BRYAN, GARNIER & CO

The Promise of Blockchain

UNDERSTANDING THE IMPACT OF AN EMERGING TECHNOLOGY

TECHNOLOGY WHITE PAPER SEPTEMBER 2017

Contents

Blockchain is a unique and promising technology, with potential application in any field where groups of people have a common aim, yet do not know or trust each other. Today, we see it more as a way of facilitating existing systems. We expect to see partnerships, investments and M&A activity targeting specialists in this technology.

In this paper we explore and explain blockchain, looking first at how bitcoin – the digital cryptocurrency that is based on this technology – works.

We examine how “mining”, the activity essential to validating bitcoin transactions and generating the currency, is driving developments in the semiconductor industry as it creates a constantly rising demand for more processing power.

Finally, we look at the many applications for blockchain technology beyond bitcoin. It is a technology that has extreme disruptive potential – for example removing the need for trusted third parties in fields ranging from banking to payment systems to t he law. However, we believe that despite this potential, blockchain will be initially used as a facilitator rather than a disruptor of existing systems. Banks and payment schemes are likely to be the first to be active in the technology so they can integrate the threat, rather than fall victim to it in the future.

For blockchain to reach its full potential, concerns over the availability of processing power, the legal status of cryptocurrencies and levels of security all need to be considered by the industries adopting it.

RICHARD-MAXIME BEAUDOUX
Equity Research Analyst
Payments and Security, Video Games

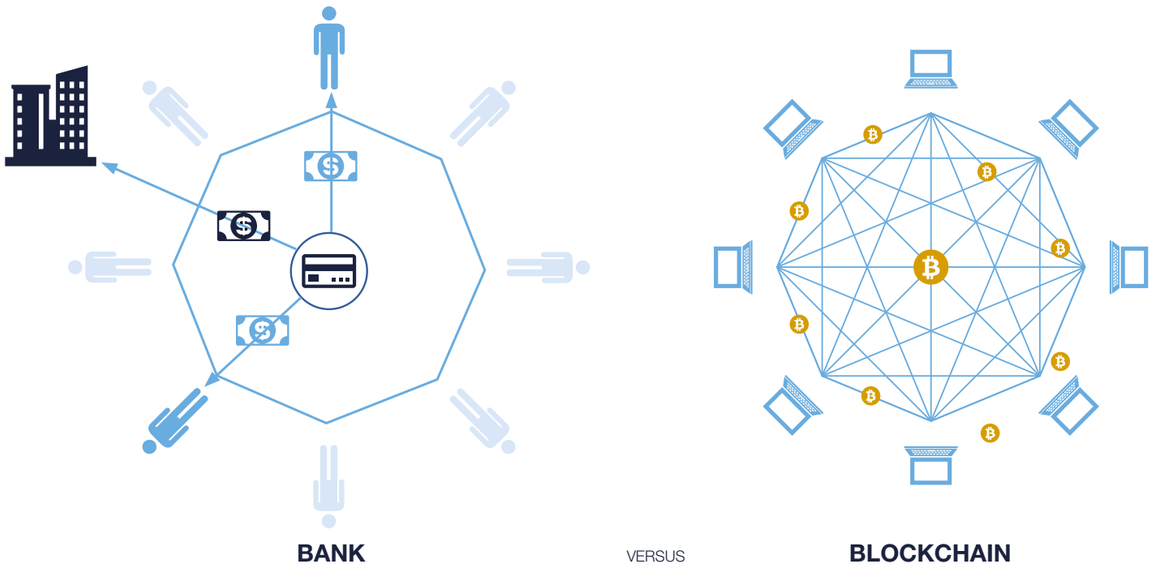
DORIAN TERRAL
Equity Research Analyst
Semiconductors

1. What is blockchain?

Blockchain is a transparent, decentralized and secure way to store and transmit information: it is the system behind the cryptocurrency bitcoin.

Blockchain is a way to store and transmit information in a way that is transparent, decentralized and secure. The technology protocol underpinning the digital currency bitcoin, it was first described in 2008 in the paper "*Bitcoin: a Peer-to-Peer Electronic Cash System*"[1] written under the pseudonym of Satoshi Nakamoto.

FIG. 1: FROM CENTRALIZED TO DECENTRALIZED



Source: Dupress; Bryan, Garnier & Co

There are several types of blockchain, which we explore later in this document. However, we focus first on the bitcoin blockchain. In this blockchain, a peer-to peer (P2P) network of computers validates and updates a global, public ledger of all the transactions that have been made since the creation of the currency. In essence, this "distributed ledger" contains the entire history of all transactions made between users. Computers on the network verify the validity of each block of transactions, and therefore the integrity of the entire ledger. This sets blockchain and bitcoin apart from traditional transaction networks, because there is no need for an intermediary or trusted third party.

BLOCKCHAIN HAS THREE MAIN CHARACTERISTICS AND ADVANTAGES:

TRANSPARENCY

Once a transaction is inserted into the block, it becomes incorruptible and permanent. When the block is validated, it is time- and date-stamped and added to the chain of blocks. At this point, it becomes visible not only to the participants but also the rest of the network. Unique signature keys help identify each block and transaction permanently and chronologically in the ledger. This means that each transaction for each block can be easily traced over its entire history, in full transparency.

DECENTRALIZED STRUCTURE

Unlike a traditional system where the register of transactions is maintained by a central body (a trusted third party), the blockchain ledger is decentralized and autonomous. A network of machines keeps an incorruptible register of all existing transactions up to date. Any computer connected to the internet can keep a copy of the ledger. The system belongs to no-one and has no central controlling authority or hierarchy.

SECURITY

Blockchain is based on asymmetric cryptography and multiple signatures. Anyone can generate a bitcoin address via a public key (enabling receipt of bitcoins), but only a private key can enable a user to prove to the network that they are indeed the bitcoin owner and that they therefore have the right to carry out a transaction in these coins. The network receives, validates, approves and authorizes transaction requests. Network "miners" (computers in the network) compete to validate the blocks to be added to the blockchain. They are paid for this work: in concrete terms, miners' machines execute complex operations to resolve the mathematical problems that will validate transaction blocks. They are collectively responsible for the validity of transactions. This guarantees that there is no fraud in the system. Once it is added to the chain, the block can no longer be modified or deleted, guaranteeing the network's authenticity and security. If a false transaction is detected, it is rejected. To break the system, everyone would have to collaborate to simultaneously modify hundreds of databases at the same time. This is virtually impossible. The system is far more secure than centralized systems, which concentrate both power and data in a way that makes them opaque and vulnerable. Blockchain is a therefore an efficient way to protect against cyber-criminality and fraud. Despite numerous attempts, the system has never been hacked.

1. "Bitcoin: A Peer-to-Peer Electronic Cash System | Satoshi Nakamoto | 2008

Blockchain in action

User A would like to transfer bitcoins to user B

HERE'S HOW THE TRANSACTION IN FIG. 2 BREAKS DOWN:

- Using a public key, user B can generate an encoded address (a row of figures, like a bank sort code) to share with all people who would like to send him bitcoins (similar to an email address that can be given to third parties). A transaction is therefore a transfer of bitcoins to an address.

- Using a software or an internet browser, user A can use their private key (like a password enabling them to access their online bank account). This enables the user to prove that they own the bitcoins and can trade them. (Note that the private key is a randomly chosen number and that the public key is calculated based on the private key via a cryptographic hash function algorithm, which helps identify each transaction block permanently and chronologically in the register). The user can then indicate the number of bitcoins they would like to transfer to the address that user B has provided. In this way, user A effectively "signs" the transaction via the private key.

