company's finances involves a dizzying array of tasks, and keeping track of a vast amount of information.

The blockchain can help here as well by contributing to the further automation of many of these processes. In a blockchain-based system smart contracts could be written to automatically pay VAT directly to the state when products are sold, and report sales directly into business accounting systems. Smart contracts could conceivably be written to automatically prepare business and corporate tax returns. More fully automated systems could also handle reporting, including the possibility of automatically generated financial statements and annual reports. Such a system could also automatically send those reports to all registered shareholders. With verified entities, businesses may also be able to automate a great deal of the auditing functions behind financial statements and greatly reduce the risk of accounting errors.

Businesses could also use the blockchain to further automate payroll, for example by devising timesheets that automatically pay hourly or freelance staff. Blockchain-based systems may make it easier to work with freelancers by making it easier to vet their credentials. The same micropayment possibilities for products and services we saw above could also be applied to contractors, so that companies only pay for the actual number of minutes worked, or lines of code written. This would make it easier for companies to manage distributed workforces, while giving contractors and freelancers more tools for interacting with – and also proving their worth – to their clients.

Keeping in touch:
Managing B2B and B2C relationships on the chain

Modern technology has made it possible for companies to collect an incredible amount of data about each and every one of us, sparking one of the great debates of our age. On the one hand, many people are becoming increasingly uncomfortable with the amount of information that is being accumulated about them. Not only do they feel their privacy is being invaded. They also have no control over how this data is collected or any means to verify that it is correct. On the other side, businesses want to understand their customers better so they can better serve them. Yet today's disorderly flood of customer data, much of which may be irrelevant or erroneous, does not necessarily help them in this endeavor.

The blockchain offers the possibility of creating a middle ground suitable to all. Using credentialed pseudonymous identities, consumers will be able to share only those parts of their identities that are relevant for the product or service they are interested in, and do so as easily as they today grant access to location information or contacts on their phones. Pseudonymity may very well make them more inclined to do so, as there are many instances where this is desirable. I want my bank and my newspaper company to know my address, for instance. I don't want to share this information with the site I use to send electronic birthday cards. Similarly, I want all businesses on the Internet to know that my son is under 18 years of age, but not his name or where he goes to school.

Businesses could profit from such a new identity paradigm. It could radically improve the reliability of their customer data. It would also relieve them from having to collect and sift through reams of irrelevant information. And it could strengthen customer loyalty, as people who choose to share information about themselves with an organization will likely feel more well-disposed to it than to organizations which gather data without their permission.

Connected with the Internet of Things, the blockchain could also revolutionize how companies sell and service their products. A car leasing company, for instance, could see to it that a car only starts if payments have been made. In a similar way, appliances connected to the Internet of Things could report back information about themselves: if they need service, for example, or if they have been illegally tampered with.

All of these possibilities apply equally to business to business relationships, where the blockchain could greatly simplify and make more efficient the way businesses work together. Once again we are dealing with a whole new paradigm, one that opens up a whole new world of possibilities.

The trust collaboration: Enabling blockchain in financial services

Imagine a technological revolution that was the result not of competition but of collaboration. Technical breakthroughs create excitement, and when they first appear people are naturally motivated to experiment with their possibilities. This is good, as it fosters innovation. But it can quickly lead to mass fragmentation of the new platform, as people create their own versions of the technology, and jockey to have their implementations become the standard. It can take years and even decades to find common ground.

And yet it is generally only when common ground is found – when standard protocols and fabrics develop – that new technologies can flourish. When it comes to the blockchain, instead of repeating the mistakes of history we think it makes sense to learn from them, developing the blockchain's common standards now, when it is easiest to do so, and together, so that we all may benefit from them.

The long and winding road: Hurdles to a blockchain future

So far in this paper we have looked at what this exciting new technology called blockchain can do, and extrapolated as to what benefits this could bring to our financial system and those who use it. This is not the same as saying it will be so. We are well aware of the hurdles that stand in the way, the questions that are yet to be answered, and the great amount of work that will need to be done.

The first set of hurdles are technical. Blockchain proper has issues of speed which need to be overcome, though much has been accomplished in this area already. There are also questions around scalability: a distributed ledger recording every transaction in a securities market would get very big very quickly, potentially overwhelming systems. There are also serious questions about security that will need to be answered in order to make an open source financial system viable.

