CAPCODIGITAL

BLOCKCHAIN IN CAPITAL MARKETS INFRASTRUCTURE

BLOCKCHAIN IN CAPITAL MARKETS INFRASTRUCTURE. NOW IS THE TIME FOR ACTION.

This paper, from Capco Digital's Blockchain Team, will be invaluable for any capital markets practitioner looking for actionable information on blockchain. It provides useful historical context and offers insights into near future applications of blockchain technology to achieve positive transformation of the capital markets infrastructure.

There is no doubt that the existing capital markets infrastructure urgently needs a new lease of technology enabled life. Credible estimates set the potential for efficiency and elimination savings at somewhere between €30 and €50 billion annually. Either the industry itself, in its current configuration, will pursue and deliver those savings, or 'outsiders' will seize the impetus.

WE CAN'T CONTINUE TO IGNORE BLOCKCHAIN

There is one certainty however: blockchain technology is starting to come of age. The confidence bestowed upon it by Bitcoin is translating daily into new initiatives and partnerships. These are creating advantages for the financial institutions at the forefront of blockchain innovation. The technology is not a panacea. Nor has it reached its final format. In particular, blockchain is vigorously rebutting the long-term charges against it that it does not scale and that it cannot satisfy complex and particular capital markets security requirements.

BLOCKCHAIN IS NEARING READINESS TO DELIVER FOR CAPITAL MARKETS

In this paper, written by members of the Capco Digital Blockchain Team, we look at historical examples of technology advancement and regulatory change impacting the market environment. We assess key blockchain architecture and protocol developments. We identify areas where blockchain has significant potential to bring about positive transformational change. And we identify some of the major barriers to adoption within the capital markets.

Blockchain used to be about possibilities and potential. Now the days of hype are coming to an end. We are entering a wave of opportunity, evolution and value delivery.

Architectural progress

Considerable progress has been achieved in several key areas of blockchain architectural development recently. Some of the issues are discussed below.

BLOCKCHAIN: THIS TECHNOLOGY DOES SCALE

The alleged lack of scalability so frequently cited as a major drawback for blockchain in financial services is undergoing a serious rebuttal. In some cases, blockchain platforms can handle more than one billion transactions a day, matching the volume of non-cash electronic payments made globally. Significantly, Microsoft recently announced Project Bletchley as part of its blockchain-as-a-service (BaaS) platform, Azure. Bletchley aims to address scalability as one of the concerns that emerged after discussions with the blockchain ecosystem.

ACCESS CONTROLS: CONSIDERATIONS OF VOLUME, SPEED, SECURITY AND SETTLEMENT FINALITY WILL DETERMINE PROTOCOLS

Blockchain solutions traverse the public/private and permissioned/permissionless axes. There are benefits and drawbacks to both.

Public blockchains are open to all users, allowing anyone to create transactions. Benefits include transparency and the added layer of security against hacking and transaction censorship that the openness of the network provides. However, public blockchains are slower because all parties must replicate the data. An additional drawback is the question of whether public blockchains can guarantee settlement finality, or if public, proof-of-work blockchains technically offer only probabilistic settlement. For this reason, they are not widely considered to be a reliable architecture for the global clearing and settling of financial transactions.

Private or permissioned blockchains only grant access to a predefined list of blockchain operators. The chain can be subject to block censorship and its private nature means the contents and the protocols governing the network can be altered. Fewer nodes operating on the blockchain translates to lower security, due to the less robust consensus mechanisms with which they are usually coupled.

The open/closed debate places security through transparency on one side of the coin, with speed and governance on the other. The Bitcoin blockchain, a public, permission-less blockchain has proven to offer a level of transparency and inherent security appropriate to its use case, through a robust - although slow and costly - proof-of-work consensus mechanism. In a regulated industry, private and permissioned blockchains are more appropriate as speed and volume take precedence, and trust is essential.

SKIN IN THE GAME: PROOF-OF-STAKE-BASED CONSENSUS CAN INCREASE TRUST AND DRIVE DOWN COST

In the proof-of-work mining system, participants solve an asymmetric computation that is hard to decipher, but easy to check. One criticism of this algorithm is the overall cost of the processing power used to solve the problem, which is then checked by other nodes and encoded onto the ledger with a fee awarded to the miner.