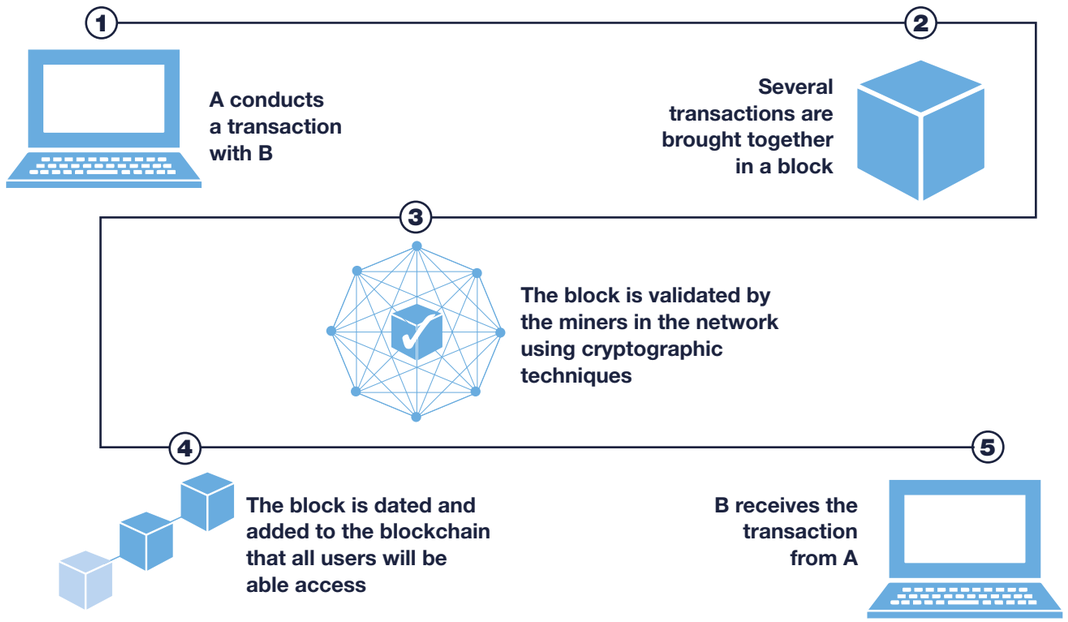
- The transaction created is then sent immediately to one of the miners on the network who sends it out to all the other machines.

- The network of miners proceeds to validate the transaction (verifying the sender, the recipient, the amount available, proof of work, addition to the ledger etc.). Once validated, the blocks are placed online on the network at all the nodes. A miner needs to have a full copy of the blockchain to check the validity of the blocks. The hash functions can rapidly verify whether any content has been modified.

- The bitcoins arrive at a kind of "bitcoin account" belonging to user B (although the term "account" is not entirely correct, it helps understand the principle). The transaction is therefore visible to user B but also to the entire network. Everyone can encode an address via the public key (it is transmissible with no restrictions). But only user B, who owns the private key – which is never transmitted to anyone – can decode it. As it guarantees the confidential nature of the content, the system is perfectly secure.

- The network is only aware of user A once the transaction has been carried out. Until that point, their bitcoin address was only a valid key among many others enabling access to existing transactions. This is why the analogy with the word "account" is not entirely correct. Since there is no real account, the system looks at all the unspent transactions ("Unspent Transaction Output") for which the person is the recipient, to work out how many bitcoins they have (this amount is therefore their "balance").

FIG. 2: TRANSACTION SCHEME IN BLOCKCHAIN SYSTEM



Source: Bryan, Garnier & Co; Bitfury

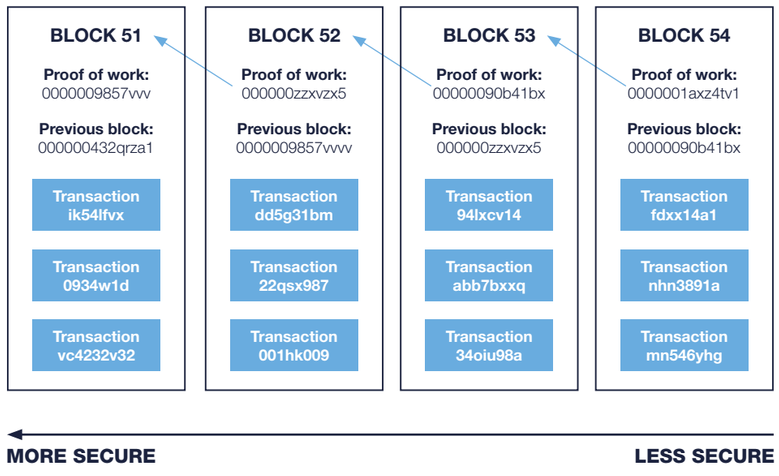
2. Mining explained

To understand how the bitcoin blockchain works, it is important to understand mining, which is the process for validating blocks of transactions.

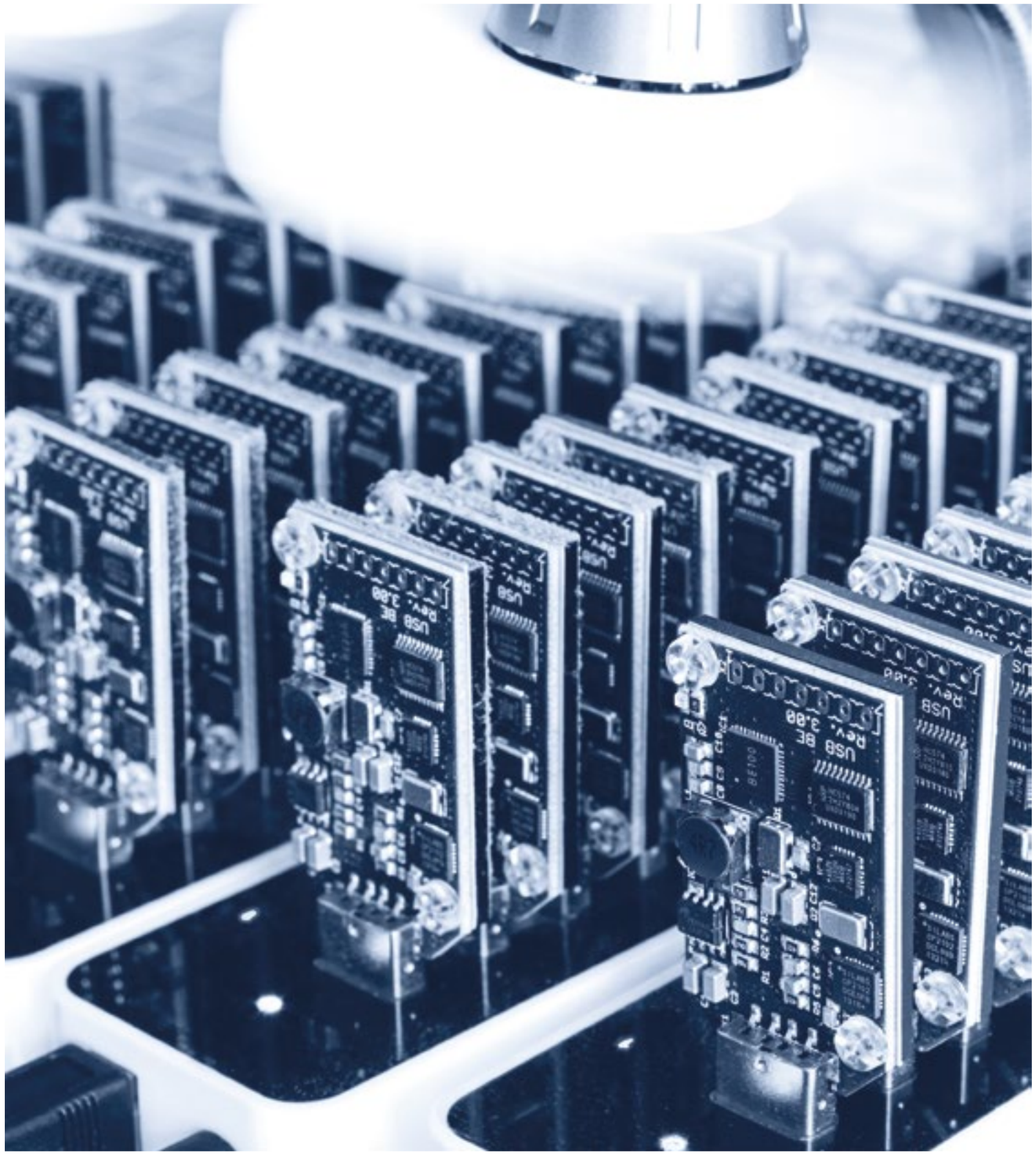
Miners group bitcoin transactions into blocks, and then apply a mathematical formula to the block, called a “hash”. Because this also includes the hash of the previous block, it confirms that this block is valid and it acts as the foundation for the following block. The bitcoin protocol deliberately makes it difficult to create a valid hash, by demanding that it must start with a certain number of zeros. It therefore requires a great deal of computing power and the resulting valid hash is called a “proof of work”. Miners compete to validate blocks and are incentivized for their work by payment in bitcoins: in effect, the process creates new currency.