The second set of hurdles revolve around the issue of mass fragmentation mentioned in the introduction to this chapter. This technology is very exciting and it is right and proper that people try to build viable businesses around it. That provides the incentives to unlock its potential. We strongly believe however that it makes sense for all involved to collaborate on the basic foundations of this new world, so that we can all build our own solid houses on top of it.

The third set of hurdles are in the area of governance. To build a large, open source system which can be shared by all will require common rules. The existing financial infrastructure has these to a great extent, but in the blockchain world, which works differently, these rules will have to be written anew. Blockchain also raises a host of

legal questions. As new types of contracts and products arise, they will need new legal frameworks.

A coat of many colors:
The need for an open source fabric layer

We think one of the most important tasks in enabling the blockchain future will be to establish a common market fabric: the common underlying layer upon which everyone will build their own service offering. If we can do this, we can truly unlock blockchain's potential to the benefit both of ourselves in the industry and our clients.

Where should we start? As part of our experimentation with the blockchain we have asked ourselves this question often. What essential capabilities at a systems level, outside of the development of blockchain technology proper, would the market most likely need in five years time in order to reap the full benefits of the blockchain? Among the many possible answers, we feel the following are particularly important.

Who is who: Baking identity into the chain.
While public-key cryptography in theory offers all of the advantages of credentialed pseudonymity we outlined above, the devil will be in the details. The truth is that identity is an issue the financial industry has long been struggling with, and not just with people. Our system connects an unfathomable number of entities, individuals, assets, and instruments together, and is composed of a complex web of internal systems, vendor systems, market wide systems, and so on. As a result, it is awash in identifiers.

While we are able to deal with these today, it is an enormous challenge, and a costly one. To bake identity into

the blockchain ledger and make it part of the new market fabric, we will need to tackle this problem at its root, through standardization. That would allow us not only to provide the credentialing for individuals that could be so beneficial, but also for all the parts of the system that will still need to talk to each other. If successful, such standardization of identifiers could drive massive efficiencies.

How much: Putting value on the chain.

We have talked throughout this paper of blockchain's ability to easily and securely transfer value. While this is true, a blockchain-based financial system will not reach its full potential until we can use it to transact in national currencies. At the moment, those using Bitcoin and other altcoins are dependent on exchanges to turn these currencies into legal tender in the real world. We will need to find a way to get legal tender onto the chain. Central banks are beginning to talk about the possibility of creating reserves directly on chain, potentially heralding the advent of cryptodollars and cryptopounds. Through blockchain reserve accounts at central banks, commercial banks may be able to do the same. Much however remains open.

Who's the boss: Settling issues of governance on the chain.

A financial system – like any large system – needs rules. As a blockchain-enabled financial system would be fundamentally different than what we have now, the rules which govern our existing system will likely not translate neatly. We will need a new rulebook.

At a technical level, this means developing a single or at least a very reduced set of protocols. The Internet, with its TCP/IP, HTML, SMTP and other base protocols, can serve as an example. In the blockchain-enabled financial system we will see something similar. But who will ultimately decide what kind of blockchain we will build? And how and when to update it?

The same will hold true for specialized protocols that will likely develop on top of the basic blockchain. Common utilities like JavaScript or PDFs have made our experience of the Internet much better. In the blockchain financial system such specialized protocols will likely be asset-class based: an equity protocol, a fixed income protocol, and so on. Here too, who will devise and manage it? Such issues of

protocol governance have not always been easy to settle in the Internet world. The recent schism in the Bitcoin world is a poignant reminder of how difficult such questions can be[10].

There will of course be a host of legal questions to tackle too. To what extent are smart contracts (or certain aspects of them) recognized as binding legal contracts? Additional legal principles may need to be created to govern them. In theory, smart contracts are self-enforceable, to help make them "airtight." In practice, they are only as good as the underlying code. Who adjudicates if a smart contract turns out to contain ambiguous conditions? Or if it has a bug?

Chain gangs:
Industry collaboration in the blockchain space

These are still early days for the mainstream adoption of blockchain – but they are already heady ones. Last year interest in the technology exploded, with over one billion US dollars having been invested in blockchain enterprises[11]. That number is set to increase dramatically in 2016.