In a regulated environment, or one with a limited number of known participants, there may be opportunities to dial back on some of the arduous cryptographic protections. Consensus is less costly to achieve when participants have some degree of trust. This can result in shorter times to commit transactions and agree on the immutable record.

An alternative system, proof-of-stake, achieves consensus by having miners prove that they control a certain amount of currency or tokens. Existing private blockchains use a round-robin approach to adding blocks onto the chain, which they digitally sign using a public-private key encryption mechanism. Ethereum, a popular and advanced blockchain platform, has been working on moving from proof-of-work to proof-of-stake in its Casper protocol, which offers a stronger technological definition of settlement.

ONE CHAIN TO RULE THEM ALL?

While all of the architectural choices listed above have their benefits and drawbacks, the real world application of designs and protocols is typically derived from the use case, as opposed to any single, dogmatic approach. This applies equally to the blockchain ecosystem in financial services where the appropriate consensus and access mechanisms offer the necessary security, speed and scalability.

Sounds familiar? Throughout history, financial services markets have adopted a series of discontinuous technological innovations. The evolution from kernel to ubiquity follows a similar pattern. A new technological mutation is propagated by small, but focused group of emergent players. What follows is a well-established cycle of natural selection and anagenesis, in which the start-ups disrupt the incumbents and technology is refined to the use cases. The pattern with this technological innovation will be no different.

> “ At a time when regulatory pressures are mounting, the financial services ecosystem, including both incumbents and emerging players, has worked together to produce functioning examples of improved and interconnected processes, record keeping and transparency, all using blockchain technology. “

A lesson in history

History shows that when a technological advance is coupled with regulatory change, challengers emerge from the Schumpeterian ashes and help force the hand of adoption.

1990S: DECENTRALISATION

In the late 1990s, the same decade that the World Wide Web started to connect us in our workplaces and homes, the U.S. introduced Regulation ATS to diminish the monopoly held by NASDAQ and NYSE.

This regulation saw the emergence of several Alternative Trading Systems (ATS) in the U.S. These were not regulated exchanges, but platforms to match buy and sell orders. Market players ultimately benefited from the newfound global and decentralised connectivity and the efficiency of electronic trading: greater speed and efficiency; lower costs; fewer manual errors; and less opportunity to skew the market direction with large orders.

Beyond financial services, the web also brought decentralised connectivity to consumers. BitTorrent, a form of peer-to-peer file sharing emerged, with files split into smaller chunks to enable faster uploading and downloading and a hash function applied to check the integrity of the data. This data verification method – known as ‘hashing’ – is now one of the constituent parts of the Bitcoin and Ethereum blockchains.

LATE NOUGHTIES: DISINTERMEDIATION, CRISIS AND BITCOIN

In Europe during the late noughties the drive to compete with the US was hampered by inter-country legal and regulatory differences. Initiatives such as MiFID (the Markets in Financial Instruments Directive) aimed to harmonise regulation in the member states of the European Economic Area (EEA), while increasing competition. MiFID made a pan-European trading facility a reality and the market saw the emergence of Multilateral Trading Facilities (MTF) and Organised Trading Facilities (OTF) in Europe.

Operators could offer dealing services at a discount compared with traditional exchanges, better bundle transactions and segment trading in a way that worked best for them: by industry. This lowered costs by a factor of seven. For an investment banker, selling a basket of sector stocks that didn't have to navigate multiple legal and regulatory jurisdictions was preferable to a portfolio organised by country.

Then came the global financial crisis. The transparency, traceability and liability of financial services came under scrutiny like never before from regulators and the wider population. For some, the trust placed in financial institutions was damaged beyond repair.

In 2008, Satoshi Nakamoto published his seminal work on a truly peer-to-peer digital currency and transaction log. Although the main goal was to replace the centralised, censorable trust-based model of financial services, the Bitcoin paper offered an elegant solution to transparency by making all transactions public while masking identity.

The technology underpinning the currency also solved the problem of double-spending a digital token. The inherent economic properties of digital goods - public, replicable and non-rival – were a cause for concern in other industries, as digitised music tracks with zero marginal cost were shared online, disrupting the music industry's ecosystem.

Bitcoin was the first decentralised ledger currency and is currently the best proof-of-concept that exists of blockchain technology.