As the blocks are dependent on one other, a change made to a block would require recalculating all the previous blocks. The older a block is, the less it can be tampered with.

FIG. 3: REPRESENTATION OF A BLOCKCHAIN



Source: Bryan, Garnier & Co



Bitcoins and the fees: the incentives for mining

As soon as a miner validates a block, bitcoins are generated and given to the miner in return for their work. The blockchain was originally intended to have no more than 21 million bitcoins in circulation, a limit set to avoid a situation where the currency's authenticity would be doubted. Remuneration for a validated block is halved for every 210,000 blocks mined (i.e. around every four years, bearing in mind that validation of a block takes around 10 minutes). Since 9th July 2016, mining operations generated 12.5 bitcoins per block validated (compared with 25 bitcoins previously). At the time of writing bitcoin's value stands at USD4,224 (Fig. 4) and around 16m bitcoins are currently in circulation (Fig. 5).

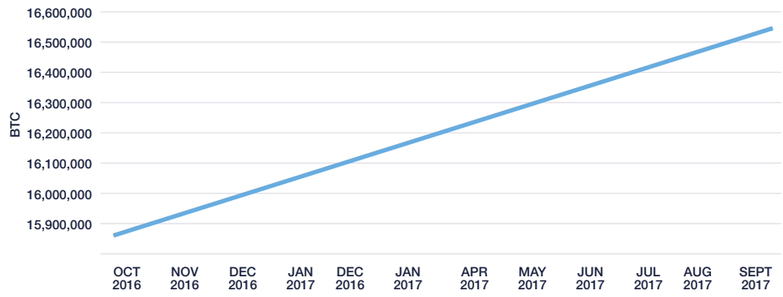
In around 100 years, nearly all 21 million bitcoins should be in circulation. Over time, mining will become less attractive and miners will need a different incentive to continue their validation work.

Bitcoin transactions can also include fees which add to the 12.5 bitcoins received per block validated. These fees are variable, calculated according to factors such as network capacity and transaction volume. Although this means transactions are not always free of charge, fees are negligible given that the various intermediaries are eliminated and there are no operating or staff costs for the transfers. When transaction fees apply, the minimum amount is 0.0001 bitcoin).

FIG. 4: CHANGE IN BITCOIN VALUE IN RECENT MONTHS (USD)

Source: Blockchain.info; Bryan, Garnier & Co

FIG. 5: BITCOINS IN CIRCULATION OVER ONE YEAR (YOY)



Source: Blockchain.info; Bryan, Garnier & Co

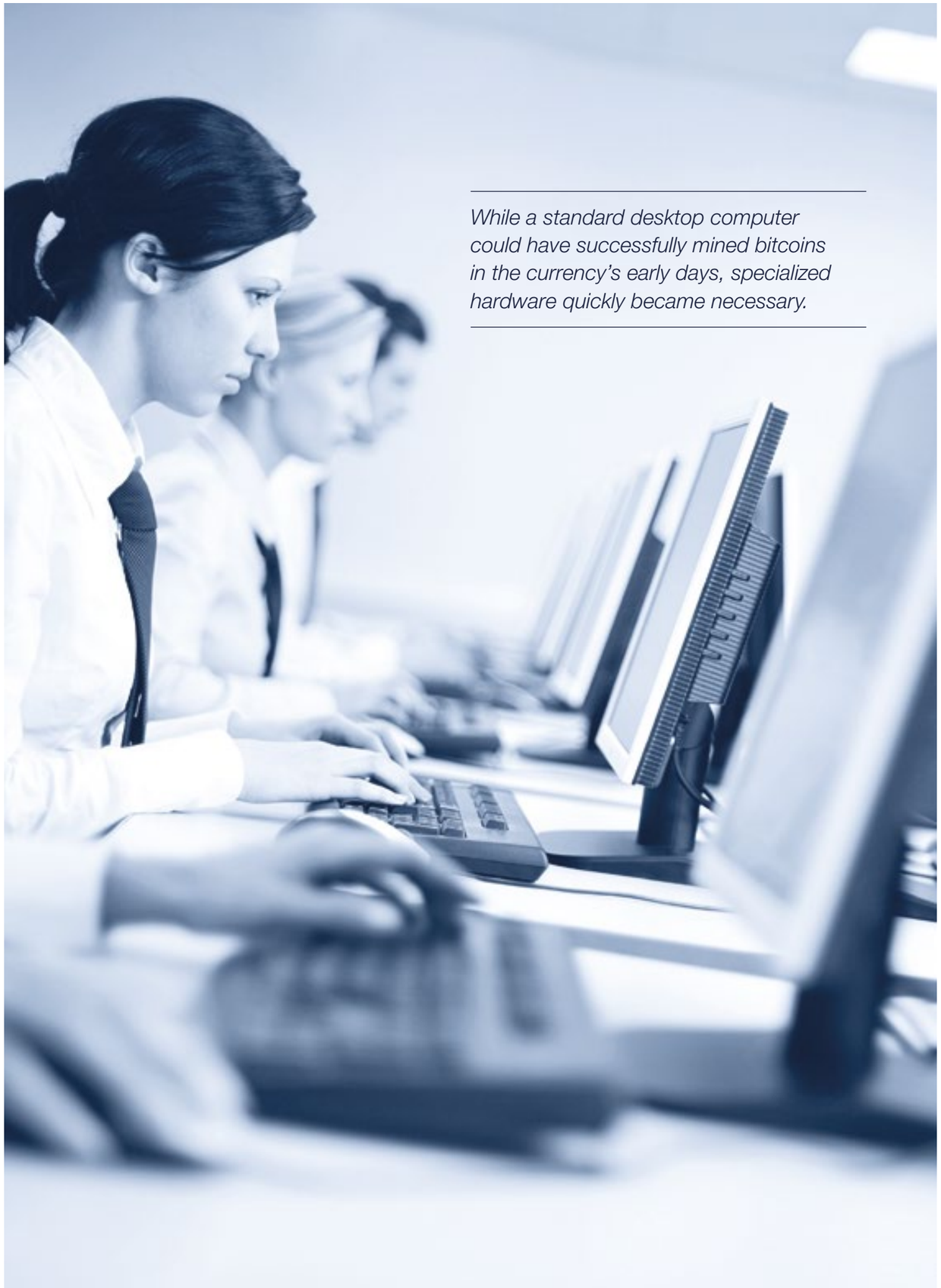
FIG. 6: PROJECTED CREATION OF BITCOINS

Source: Bitfury; Bryan, Garnier & Co

FIG. 7: BITCOIN FEES VERSUS TRADITIONAL SYSTEMS

	REMITTANCE	CREDIT/DEBIT CARD TRANSACTIONS	MICROPAYMENTS / UNBANKED	IOT OPPORTUNITY
BITCOIN	1% fee x USD580bn = USD6bn	0.25% fee x USD20.6tn = USD52bn	0.25% fee x 2.0bn world unbanked = USD16bn	0.1% fee x USD2.1tn + USD0.004 fee x 1.6tn = USD26bn
EFFICIENCY	8x	6x	3x	New
TRADITIONAL	7.7% fee x USD583bn = USD45bn	1.4% fee x USD20.6tn = USD292bn	0.78% M-PESA fee x USD45bn = USD0.35bn	N/A

Source: Bitfury; Bryan, Garnier & Co



While a standard desktop computer could have successfully mined bitcoins in the currency's early days, specialized hardware quickly became necessary.