This interest can be gauged in other ways as well. Central banks, including those of England, Europe, Japan, Holland, Russia and China, to name a few, have announced plans to experiment with the technology, or have published papers on its possible uses. Regulators, for example those of Singapore and the UK, have also expressed great interest in blockchain. Organizations that make up the common financial infrastructure, like DTCC, Euroclear and SWIFT, have endorsed the potential of the blockchain as well. And we have seen exchanges begin to embrace the technology too, for instance Nasdaq, whose Linq platform uses blockchain to provide a market for private securities issuance.

The fintech community has of course been very active in blockchain. New ventures like Digital Asset Holdings, Ripple, Clearmatics and Ethereum have been developing blockchain-based applications to meet a wide variety of use cases, and industry stalwarts like Microsoft and IBM are also offering blockchain-based services. At the same time we are seeing important open source projects in the blockchain space, for example Hyperledger.

A great many of our bank peers have also stated that they are investing in and working with blockchain. Companies like Santander, Goldman Sachs, Citicorp, and many others have begun investigating and/or experimenting with blockchain use cases. The good news is that there seems to be a clear desire among banks to collaborate. This can best be seen in the R3 CEV consortium, which consists of over 40 global banks including UBS. A concerted effort to help build the base layer blockchain technology that may underpin a blockchain-enabled financial system, and to do so with bank input, it is perhaps the most far-reaching blockchain collaboration platform in existence at the moment in our industry.

Come in to the lab:
Blockchain innovation at UBS

How does blockchain innovation take place? Like any other kind: through a bit of inspiration and lots of perspiration. This is certainly the case at UBS where, like many of our peers, we have been busy exploring blockchain and experimenting with its possibilities.

In 2015 we launched our own in-house blockchain program called "Crypto 2.0 Pathfinder". As part of this we opened our own innovation lab, making a conscious decision not to place the lab within the bank but rather in an external fintech startup environment. We found the perfect location when we joined the Level39 fintech incubator in London, the first and only global bank to do so. At Level39 our experts can easily exchange ideas and insights with the wider fintech community, and so collaborate on pushing this technology forward.

The lab has provided a platform for us to carry out a number of experiments that serve as proof of concept for various blockchain use cases. In one, we created a "smart bond" to validate the feasibility of the overall blockchain approach as well as our initial smart contracts hypothesis. Our application was able to recreate a bond's issuance, interest calculation, coupon payments and maturation processes without pre- or post-trade intermediaries. To achieve this we created our own virtual coin, which we dubbed the BondCoin, and which functioned as a token intended to be linked to real-world currencies via a central bank account. We have also conducted an experiment with a 'utility settlement coin' which is intended as a token of value linked to a real fiat currency on blockchain and used to settle transactions in multiple asset classes.

These kinds of experiments help us to both test hypotheses and gain experience in this new world. Small steps at the moment, we hope they will be the basis for large strides in the future.

10 For more see: http://www.theverge.com/2016/2/9/10946072/bitcoin-core-classic-software-block-size-debate.

11 See: http://money.cnn.com/2015/11/02/technology/bitcoin-1-billion-invested/

The future of trust

Afterword: The future of trust

We have just taken a long trip down the potential path of the upcoming blockchain transformation. As we hope has come through in these pages, we are very optimistic about the possibilities of this new technology. We are however not naïve about its potential to disrupt our business.

Quite the contrary, the more we learn about blockchain, the more we understand how transformative it may be. It will force us as banks, as it will force many other types of institutions in our industry, to re-evaluate what we do, sometimes radically. To close then, we provide a thought on what might be the most important blockchain-driven paradigm shift for our business in the future – the disintermediation of trust.

In the pre-blockchain world, being a large financial institution was good for many things. Large banks like ourselves could take advantage of economies of scale to provide more cost-effective transaction services. Having large brick and mortar operations also helped foster trust: it showed that we were serious and successful, competent and solid. Banks of course are required to hold a lot of capital as a sign of their trustworthiness as well.

In a blockchain-enabled future, all of this may be turned on its head. If trust is moved from private institutions to a public chain, then large, expensive, highly capitalized entities will not be necessary to enforce it. Since centralized systems are more expensive and less agile then public ones, they will be at a disadvantage. These developments will also significantly lower the barrier for entry for new players. Without expensive legacy platforms to deal with, these will be free to concentrate on innovation.