CURRENT STATE: INCREASING REGULATION AND TRANSPARENCY

With the ambitious MiFID II directive and its complementary regulation, MiFIR, set to come in to force in Europe in January 2018, trading processes and venues are once more on course to change. MiFID II was, with the exception of three amendments, endorsed by the European Commission and is currently being organised into a 1,000 page technical document. Although recent regulatory change such as MiFID II, is born out of positive intent, it has far-reaching implications for capital markets and presents its own challenges. Alongside MiFID II in Europe, the EMIR directive mandates the introduction of transaction reporting for derivatives. The execution of this directive, in the absence of a golden source of data or standards, is proving difficult to manage, leaving regulators with high volumes of irreconcilable transaction data.

After a somewhat successful decoupling from Bitcoin, blockchain technology has completed several reportedly successful proofs-of-concept including Bank of Ireland's golden source of information across an entire trade lifecycle, Icap's smart contract representation of spot/forward FX block trades and a large collaborative effort improving record-keeping on CDS trades. So at a time when regulatory pressures are mounting, the financial services ecosystem, including both incumbents and emerging players, has worked together to produce functioning examples of improved and interconnected processes, record keeping and transparency using blockchain technology.

OPPORTUNITIES

Consider the example of TARGET2 Securities (T2S), the Europe-wide integrated platform on which Central Security Depositories (CSDs) settle securities in central bank money. This high profile initiative has cost the ECB €1 billion and taken a decade to discuss, design, build and implement. The platform was intended to increase competition and reduce costs of cross-border European settlement. However, the settlement process is necessarily reciprocal, meaning that the CSDs still have to consume the settlement with the T2S platform in order to provide other services, such as asset servicing, and therefore have been unable to dismantle the incumbent infrastructure.

Technology and regulation-driven change can combine to create the 'perfect storm' of demand for a blockchain approach. So, just as MiFID's drive for competitiveness across Europe resulted in a reorganisation of portfolios by sector, perhaps a combination of the global regulatory push could result in a redesign of the infrastructure to remove silos and, ultimately, dismantle more of the Giovanni Barriers[1] than any preceding regulation.

Blockchain characteristics and architecture: Some open questions

IDENTITY: WHAT ROLE CAN BLOCKCHAIN PLAY IN ADDRESSING THE MARKET'S IDENTITY CRISIS?

Highly manual Know Your Customer (KYC) and ongoing Anti-money Laundering (AML) processes are costly for businesses. A universal KYC blockchain could remove some of the duplication of effort both inter-firm and industry wide. There already exist in many cases unique identifiers such as Legal Entity Identifiers (LEIs) and BICC account numbers that could be leveraged. An account holder could have a digital identifier that contains authenticated proof of identity, certifications such as licences or incorporation documents, and potentially even digital currency. Account holders might even get to claim ownership of their currently fragmented and ungoverned identity.

ON SETTLEMENT FINALITY: HOW BLOCKCHAIN CAN HELP ARRIVE AT DEFINITIVE SETTLEMENT FASTER AND MORE SECURELY

The market definition of settlement finality is aimed at reducing the systemic risk associated with participation in payment and securities settlement systems, and in particular the risk linked to the insolvency of a participant in such a system. In practice, a system must be officially designated in order to provide settlement finality of a given security and enforcement must occur in the real world. Blockchain could offer increased effectiveness of settlement by reducing settlement time, and therefore systemic counterparty risk. It could also provide an extra layer of technological comfort that a trade or payment has indeed settled.

The Casper proof-of-stake protocol in Ethereum, for example, is intended to offer stronger finality guarantees than a proof-of-work consensus mechanism. The protocol has now defined a standard definition of "total economic finality": when two thirds of all validators (participating nodes) make maximum-odds bets that a given block, or state, will be finalised. This condition strongly discourages validators from colluding to revert the block and risk losing their entire deposits.

> "There is a large skillset difference between the clearing and settlement of today and a post-blockchain ecosystem."

TURING COMPLETENESS: FLEXIBILITY VS UNCERTAINTY

Turing completeness is a property of a programming language or system, whereby all Turing complete systems can compute the same set of operations, such as conditional branching or loops.