3. Mining: an increasingly industrialized activity

Miners allocate part of their machine's computing power to resolving the cryptographic problems needed to validate transactions. The first miner to successfully validate a block of transactions wins the bitcoins and can receive transaction fees.

This opportunity for financial gain generates competition to be the first to resolve the problem and offer a proof of work. As a result, miners invest in increasingly powerful machines – and the power of the network is increased too. Mining is becoming professionalized. Overall there are three types of bitcoin miner:

INDIVIDUALS

While it is possible to set up alone with a single computer to mine bitcoins, the investment in equipment and energy now needed to be successful means individual miners are now rare.

GROUP, OR POOL

In group mining, several people or organizations pool their computing power to maximize their probability of success in validating a block. Each miner typically receives payment based on the total volume of bitcoins received by the group, in proportion to the power that was made available to the community.

PROFESSIONAL

Highly organized professional mining companies have developed techniques for mastering the mining chain from end to end and maximizing use of their hardware and computing power.

Two factors are driving this professionalization: a technology "arms race", as miners to be the first to validate blocks; and the fact as that mining becomes less financially attractive over time, more validation is needed to maximize the chance of a return.

While a standard desktop computer could have successfully mined bitcoins in the currency's early days, specialized hardware quickly became necessary: first graphics processors (GPUs), more powerful and energy-efficient than a desktop's CPU; then FPGAs, which offer yet more power and energy efficiency; and now ASIC chips designed specifically for bitcoin and with 100x the computing power of FPGAs.

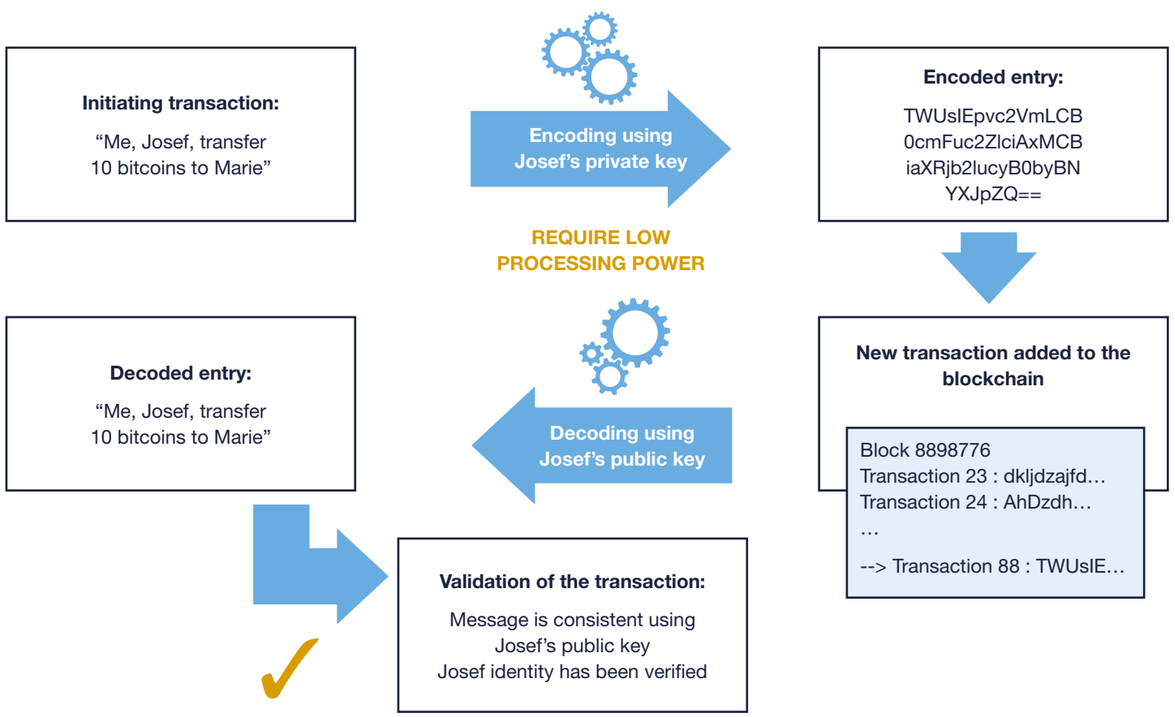
To understand in detail why and how the bitcoin blockchain impacts technology and hardware, it's instructive to look at the cryptography behind it.

Asymmetric cryptography

The first aspect of blockchain cryptography uses relatively little processing power. Asymmetric cryptography, the public/private key system discussed and illustrated on page 5, ensures that transactions are authentic and impossible to fake or repudiate.

While these asymmetrical encoding/decoding operations require little computing power, when aggregated, they are still visible in the network.

FIG. 8: ASYMMETRIC CRYPTOGRAPHY IN ACTION



Source: Bryan Garnier & Co (base64 encoder/decoder used for this example)

Cryptographic hash functions

To make the ledger unbreakable, blockchain relies on a double use of hash algorithms (SHA256 in the case of bitcoin).

The system works with a digital register duplicated across various network nodes. This partially ensures its integrity. To be fully secure, blockchain also needs a mechanism that prevents the ledger from being modified or corrupted while still allowing new transactions to be added. In a digital world where everything can be infinitely changed and copied, this is complicated. As we've seen, to solve this problem, blockchain uses the concept of "proof of work", which demands that the validation of each new block is accompanied by a quantity of computer processing effort.

FIG. 9: VERY DIFFERENT HASH RESULTS BUT ALL THE SAME LENGTH

INPUT	OUTPUT
Hello	3615f80c9d293ed7402687f94b22d58e529b8cc7916f 8fac7fddf7fbd5af4cf777d3d795a7a00a16bf7e7f3f b9561ee9baae480da9fe7a18769e71886b03f315
Hello.	5439af640016553bac5726af138a5bca64e6aab0a33e 21ecb1b3c9525cadcb834c625f1b9fe254dae726c7223e a776e48b7afdb6747b0f96f78b6e46777622b3
Hello, with that spelling, was used in publications in the US as early as the 18 October 1826 edition of the Norwich Courier of Norwich, Connecticut. Another early use was an 1833 American book called The Sketches and Eccentricities of Col. David Crockett, of West Tennessee, which was reprinted that same year in The London Literary Gazette. The word was extensively used in literature by the 1860s.	ae94ba80beb058b212ae3a745ccd2f1f21f62c7aed18ea 4c0a6a3316f6a2faaa7380bc86e8acc5b2799b0340cd 228945b5a2ade55c03ebbccf19fd5f0a78c7cb

Source: Bryan Garnier & Co (SHA512; hexadecimal output)

A minor change, like adding a full stop to a sentence, completely changes the hashed output – but the length of the hash stays the same.

This process uses hash functions, which transform transaction details into a unique character chain that is unpredictable and of a fixed length. Making a minor change, like adding a full stop (see Fig. 9), completely changes the hashed output – and the length of the hash is the same, regardless of the size of the input.

Hash functions are central to blockchain. The ledger is made up of the full list of transactions, sequenced as blocks. As well as recent "pending" transactions (those not yet added to the ledger) each new block must contain the result of the hash of the previous block. This makes it impossible to change a block in the middle of the ledger because this would mean changing the hash result included in the following block, which would also require changing the hash of the following block, and so on. To change a single transaction in the ledger, hash operations would be necessary on all subsequent blocks.