Does this mean the end of banks? We don't think so. The developments we have been describing mostly affect the world of financial transactions. Long before the blockchain arrived, the tendency had been for these services to be commoditized and become common utilities. Bank revenues from transactions have been steadily falling for years. The blockchain simply offers us a way to bring this trend to its logical conclusion. As we said in the foreword, it would be irresponsible of us to ignore such a significant development. Instead, working with fintech, we will transform ourselves, continuing to innovate and to change into the new paradigm.

Banks however do more than just carry out transactions. Since the dawn of our industry, we have also offered advice and a host of other value added services to help clients manage and protect their money. This will not change. Indeed, in an ever more complex, technologically driven world, the need for knowledge and experienced-based services may well increase. Banking has also always been a business based on relationships. We think bank clients will continue to value the human touch.

Other organizations in the financial system will go through similar transformations. While the blockchain may replace a great deal of our clearance and settlement infrastructure, for instance, the functions themselves will not disappear. They will simply be handled in a different way. There will always be a need for those with knowledge of these functions to help set standards, build the new infrastructure and maintain it.

Finally, while we have concentrated on the financial use cases for the blockchain, there are a great many other areas where blockchain technologies could – and likely will – cause great transformation. From government records to art markets to intellectual property to consumer protection to real estate registries and on and on. Wherever we have need of lists – and that means almost everywhere in our complex world – that is where the blockchain can be profitably employed.

We are happy to be a part of the effort to build the new trust engine because it is the right thing to do. If this engine is as powerful as we think it can be, it should drive us all a very long way.

Appendix

An (important) note on terminology

It is not uncommon when a new technology gets introduced for there to be confusion as to correct terminology. This is certainly the case in the world of blockchain as it evolves. Here is a short glossary:

– The **blockchain** proper is the distributed ledger used to record Bitcoin transactions. The methodology behind it has since been employed to record many other things, so it has become common to use the term blockchain to refer by extension to the technology, as we do in this paper.

– A **distributed ledger** is a ledger – a list, spreadsheet or database – that is shared among nodes in a decentralized network. It is not uncommon these days for people to use the term interchangeably with blockchain. Correctly speaking, the blockchain is a type of distributed ledger.

– A **digital currency** is a currency that relies on digital technologies. A **cryptocurrency** is a type of digital currency that employs digital cryptographic techniques. Bitcoin was the world's first decentralized cryptocurrency.

– The word Bitcoin is capitalized when referring to the concept or the overall network; it is written in lowercase when referring to the actual currency, as in the sentence "A friend of mine explained **Bitcoin** to me, and then showed me how she used her wallet to transfer one **bitcoin**."
See https://bitcoin.org/en/vocabulary.

A final note: In this paper we refer almost exclusively to **banks** when talking about trusted financial intermediaries. We are of course aware that there are many other types of organizations, like clearing houses or exchanges, which are vital to the financial system and provide similar intermediary roles. For the sake of simplicity, we have at times used the term bank to refer to these as well.

For further reading

Books and papers:

Bitcoin: A Peer-to-Peer Electronic Cash System
Satoshi Nakamoto, 2008
Available for download at https://bitcoin.org/bitcoin.pdf. This is the paper that started it all, and is now a classic. Short and very well written, it is surprisingly accessible despite being a technical paper.

The Age of Cryptocurrency - How Bitcoin and the Blockchain Are Challenging the Global Economic Order
Paul Vigna and Michael J. Casey, 2016 edition
An excellent recap of the rise of Bitcoin and blockchain as well as possible blockchain use cases.

Mastering Bitcoin: Unlocking Digital Currencies
Andreas M. Antonopolous, 2015
While written for programmers, the initial chapters of this book provide an excellent introduction to how Bitcoin and the blockchain work in a way that can be understood by non-specialists. Highly recommended.

Identity is the New Money (Perspectives)
David Birch, 2014
Not about blockchain *per se*, this book provides an excellent discussion of the changing identity paradigm in our digital world, a paradigm which a blockchain-enabled financial system will likely make use of.

Websites:

https://bitcoin.org/en/ - the original Bitcoin site.

https://bitcoinmagazine.com - a leading source of information on Bitcoin, the blockchain and the digital currency industry.

http://r3cev.com - website of the R3 consortium.

https://www.hyperledger.org - website of the Hyperledger Project.