The Bitcoin blockchain was not Turing complete; it could perform some conditional operations, such as 'check timelock' (a contract which enforces a certain passage of time before coins could be spent) but not for example, execute a payment if a certain exogenous condition is met. Coding Turing complete business logic (a virtual machine) on top of distributed ledger technology, for example, can enable flexibility such as automating or netting of payments, or any other algorithmic operation that maps to a real-world event. Some argue that it is unnecessary for blockchains to be Turing complete (the creators of the Bitcoin blockchain turned off this property) and furthermore that it is unsafe, due to dynamic typing of such languages that potentially produce unpredictable results.

Extra complexity comes with additional challenges. At the time of writing, the $150 million fund existing on the Ethereum blockchain known as The DAO (distributed autonomous organisation) is in turmoil after an attack saw the equivalent of $45 million siphoned into an account, like a cash machine that keeps spitting out cash without updating your balance. This happened because the language in which the protocol for the DAO was written is procedural, rather than functional – meaning that it is impossible to fully determine the behaviour of the smart contract before executing. The language, Solidity, was Turing complete.

However, the functionality can be achieved without this danger. Smart contracts themselves are not a new idea. Many 'Domain Specific Languages' for financial services already exist and are being used today to code smart contracts. There exist ecosystems of languages, such as functional languages, or specification/implementation (what a contract does / how it does it) pairs. These come with formal reasoning and verification tools that can be used to prove a contract's behaviour mathematically before running it. These tools are not applicable to Turing complete languages.

LET'S NOT MAKE A HASH OUT OF IT

We can shape the future in pursuit of agreed objectives. Yes, there are still many on-going debates about the architectural choices to be made in potential blockchain solutions. And yes, it goes without saying that there will be differences of opinion. But tangible results will continue to cut through the noise. Without doubt, there are certain choices to be made today to future-proof this technology and we can learn lessons from recent history, the Internet being a good example. .

The fundamental protocols of the Internet were created when it was impossible to imagine just how ubiquitous it would become. As a result it suffers from two underlying issues: security and scalability. Vint Cerf, one of the founders of the Internet and academically decorated net evangelist, claims that the NSA prevented the addition of an encryption layer during the construction of the Internet. He laments that if he could start again he would introduce stronger authentication and cryptography into the system.

The scalability issue stems from the sheer number of devices that now connect to the Internet. The Internet Protocol (IP) version 4 used 32-bit addresses, supporting 2^32 addresses, which was exhausted in 2011. This is being replaced by IPv6, with 128-bit (2^128) addresses, more than the number of atoms in the universe.

The lesson is clear: scalability and security are two issues that cannot be ignored in global financial markets. We have the opportunity to think about future-proofing now, ahead of major systemic problems. With theoretical near-possibilities and practical realities coming down the pipe, such as micropayments, the Internet of Things and quantum computing, we must ensure that the architecture is well thought through. The lessons of history are clear: future volume must be catered for; and security protocols must be suitable for a connected global financial system. Furthermore the underlying languages must be well understood and not just easy-to-use (See Turing completeness and the DAO mentioned earlier). As an industry and as a technology ecosystem, we must work with our peers and the regulatory bodies to ensure these criteria are fully satisfied.

Oversight

Clearly, future adoption and evolution of blockchain technology within the capital markets infrastructure is not going to happen in a regulatory vacuum. The current and likely on-going impact of regulatory compliance must be factored into the decisions we take. Encouragingly, many regulators have announced a light-touch approach to blockchain technology. The challenge comes with ensuring that they are up-to-date with the latest advances. Given the scale of that recent event on The DAO, it is more pertinent than ever to ensure that the regulatory workforce has the appropriate level of technological and theoretical skill. They will need it, not only to understand developments but to challenge them as well.

SETTING THE STANDARDS: INNOVATION, COMPETITION AND MARKET DYNAMISM ARE AS IMPORTANT AS SECURITY, SPEED AND EFFICIENCY

A market-wide technology built to handle anticipated volumes of trading, while remaining robust, secure and compliant must have equitable standards that also foster innovation and competition.

It will be necessary to define not only what those standards will be, but who will oversee their implementation and monitor any deviance. Any approach should also take into account consortiums and their power in comparison to smaller, emergent players, whose innovative capabilities are disproportionate to their size. We may also find that larger players in infrastructure space - firms that make profit in the current environment - will want to remain profitable and may lobby against cannibalisation of their profits. Being mindful of this dynamic in the ecosystem will ensure that large firms do not gain unfair advantage simply because size is their greatest asset.