Compared to asymmetric cryptography, hash operations need greater computing power. But to further guarantee the ledger's integrity – by increasing the computing power needed to validate it – new blocks also need to embed a unique identifier, called a nonce. This is a hash result that must begin with a defined number of zeros. Since a hash result is unpredictable, creating one that includes specific values is extremely difficult: it can only be done by hashing random character chains until a hash beginning with the required number of zeros is found. It's this operation that consumes vast amounts of computing power, and it is why validation of a block takes around 10 minutes – the time needed for all computers connected to the network to find an acceptable result.

The difficulty of finding these unique identifiers is what gives blockchain its integrity. To change a transaction not only requires recalculating the hash of the previous block: it also means finding a new identifier for that block. The computing power needed to do this makes it technically impossible to change part of the ledger at any level. Any potential fraudster would need calculation capacity equivalent to over 51% of the entire network's aggregate calculation power.

Blockchain also protects itself against evolution in processing power by adding more zeros over time to the identifiers required to validate blocks.

Creating the special hashes needed to validate bitcoin transactions requires immense computing power.

Chip developments

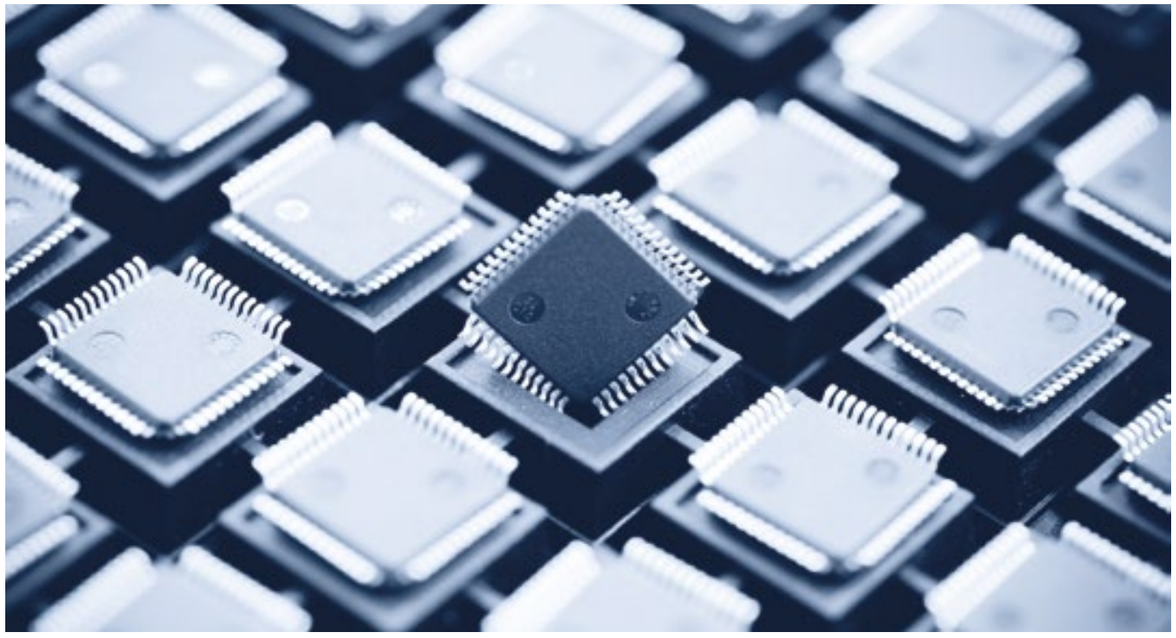
The increasing complexity and competitiveness of validation has driven developments in processor technology. Simple CPUs were rapidly outpaced by faster GPUs, which in turn were outperformed by more expensive Field Programmable Gate Array (FPGA) modular chips, which can be adapted for hash functions and are more energy efficient. (For some miners, energy bills exceeded the returns on mining).

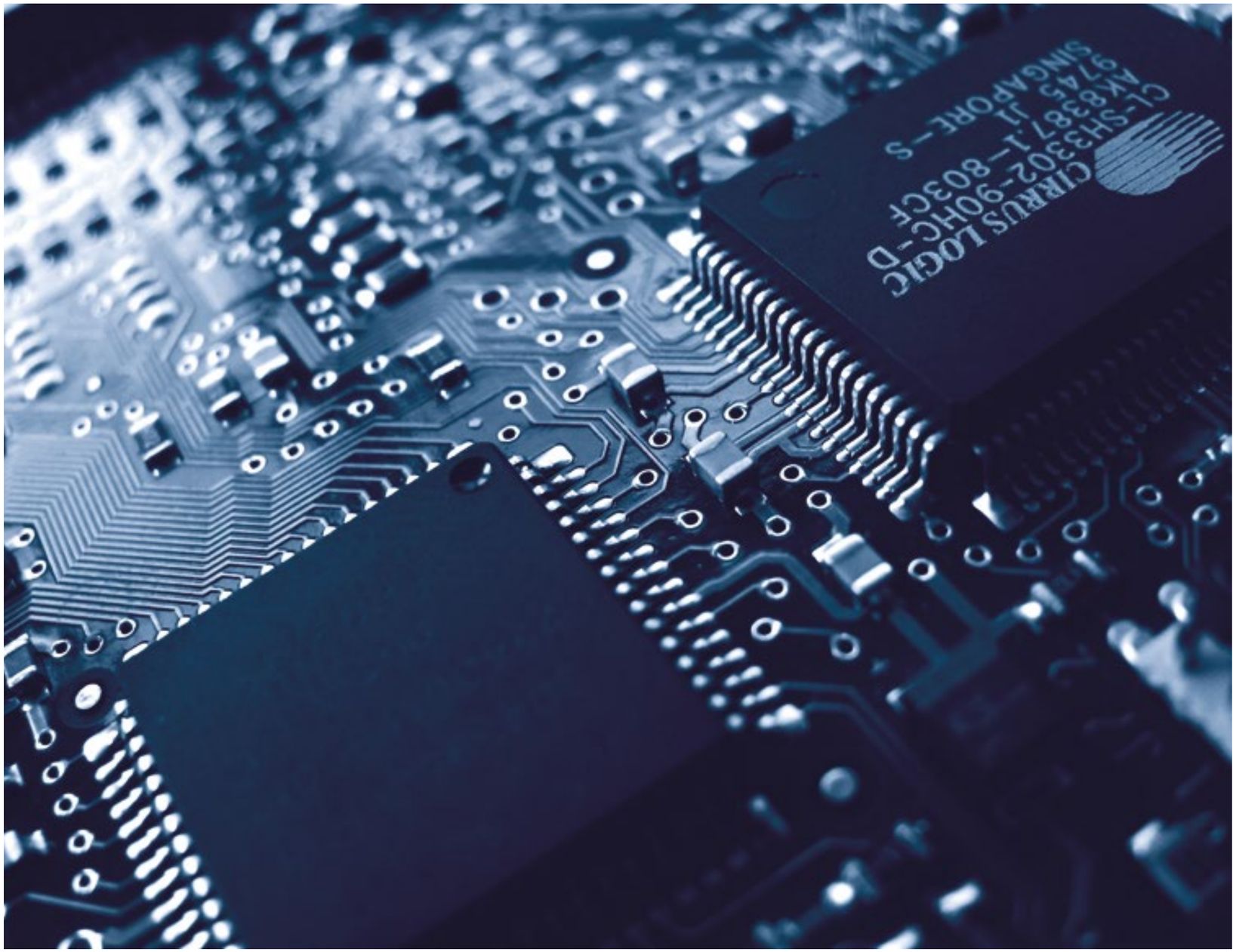
Since 2013, the most efficient miners have focused on Application Specific Integrated Circuits (ASICs) designed specifically for mining.

ASICS: FROM 130NM TO 10NM

The first successful ASIC initiative dates back to the end of 2012, when ASICMiner launched its BE100, an ASIC produced in 130nm by TSMC. Although its ran at 0.4GH/s and consumed just 4.2 J/GHs, this performance has now been completely surpassed.