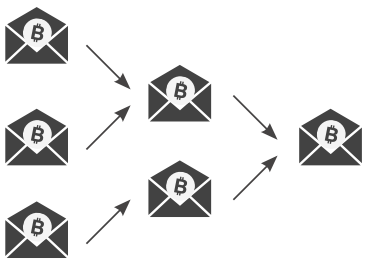
How the Bitcoin blockchain works

While there are now many different methods for creating blockchains, to understand the basic blockchain concept it makes sense to look at the original Bitcoin blockchain. The details are rather complex, and involve sophisticated cryptographic techniques. Here is a somewhat simplified overview of the process.

1 Signed Transaction

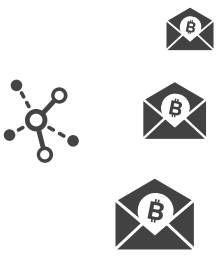
Selena wants to send 1 bitcoin to her friend Martin. She uses her Bitcoin wallet app to create an instruction to send 1 bitcoin from her public key address to Martin's public key address, which she happens to know. The wallet signs the transaction with the signatures authorizing the spending of the funds referenced by the transaction. Although the transaction is now public, only Selena and Martin know they are the parties involved. Everyone else only sees that bitcoin has been transferred between two public key addresses.

2 Transaction Chain



The transaction is then broadcast on the blockchain P2P network, which propagates the transaction across nearly every node. Each node validates the transaction for correctness before relaying it to its peers. For example, it is easy to check if the public key address Selena used actually has 1 bitcoin to spend by consulting the existing blockchain, which is a record of all previous transactions. This makes it impossible for Selena (or anyone else) to double spend bitcoin.

3 Network

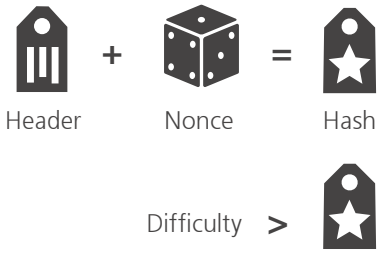


Special nodes known as Miners aggregate the valid transactions they receive and...

4 Block

... generate transaction blocks of 500 transactions each through solving a difficult cryptographic puzzle.

5 Proof of Work



The solution to the puzzle, which is called Proof of Work, is included in the new block to prove its validity. The solution involves incrementing a number known as a nonce in the block header and seeing if the resultant hash of the header satisfies the block difficulty target. The Bitcoin protocol constantly adjusts this target so that it takes on average 10 minutes for a computer to guess the right answer. This is a failsafe: it makes it expensive in terms of computing power (electricity) to carry out mining, and therefore prohibitively expensive for anyone to gain enough computing power to overrun the system.

Miners receive two types of reward for mining, new funds (UTXO) created with each block and transaction fees from all the transactions included in a block. As of this writing, the reward for solving a single block was worth around USD 11,000.00.

6 Blockchain

Once a miner has created a valid block it will broadcast it on the blockchain network where it will propagate to every node. Each node performs some checks to validate it before forwarding to its peers. If valid the node will then attempt to add the block to its existing copy of the blockchain. Each block carries a reference to its previous block (block hash) to facilitate this. Once a transaction is included in the blockchain it is said to be confirmed and the fund transfer has completed. After six confirmations (additional blocks) the transaction is effectively immutable.

Disclaimer

This document has been prepared by Alex Batlin, Hyder Jaffrey, Christopher Murphy, Andreas Przewloka and Shane Williams at UBS AG.

This document is for distribution only as may be permitted by law. It is published solely for information purposes; it is not an advertisement nor is it a solicitation or an offer to buy or sell any financial instruments or to participate in any particular trading strategy. No representation or warranty, either expressed or implied, is provided in relation to the accuracy, completeness or reliability of the information contained in this document ('the Information'), except with respect to Information concerning UBS.

UBS does not undertake to update or keep current the Information. Any opinions expressed in this document may change without notice and may differ or be contrary to opinions expressed by other business areas or groups of UBS. Any statements contained in this report attributed to a third party represent UBS's interpretation of the data, information and/or opinions provided by that third party either publicly or through a subscription service, and such use and interpretation have not been reviewed by the third party.