INTERVENTION: WHEN IT PROVES NECESSARY, THE TECHNOLOGY SHOULD NOT SYSTEMICALLY PREVENT IT

Intervention is a reality in capital markets, but appears to conflict with the 'immutability' property of blockchain. Firstly, permissioned blockchains that restrict access should go some way towards satisfying questions around the need to intervene. If not, here are three examples of when public blockchain transactions were reverted.

- In 2010, a malicious actor gave itself 186 billion Bitcoin by exploiting a particular vulnerability. This was fixed, but it cost half a day's worth of transactions.
- In 2015, roughly six blocks were reverted because a Bitcoin mining pool was mining invalid blocks without verifying them.
- In June 2016, The DAO was attacked through an exploitation of code, resulting in $45 million worth of digital currency being captured by the attacker. The Ethereum community decided to intervene to reverse the attack, through a process known as a hard fork, intended to protect integrity. While satisfying some, it remains to be seen if, politically, the code will ever be the law.

Blockchain is a nascent technology and is not the answer to all the challenges facing the current system. Instead, it is a solution that offers efficiencies and lowered systemic risk. Intervention can still occur where necessary and the remedies will comply with regulations.

BARRIERS TO ADOPTION: ANY 'FAILURES' ATTRIBUTABLE TO BLOCKCHAIN ARE MORE THAN MATCHED BY LOSSES INCURRED THROUGH EXISTING TECHNOLOGIES

Attacks on The DAO and occasional failure of protocol might appear to be barriers to adoption, but other well-established protocols are equally vulnerable. Take the use of forged SWIFT messages to hack the Bangladesh Central Bank in Februarly 2016 which resulted in losses twice as high as The DAO-Ethereum incident. In fact the real barriers to widespread blockchain acceptance relate to cost and lack of resources. First and foremost, the cost of technological transformation; it can take a number of years to realise return on investments. There will be costs associated with the implementation and the large-scale organisational change it takes to unbundle complexity, coexist, redefine and simplify.

Staffing teams with the right skillset to code a security contract will be a challenge. Smart contracts are a novel discipline and the attack on The DAO shows that it is still in its learning phase. There is a large skillset difference between the clearing and settlement of today and a post-blockchain ecosystem.

Firms such as custodian banks that currently extract profits from the post-trade lifecycle will understand the need to reduce their costs and increase efficiencies, but will need to balance that with return on investment and be mindful of cannibalising their profits. Equally, firms that rely on opaque and often personalised pricing structures could find that this has an effect on the way relationships are managed and the creation and marketing of their products.

EVEN ATTRACTIVE COST REDUCTIONS DO NOT GUARANTEE UPTAKE OF INNOVATION

Historically, there have been instances where technological solutions were not adopted en masse, even when they appeared to be an elegant solution to soaring administrative costs. The potential of the utilities model in banking, for example, has yet to be realised. Although successful in other industries, such as aircraft and car manufacturing, the shared services model for KYC/onboarding, reconciliation and other administrative tasks has struggled to grow in the capital markets industry.

Linking it all together

The case for pushing forward with blockchain and to develop a fully viable and ubiquitous technology alternative to today's infrastructure is strong if not overwhelming. But the solution will not be a quick fix. Nor will it come from a single source, or be driven by limited acceptance and implementation. As an industry, we must examine and refine all the elements that work together to create a truly robust, secure and scalable blockchain.

CAPITAL MARKETS TECHNOLOGY INFRASTRUCTURE TODAY: UNDESIRABLE, BORDERING ON UNWORKABLE, AND CERTAINLY UNSUSTAINABLE

This is our current reality: aging infrastructure design and implementation. Institutions and market infrastructure operators continue to build bolt-on, single-use technology on top of ancient architecture, which often results in inefficient and costly solutions. Ultimately, these will be passed on to their respective user communities, thereby diluting the benefit of big-ticket initiatives such as a single European settlement platform. Now, the market infrastructure providers have the opportunity to drive down costs, as well as to future-proof their offering and meet demands for return on investment.