Other groups developed their own ASICs, including Avalon Project, BitFury, BitMain, Butterfly Labs, InnoSilicon, KnCMiner and SFards, all aiming for maximum computing capacity (GH/s) with minimum energy consumption (J).



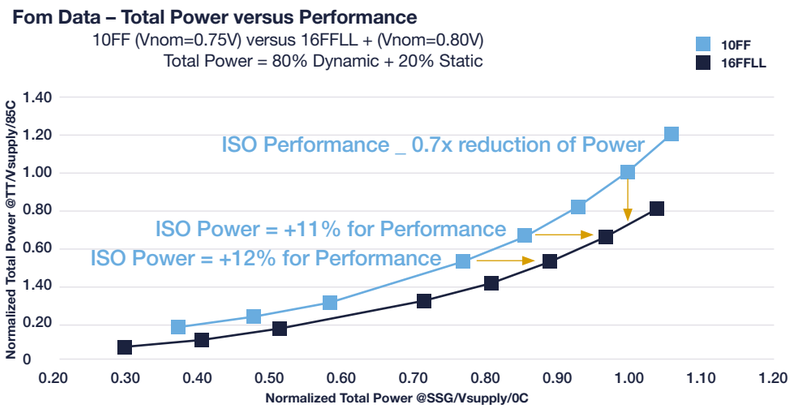


To improve J/GHs ratios, ASIC developments rapidly shifted towards more efficient chip production processes. Reducing the size of transistors (in nanometres, nm) helps massively reduce the energy consumption of the chips while improving their computing capacity. For example, the adoption of 20nm at TSMC, the world's largest semiconductor producer, helped reduce energy consumption by 25% while increasing computing capacity by 30% relative to the equivalent chips in 28nm. Although the gains from these advances are declining (the switch from 16nm to 10nm only helped gain 11% and 12% in energy and computing performance respectively), mastering chip design has become essential in the race for power and efficiency in blockchain networks.

At present, the most advanced ASICs are those by BitFury (16nm chip: 180GH/s @ 0.06J/GHs); BitMain (16nm chip: 68GH/s @ 0.1J/GHs); and Canaan (16nm chip: 83GH/s @ undisclosed power consumption performance).

Since mid-2016, the semiconductor industry has rolled out production capacity in 10nm, but to our knowledge, no 10nm ASIC dedicated to mining has been announced so far. It is nevertheless reasonable to believe that the various groups are already working on the adoption of this new technology in order to improve the performance of their ASICs and gain an edge over rivals.

FIG. 10: CHIP DESIGN SIGNIFICANTLY IMPROVES THE PERFORMANCE AND ENERGY EFFICIENCY OF MINING OPERATIONS



Sources: ARM; Bryan, Garnier & Co

4. Other applications for blockchain

Blockchain is useful all cases where a group of people have a common aim, do not know each other and therefore do not trust each other, and where at least one person would like to have a history of the transactions.

Primarily used in the cryptocurrency universe, blockchain is being experimented with in other environments where there are issues around data storage or the traceability of transactions. It is adapts easily via existing APIs, and its security and transparency levels make it appropriate to many fields. We estimate that blockchain could be useful in three main areas:

TRANSFERRING ASSETS

Blockchain can also be applied to other assets such as securities, shares, bonds, currencies, votes etc.

AS A LEDGER

It allows perfect traceability of products and assets over their entire lifespan: securities operations, decisions by social organizations, extracts from official registers such as civil status, company status, brands and patents, vehicle service manuals etc.

FOR SMART CONTRACTS

These are autonomous programs that automatically execute the conditions and terms of a contract without requiring human intervention. Self-executing contracts ensure that once the right conditions are filled, the contract will be honored with no possibility of fraud, bad will or interference from a third party. The contract is in fact an IT programme integrated into a blockchain that is automatically applied when the conditions defined by the two parties are met. Overall, any agreement between two parties has the potential to be digitized and automated.

Blockchain has vast scope for potential application. By replacing the majority of trusted third parties in centralized systems like banks, payment schemes, contracts and land registers with collaborative IT systems, it could make many sectors more efficient: banking, payments, insurance, retail, property, health, energy, transport, logistics, media, the public sector.

FIG. 11: POTENTIAL BLOCKCHAIN APPLICATIONS

NON-FINANCIAL USE CASES	FINANCIAL USE CASES
▪ Digital Content / Documents, Storage and Delivery	▪ Currency Exchange and Remittance
▪ Authentication and Authorization	▪ P2P Transfers
▪ Digital Identity	▪ Ride Sharing
▪ Marketplace – Providing premium rights and brand based coins	▪ Data Storage
▪ Smart Contracts	▪ Trading Platforms
▪ Real Estate	▪ Gaming
▪ Diamonds	
▪ Gold and Silver	
▪ Reviews / Endorsment	
▪ Blockchain in IoT	
▪ App Development – Proof of ownership for modules in app development	
▪ Network Infrastructure and APIs	
▪ Other – Prediction platform – Election voting – Patient Records management	

Source: Bryan, Garnier & Co

FIG. 12: USE CASES FOR BLOCKCHAIN

Sources: GrowthPraxis; Bryan, Garnier & Co

Blockchain in the payments sector

A recent survey undertaken by the European Payments Council[2] showed that 90% of sector professionals believe that the technology could have an impact on payments by 2025. Blockchain could help increase the speed of money circulation, and enable banks to interact more with one another to make the banking system more efficient.

With a blockchain payment system, it is possible to carry out a secure account-to-account transaction virtually instantaneously throughout the world and at a lower cost. For example, in the bitcoin blockchain, each participant can easily create a totally anonymous account using a computer. Compare this with the traditional model in which a client has to involve a central authority (their bank), an account is often complicated to set up and involves sensitive data, a transaction takes several days to carry out, and the fees levied are high.

HOW BLOCKCHAIN TRANSACTIONS CAN WORK IN REAL LIFE

Unlike traditional D+2 systems, the bitcoin blockchain offers virtually immediate payment processing, which could create a better relationship between consumers and merchants. Bitcoins are accepted at some retailers and already exist in mobile bitcoin portfolios using the blockchain technology.

A bitcoin portfolio can process transactions much like a mobile payment, by using contactless technology to interact with a payment terminal and buy articles with bitcoins. For example, a merchant enters the price of an item in their local currency into the terminal, which generates a QR code with the corresponding amount in bitcoins. The consumer simply needs to scan this using their mobile phone to make the payment.

However, it is worth noting that blockchains are so large that most smartphones cannot contain the full chain in their memory to undertake payments. Instead, bitcoin portfolios only download part of the blockchain by using other elements in the bitcoin network to ensure that all the information is correct.

The blockchain system's large public ledger is what makes it immune to pirating or forgery. This is an interesting illustration in today's highly regulated universe.

The blockchain has also attracted the interest of financial institutions and fintechs. Central banks are even exploring the opportunity of issuing their own national digital currencies based on a digital register. As is often the case with innovation in the fields of payments and security (where challenges are sensitive), we expect a very gradual adoption of blockchain technology. Players interested in the technology are often at the "proof of concept" stage and act in a closed environment.

This currently involves organic development or partnerships and in the future is likely to involve investments in or acquisitions of blockchain solutions suppliers. Several major global financial institutions such as Barclays, Banco Santander, Citibank and Goldman Sachs are already studying blockchain technology for a wide range of applications (for example, to step up transaction processing, handle large transaction volumes, reduce operating/infrastructure costs, eliminate defaults, improve transparency, reduce cross-border transaction costs and for real-time transfer of funds between clients of various banks).

2. EPC Poll: How may Blockchain Technology Impact the European Payments Landscape? | European Payments Council | May 2016

FIG. 14: STUDIES AND EXAMPLES AT BANKING GROUPS

STUDIES	BANKS ARE AMONG MAJOR INVESTORS
A study from IBM[3]: commercial blockchain solutions are undergoing rapid adoption at banks and financial markets. In fact, 15% of banks and 14% of financial institutions surveyed intend to implement large-scale commercial blockchain solutions in 2017 and 65% of banks plans to have solutions in production in the next 3 years.	Over 80 of the world's leading financial institutions including BNP Paribas, Citi, JPMorgan, SBI, Bank of America Merrill Lynch, HSBC, ING, Unicredit, Intesa Sanpaolo and regulators joined together in a consortium sponsored by the US digital ledger start-up R3 CEV to study and define the future of blockchain. This consortium has been created to develop custom blockchain-enabled solutions for the financial sector.
A study called "Blockchain Rewires Financial Markets: Trailblazers Take the Lead"[4] analyzed 200 global financial institutions and showed that 7 out of 10 pioneers are focusing their efforts on blockchain in four distinct areas: clearing and settlement of transactions, wholesale payments, issuance of debt and equity, and reference data.	UBS and Barclays are already using blockchain as a way to speed up back-office operations and management. Some professionals in the banking sector claim it could deliver a global saving in administrative costs of up to USD 20bn a year for the industry.
According to a 2015 study from Santander[5], the use of blockchain could help banks save USD 15-20bn a year by 2022, thanks to a reduction in "infrastructure costs related to international payments, trading and compliance". Blockchain could, for example, enable them to dispense with clearing and settlement systems, which are complex, centralized, and can take two and a half days to ensure complete clearing. Blockchain transactions would be more reliable, faster, and cheaper.	A group of 7 major European banks (Deutsche Bank, HSBC, KBC, Natixis, Rabobank, Société Générale and UniCredit) has agreed to develop a ground-breaking shared platform called Digital Trade Chain (DTC) that aims to make domestic and cross-border commerce easier for European small and medium-sized businesses by harnessing the power of blockchain technology.
	JP Morgan launched a consortium, the Enterprise Ethereum Alliance, with Microsoft, Santander, ING and UBS, Goldman Sachs and Morgan Stanley.
	Citigroup, Capital One, Nasdaq and Visa have invested in the Californian startup Chain Inc (alongside the French fund Orange Digital Ventures) to build a blockchain infrastructure dedicated to financial services.
	A group called Thought Machine developed the Vault OS operating system, which uses private blockchain technology combined with a distributed encryption registers to allow any bank to provide secure end-to-end financial systems.
	The ECB itself wanted to explore the theme and was interested in understanding the mechanisms in depth.
	Nasdaq partnered with bitcoin start-up Chain (funded by Nasdaq, Citi Ventures, and Visa).
	DH Corp announced a partnership with Ripple Labs.

3. "Leading the Pack in Blockchain Banking: Trailblazers Set the Pace" | IBM | 2016
4. "Blockchain Rewires Financial Markets: Trailblazers Take the Lead" | IBM | 2016
5. "The Fintech 2.0 Paper: rebooting financial services" | Santander InnoVentures | June 2015

On paper, banks and card schemes could be threatened to the extent that authentication systems between peers do not trust each other. In reality, we estimate that the blockchain is above all a facilitator of the systems currently in place. It is non-intrusive and can be easily used as a complement to existing systems via APIs. We therefore expect banks and payment schemes to be the first to be active in blockchain, via partnerships and/or acquisitions, to integrate the threat upstream rather than potentially be victims later on.

Meanwhile, payment services providers (PSPs) are likely to develop the technology organically (with specific internal teams) and then probably via partnerships at a later stage, and possibly M&A thereafter. In our view, the system most at threat is SWIFT, which offers account-to-account services, operations in currencies or securities, recovery etc. The unique selling point of the SWIFT network is that no third party can deny having made a transaction, because SWIFT undertakes the equivalent of a notarial act on all of the transactions made, regardless of their amount. It guarantees the integrity and archiving of all receipts, which are decoded in its archive servers. That said, the process is slow, costly, lacks flexibility and its level of security is questionable because the network has not been updated since the early 1990s. Because it is a perfect response to all of SWIFT's weaknesses, blockchain could totally replace it.

More generally, we believe that blockchain is far more of a threat to paper money than to payment cards, since 85%[6] of payment volumes are still carried out in cash or by check (representing 60% in value terms). As such, development potential for new forms of digital payments is high.

Before the use of the blockchain technology becomes more widespread externally, fears about flexibility, cost, transaction speed, regulations and security need to be addressed.

SPEED

Validating a high volume of transactions requires exponential computing power. As such, an open question is to know whether decentralized architecture and regulatory uncertainty could handle the processing speed requested from a secure system of payment transfer that connects various financial institutions to each other. The bitcoin blockchain processes between three and five transactions per second on average, with a maximum limit of seven or eight/second, while Visa handles 20,000 transactions per second. This could require hefty server investments.

LEGAL ISSUES

The legal status of cryptocurrency varies significantly from one country to the next and it is currently changing or is undefined in most countries. Virtual currencies and blockchain are still not regulated. For bitcoin, this is because a traditional currency needs to have an official price to exist legally. It must be issued under the framework of national sovereignty, which is clearly not the case with stateless digital currencies. This lack of legislation prompts fears for consumers and is hampering the development of fintechs present in these market segments. In our view, we will have to wait to see potential applications before legislation is made, because regulations should target the applications rather than the technology itself. The transnational aspects of this type of business can conflict with national or European rules. A balance will have to be found.

SECURITY

From a security viewpoint, the blockchain structure is based on advanced cryptographic algorithms but this advantage could theoretically disappear if a person found an algorithm capable of hacking information in the chain and reproducing it. This risk exists theoretically but is technically very unlikely. However, it would cause a wave of panic and a nosedive in the value of bitcoin. Finally, the rising adoption of blockchain in payments would increase the number of participants and the risk value. Depending on the pace of adoption, the question is whether higher transaction volumes using blockchain technology would reduce costs enough to make the technology more competitive than traditional payment systems.

6. "The Cashless Journey Study | Mastercard | September 2013

Summary: blockchain's advantage in the payments industry

The advantages of blockchain technology (transparency, decentralized structure and multi-signature) could fulfil the expectations of payments and security companies. In particular, we estimate that private blockchains are currently the most suitable for improving existing systems (efficency, rapidity and costs).

More generally, the technology could step up the speed of money circulation, in a cheaper and more secure way.

With the bitcoin blockchain, the client decides how much money they would like to transfer without providing any sensitive information. This differs from debit card payments, which include encoded sensitive information and are linked to a bank account. In this respect, bitcoin is more like cash than a bank card.

Virtually instantaneous payment in stores become possible (e.g. via bitcoin portfolios) compared with a traditional system (D+2).

Blockchain could be particularly well suited to cross-border transactions. International payment services are often complicated, slow, lack in transparency and security, and are not attractively priced.

Applications for blockchain in payments are numerous: crypto-currency, mobile payments, P2P transfers, cross-border, transactions, micro-payments, clearing/settlement.

In summary, we believe that the priorities in the payments sector are to achieve efficiency, speed and transaction costs, and that this can be achieved without removing all the trusted third parties. It is possible to reduce the number of intermediaries – the shorter the chain, the easier it is to undertake instantaneous transactions – but an infrastructure operated in some way by a market-approved trusted third party will always be necessary. As such, we see blockchain as a facilitator of existing systems.

In the bitcoin blockchain, what takes time is granting a participant in the chain the right to validate a transaction. As it is open, anybody can take part. To avoid abuse and maintain the integrity of the chain, anyone wanting to validate a transaction first needs to mobilize significant processing power to resolve algorithmic problems (proof of work).

A private blockchain is owned and operated by a group of authorized participants in a closed environment. This system could be more acceptable to companies, financial institutions and regulatory bodies, who are often skeptical of large shared registers and concerned by confidentiality issues. In a private or semi-private blockchain, validation can only be carried out by specific regulated participants. These participants work in an integrated way and if not, they will be sanctioned by their supervisory authority. The "proof of work" stage is therefore unnecessary.