TECHNOLOGY AND REGULATION WILL COINCIDE, TO DRIVE POSITIVE MARKET INFRASTRUCTURE CHANGE

Market desire for a single electronic system for trading and a single electronic system for clearing and settlement has clearly been interpreted as a case for two discrete systems. Front office systems have improved radically, leaving the middle and back office trailing behind. And still the market tends to regard each part of the end-to-end transaction lifecycle as a siloed function: trading, clearing and settlement, corporate actions. However, as blockchain implementation becomes more tangible, so too does the idea of a single electronic system for settlement.

In this context of creaking infrastructure and profound regulatory driven change, blockchain's characteristics have the potential to provide a market model of straight-through-processing, from execution to post-trade, in a secure, transparent and efficient manner. Although a glance at the blockchain-related news on any given day will show that there are still design questions from a technology perspective, the technology itself offers real business value, at a time when regulation is squeezing profits and capital requirements are inhibitive.

1. The Giovannini Group of financial market experts formed in 1996 to advise the European Commission on market issues. The Group's two reports identified a total of 15 barriers preventing efficient EU cross-border clearing and settlement. Source: European Central Bank.

AUTHORS

Kim Sgarlata
kim.sgarlata@capco.com

Alan Philpot
alan.philpot@capco.com

Sara Feenan
sara.feenan@capco.com

ABOUT CAPCO DIGITAL

Innovation begins with a vision. But bringing any vision to reality requires a lot more than imagination. It requires a complete understanding of what's possible and the know-how to make it happen. Regardless of the scope of our clients' visions for their future, at Capco Digital, we have the financial services experience and expertise necessary to bring those visions to life.

Where our clients bring a deep understanding of their own institutions, our global team of financial services and technology specialists brings a deep understanding of technological advancements, user-experience possibilities, and cultural savvy.

Not to mention, they're 100% dedicated to technology for financial services. We champion our clients' ideas with leading-edge design and technologies. We work with you rather than around you, collaborating to build solutions that will drive your institution, today and five years from now — solutions which businesses, consumers and investors can use every day.

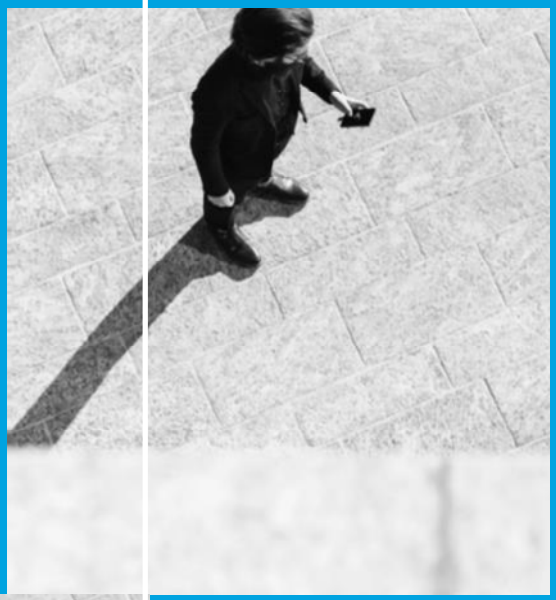
Capco Digital. Collaboration to power finance. Ingenuity to push it forward.

WORLDWIDE OFFICES

Bangalore – Bratislava – Brussels – Chicago – Dallas – Edinburgh – Frankfurt – Geneva – Herndon – Hong Kong – Houston – Johannesburg – Kuala Lumpur – London – New York – Orlando – Paris – Singapore – Toronto – Zurich

To learn more, contact us in the UK on +44 20 7426 1500, in Continental Europe on +49 69 97 60 9000, in North America on +1 212 284 8600, visit our website at CAPCO.COM, or follow us on Twitter @Capco

CAPCODIGITAL



CAPCO WORLDWIDE:

AMSTERDAM
BANGALORE
BRATISLAVA
BRUSSELS
CHARLOTTE
CHICAGO
DÜSSELDORF
EDINBURGH
FRANKFURT
GENEVA
HONG KONG
JOHANNESBURG
LONDON
MALAYSIA
NEW YORK
ORLANDO
PARIS
RICHMOND
SINGAPORE
TORONTO
VIENNA
WASHINGTON D.C.
ZURICH