Infrastructure is spread between several nodes capable of working and talking to one another at the same time, and this avoids reconciliation problems. It is the distributed aspect of the technology that makes it efficient and fast: it makes it possible to reach a higher volume of transactions processed per second than that of a network like Visa. Some private blockchains reach 80,000 transactions per second. Furthermore, it is virtually impossible to pirate, as the ledger is constantly updated in real-time on servers that are geographically separate.

Finally, private blockchains often help participants to assess the technology to see how it would work in specific scenarios.

Guest article

On 16 June 2017, Bryan Garnier & Co ran a client breakfast meeting on the subject of "Blockchain: a technology to be reckoned with in the future in many business sectors." Our panel included specialists from consultancy, insurance and technology:

- **ACCENTURE: Stéphane Geyres** | *Security Advisory Services Managing Director, Europe*
- **AXA GROUP: Laurent Benichou** | *Research & Development Director*
- **WORLDLINE: Nicolas Kozakiewicz** | *Head of Research & Development and Innovation*

As a contribution to this study about blockchain in the payments sector, Nicolas Kozakiewicz from European payments leaders Worldline was kind enough to write the following article.

BLOCKCHAIN IN A NUTSHELL

Nicolas Kozakiewicz,
Head of R&D and Innovation, Worldline

The most significant features of blockchain are its decentralized governance and its technical versatility. As a decentralized protocol, it has no need for a trusted third party at its center, meaning peers with the same goal can trace and log events and data without the need to trust one another. It is also secure and scalable by design. In blockchains such as bitcoin, peer users are authenticated anonymously and access to data is easily tailored. With blockchain, everyone is custodian of all the data. And because blockchain is a standalone protocol that can be implemented via simple APIs, it can be easily interfaced with any information system.

Two current use cases beyond bitcoin include the Swedish real estate industry, where blockchain is being used to register and record land titles in a bid to digitize real estate processes; and NASDAQ, which is using blockchain for its internal management system for assets and transactions. There are many other potential uses for blockchain:

- **Object-to-object** – updating shared data for a group of physical objects in real time, for example cameras, terminals, IOT (internet of things) devices.
- **Business-to-consumer** – this is natural territory for blockchain, with a wide variety of applications. Worldline partner SnapSwap, for example, offers cross-border instant payments; banks and insurance companies can use blockchain to offer "smart contracts"; and it can help offer secure public identity services in areas such as voting and personal health information.
- **Consumer-to-consumer** – bitcoin is the most visible and well-known C2C application
- **Business-to-business** – services include clearing and settlement between financial institutions and creating end-to-end supply chain traceability, from raw materials through to recycling.

Blockchain could solve several issues that currently do not have appropriate solutions. It has applications across sectors including energy, insurance, media, government, transport and IOT, to name but a few. It's a disruptive technology to which industries, corporations and governments will need to adapt– but its highly secure and scalable nature make it a viable technology for the long term.

BRYAN, GARNIER & CO

White Paper Contributors

GREG REVENU
Managing Partner
Investment Banking
grevenu@bryangarnier.com

PIERRE LAFITTE
Director
Technology, Investment Banking
plafitte@bryangarnier.com

RICHARD-MAXIME BEAUDOUX
Equity Research Analyst
Payments and Security, Video Games
rmbeaudoux@bryangarnier.com

DORIAN TERRAL
Equity Research Analyst
Semiconductors
dterral@bryangarnier.com

Technology Investment Banking Team

Since 1996, more than 300 companies have trusted us to deliver more than €10 billion in investment banking transactions, raising private and public financing, as well as advising on mergers and acquisitions.

PARTNERS
Olivier Beaudouin | Technology & Smart Industries
Falk Müller-Veerse | Technology
Guillaume Nathan | Digital Media & Business Services
Greg Revenu | Technology
Thibaut De Smedt | Application Software

MANAGING DIRECTORS
Jay Marathe | Technology & Smart Industries
Philippe Patricot | Technology
Robert Pfeiffer | Media

DIRECTORS & VICE PRESIDENTS
Jonathan Bohbot
Lars Dürschlag
Jonathan Foiret-Hurbin
Marc-Antoine Janny
Berk Kirca
Pierre Lafitte
Frans-Matthis Pleie

ASSOCIATES & ANALYSTS
Priyanshu Bhattacharya
Alexandre Brestin
Pierre Cuer
Clement Decante
Dipam Patel
Amina Sagou
Marc-Antoine Serfaty
Jakub Simon
Awa Sow

Technology Equity Research Analyst Team

With seasoned research methodology and fundamental bottom-up approach, Bryan, Garnier's analysts provide opinionated investment insights with leading perspective across the most dynamic Technology sectors in Europe. Bryan Garnier & Co developed the most dedicated Technology research platform in Europe, with more than 150 stocks covered.

ANALYSTS & RESEARCH ASSOCIATES
Richard-Maxime Beaudoux | Video games / Payments
Xavier Caroen | Automotive Technologies
Pierre Antoine Chazal | Smart Energy
Thomas Coudry | Telecoms
Antoine Parison | Ecommerce / Market Place
Gregory Ramirez | Software & IT Services
Cédric Rossi | Ecommerce / Market Place
Dorian Terral | Semiconductors
Fréderic Youboué | Technology, Media, Telecoms

Corporate Transactions

Bryan, Garnier & Co leverage in-depth sector expertise to create fruitful and long lasting relationships between investors and European growth companies.

Prima Solutions Acquired by The Carlyle Group **Undisclosed** *Advisor to the Sellers*	smartTrade Acquisition of a minority stake by KEENSIGHT CAPITAL **Undisclosed** *Advisor to the Buyer*	Viveo Acquired by TEMENOS **€ 81 000 000** *Advisor to the Sellers*	KEENSIGHT CAPITAL / PARIS ORLÉANS Sold FircoSoft to Reed Elsevier **Undisclosed** *Advisor to the Sellers*	SUMMIT PARTNERS ogone Aquired EBS **Undisclosed** *Advisor to the Buyers*

About Bryan, Garnier & Co

Bryan, Garnier & Co is a European, full service growth-focused independent investment banking partnership founded in 1996. The firm provides equity research, sales and trading, private and public capital raising as well as M&A services to growth companies and their investors. It focuses on key growth sectors of the economy including Technology, Media, Telecoms, Healthcare, Smart Industries and Energy, Consumer, Brands & Retail and Business Services. Bryan, Garnier & Co Ltd is a fully registered broker dealer authorized by the FCA in Europe and the FINRA in the U.S. Bryan, Garnier & Co is headquartered in London, with additional offices in Paris, Munich and New York. The firm is a member of the London Stock Exchange and Euronext.

JMP Bryan Garnier Technology Equity Research Coverage

In November 2016 Bryan, Garnier & Co formed a partnership with JMP Securities LLC (NYSE : JMP) to create JMP Bryan Garnier, a full-service transatlantic investment banking alliance for technology and healthcare companies.

18 Analysts | 130+ Stocks Covered

With more than 150 professionals based in London, Paris, Munich and New York, Bryan, Garnier & Co combines the services and expertise of a top-tier investment bank with client focus of a boutique.

LONDON
Beaufort House
15 St. Botolph Street
London, EC3A 7BB
UK
T: +44 (0) 207 332 2500
F: +44 (0) 207 332 2559

Authorized and regulated by the Financial Conduct Authority (FCA)

PARIS
26 Avenue des Champs Elysées
75008 Paris
France

T: +33 (0) 1 56 68 75 00
F: +33 (0) 1 56 68 75 01

Regulated by the Financial Conduct Authority (FCA) and the Autorité de Contrôle prudential et de resolution (ACPR)

MUNICH
Widenmayerstrasse 29
80538 Munich
Germany

T: +49 89 2422 62 11

NEW YORK
750 Lexington Avenue
New York, NY 10022
USA

T: +1 (0) 212 337 7000
F: +1 (0) 212 337 7002

FINRA and SIPC member

IMPORTANT INFORMATION